



第三方云计算安

全服务商安全体系

先的

版权声明

本文档本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程 等内容,除另有特别注明,均为保密信息。任何个人、机构未经杭州默安科技有 限公司的书面授权许可,不得复制、引用或传播本文件的任何片段,无论通过电 子形式或非电子形式。

1	概述.		1
	1.1	产品概述	
	1.2	公司简介	
2	系统维	护	未定义书签。
	2.1	账号维护	未定义书签。
	2.2	重启设备 错误!	未定义书签。
3	Web 管	理界面	1
	3.1	用户登录	5
	3.2	项目总览	9
		3.2.1 新手提示	9
		3.2.2 数据统计	
		3.2.3 漏洞趋势和漏洞状态	
	3.3	应用管理	
		3.3.1 新建应用	
		3.3.2 编辑应用	
		3.3.3 删除应用	
		3.3.4 应用详情	
	3.4	项目管理	
		3.4.1 项目模板	
		3.4.2 项目列表	
		3.4.3 新增项目	
		3.4.4 基础信息	
		3.4.5 项目概况	
		3.4.6 逻辑漏洞检测(扫描类)	49
		3.4.7 Sitemap (扫描类)	
		3.4.8 Sitemap(插桩类)	
	3.5	漏洞管理	55
		3.5.1 漏洞列表	
		3.5.2 数据安全漏洞	
	3.6	第三方库(插桩类)	
		3.6.1 概述	
		3.6.2 图表分析	
		3.6.3 第三方库展示列表	
	3.7	插桩 AGENT (插桩类)	
	3.8	镜像扫描	
		3.8.1 镜像仓库	
		3.8.2 流水线任务	
	3.9	报告管理	
		3.9.1 报告列表	
		3.9.2 检测报告	
	3.10) 帐号管理	111
		3.10.1 用户管理	111
		3.10.2 部门管理	
		3.10.3 角色管理	

目 录

3.10.4 权限审批	
3.10.5 认证源	
3.10.6 AK/SK	
3.10.7 登录安全设置	
3.11 系统配置	
3.11.1 系统信息	
3.11.2 授权配置	
3.11.3 请求黑白名单(扫描类)	
3.11.4 消息通知	
3.11.5 网络配置	
3.11.6 系统升级	
3.11.7 流量信使(扫描类)	
3.11.8 规则列表	
3.11.9 漏洞类型	
3.11.10 web/ldaplog 查询	
3.11.11 自定义设置	
3.11.12 流量镜像管理(扫描类)	
日志审计	
3.12 帮助中心	
3.13 消息中心	
3.14 第三方插件(扫描类)	
3.14.1 漏洞扫描插件	
3.14.2 镜像扫描插件	
4 附录:配置证书及代理说明(扫描类)	173
4.1 为什么要设置代理	
4.2 对正常功能测试影响	
4.3 设置证书步骤	
4.3.1 PC 端配置	
4.3.2 移动端配置	
4.4 设置代理步骤	
4.4.1 PC 端配置	
4.4.2 移动端配置	
4.4.3 浏览器插件配置	
4.5 配置检测环节	

杭州默安科技有限公司

插图目录

图表	1 雳	鉴云端 WEB 管理登录界面	6
图表	2 登录	录-同意免责声明	6
图表	3 登录	录-免责声明	7
图表	4 登录	录-忘记密码	7
图表	55 登	录-注册	8
图表	6 用月	^白 注册	8
图表	77角	色升级	9
图表	88 登	录失败	9
图表	9 账/	^つ 锁定	9
图表	1010	管理员修改密码	10
图表	1111	数据统计	10
图表	1212	服务概况	11
图表	1313	应用管理	11
图表	1414	新建应用	12
图表	1515	编辑应用	12
图标	1616	删除应用	13
图标	1717	应用详情	13
图表	1818	应用中新建项目	14
图表	1919	项目管理	14
图表	2020	项目模板列表	15
图表	2121	模板列表操作中可选择编辑/删除模板	15
图表	2222	新建项目模板	15
图表	2323	项目列表	16
图表	2424	项目批量管理	16
图表	2525	项目筛选及搜索栏	16
图表	2626	项目优先检测及删除	17
图表	2727	项目列表中的收藏夹	17
图表	2828	新建项目	18
图表	2929	新增项目-使用模板-扫描类-选择检测模式	19
图表	3030	新增项目-使用模板-扫描类-项目基本设置	19
图表	3131	新增项目-使用模板-扫描类-项目高级设置	20
图表	3232	新增项目-使用模板-扫描类-项目高级设置-开启检测增强	20
图表	3333	新增项目-使用模板-扫描类-漏洞类型配置	21
图表	3434	新增项目-使用模板-扫描类-自定义配置	21
图表	3535	新增项目-使用模板-插桩类-选择检测模式	22
图表	3636	新增项目-使用模板-插桩类-项目基本设置	22
图表	3737	新增项目-使用模板-插桩类-项目高级设置	23
图表	3838	新增项目-使用模板-插桩类-项目高级设置	24
图表	3939	新增项目-使用模板-插桩类-项目高级设置-检测增强	25
图表	4040	新增项目扫描类-选择项目模式	26
图表	4141	新增项目-项目基本配置	27
图表	4242	项目高级设置	28
图表	4343	项目高级设置-漏洞类型	28

图表	4444	项目高级配置-自定义配置	29
图表	4545	新增项目插桩类-选择项目模式	30
图表	4646	新增项目插桩类-项目基本配置	31
图表	4747	插桩类项目高级设置-漏洞类型	32
图表	4848	插桩类项目高级设置	32
图表	4949	插桩类项目高级设置-主动 IAST	33
图表	5050	插桩类项目高级设置-检测增强	33
图表	5151	基础信息	35
图表	5252	编辑项目	36
图表	5353	用户凭证替换	36
图表	5454	输出报告	37
图表	5555	回归操作	37
图表	5656	插桩类项目基础信息	38
图表	5757	编辑插桩类项目	38
图表	5858	插桩类项目输出报告	39
图表	5959	非鉴权模式项目概况	39
图表	6060	扫描动态	40
图表	6161	生成提示框	40
图表	6262	漏洞列表	41
图表	6363	扫描类项目 SITEMAP	41
图表	6464	添加漏洞	42
图表	6565	扫描类项目爬虫动态	42
图表	6666	扫描类项目爬虫动态-开始爬取	43
图表	6767	扫描类项目爬取动态-正在爬取	43
图表	6868	插桩模式项目概况	. 44
图表	6969	漏洞列表	44
图表	7070	插桩项目 SITEMAP	45
图表	7171	添加漏洞	45
图表	7272	插桩项目 API 发现	46
图表	7373	项目第三方库列表	46
图表	7474	项目第三方库忽略	47
图表	7575	第三方库信息	47
图表	7676	第三方库详情	48
图表	7777	第三方库漏洞详情	48
图表	7878	生成项目第三方库报告	48
图表	7979	项目 AGENT 列表	. 49
图表	8080	主动模式扫描动态	49
图表	8181	添加用户凭证权限	50
图表	8282	逻辑漏洞检测中	50
图表	8383	逻辑漏洞检测完毕	50
图表	8484	逻辑漏洞展示	51
图表	8585	SITEMAP 列表-URL 覆盖度	51
图表	8686	SITEMAP 列表-请求详情 1	51
图表	8787	SITEMAP 右侧列表 1	52
图表	8888	添加漏洞	52

图表	8989 🖣	异入日志接口	53
图表	9090 S	ITEMAP 列表−请求详情 2	53
图表	9191 S	ITEMAP 右侧列表 2	54
图表	9292 🕅	忝加漏洞	54
图表	9393 🖣	} 入日志接口	55
图表	9494 漏	洞列表	55
图表	9595 扫	I描类漏洞列表概述	56
图表	9696 漏	洞列表	56
图表	9797 漏	洞分享	57
图表	9898 漏	洞详情	57
图表	9999 浙	漏洞演示及编辑一	58
图表	100100	SQL 延时注入漏洞演示	58
图表	101101	漏洞演示及编辑二	58
图表	102102	漏洞历史动态	59
图表	103103	同步 JIRA - 填写 JIRA 系统账号信息	59
图表	104104	同步 JIRA - 同步配置	59
图表	105105	同步 JIRA - 弹框	60
图表	106106	同步 JIRA - 自定义字段	60
图表	107107	同步 JIRA – 自定义同步漏洞信息	61
图表	108108	同步 JIRA – 记住选项及填写信息	61
图表	109109	同步 JIRA - 查看同步情况	61
图表	110110	同步 JIRA – 重新同步配置	61
图表	111111	同步 JIRA – 重新同步配置弹框	62
图表	112112	漏洞列表 - 查看 JIRA 同步情况	62
图表	113113	同步禅道 – 填写禅道系统账号信息	62
图表	114114	同步禅道 - 同步配置	63
图表	115115	同步禅道 - 弹框	63
图表	116116	同步禅道 - 自定义字段	64
图表	117117	同步禅道 – 自定义同步漏洞信息	64
图表	118118	同步禅道 – 记住选项及填写信息	64
图表	119119	同步禅道 - 查看同步情况	65
图表	120120	同步禅道 - 重新同步配置	65
图表	121121	同步禅道 - 重新同步配置弹框	65
图表	122122	漏洞列表 - 查看禅道同步情况	66
图表	123123	漏洞列表 - 查看 JIRA 和禅道同步情况	66
图表	124124	插桩类漏洞列表	67
图表	125125	插桩类漏洞分享	68
图表	126126	插桩类漏洞概述	68
图表	127127	漏洞演示及编辑二	69
图表	128128	插桩模式漏洞详情-数据流信息	69
图表	129129	插桩模式漏洞详情-历史动态	70
图表	130 插	桩模式漏洞详情-AGENT	70
图表	131130	同步 JIRA – 填写 JIRA 系统账号信息	70
图表	132131	同步 JIRA - 同步配置	71
图表	133132	同步 JIRA - 弹框	71

图表	134133 同步 JIRA - 自定义字段	72
	135134 同步 JIRA - 自定义同步漏洞信息	72
图表	136135 同步 JIRA - 记住选项及填写信息	72
图表	137136 同步 JIRA - 查看同步情况	73
图表	138137 同步 JIRA - 重新同步配置	73
图表	139138 同步 JIRA - 重新同步配置弹框	73
图表	140139 漏洞列表 - 查看 JIRA 同步情况	73
图表	141140 同步禅道 - 填写禅道系统账号信息	74
图表	142141 同步禅道 - 同步配置	74
图表	143142 同步禅道 - 弹框	75
图表	144143 同步禅道 - 自定义字段	75
图表	145144 同步禅道 – 自定义同步漏洞信息	76
图表	146145 同步禅道 - 记住选项及填写信息	76
图表	147146 同步禅道 - 查看同步情况	76
图表	148147 同步禅道 - 重新同步配置	77
图表	149148 同步禅道 - 重新同步配置弹框	77
图表	150149 漏洞列表 - 查看禅道同步情况	77
图表	151150 漏洞列表 - 查看 JIRA 和禅道同步情况	78
图表	152 安全漏洞列表概述	78
图表	153 安全漏洞列表	79
图表	154 漏洞分享	79
图表	155 安全漏洞详情(扫描类)	80
图表	156 漏洞演示及编辑	80
图表	157 SQL 延时注入漏洞演示	80
图表	158 漏洞演示及编辑二	
图表	159 漏洞历史动态	
图表	160 安全漏洞详情	
图表	161 插桩模式安全漏洞详情-数据流信息	
图表	162 插桩模式安全漏洞详情-AGENT	
		82
图表	163 同步 JIRA - 填写 JIRA 系统账号信息	82
图表 图表	163 同步 JIRA - 填写 JIRA 系统账号信息 164 同步 JIRA - 同步配置	82
图表 图表 图表	 163 同步 JIRA - 填写 JIRA 系统账号信息 164 同步 JIRA - 同步配置	
图表 图表 图表 图表	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图 表 表 表 表 表 表 表 表 表	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图图表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图图表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图图图	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图图图图图	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图图图图图表表表表表表表表表表表表表表表表表表表表表表表表表表表	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图	 163 同步 JIRA - 填写 JIRA 系统账号信息	
图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图图	 163 同步 JIRA - 填写 JIRA 系统账号信息	

图表 179 同步禅道 - 查看同步情况	
图表 180 同步禅道 - 重新同步配置	
图表 181 同步禅道 - 重新同步配置弹框	
图表 182 漏洞列表 - 查看禅道同步情况	
图表 183 漏洞列表 - 查看 JIRA 和禅道同步情况	
图表 184151 第三方库管理	
图表 185152 第三方库概述	
图表 186153 第三方库列表图表分析	
图表 187154 第三方库列表	
图表 188155 第三方库信息	
图表 189156 第三方库详情	
图表 190157 第三方库漏洞详情	
图表 191158 生成项目第三方库报告	
图表 192159 插桩 AGENT 列表	
图表 193160 JAVA 语言插桩 AGENT 详情	
图表 194161 GOLANG 语言插桩 AGENT 详情	
图表 195162 . NET FRAMEWORK 语言插桩 AGENT 详情	
图表 196163 . NET CORE 语言插桩 AGENT 详情	
图表 197164 Node. JS 语言插桩 AGENT 详情	
图表 198165 PYTHON 语言插桩 AGENT 详情	
图表 199 PHP 语言插桩 AGENT 详情	
图表 200166 镜像仓库	
图表 201167 镜像仓库-重新扫描	
图表 202168 编辑镜像仓库	
图表 203169 镜像仓库-删除	
图表 2041 70 新建镜像仓库	
图表 205171 镜像仓库详情	
图表 206172 镜像仓库-批量删除	
图表 20717 3 镜像详情	
图表 20817 4 镜像详情-漏洞详情	
图表 20917 5 镜像详情-忽略漏洞	
图表 21017 6 流水线任务	
图表 211177 流水线任务-合并任务	
图表 212178 流水线任务-删除任务	
图表 213179 流水线任务-构建详情	
图表 214180 流水线任务-漏洞详情	
图表 215181 流水线任务-忽略漏洞	
图表 216182 选择报告目标	
图表 217183 报告管理	
图表 218184 报告下载	
图表 219185 检测报告	
图表 220186 用户管理	
图表 221187 编辑资料	
图表 222188 修改密码	
图表 223189 新增用户	

杭州默安科技有限公司

图表	224190	编辑资料	115
图表	225191	修改密码	115
图表	226192	删除用户	115
图表	227193	部门管理	116
图表	228194	修改用户部门	. 116
图表	229195	部门管理-编辑部门	
图表	230196	角色管理	117
图表	231197	角色管理-重命名	. 117
图表	232198	角色管理-删除	. 118
图表	233199	用户注册控制	. 118
图表	234200	权限审批	118
图表	235201	审批记录	119
图表	236202	认证源	. 119
图表	237203	认证源管理	.119
图表	238204	编辑认证源	.120
图表	239205	删除认证源	.120
图表	240206	添加认证源	.120
图表	241207	添加认证源-LDAP	. 121
图表	242208	添加认证源-AD 域	. 121
图表	243209	添加认证源-CAS	121
图表	244210	AK/SK	. 122
图表	245 AK	/SK-查看 SECRETKEY	122
图表	246211	AK/SK 编辑页面	.122
图表	247 登录	录安全设置	123
图表	248212	系统信息	124
图表	249213	授权配置	124
图表	250214	站点黑名单	.125
图表	251215	新增站点黑名单	125
图表	252216	源 IP 黑名单	125
图表	253217	新增源 IP 黑名单	. 126
图表	254218	源 IP 白名单	126
图表	255219	新增源 IP 白名单	. 126
图表	256220	请求特征黑名单	127
图表	257221	新增请求特征黑名单	. 127
图表	258222	代理黑名单	. 127
图表	259223	新增代理黑名单	128
图表	260224	邮件通知设置	. 128
图表	261225	消息通知-WEBHOOK	. 129
图表	262226	消息通知-添加 WEBHOOK	.130
图表	263227	网络配置-网络测试	130
图表	264228	网络配置-DNS 配置	.131
图表	265229	网络配置-HOST 配置	131
图表	266230	网络配置-HOST 配置-添加弹框	131
图表	267231	系统升级	132
图表	268232	维保时间到期提示	. 132

图表	269233	流量信使查看页面	133
图表	270234	流量信使-标签	133
图表	271235	流量信使-修改标签	133
图表	272236	流量信使-监听端口	134
图表	273237	流量信使-修改监听端口	. 134
图表	274238	流量信使-启动	134
图表	275239	流量信使-卸载	134
图表	276240	流量信使-详情	135
图表	277241	流量信使-删除	135
图表	278242	流量信使下载	. 135
图表	279243	流量信使安装成功样例	138
图表	280244	流量信使安装常见错误 1	. 139
图表	281245	流量信使安装常见错误 2	. 139
图表	282246	流量信使安装常见错误 2 G++	. 140
图表	283247	流量信使安装常见错误 2 G++安装	140
图表	284248	规则列表	141
图表	285249	添加规则	141
图表	286250	测试规则	142
图表	287251	规则列表	142
图表	288252	编辑规则	142
图表	289253	删除规则	143
图表	290254	插桩类规则列表	143
图表	291255	添加插桩类规则	144
图表	292256	插桩类规则列表	144
图表	293257	编辑插桩类规则	145
图表	294258	删除插桩类规则	145
图表	295259	插桩类自动发现规则	146
图表	296260	应用规则	146
图表	297261	忽略规则	147
图表	298262	个人隐私数据泄漏规则	147
图表	299263	个人隐私数据泄漏添加规则	148
图表	300264	漏洞信息目定义	148
图表	301265	编辑漏洞信息	150
图表	302266	WEB/LDAPLOG 查询	. 151
图表	303267	贝囬目定义	151
图衣	304268	日定乂机畚饪能阈值	152
图衣	305269	自定义业节	153
图衣	306270	自定义业书上传业书	. 153
含衣 図 ==	30/2/1	日尺入Ш丁一修以协金	. 153
(当衣)	308272	日尺入Ш ⁷	. 154
凶衣 図主	309273	¹	154 155
(2)衣 因主	31UZ/4	次口/Y凹旧日た入	155 155
(1)衣 (2)衣	3112/5 210076	NOS WEDHUVA 前者日止入	155 155
回衣	312270	円/ 豆ぷ江町 新協田白白夕苗	150 150
含衣	313277	が「「「「」」」「」」」「」」」」「」」」」」」」」」」」」」」」」」」」」	120

314278	流量镜像管理	.156
315279	流量镜像请求信息	157
316280	日志审计	158
317281	帮助中心	.158
318282	消息中心	.159
319283	JENKINS 插件下载	159
320 雳響	资代理模式工作流程	173
	314278 315279 316280 317281 318282 319283 320 房鉴	 314278 流量镜像管理

杭州默安科技有限公司

1 概述

1.1 产品概述

需鉴是一款在业务上线前进行安全自检的智能工具。利用网关代理和快速诊断技术实现 全面、快速漏洞扫描,通过弹性私有云部署模式建立一站式服务解决方案,对项目安全进行 高度可视化、可持续化管理。通过使用本产品,帮助安全人员将安全问题更透明、更简单的 呈现在开发、测试面前,将漏洞发现能力贯穿于项目开发周期中,确保 99%的安全隐患在业 务系统上线前被提前发现并及时得到解决。

1.2 公司简介

杭州默安科技有限公司是由来自 BAT 等知名互联网安全团队资深专家及业内精英组建 成立的一家安全公司,致力于用创新技术解决企业安全问题的高新企业。将威胁情报技术和 人工智能技术融入企业真实安全防御体系,提供企业在云计算和 IOT 时代的安全整体解决方 案。默安科技将不断创新、积极探索,用专业服务成为企业信赖的安全伙伴。

2.软件部署--设备环境需求:

系统要求: Centos 操作系统 7.7+版本(系统设置参照操作系统安装.pdf) 性能要求: 8Core、16G 内存要求:不低于 500G 硬盘(系统分区/home 应大于 300G) 安装操作系统时请勾选:开发者工具组件 Development Tools (请勿选择最小化安装,不要安装自带的 mysql、nginx 等软件)

2.1 网络需求:

1. 提供一个 IP 地址。

2. 需要提供 DNS 和网关地址。

- 3. 防火墙策略保障预留的物理机 IP 之间网络连接。
- 需要开放的端口:

序号	源地址	目的地址	开放端口	协议	用途	描述
1			22	TCP	SSH (远程管理)	可自定义
2	管理员地址段	電收抽机	443	TCP	web 管理	
3		房釜地址	81	TCP	web 管理	
4			5000	TCP	程序安装端口	
E	测试终端地址段	雳鉴地址	9000	TCP	代理端口	鉴权代理
5			9002	TCP	代理端口	非鉴权代理
6	目标服务器	雳鉴地址	8989	ТСР	agent 管理 漏洞上报	插桩模式
8	目标服务器	雳鉴地址	9003	TCP	流量信使	
9	智能终端地址段	雳鉴地址	500、4500	UDP	VPN 端口,手机 APP 测试用	
10	日志服务器	雳鉴地址	9092	TCP	Kafka	日志导入

2.2 初始化安装

初次拉起 IAST 镜像后,可能需要进入后台配置地址信息, IAST 产品安装在 ubuntu20.04 操 作系统上,请先配置/*etc/netplan*下的网卡文件,确保 IAST 跟外部能联通再进行以下初始 化操作

初始化: 首先从浏览器访问 IAST5000 端口的初始化配置页面 <u>http://<IAST 地址>:5000</u>,

172.1	6.1 .8 0:5	i000/login										
Stack	┛ 登录	- VMware ESXi	② 震腦产品部署文档·	◎ 开发安全产品FAQ ·	🧐 IAST 😗 IAST	🕑 sast 🤨	SCA 😢 DSMP	9 研入 全管理平台	💅 stac	🧭 IAST-125	👲 工作台 [Jenkins]	🔀 默安统
							5					
					a	. چال≣	ACT.5	± x±				
					, IF	5金:1/	AS1.3	ズ衣				
					8 admin							
					, r danim							
								Ø				
					32		8	4ª?				
							登录					

💊 19段置 | 配置外路地址 | 恢复出厂设置 | 诗

注:初始化配置页面用户名密码请联系销售人员获取。

登录安装页面后,	点击右上角的 IP 设置
⑦ 雳盜・IAST・安装	

网络信息		
	1. 阿卡信息	
	2: em1: <broadcast,multicast,up,lower_up> mtu 1500 qdisc mq state UP group defa</broadcast,multicast,up,lower_up>	
	uit glen 1000 link/ether 78.2bxb/57.29/69 brd ff.ff.ff.ff.ff.ff.ff.	
	inet 172.16.1.80/24 brd 172.16.1.255 scope global em1	
	valid_ift forever preferred_ift forever inat6.fe80:7a28vzbff1e57/2969/64.scone.link	
	valid_lft forever preferred_lft forever	

填写相应的 IP 地址信息,掩码,网关,DNS 信息后,点击确定保存

0 点击保存后	会修改系统网卡配置文件, 请谨慎检查填写项是否正确	
<mark>*IP地址</mark> :		
*网络掩码:		
* 网关:		
* DNS:		

点击确定之后, IAST 会自动进行地址的配置以及相关服务的配置

3

完成地址配置后可正常使用,访问 http://<IAST 地址>:81 即可进行 web 页面使用

	\ST →	
A 用户名		
▲ 密码 Local	Ø 01 576	
 我已阅读并同意 (免责声明) 登录 用户注册 	忘记營码	

注:初始用户名密码可联系销售获取,初次登录需要激活产品,激活产品的请将设备指纹提供给销售,销售会提供激活码以激活

备注:如果为产品配置了域名、NAT 映射,或者 agent 与产品的通信地址不是网卡地址,请 在此处添加外部域名或 IP

♥ 雳鉴·IAST·安装		IP设置 高型型外路地址 杨家田山下设置 🕞
婚信息		
	1. 网卡伯思	
	2: em1: <broadcastj.multicastj.vplower_up> mtu 1500 qdisc mq state UP group defa ulti qlen 1000 link/ether 782bxbs72969 brd ff:fftf:fffff inet 172.16.180/24 brd 172.161.255 scope global em1 vald.Jft forever preferend Jft forever inet6 re80_7a2bxbftfe572969/64 scope link valid_Jft forever preferend_Jft forever</broadcastj.multicastj.vplower_up>	
	2. 路由信息	
	a na sanana na sa	

』果为产品 卡地址,谓	。配置了域名、NAT映射,或者agent与产品的通信地址不是网 在此处添加外部域名或IP
51 6 71161.1	
个部地址	请搁入外部地址
SSL证书	
	开启后可自动生成新的SSL证书并替换

3 Web 管理界面

1.3 用户登录

雳鉴云端 Web 管理界面的登录方法:

- 1) 确保设备已被正确配置。
- 打开浏览器 Google Chrome(支持以下浏览器: Google Chrome、Firefox、IE10、 IE11、safari)
 - ▶ 用 HTTP 方式连接雳鉴的 IP 地址,如: <u>http://192.168.199.80:81</u>
 - ▶ 用 HTTPS 方式连接雳鉴的 IP 地址,如: <u>https://192.168.199.80</u>
- 回车后进入如图所示的登录页面,输入正确的用户名、密码及验证码,选择需要登录的认证源,勾选免责声明同意框后单击登录。

Ø 需鉴·IAST	
A 用户名	
日家四	6
Local	V.
验证码	08
─ 我已阅读并同意 《免责声明》	
登录	
用户注册	忘记密码

图表 1 雳鉴云端 Web 管理登录界面

用户登录前需要勾选免责声明的同意框才可进行登录操作,点击免责声明后会出现免责声明
 的具体内容弹框,用户可以进行了解阅读。

炒 需鉴	·IAST		
久 用户名			
▲ 密码		Ø	
Local		~	
验证码	90	8	
3 我已阅读并同意 《	免责声明》		
	登 录		
用户注册		忘记密码	

图表 2 登录-同意免责声明

R户在接受服务之前,请务必仔细阅读	系款并同意本声明。	
用户直接或通过各类方式(包括API引)	等)间接使用此服务和数据的	的行为,都将
被视作已无条件接受本声明所涉全部内	\$;	
苦用户对本声明的任何条款有异议, 请	即止使用其所提供的全部服务	
用户使用此服务的过程中,不得以任何	5式利用其直接或间接从事进	返中国法
律、中国网络安全法的行为,且用户应	省格守下述承诺:	
1. 仅用其为用户企业自主研发的软件提	共安全测试和风险检测服务;	
2. 不得利用其在未经授权时擅自对其他	业或机关单位等进行漏洞扫	描活动;
3. 不得利用其扰乱、损害当地网络安全	专家;	
浸醒		
1. 若用户违反上述承诺,本公司有权举	员并移交司法机关处理的权利].
2. 若用户违反上述承诺,本公司有权约	上为您提供服务。	
3. 若用户违反国家法律规定,该用户将	(担全部法律及连带责任, 本	公司不承担
任何法律责任及连带责任		
附则		
对免责声明的解释、修改及更新权均属	本公司。	
	2	018年8月23日
世口 闾	,并同意	

图表3登录-免责声明

若忘记密码时,可点击登录按钮右下方的"忘记密码"按钮,页面将会弹出提示,告知
 用户如何进行密码找回。

1	安全人员,项目经理及测试人员忘记密码,请联系管
	理员进行重置
2	.管理员忘记密码,请联系我们进行重置
3	. 重置成功后可自行修改

图表 4 登录-忘记密码

若需要注册,可点击登录按钮左下方的"注册"按钮,默认情况下未开启注册功能,可
 使用管理员账户登录系统进入-权限管理中开启,如图5所示。



图表 5登录-注册

开启注册后,点击"注册"按钮,在弹出用户注册页面中依次输入必要信息,如图 5 所示;若需要项目经理的角色,可点击"如何申请当项目经理"进行查看,密码长度要求最小长度为 8 位,必须包含数字、大写字母、小写字母、特殊符号等,口令有效期为90 天(若用户 90 天未修改密码,点击登录后弹出修改密码窗口),注册后需管理员审批后才可登录系统,如图 6 所示。

		用户注册
	* 用户名	支持英文、数字及下划线
	* 密码	支持中英文、数字及符号
	* 确认密码	请再次输入密码
	角色	测试人员(如何申请当项目经理)
	* 部门	请选择部门
	邮箱	请输入您的电子邮箱
	电话	请输入您的手机号或座机
		注册 取消
		图表 6 田户注册
认密码	请再次输入密码	
角色	测试人员 (如何申请	 暂不支持目王汪册为项目经理
*部门	请选择部门	

- 4) 账号防暴力破解。
- 用户输入错误的用户名或密码后,提示错误原因及剩余可尝试登录次数,如图8所示。





● 同一用户连续登录失败大于或等于五次后,锁定当前账号十五分钟,如图9所示。



图表 9 账户锁定

1.4 项目总览

展示目前用户环境所有应用、项目的漏洞情况。具体包括项目数、请求数、漏洞数、项 目漏洞 Top5、漏洞等级分布、漏洞类型分布 Top10、漏洞趋势、漏洞状态。

1.4.1新手提示

管理员用户第一次使用默认密码登录用户的时候,需要强制修改密码,不能使用默认密 码

Tel: (+86) 400-0571-211

Email: market_moresec.cn

	用户角色	用户邮箱	
	行水 管理 管理员首次登陆, i	青修改密码	
	新密码:	输入新密码	
	确认新密码:	再次输入新密码	
	旧密码:	旧密码	
1			目活
		LIMI .	5623
ł	z@c	Iq.com	56895689
	222	@qq.com	1245788956

图表 10 管理员修改密码

1.4.2数据统计

由4部分组成:当前项目/请求/漏洞数、项目漏洞 Top5、漏洞等级分布图、漏洞类型分布 Top10。

勞雳鉴·IAST					yy i 🚅 i 🕞
幽韵位置:项目总范					
	188 项目数	Ð	470367 读求款		5610
Kellimatops ddddd bechmurk 2. Micholyster tainteetaipp. 0 300	ero 160 1,200 1,500	期 前特徴分右)	選邦支受分的Top10	улавнацион - 50/25А - Танаравия
HEADE99 4.0000 4.00000 4.0000 4.0000 4.0000 4.0000 4.00000 4.0000 4.0000 4.00000 4.00000 4.00000 4.00000 4.000000 4.00000 4.00000000	iltes ilter o	● ### ● E## 7天 ● ### ● E## 7天 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	masta 1.000 2.000 1.000 1.000 500 0 mm	+8. 6. 8	● 20101 ● Datx ● Adtx (0,0)

图表 11 数据统计

- 项目/请求/漏洞数:用于统计用户的项目数、发起的请求数和漏洞数,帮助用户直观了 解当前服务概况。
- 项目漏洞 Top5:所有测试项目中发现的漏洞数最多的前五个项目,点击可跳转至相应的项目详情页面。
- 漏洞类型分布 Top10:所有测试项目发现的所有漏洞类型中漏洞数最多的十个类型,点 击可以跳转至漏洞列表页面并自动筛选展示。
- ▶ 漏洞等级分布:所有测试项目发现的所有漏洞危害按高、中、低、提示类型分布,点击

杭州默安科技有限公司

可以跳转至漏洞列表页面并自动筛选展示。

1.4.3漏洞趋势和漏洞状态

由2部分组成:漏洞趋势、漏洞状态。



图表 12 服务概况

- 漏洞趋势图:所有测试项目发现的未修复,已修复漏洞的趋势,可按照时间阶段(7天、15天、30天、90天筛选)。
- 漏洞状态:展示所有项目高危,中危,低危,提示类漏洞,漏洞数/已修复/未修复的柱状图。

1.5 应用管理

应用管理界面主要管理客户当前所有已经创建的应用情况,主要展示应用列表以及应用 的包含项目数、成员、归属人等。同时可对应用做相关操作,以及查阅应用的统计内容。项 目可以与应用做关联,多个项目可以同时关联同一个应用。关联关系建立后,可以在应用管 理中查看对应的应用情况。

🍠 雳鉴·IAST	日本 日											🚅 ! 🕞
当前位置: 应用管理 > 应用列表												
										应用名称/归属人	Q	新建应用
	test_y	t_001										
yy_test 项目数: 0	项目数	t: 20							应用成员: -			
	创建日]期: 2022-08-	24 20:43:33						应用归属人: -			
1313 项目数: 0	成用统	计项目列表										
	测试器	豐盖度						夏豐率	漏洞状态 ● 滝湾数 ● 已修复 ● 月	未掺复	۳.	
guishuren 项目数: 0	80%								3			
xzm测试	60%								2			
项目数: 4	20%								1			
SOFABoot 项目数: 3	0%	linyueqi	xzm-php2	2 fyfDl	DDDD	xzm-php1	xzm-py	th	0 linyueqi xzm-php2	fyfDDDDD xzm-php1	xzm-	pyth
test_yt_001 🛛 🗐	7											
项目数: 20												

图表 13 应用管理

1.5.1新建应用

点击新建应用按钮,填写应用名称和应用归属人即可以进行新建操作,应用归属人默认为当前用户。应用成员属于非必填项。如需关联项目至应用中,可至 3.4.3.1 和 3.4.3.2 中查看。

∯雳鉴·IAST	日 成月営理												
当前位置: 应用管理 > 应用列表				新建应用									
	test_yt_001			* 应用名称		入应用名称				RCPHERI			MELLY H
yy_test 项目数: 0	项目数: 创建日期:	20 2022-08-24	20:43:33	* 应用归属 应用成员	人 yy 请問	彩放用成员							
1313 项目数:0	<u>ко</u> лтен:†	项目列表				取消	确定	1					
guishuren 项目数: 0	测试覆盖度 100% 80%							244	3	● 末弓数 ● 已待复 ● 未得算			
xzm测试 项目数: 4	60% 40% 20%								2				
SOFABoot 项目数:3	0% Nr	yueqi	szm-php.	6yfD0	DDD	szm-php1	szm-py	h	0 linyu	ngi xzm-php2 fy/DDDD	D xzm-php1	×27	m-pyth_
test_yt_001 2 1 项目数: 20													

图表 14 新建应用

1.5.2编辑应用

🤔 雳鉴・IAST 编辑应用 Q MELAH • 应田名称 test_yt_001 · 应用归属人 yy_test 项目数:0 项目数 应田成長 创建日期: 1313 取満 确定 项目数: guishure 项目数: 0 xzm测证 项目数: 4 SOFABoo test_yt_001 项目数: 20 08

可以对已经创建好的应用进行编辑,重新编写应用名称、应用归属人和应用成员。

图表 15 编辑应用

1.5.3 删除应用

点击删除应用,弹出确认窗口后,可以删除已经创建好的应用。删除应用后,项目设置 中所关联的应用选项将清空。

♥ 雳鉴·IAST	88 	
当前位置: 松用管理 > 松用列表	① 提示	
yy_test	田崎田地區、田中等所包括否由此增成時後度田田 日次長後、他仍將顧石造自約後半、清陽以復召前 除?	
项目数: 0	项目数: 20 页 词 电定 创键目隙: 2022-08-24 20:43:33 页用目	ti - RAG -
1313 项目数:0	<u>前川時出</u> 項目列表 制成委員友 ● 夏夏年 風報	47.5 ● 用用取 ● 日月東 ● 木明 東 全部
guishuren 项目数:0	4 4 30%	
xzm测试 项目数: 4	40% 2	
SOFABoot 项目数:3	0% linyuxqi xom.php2 fyf00000 xom.php1 xom.pyth 0	III III Inyunçi. xam-php2 (yK0000 xam-php1 xam-pydk.
test_yt_001 团 窗 项目数: 20		

图标 16 删除应用

1.5.4应用详情

应用详情界面展示当前应用的项目数、创建日期、应用成员、应用归属人、所包含每个项目的测试覆盖度、所包含每个项目的漏洞状态以及项目列表。

📁 雳鉴·IAST	88 项目英	0 Vinter											yy I 🚅 I 🕞
当前位置: 应用管理 > 应用列表													
											应用名称/归属人	Q	新建应用
	tort	t vt.001											
yy_test		Cycloo1											
项目数: 0	項目	目数:	20							应用成员: -			
	016	主日期:	2022-08-24	20:43:33						应用归属人: -			
1313 项目数:0	应用	疏计	项目列表										
	201	试覆盖度							夏盖车	漏洞状态 ● 漂河数 ● 已修复 ● 未付	步复	全部	
guishuren	100	196								4			
项目数: 0	80	196								3			
	60	196								2			
xzm测试	40	196								-			
观日奴、9	20	196								1			
SOFABoot	0	196 ling	yueqi	xzm-php2	fyfDI	DDD	xzm-php1	xzm-py	th	0 linyueqi xzm-php2	fyfDDDDD	xzm-php1	xzm-pyth
项目数: 3													
test_yt_001	r												

图标 17 应用详情

也可以在应用的项目列表 tab 页中,点击"新建项目"按钮,直接创建与当前应用关联

杭州默安科技有限公司

雳 宏・IAST ⁸⁸ ^{第目影}							
当前位置: 应用管理 > 应用列表		新建项目	ſ				
yy_test 项目数: 0	test_yt_001 项目数: 20	 项目核 ● 自由商 	■一個 「「「「」」」 「「「」」」 「「」」」 「「」」」 「」」 「」」	版 理] - 【项目模板】 添	> 加项目模板		
1313 项目数: 0	创建日期: 2022-08-24 应用统计 项目列表	1 20:43:33	取消	确定	1 -		
guishuren 项目数:0	项目模式 调动制作	▼ 安全等級 项目模式	全部 • 安全等级	项目状态全部	项目状态	如建日期	 C 天就換目 新建项目 条件
xzm测试 项目数: 4	linyueqing xzm-php2	插桩模式 流量信使模式	 商危 安全 	lyq2 cmtest	• 扫描中 • 已完成	2022-08-29 17:01:03 2022-08-29 16:58:26	查看详情 取消关联 查看详情 取消关联
SOFABoot 项目数: 3	fyfDDDDD	播桩模式	0安全	admin	 已暫停 	2022-08-29 16:58:11	查看许情!取消关联
test_yt_001 🛛 🗐	xzm-php1	插桩模式	♥ 高危	cmtest	• 扫描中	2022-08-29 16:37:33	查看详情 取消关联

的项目,也可点击"关联项目"按钮进行批量项目关联应用。

图表 18 应用中新建项目

1.6 项目管理

项目管理页面主要管理当前用户的所有上线前需要安全测试的项目,重点展示所有项目 的测试情况,可查看此项目的基础信息,同时可对项目检测状态及项目的检测优先级进行操 作。

ジ 雳鉴・IAST 🐰 🙃			yy I 😅 I 🕞
当前位置: 应用管理 > 項目列表 全部 枚度決 排作方式 技術时间排序 * 項目状态 (語点)汗	 安全等级 道品符 • 项目模式 前 	ana 🔹 🔹	
saomiao8079 原目構式: 流磁倍映模式 項目状态: • 排刷中 0 安全 環由信気: * 竹樹、中 副際 全全等現 清末数: 7 副開発要点社: 0.00%	 ・	ms_p 项目模式: 流風信使模式 项目技法: • 上翻中 56 高危 或目目从: • frf 國際政 安全等级 调定数: • 45 新神社政 副院務委員法: 0.00% 国際政政会研究1.11% 。	ms_proxy 局援式:該風信受機式 项目技式: 13時中 68 高危 项目目調人: 5f 期間数 金金号吸 消失数: 52 暂停检测 週間時回点計:: 0.00% 100% 100%
233rrfegt 项目模式: 流晶微微模式 项目标志: • 已完成 34 高后 项目标志: 23 國際 安全等级 游求数: 23 图称数多数 23 图称数多数 23 图称数多数 23 图称数多数 23 图称数多数 23 图称数多数 24 00%	 dadadadadada 原目載式: 括於様式 原目が広: ・ 打勝中 原目に置人: admin 原用数: 2 空音等系 読み表: 1 通時第五法比: 0.00% 	金 test_host_22 项目根北: 括射機式 项目成志: • 三路停 1 项目日風人: zhangzc 潮田駅 端末款: 1 建築地図 遍明修業占社比: 0.0076 建築地図	まtest_host_11 球目模式: 捕捉換式 項目模式: 油田提載: 項目見人: zhangz: 環境数: 0 職同等業品比: 0.00%
🏄 taintwebapp-20220830	🌲 taintwebapp-20220830	🎄 dddadadaADAdaasd 🔹 🚖	🎄 3131



1.6.1项目模板

项目模板是为了减少新建相同配置项目的重复劳动、简化流程而设置。管理员、安全人

14

员、项目经理均可新建、查看、编辑和删除项目模板,区别不同的是管理员和安全人员对所 有模板均有上述四种权限,而项目经理可新建模板和查看所有模板,但是只能编辑和删除自 己创建的项目模板。

查看所有的项目模板。

欄板名称	应用项目	更新的时间 💠	创建人	操作
插桩test213123	88888	2020-03-30 10:29:36	admin	编辑丨删除
流量信使模板	aaaaaqweq 🔤	2020-03-28 11:06:11	admin	编辑丨删除
插性模板	播柱模板项目 🔤	2020-03-28 17:28:59	admin	编辑丨删除
同步模极测试	同步模板测试 🔤	2020-03-30 11:33:26	admin	網續 删除
播桩ters		2020-03-30 10:23:18	admin	编辑丨册除

图表 20 项目模板列表

欄板名称	应用项目	更新时间 ⇔	创建人	操作
插桩test213123	88888	2020-03-30 10:29:36	admin	编辑丨删除
流量信使模板	aaaaaqweq 🔤	2020-03-28 11:06:11	admin	(#16) #199
插桩模板	播桩模板项目 🔤	2020-03-28 17:28:59	admin	编辑 删除
同步模极测试	同步模极测试 🔤	2020-03-30 11:33:26	admin	網羅 删除
播桩ters	¥	2020-03-30 10:23:18	admin	编辑丨册除

图表 21 模板列表操作中可选择编辑/删除模板

1.6.1.1 新建项目模板

新建项目模板和新建普通项目时流程一致(每个项具体含义请参考新增项目-自由配置)。

1 选择检测模式			2 项目基本设置	3 项目高级设置
1.选择检测模式				
* 模板	名称 请详细输入模板名	你		
项目	类型 ● 插桩模式 ● 非鉴权代理模式	 流量信使模式 流量镜像模式 	○ 鉴权代理模式 ○ VPN模式	
播桩模式介绍 适用场景 模式特点 注意事项	适用于 Java/Golang/.NET I 对误报奉和漏报率要求特别 项目存在token,传输加密, 对通用漏間误报奉几乎为0% 能够获取最详细的漏洞信息, 插桩模式离在被测业务服务者	Framework/.NET Core/Node 雪格的项目 验证码等防重放机制 包括代码执行数据流,请求 最上按要求配置相应的Agent,	a.js/Python/PHP 语言开发的web/app项目,基于http/https进行数据储 数据包, 瀰洞代码行数 若未配置, 请先前往【播桩Agent】 页面,进行Agent下载和配置	输
			下一步 取消	

图表 22 新建项目模板

1.6.2项目列表

项目列表简要记录当前用户的所有项目的信息,列表中可查看到项目名称、项目模式、

项目安全等级、项目状态、项目测试进度、请求数、漏洞修复占比、漏洞数、项目归属人。 此列表可根据项目名称/归属人/项目地址进行查询,并可进行项目新增。

💋 雳鉴・IAST		日 む 🕢 同管理 第三方库 活柱Agent 蟻		② 目 系統配置 帮助中心				w	· 🚅 · 🕞
4前位置:应用管理 > 项目列表									
部收藏夹									
除方式 按照时间排序 🔹	項目状态 请选择	▼ 安全等级 请选择	· 项目模式 请选择	*			项目名称/归属人/项目地址	然量管理	新建项目
aomiao8079 和日初: 加量信件地で 相行志: 神政中 相日編人: fyf 等求数: 7 解除変点比: 0.00% 和時期を通知0.0%	0 安全 黑際政 安全等级 第停检测	 ýwk_test ぶ回様式: 時日使に ぶ回様式: 6 已解体 ぶ回目に減入: 9 wk 済ず数: 2 編用除数に出: 0.00% 	3 中危 運用数 安全等税 (組織性)別	ms_p 和目板式:近星の存板式 双目板式:•13時中 双目和風人:54 國際等品は:200% 五年現在251119 。	56 潮河政	☆ 前 ☆ ☆	ms_proxy 项目电比: 近型闭接电比 项目印题: 19届中 项目印题: 191 调序数: 52 週間等数:11:000% 量明形成的:385%	68 கால	高危 安全等等 暂停检测
33rrfegt 日相式: 近量信使相式 日気法: 20円成 日日風人: xzm 実数: 23 同時終点上に: 0.00% - 当前期に出資13.04%	34 高危 第月回数 全全等级 貿保総務	 dadadaddadaa 項目構成: 調控構成 項目状成: • 13編中 項目状態: • admin 導示家: 1 諷明等最広社: 0.00% 	1 高危 原用数 空全部段 1 1 1 1 1 1 1 1 1 1 1 1 1	▲ test_host_22 30日根3:: 調性性3: 30日月35(4): → 已着卓 30日月35(4): zhangzc 第5年表: 1 週刊時85(2)12: 0.00%	1 最高数	高危 _{交全等吸} 继续检测	test_host_11 項目成:: 添於版式 项目成:: ふ於版式 项目式D:: - 已醫學 项目に置ん: zhangz 请求款: 0 週間修覧と記:: 0.00%	0 ###	安全 ^{安全朝初}
: taintwebapp-2022083(目標式: 添姓機式 目板式: • 扫描中 日初葉人: chanhu	D120955 79 高危 展版 安全年夜	ま taintwebapp-20220 项目模式: 插鼓模式 项目状态: • 扫描中 下面に用意 - chealu	330120017 81 高危 ^{展現数} 史全年级	dddadadaADAdaasd 項目模式: 添桩模式 項目状态: • 已聲傳 项目目標 A: fut pm	4 #R0	★ 高危 22900	3131 项目機式: 添胜模式 项目状态: • 已暫序 项目印度人: fuf nm	4 #####	高危

图表 23 项目列表

▶ 点击"批量管理"后,可以选中多个项目进行删除或者暂停,完成操作后点击"退出批 量"即可。

🍠 雳鉴 · IAST		日 ① ④ ④	□□	 			yy	😅 ! 🕞
当前位置: 应用管理 > 项目列表 全部 收缩表 ● 单页全选 删除项目) 暂停检测	n				1	项目名称/归属人/项目地址	退出批量	新建項目
saomiao8079 阿根本:: 沈星市産業の 福田本 昭本 昭和本 昭本 昭和本 昭和本 昭本 昭本 昭本 昭和本 昭本 田	0 安		3 中危 第19世 安全中位 1957年1月	○ ms_p 和目前::: 法国用原稿: 和目前紙:: 外目 通常:: 45 國際時間点::: 000% 風俗になる51.11% 、	56 高危 ^{国际数 全线领 官等注照}	 ms_proxy 場目頃た: 近島県使後期に 場目頃長ん: fyf 病子院: 52 通時参見ご託: 0.00% 出目がたま51.85% 	68 ####	高危 安全等级 新學检測
项目模式: 近服 使使模式 项目 机式: 0 已完成 项目 日頃人: xzm 请求款: 23 课用 移動占比: 0.00% _ 单和前前定度13.04%	34 高 編用数 文全 留得检惑	项目構成: 調整機成 项目構成: 調整機成 项目対応: • 扫漏中 项目対策人: admin 或目対策人: admin 或言対策人: admin 國際機能出: 0.00%	1 高危 案務 安全地校 哲学检測	项目推动: 總位構成 项目技巧: • 已對導 项目到版: zhangzc 读示款: 1 题明時意識出社: 0.00%	1 高危 高時数 安全等级 	項目構成:に 御社構成で 項目状態: ・ 已留停 項目日源人: zhangzc 領示版: 0 週間除線点出:: 0.00%	0 181930	安全 ^{安全ф収}
▲ taintwebapp-2022083 項目機式: 添担機式 項目状态: ●扫描中 仮目引用 A : chanla	20120955 79 高 展現数 安全		330120017 81 高危 ^{展開数} 安全等级	□ 🤹 dddadadaADAdaasd 原目機式: 施田機式 原目状态: ● 己醫療 販目原本: - 6月 cm	4 高危 第四款 空全等政	 ● 3131 项目模式: 施班機式 项目状态: ●已聲傳 び母日輝人: fof pm 	4 96/900	高危

图表 24 项目批量管理

▶ 可以根据排序方式、项目状态、安全等级、项目模式对项目进行筛选,可以根据项目名 称、归属人、项目地址进行搜索。

排序方式 按照时间排序 × 项目状态 诵选择 × 安全等级 请选择 × 项目模式 请选择 ×

图表 25 项目筛选及搜索栏

▶ 鼠标悬停并点击项目右上角的箭头按钮可将该项目置于优先检测队列中,点击右侧垃圾 桶图标在二弹框中确认即可删除该项目,点击星号图标,可以将该项目添加至收藏夹。

项目名称/归属人/项目地址 Q 批量管理 新改项目

新建项目测试(非插桩)yt003	2	ን ₪ ☆
项目模式:流量信使模式		
项目状态:已完成	0	安全
项目归属人:	漏洞数	安全等级
请求数:0	ſ	暂停检测
漏洞修复占比: 0.00% ▼当前测试进度0.00%		

图表 26 项目优先检测及删除

点击项目列表中的收藏夹选项卡,可以跳转至项目收藏夹页面,在此页面中可以查看所 有添加到收藏夹中的项目,并且对项目进行相关操作。在收藏夹中对项目的操作,与项 目列表中操作方法一致。

🇭 雳鉴・IAST											yy (🚅 (🕞
当前位置: 应用管理 > 项目列表											
全部 校藏夫											
🎄 dddadadaADAdaasd		8	*								
项目模式: 龋胜模式											
项目状态: •已暂停	4	高角	2								
项目归属人: fyf_pm	展河政	安全等	NR.								
请求数: 2		101000									
延同修复占比: 0.00%			-								

图表 27 项目列表中的收藏夹

1.6.3新增项目

新增项目有两种方式,分别是通过模板新增和自由配置。

○ 项目模板	× .
	可前往【项目管理】- 【项目模板】 添加项目模板
● 自由配置	

图表 28 新建项目

1.6.3.1 使用模板

管理员、安全人员及项目经理可进行项目创建,点击"新建项目"按钮,选择项目模板, 并且选择已创建的模板。使用模板创建项目时,允许更改的项包括项目名称、项目地址、项 目成员、邮件通知、检测方式、扫描速度、检测黑名单、用户认证凭据、过期特征、参数黑 名单。其中,若漏洞类型在创建或编辑模板时为解锁状态,则使用该模板新建项目时,漏洞 类型可更改;若漏洞类型在创建或编辑模板时为锁定状态,则使用该模板新建项目时,漏洞 类型不可更改。

1.6.3.1.1 扫描类

选择检测模式中,项目名称必填,检测模式从模板中继承且不可编辑。 关联应用名称默认为空,如果需要与已有应用做关联,在此处选择即可。 自动爬取复选框默认不勾选,项目使用模板时可编辑。

1 选择检测模式		2 项目基本设置	3 项目高级设置
1.选择检测模式			
*项目名称	请详细输入项目名		
关联应用名称 🥝	请选择该项目需关联的应用 🗸		
项目类型	 ● 插桩模式 ● 流量信使模式 ● 流量镜像模式 	 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
自动爬取	✔ 勾选后项目创建完成自动开始爬取所有项目地址		
非鉴权代理模式			
适用 测试 适用场景 项目	于http/https 协议数据传输的 web 和 app 项目 人员能够自主配置浏览器代理 不存在或者少数功能存在防重放机制		
能够 (/) 模式特点 请求	时https进行劫持,还原明文请求包进行安全测试 试逻辑漏洞 录入不需要进行代理鉴权,测试者无需分配last系统账号		
测试 注意事项 请将	人员需配置代理,代理服务器地址为192.168.120.62,端 心】【浏览器插件】查看 登入,登出等接口加入"项目高级设置"的黑名单中	ロ为9002, 详细配置前往【帮助中心】【代理配置】查看 或下载安装浏览器	發播件,详细配置前往【帮

图表 29 新增项目-使用模板-扫描类-选择检测模式

项目基本设置中,项目地址、项目归属人、项目成员、检测方式、最大扫描并发、每分 钟发包数量、项目描述为自定义项,其中项目地址可填写无域名后缀的地址。

圣检测 模式		项目基本设置		项目高
译项目基本信息				
*项目地址 🥝	请详细输入项目地址	nttps	+	
*项目归属人	уу	V.		
项目成员	lyq × zhangzc × xzm1 × cmtest × zhanghao × xzmtest1 ×			
	5			
检测方式) 延时检测 () 实时检测 () 定时检测			
检测方式 定时检测	 延时检测 实时检测 定时检测 开始时间: 15:01 结束时间: 15:01 			
检测方式 定时检测 最大扫描并发	延时检测 实时检测 定时检测 开始时间: 15:01 结束时间: 15:01	0		
检测方式 定时检测 最大扫描并发	延时检测 实时检测 定时检测 开始时间: 15:01 (5) (3		
检测方式 定时检测 最大扫描并发 每分钟发包数量	223 223 223 223 223 223 223 223 223 223	3		
检测方式 定时检测 最大扫描并发 每分钟发包数量	 延时检测 实时检测 ● 走时检测 开始时间: 15:01 ● 结束时间: 15:01 223 223 223 223 223 223 223 223 224 223 225 225 225 226 227 227 228 229 229 229 229 229 220 220 223 223 223 224 225 225 226 227 227 228 229 229 229 229 229 220 220 220 220 223 223 224 223 225 223 224 223 225 223 224 223 224 223 223<td> ③ 23 </td><td></td><td></td>	 ③ 23 		

图表 30 新增项目-使用模板-扫描类-项目基本设置

项目高级设置中,消息通知、检测黑名单初始值继承自项目模板且可自由编辑。可以开 启消息通知,编辑推送内容的风险类别(全部风险、低危及以上风险、中危及以上风险、高 危风险)、WebHook 和邮箱地址,、webhook 可以选择此项目需要推送的 webhook 地址,具体 webhook 添加方法,请参照 3.10.4.2 部分。

Tel: (+86) 400-0571-211

Email: market_moresec.cn

1 选择检测模式	项目	2 基本设置	3.1 项目高级设置	3.2 漏洞类型	3.3	記豊
3.1项目高级设置						
消息通知 🦲	C					
	推送内容	全部风险	×			
	WebHook	无	×			
	邮箱地址	以分号间隔邮箱				
			1.			
		配置邮件服务器后,可使用邮件通知				
检测黑名单	批量导入 💿 单务	《导入 【推荐黑名单设置】				
H	lost:		包含子域名	+		
c	gi:		前缀匹配 🗸			
分节点扫描 🗌	开启后可指定扫描,	5点进行扫描				
Cookie保持 🕢	开启Cookie保持 (ヲ	F启后会定期访问相关HOST,保持Cod	kie的有效性)			
漏洞检测 🖌	开启漏洞检测 (勾递	后将默认开启漏洞检测功能)				
检测增强	开启后可增强部分》	漏洞的检测能力				
		返回上—步	完成下一步	取消		

图表 31 新增项目-使用模板-扫描类-项目高级设置

当开启检测增强模式时,可以配置需要检测弱口令的服务类型。

漏洞检测	☑ 开启漏洞检测(勾选后将默认开启漏洞)	测功能)
检测增强	✔ 开启后可增强部分漏洞的检测能力	
弱口令漏洞类型	□ 全部	
	smtp弱口令漏洞	pop3弱口令漏洞
	SMB弱口令漏洞	SNMP未授权访问漏洞
	FTP弱口令漏洞	PostgreSQL弱口令漏洞
	DB2弱口令漏洞	Oracle弱口令漏洞
	■ RDP弱口令漏洞	Telnet弱口令漏洞
	phpmyadmin弱口令	MySQL弱口令漏洞
	MongoDB弱口令漏洞	LDAP弱口令漏洞
	Tomcat弱口令漏洞	SSH弱口令漏洞
	HTTP 401认证弱口令漏洞	HTTP网站表单弱口令
	MSSQLServer弱口令漏洞	Redis弱口令漏洞
	Memcached弱口令漏洞	rsync 未授权访问漏洞
		返回上一步 完成 下一步 取消

图表 32 新增项目-使用模板-扫描类-项目高级设置-开启检测增强

漏洞类型配置中若模板为解锁状态,则可进行配置;若模板为锁定状态,则不可进行自 由配置。

5)

图表 33 新增项目-使用模板-扫描类-漏洞类型配置

自定义配置中用户认证凭据、过期特征、参数黑名单、登入登出请求特征、扫描超时时间继承自项目模板且可自由编辑。

选择检测模式	项目基本设置		3.1 项目高级设置	3.2 漏洞类型配置	3.3 自定义配置
3.3自定义配置					
用户认证凭据位置	HTTP header v	Cookie	+		
用户凭据过期特征 🥥	响应码特征 🗸	响应码值	+		
参数黑名单设置			+		
扫描超时时间 🥝	15 秒				

图表 34 新增项目-使用模板-扫描类-自定义配置

1.6.3.1.2 插桩类

选择检测模式中,项目名称必填,项目类型为继承自模板不可编辑。 关联应用名称默认为空,如果需要与已有应用做关联,在此处选择即可。

1 选择检测模式			2 项目基本设置	3 项目高级设置
.选择检测模式				
*项目名称	请详细输入项目名			
关联应用名称 🕜	请选择该项目需关联的	が用いく		
项目类型	 插桩模式 非鉴权代理模式 	 流量信便模式 流量镜像模式 	◎ 鉴权代理模式 ◎ VPN儀式	
播桩模式介绍 适用场票 适用 使式符点 和线 注意事项 加速 注意事项 加速	于 Java/Golang/.NET Fran 报奉印讀根率要求特别严格 存在token,传输加密,验 明識潤與稅率几乎为0% 获取最详细的漏屑信息,包 模式需在被测业务服务器上	nework/.NET Core/Node.js// 的项目 证码等防重放机制 括代码执行数据流,请求数据 按要求配置相应的Agent,若:	Python/PHP 语言开发的web/app项目,基于http/https进行数据传输 包,漏洞代码行数 未配置,请先前往【插桩Agent】页面,进行Agent下载和配置	

图表 35 新增项目-使用模板-插桩类-选择检测模式

项目基本设置中,项目语言为必填项,这里决定了此项目需要归并哪个语言类型的 agent。 项目规则为必填项,三个维度的规则至少填写一个,以及项目成员与项目描述。

1 选择检测模式	μρ	2 基本设置	—————————————————————————————————————
2.选择项目基本信息			
* 项目语言	Java Golang .NET Framework .NET Core	Node.js Python PHP	
* 项目规则 🥝	Agent • * 插桩模式下需要先在被测应用服务器上安装Agent后再创建项目, * Tag标签需要通过启动参数或环境变量指定,详见项目规则提示	请前往【播桩Agent】下载安装Agent	
*项目归属人	уу		
项目成员	请选择项目成员		
项目描述	请输入项目描述		
	返回上一步 高级设	完成取消	

图表 36 新增项目-使用模板-插桩类-项目基本设置

项目高级设置中,若模板为解锁状态,则可进行配置;若模板为锁定状态,则不可进行 自由配置。在此处自行勾选需要检测的漏洞类型。

<u> 剥模式</u>	IJ	而目基本设置	本设置 漏洞类型配置			
編洞类型						
选择漏洞类型	■ 选择全部漏洞类型					
	✔ 高危漏洞(45)	🖌 中危漏洞(14)	■ 低危漏洞(14)	■ 提示漏洞(22)		
	✓ 表达式注入攻击		✓ 文件上传			
	✓ 任意文件下载		✓ 跨站脚本攻击(XSS)			
	SMTP邮件注入		🗹 命令执行			
	☑ NoSQL注入		✓ SQL注入			
	✓ 代码执行		✓ 不安全的反序列化			
	✓ 任意文件写入		✓ 任意文件删除			
	✓ 服务端模版注入(SSTI)		🛃 api接口未授权访问			
	☑ JNDI注入		✓ 不安全的Spring自动绑定	(JDK9以上)		
	✓ auto_test_1658460682		auto_test_1658829315			
	auto_test_1658891923		🤕 auto_test_1658909891			
	🗹 auto_test_1658913361		auto_test_1658913504	_		

图表 37 新增项目-使用模板-插桩类-项目高级设置

在项目高级设置中,可以开启消息通知,编辑推送内容的风险类别(全部风险、低危及 以上风险、中危及以上风险、高危风险)、WebHook 和邮箱地址,webhook 可以选择此项目需 要推送的 webhook 地址,具体 webhook 添加方法,请参照 3.10.4.2 部分,支持自定义编辑漏 洞展示规则,可选择漏洞去重条件"相同因素"(漏洞类型、Host、漏洞 URL、自定义 header 参数)和相同因素漏洞处理方式,Java 语言下可配置漏洞地址黑名单,可选择开启漏洞修复 识别、主动验证和主动扫描功能,Golang、.NET Framework、.NET Core、Node.js、Python、 PHP 暂时不支持。

- 消息通知:开启消息通知按钮后,需选择推送内容的风险类别,风险包括全部风险、低 危及以上风险、中危及以上风险、高危风险。编辑 WebHook 和邮箱地址,webhook 可以 选择此项目需要推送的 webhook 地址;
- 漏洞展示规则:开启漏洞展示规则按钮后,需填写漏洞地址黑名单,编辑相同因素对漏洞去重条件进行选择,去重条件包括漏洞类型、Host、漏洞 URL、自定义 header 参数。
 编辑漏洞处理对相同因素漏洞处理方式进行选择,处理方式包括聚合、丢弃、误报和忽略;
- 漏洞修复识别:仅用于被动检测时识别漏洞是否已经被修复,开启后若漏洞已修复,则 将未修复状态变更为已修复,但该功能可能存在误报;
- 主动验证:用于辅助插桩模式的漏洞验证,开启后可自动对漏洞进行主动验证,并提供
 验证结果,详见漏洞列表-主动验证列及漏洞详情-判断依据 Tab 页;
- 主动扫描:开启后可附加主动扫描方式;

● 检测增强:开启后可增强部分漏洞的检测能力。

1 选择检测模式	2 项目基本设置	3.1 漏洞类型配置	3.2 项目高级设置
3.2 项目高级设置			
消息通知 🚺			
推送内容	全部风险		
WebHook	无		
前釋地址	以分号间隔邮箱		
漏洞展示规则 🔵	記畫部件額毋穩后,可使用部件通知 	6	
漏洞地址黑名单 🕜	请填写漏洞url正则表达式	+	
相同因素 🔷	漏洞送型 Host 漏洞URL 自定义header参数 湖榆入自定义h	sader参数 +	
漏洞处理 💈	请选择		
漏洞修复识别 📀 🗌 开启后可自动识别漏洞是否已经被修复 (测试功能,可能存在误判的情况)			
主动验证 🔮 🗌 开启后可自动对黑陶进行主动验证,并提供验证结果(测试功能)			
主动扫描 🗌 开启后可附加主动扫描方式			
"注:请确认【插班Agent】中请求收集开关已经开启。			
检测增强 🗌 开启后可增强部分漏洞的检测能力			
返回上一步 完成 取消			

图表 38 新增项目-使用模板-插桩类-项目高级设置

在项目高级设置中配置是否开启检测增强功能,以支持对更多服务的弱口令漏洞的扫描。

Tel: (+86) 400-0571-211

Email: market_moresec.cn
主动扫描	☑ 开启后可附加主动扫描方式			
	*注: 请确认【插桩Agent】中请	求收集开关已经开启。		
选择漏洞类型	□ 全部类型			
	高危漏洞(11)	_ 中危漏洞(15)	(12) 低危漏洞(12)	_ 提示漏洞(11)
	SQL布尔注入		SQL延时注入	
	🗌 破壳漏洞		struts2漏洞	
	参数遍历		验证码回显	
	666哇		test_melody222	
	hyk_test		□ 压力山大	
	123123			
检测方式 最大扫描并发	 延时检测 ③ 实时检测 4.1 4.1 法通速度慢,适用于服务配置低的; 	0		
每分钟发包数量	0			
	* 控制所有并发连接的每分钟发包总额	数,设置为0时表示不限制发包数		
检测黑名单	○ 批量导入 (● 单条导入 【推荐	李黑名单设置]		
	Host:	□ 包含子!	或名 +	
	Cgi:	前缀匹配	\sim	
		返回上一步 完成	下一步 取消	

图表 39 新增项目-使用模板-插桩类-项目高级设置-检测增强

1.6.3.2 自由配置

管理员、安全人员及项目经理可进行项目创建,点击"新建项目"按钮,选择自由配置。 自由配置中,创建者可以编辑所有配置项。

1.6.3.2.1 扫描类

管理员、安全人员及项目经理可进行项目创建,点击"新建项目"按钮,输入项目名称 后根据具体场景选择项目模式,填写项目基本信息包括项目地址,项目成员,项目地址协议, 检测方式,扫描速度,此时项目归属人为当前登录人员,点击保存即项目被创建成功,此时 会自动为成员分配对应任务。若有需要可点击高级设置,进行项目黑名单设置,用户凭据配 置,邮件通知填写,选择检测漏洞类型,自定义配置等。

关联应用名称默认为空,如果需要与已有应用做关联,在选择检测模式步骤时填写即可。

Tel: (+86) 400-0571-211

Email: market moresec.cn

1 选择检测模式		2 项目基本设置	3 项目高级设置
1.选择检测模式			
*项目名称	请详细输入项目名		
关联应用名称 🤇	请选择该项目需关联的应用 🗸 🗸		
项目类型		2	
非鉴权代理模式 运 测	拥于http/https 协议数据传输的 web 和 app 项目 1试人员能够自主配置浏览器代理		
适用场景 可 能 模式特点 译	目不存在或者少数功能存在防重放机制 1够对https进行劫持,还原明文请求包进行安全测试 测试逻辑漏洞 1求录入不需要进行代理鉴权,测试者无需分配last系绑	党账号	
》 注意事项 详	(试人员需配置代理,代理服务器地址为192.168.120.6)中心】【浏览器插件】 查看 (将登入,登出等接口加入'项目高级设置'的黑名单中	32, 端口为9002, 详细配置前往【帮助中心】【代理配置	】 童看 或下载安装浏览器插件,详细配置前往【帮

图表 40 新增项目扫描类-选择项目模式

- 项目模式选择:新建项目的时候需先选择项目模式,共有流量信使模式,鉴权代理模式, 非鉴权代理模式,流量镜像模式,VPN模式,各个模式的适用场景、模式特点、注意事 项在模式介绍中都有说明。
- 自动爬取:默认不勾选,勾选后项目创建后雳鉴开始执行主动爬虫功能爬取所有项目地址,爬取配置按照默认配置。
- 项目基本信息:项目地址、项目归属人、项目成员、最大扫描并发、每分钟发包数、项目描述六部分组成。
 - 项目地址:可直接输入 host 及 host+path 两类,可直接输入根域名(如: www.test.com) IP 地址(如: 192.168.1.1)或无域名后缀的地址,并可选择是否 包含子域名,或者输入带路径的 URL(项目地址目前可支持 IPV4 地址和域名以及 IPV6 域名)。
 - 2)项目地址协议:供主动爬虫爬取站点使用,默认不勾选。
 - 3)项目归属人:可选一人,默认为当前用户。
 - 4)项目成员:可以拉取其他用户进入项目中。
 - 5) 最大扫描并发: 控制扫描器最大扫描的并发数。
 - 6) 每分钟发包数: 控制扫描器所有并发每分钟发送请求包总数。
 - 7)项目描述:添加对项目的描述,150字以内。

Tel: (+86) 400-0571-211

Email: market moresec.cn

西岸位则惧 式	项目基本设置	项目高级设
选择项目基本信息		
*项目地址 🥝	请详细输入项目地址 🗌 https 🗌 包含子域名 🕇	
*项目归属人	УУ	
项目成员	请选择项目成员	
检测方式	○ 延时检测 ● 实时检测 ○ 定时检测	
最大扫描并发	25 25	
	* 扫描速度價, 适用于服务配置低的业务	
每分钟发包数量	0	
	* 控制所有并发连接的每分钟发包总数,设置为0时表示不限制发包数	

图表 41 新增项目-项目基本配置

- 检测内容设置:选择检测模式,分为延时检测,实时检测,定时检测三种,可设定最大 扫描并发以及每分钟发包数。
 - 1) 任务初始默认开启漏洞检测行为,并可选择进行延时或实时或定时检测。
 - 2)最大扫描并发控制扫描器并发池最大并发数,每分钟发包数控制扫描器每分钟发包 总数。
- 高级设置:设置黑名单,选择是否开启 Cookie 保持,设置邮件通知、扫描漏洞类型、用 户认证凭据、漏洞检测模式、是否开启弱口令检测增强等。
- 项目成员:将需要进行测试工作的项目成员添加进来,而后会自动为该项目成员分配 检测任务。
- ▶ webhook:选择此项目需要推送的 webhook 地址,具体添加方法,请参照 3.10.4.2 部分

1 法经检测模式	2 项目基本设备	3.1	3.2 漫词送刑帮骂	3.3 白中小野間
3.1项目高级设置			THE OF CAREFUL	
消息通知				
(PARAGAR)	推送内容全部风险	2		
	WebHook 王			
	Vicensor Ju			
	邮箱地址 以分号间	同隔邮箱		
		li		
	創塑取件設	將醫后,可便用鄧件通知		
检测羔名甲	○ 批重時入 ● 単余時入 【	推存兼名単设置]		
	Cqi:	□包含于或名		
分节点扫描	开启后可指定扫描节点进行扫	描		
Cookie保持	✔ 开启Cookie保持 (开启后会定	期访问相关HOST,保持Cookie的有效性)		
漏洞检测	开启漏洞检测(勾选后将默认)	千启漏洞检测功能)		
松迎ば曾强	开启后可增强部分漏洞的检测	能力		
		返回上一步 完成 下一步	取消	
		因主 40 项目言	加加型	
		含衣 42 坝日尚	级反直	
_	_		_	-
1	2	3.1	3.	3.3
选择检测模式	项目基本设置	项目高级设置	漏洞类型	型 配置 自定义配置
3.2 选择漏洞类型				
✓ 全部类型				
「古会混泪(の)	一 古谷混泪(16)			
✓ 商/已濟刑(9)	✓ 甲心癖池(10)	≤ 1広/已湖新月(13)	✓ 提示痛加(15)	
✓ struts2漏洞		✔ 任意文件下载		
✓ SQL布尔注入		✓ SQL延时注入		
☑ 文件上传		✔ 参数遍历		
🔽 命令执行		✔ 代码执行		
✓ 破売漏洞				
对支持的漏洞户用OOR	(数据带办检测) 检测	方式		
		返回上一步 完成 下一	步 取消	

图表 43项目高级设置-漏洞类型

新建项目 				
1 选择检测模式	2 项目基本设置	3.1	3.2 海海类型配置	3.3
3.3自定义配置				
用户认证凭据位置	HTTP header V Cookie	ie +		
用户凭据过期特征 🔇	响应码特征 > 响应码	3值 +		
參数黑名单设置		+		
扫描超时时间	15 秒			
		返回上一步 完成 取消		

图表 44 项目高级配置-自定义配置

注意:每种模式所进行的高级配置略有差别,请以产品中的新建项目页面为准

- 消息通知:开启消息通知按钮后,需选择推送内容的风险类别,风险包括全部风险、 低危及以上风险、中危及以上风险、高危风险。编辑 WebHook 和邮箱地址,webhook 可以选择此项目需要推送的 webhook 地址;
- 2)检测黑名单:可批量导入和单条导入,单条导入支持前缀匹配,后缀匹配,正则匹配三种模式;批量导入,不同的URL通过回车分割;
- 3) 分界点扫描: 开启后可指定扫描节点进行扫描;
- 4) Cookie 保持:选择是否开启 cookie 保持;
- 5) 漏洞检测:选择是否默认项目创建后开启漏洞检测功能;
- 6) 检测增强:开启后可增强部分漏洞的检测能力;
- 7) 用户认证凭据: 自定义认证凭据的位置, 可设置多个;
- 8)漏洞类型:设置所创建的项目需要扫描的漏洞类型,可在高危漏洞、中危漏洞、低 危漏洞及提示漏洞四个大类中进行选择,也可以在大类下就具体漏洞类型进行勾选。 支持 00B 带外检测,用户根据自身的情景去配置 00B 开关是否开启,默认为关闭状态,开启后对支持的漏洞执行扫描时使用普通规则加 00B 规则扫描;
- 9)用户凭据过期特征:用户可自定义凭据过期后系统的响应特征,帮助系统更好的判断用户凭据是否过期;
- 10)参数黑名单:可设置不需要扫描的参数;
- 11)登入登出请求特征:用户可自定义登入请求和登出请求特征,帮助系统更好的判断 用户登入行为和登出行为,该特征仅鉴权代理模式可配置。
- 12) 扫描超时时间: 配置扫描器发送请求后,等待响应的超时时间。;
- 13)请求去重方式:用户可选择请求路径和请求路径与参数。

点击项目列表里面需要查看的项目,会跳转到该项目的详情页面,页面中显示该项目的 基础信息、项目统计、sitemap 列表、扫描动态及该项目的漏洞列表。

1.6.3.2.2 插桩类

管理员、安全人员及项目经理可进行项目创建,点击"新建项目"按钮,输入项目名称 填写项目基本信息包括项目语言、项目规则,项目成员,项目描述,此时项目归属人为当前 登录人员,点击完成即项目被创建成功,此时会自动为成员分配对应任务。若有需要可点击 高级设置,选择检测漏洞类型,进行主动扫描(Active IAST)配置等。

主动 IAST 为被动 IAST (Passive IAST)的补充检测模式,通过主动 IAST 和被动 IAST 结合,增强漏洞检测的覆盖能力,提高漏洞的检出率。选择开启主动扫描需同步开启【插桩 Agent】详情中对应 Agent 控制下的请求收集开关。

关联应用名称默认为空,如果需要与已有应用做关联,在选择检测模式步骤时填写即可。

1 选择检测模式				2 项目基本设置	3 项目高级设置
1.选择检测模式					
*项目行	名称	请详细输入项目名			
关联应用名称	0	请选择该项目需关联的	並用・		
项目的	赵	● 插桩模式	○ 流量信使模式	○ 鉴权代理模式	
		○ 非鉴权代理模式	○ 流量镜像模式	○ VPN模式	
插桩模式介绍					
H	适用于	- Java/Golang/.NET Fram	ework/.NET Core/Node.js	/Python/PHP 语言开发的web/app项目,基于http/https进行数据传输	
适用场景	项目存	在token,传输加密,验证	GG96 EG9等防重放机制		
	对通用	到漏洞误报率几乎为0%		86 · · · · · · · · · · · · · · · · · · ·	
	插桩横	(或嚴許細的漏洞)同志, 已前 試需在被测业务服务器上指	安要求配置相应的Agent, 老	ace, minin Cenjax 告未配置,请先前往【插桩Agent】页面,进行Agent下载和配置	
注意事项					

图表 45 新增项目插桩类-选择项目模式

下一步 取消

项目模式选择:新建项目的时候需先选择项目模式,插桩类仅有插桩模式,模式的适用 场景、模式特点、注意事项在介绍中有相应说明。

选择检测模式	项目基本设置	项目高级设置
选择项目基本信息		
*项目语言	Java Golang .NET Framework .NET Core Node.js Python PHP	
* 项目规则 🥝	Agent v 📃 🛨	
	*插桩模式下需要先在被测应用服务器上安装Agent后再创建项目,请前往【插桩Agent】下载安装Agent * Tag标签需要通过启动参数或环境变量指定,详见项目规则提示	
*项目归属人	уу ~	
项目成员	请选择项目成员	
项目描述	请输入项目描述	

图表 46 新增项目插桩类-项目基本配置

- ▶ 项目基本信息:项目语言、项目规则、项目归属人、项目成员、项目描述五部分组成。
 - 项目语言:选择此插桩项目检测的系统使用何种代码语言编写。选择后,会决定 与此项目进行归并的插桩 agent 的语言。
 - 2)项目规则:可直接输入或选择 Agent、Tag、IP,默认只展示 Agent 规则,点击展 开后显示其余两个规则,各规则均可通过输入搜索筛选。除 Agent 外,其余四项 均以下拉列表的形式展示。具体的规则说明及指定均展示在项目规则提示中。当 项目规则为空时,将无法点击下一步或者完成按钮,会有标红提示。
 - 3) 项目归属人:可指定项目负责人。
 - 项目成员:将需要进行测试的项目成员添加进来,而后会自动为该项目成员分配 检测任务。
 - 5) 项目描述:为项目添加描述,150字以内。

1 选择检测模式		2 项目基本设置	3.1 漏洞类型配置	2	3.2 项目高级设置
3.1 选择漏洞类型					
选择漏洞类型 🚺	■ 选择全部漏洞类型				
	✓ 高危漏洞(45)	✔ 中危漏洞(14)	■ 低危漏洞(14)	■ 提示漏洞(22)	A
	✓ 表达式注入攻击		✔ 文件上传		
	☑ 任意文件下载		✓ 跨站脚本攻击(XSS)		
	✓ SMTP邮件注入		🗹 命令执行		
	☑ NoSQL注入		✓ SQL注入		
	🗹 代码执行		🗹 不安全的反序列化		
	✓ 任意文件写入		✓ 任意文件删除		
	✓ 服务端模版注入(SSTI)		🔽 api接口未授权访问		
	✓ JNDI注入		✓ 不安全的Spring自动绑定 (JDK9以上)	
	🗹 auto_test_1658460682		✓ auto_test_1658829315		
	🗹 auto_test_1658891923		🗹 auto_test_1658909891		
	🗹 auto_test_1658913361		🗹 auto_test_1658913504		*
	-	返回上一步 完成	下一步 取消		

杭州默安科技有限公司

31

图表 47 插桩类项目高级设置	置-漏洞类型
-----------------	--------

1 选择检测模式	2 项目基本设置	3.1 濕洞类型配置	3.2 项目高级设置
3.2 项目高级设置			
消息通知 💽			
推送内容	全部风险		
WebHook	无义		
曲印释自地站上	以分号间隔邮箱		
	配置部件服务器后,可使用部件通知	s	
漏洞展示规则			
漏洞地址黑名单 🥝	请填写漏洞url正则表达式	. +	
相同因素 📀	□ 漏洞类型 □ Host □ 漏洞URL		
	自定义header参数 请输入自定义he	ader参数	
漏洞处理 📀	- 请选择		
漏洞修复识别 💿 🗌 开启后可自动识别	氟洞是否已经被修复 (测试功能,可能存在误判)	5博况)	
主动验证 🕘 🗌 开启后可自动对漏	同进行主动验证,并提供验证结果(测试功能)		
主动扫描 🗌 开启后可附加主动	扫描方式		
*注: 请确认 [插板	[Agent] 中请求收集开关已经开启。		
检测增强 🗌 开启后可增强部分	扁洞的检测能力		
	返回上一步 💡	8成 取消	
		医舌口 宣加 四四	

图表 48 插桩类项目高级设置

Email: market_moresec.cn

	*注: 请确认 [插桩Agent] 中部	青求收集开关已经开启。		
选择漏洞类型	■ 选择全部漏洞类型			
	■ 高危漏洞(8)	■ 中危漏洞(13)	■ 低危漏洞(13)	■ 提示漏洞(15)
	SQL她的注入 SqL她的注入		SQL布穴注入 Ø 破売漏洞	
	chenl测试漏洞		31313	
检测方式	〇 延时检测 💿 实时检测			
星大扫描并发	25	25		
	 * 口描声度信 活用工程を和学げん 	23 bulkæ		
	- OPAGELE, LETT J WESTIGENUM	00120		
汾钟发包数量	0			
	* 控制所有并发连接的每分钟发包总	总数,设置为0时表示不限制发包数		
检测黑名单	○ 批量导入 (◎ 単条导入 () 推	转黑名单设置】		
	Host:		含子域名 +	
	Cgi:	前缀	兀配	
检测增强	Cgi: 开启后可增强部分漏洞的检测能	前缀	兀配 ∨	
检测增强	Cgi: 开启后可增强部分漏洞的检测能	前缀	五百: ~	
检测增强	Cgi: 开启后可增强部分漏洞的检测能	前缀 訪 返回上一步	元配 >	
检测增强	Cgi:	前缀 汤 週上一步		
检测增强	Cgi:	助 減回上→步]表 49 插桩类项目	ब्ब ∨ ^{完成} 및満 高级设置−主动 IAST	
检测增强	Cgi: 开启后可增强部分漏洞的检测能	龄 逾上→⊅]表 49 插桩类项目	ஊ ŝ成 高级设置−主动 IAST	
检测管强 检测增强	Cgi:	前缀 新 這回上一步]表 49 插桩类项目 则能力	ஊ ^{第成} 高级设置−主动 IAST	
检测增强 检测增强 8口令漏洞类型	Cgi:	前缀 該D 減回上→步]表 49 插桩类项目 则能力	≅ ♥ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	
检测增强 检测增强 B口令漏洞类型	Cgi:	前缀 あ 減回上→步]表 49 插桩类项目 ^{则能力}	End	
检测增强 检测增强 引口令漏洞类型	Cgi:	im級 image: image: im	[□] 配 [●] 成 高级设置-主动 IAST ○ MongoDB弱口令漏洞 ○ Tomcat弱口令漏洞 ○ HTIP 401111元8日○◇■第	3
检测增强 检测增强	Cgi:	前缀 該功 返回上─步 【表 49 插桩类项目 则能力	E IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	
检测增强 检测增强 B口令漏洞类型	Cgi:	前缀 适功 這回上─步 見表 49 插桩类项目 则能力	空配 学成 取消 高级设置-主动 IAST MongoDB弱口令漏洞 Tomcat弱口令漏洞 HTTP 401以证弱口令漏洞 MSSQLServer弱口令漏洞 MSSQLServer弱口令漏洞 Memcached弱口令漏洞	9
检测增强 检测增强 引口令漏洞类型	Cgi:	im級 image: image: im	² 配	
检测增强 检测增强 8口令漏洞类型	Cgi:	前照 透回上→⊅ 別表 49 插桩类项目 则能力	空配 学成 取満 高级设置-主动 IAST MongoDB弱口令漏洞 Tomcat弱口令漏洞 HTTP 401认证弱口令漏洞 MSSQLServer弱口令漏洞 Memcached弱口令漏洞 SNMP末授权访问漏洞 PostgreSQL弱口令漏洞	
检測増強 检測増強 周口令漏洞类型	Cgi:	前照 透印上—步 「 「 表 49 插桩类项目 则能力	空配 学成 取満 高级设置-主动 IAST MongoDB弱口令漏洞 Tomcat弱口令漏洞 HTTP 401认证弱口令漏洞 MSSQLServer弱口令漏洞 SNMP未授权访问漏洞 PostgreSQL弱口令漏洞 Oracle弱口令漏洞	
检测增强 检测增强 调口令漏洞类型	Cgi:	前梁 新 》 》 》 》 》 》 》 》 》 》 》 》 》 》 》 》 》 》	ERE × 家演 高级设置-主动 IAST MongoDB弱口令漏洞 Tomcat弱口令漏洞 HTTP 401认证弱口令漏洞 MSSQLServer弱口令漏洞 MSSQLServer弱口令漏洞 SNMP未授权访问漏洞 PostgreSQL弱口令漏洞 Oracle弱口令漏洞 Telnet弱口令漏洞	
检测增强 检测增强 弱口令漏洞类型	Cgi: 开启后可增强部分漏洞的检测部 第 开启后可增强部分漏洞的检测部 2 全部 MySQL弱口令漏洞 LDAP弱口令漏洞 LDAP弱口令漏洞 SSH硯口令漏洞 SKH硯口令漏洞 SMB锅口令漏洞 FTP弱口令漏洞 BZ弱口令漏洞 DB2弱口令漏洞 RDP弱口令漏洞 即時明勾dmin弱口令	imæ imæ imæ imæ imæ imæ imæ imæ	空配 学成 取満 高级设置-主动 IAST MongoDB弱口令漏洞 「Tomcat弱口令漏洞 HTTP 401认证弱口令漏洞 MSSQLServer弱口令漏洞 Memcached弱口令漏洞 SNMP未授权访问漏洞 PostgreSQL弱口令漏洞 Cracle弱口令漏洞 Telnet弱口令漏洞 Smtp弱口令漏洞 Smtp弱口令漏洞	



图表 50 插桩类项目高级设置-检测增强

- ▶ 项目高级配置:检测漏洞类型选择、主动 IAST 配置两部分组成。
 - 1) 消息通知:开启消息通知按钮后,需选择推送内容的风险类别,风险包括全部风险、

杭州默安科技有限公司

低危及以上风险、中危及以上风险、高危风险。编辑 WebHook 和邮箱地址, webhook 可以选择此项目需要推送的 webhook 地址;

- 2) 漏洞展示规则:开启漏洞展示规则按钮后,需填写漏洞地址黑名单,编辑相同因素 对漏洞去重条件进行选择,去重条件包括漏洞类型、Host、漏洞 URL、自定义 header 参数。编辑漏洞处理对相同因素漏洞处理方式进行选择,处理方式包括聚合、丢弃、 误报和忽略;
- 3)漏洞修复识别:用于被动检测时识别漏洞是否已经被修复,开启后若漏洞已修复,则将未修复状态变更为已修复,但该功能可能存在误报。仅项目语言选择为 java 时才展示此开关。选择 Golang、.NET Framework、.NET Core、Node.js、Python、 PHP 时没有此开关;
- 4) 主动验证:用于辅助插桩模式的漏洞验证,开启后可自动对漏洞进行主动验证,并 提供验证结果,详见漏洞列表-主动验证列及漏洞详情-判断依据 Tab 页。仅项目语 言选择为 java 时才展示此开关。选择 Golang、.NET Framework、.NET Core、Node. js、 Python、PHP 时没有此开关;
- 5) 主动扫描:此功能只有项目语言选择 Java 时才展示,选择 Golang、.NET Framework、.NET Core、Node.js、Python、PHP 时无此功能。在项目管理-->新建 插桩模式项目-->项目高级设置中选择是否开启主动扫描开关并对主动 IAST 进行配 置,勾选主动扫描后,选择待检测的漏洞类型、检测方式、最大扫描并发数、每分 钟发包数以及检测黑名单,完成主动 IAST 补充测试配置。
- 检测增强:此功能开启后,会增加对部分服务的弱口令漏洞检测的功能,可以按需选择需要支持的服务。

点击项目列表里面需要查看的项目,会跳转到该项目的详情页面,页面中显示该项目的 基础信息、项目统计、第三方库及该项目的漏洞列表。

1.6.4基础信息

1.6.4.1 扫描类

展示当前项目的基础信息,其中可看到项目名称、项目模式、项目归属人、项目成员、 项目模板、测试人员数、请求数(待检测数)、漏洞数(未修复数)、项目地址、创建时间、 用户凭证状态、项目描述、项目安全系数及安全等级,并且可对项目进行录入/检测的控制, 进行逻辑漏洞检测和用户凭证替换等操作。

- 注:安全系数为百分制,数值越低对应的安全等级越危险:0[~]60 分高危,61[~]90 中危,91[~]99 低危,100 分时暂无风险。
- 用户可对该项目进行编辑、删除、输出报告、回归操作、检测逻辑漏洞、用户凭证替换 等操作。

当前位置:应用管理: iastrange-20211	 > 项目列表 > 项目详情 227231129 非签权代理模式 				
0 安全系数	去重请求数:105 9 0 00 检测中 已检测 符检测	项目地址: 请求数: 测试人员数: 创建日期:	192.168.30.68:31180 99 0 2021-12-27 23:10:51	项目描述: -	項目控制
高危	漏洞数: 72 72 0 末修复 已修复	项目归属人: 项目成员: 项目模板: 用户凭证状态:	cheniu 无 无 无法获取 (未设置过期页面请前往设置)		
			用户凭证替换	逻辑漏洞检测中 回归源	1试 × 编辑 删除 输出报告

图表 51 基础信息

点击"编辑",可对项目信息进行编辑,如果项目为自由配置,可以修改所有配置项, 如项目名称、新增项目地址、设置黑名单、选择检测方式、开关 cookie 保持、调整扫 描速度、编辑项目成员、修改邮件通知、进行漏洞类型配置或自定义配置等;如果为使 用模板创建的项目,只能修改部分项,如项目名称、项目成员、邮件通知、检测方式、 最大扫描速度、检测黑名单、用户认证凭据、过期特征、参数黑名单、登入登出特征、 请求地址重定向(用于需要扫描的应用的 IP 地址发生变更,同时希望复用已录入的请 求的情况)等。如果需要修改应用的关联关系,也在此处修改。

1 选择检测模式		2 项目基本设置	调高级设置
1.选择检测模式			
*项目名称	鉴权代理模式		
关联应用名称 🥝	非插桩应用 ∨		
项目类型	 ● 插桩模式 ● 流量信使模式 ● 非鉴权代理模式 ◎ 流量镜像模式 	 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
自动爬取	□ 勾选后项目创建完成自动开始爬取所有项目地址		
鉴权代理模式介绍			
适用 适用场景 项目	于 http/https 协议数据传输的 web 项目 人员能够自主配置浏览器代理 不存在或者少数功能存在防重放机制		
能够 	对https进行劫持,还原明文请求包进行安全测试 试逻辑漏洞 录入需要进行代理鉴权,测试者需分配last系统账号		
测过 注意事项 助中 请将	人员需配置代理,代理服务器地址为192.168.120.62, 心】【浏览器插件】查看 登入,登出等接口加入'项目高级设置'的黑名单中	端口为9000,详细配置前往【帮助中心】	【代理配置】查看,或下载安装浏览器插件,详细配置前往【幣

图表 52 编辑项目

 若用户凭证状态显示为过期,点击"用户凭证替换",可对失效的用户凭证进行替换, 根据雳鉴提示的用户名对用户凭证进行替换。

用户凭据替换					
HOST: baidu.com					
角色: 未识别用户					
凭据位置	字段名称	字段值			
HTTP header	Cookie				
				替换	取消
					ETT AP

图表 53 用户凭证替换

- 点击项目控制下"允许录入"控制按钮,停止该项目下所有请求的录入,且录入状态变为已停止。
- 点击"录入暂停中"控制按钮,开启该项目的请求录入。
- 点击项目控制下"允许检测"控制按钮,停止该项目下漏洞检测。
- 点击"检测暂停中"控制按钮,开启项目的漏洞检测。
- 点击"删除",弹出二次确认提示框,点击"确定"后该项目即被删除,对应漏洞关联 删除。

点击"输出报告",输入报告名称,选择日期区间。点击"确定"后,页面跳转至报告
 管理页面(详见当前文档 3.6 报告管理)。

输出报告		
项目名称:	benchmark_211	
报告名称:		
报告维度:?	漏洞类型	\vee
报告日期: 🥐	2022-01-05 - 2022-01-11	
	确定取消	

图表 54 输出报告

 点击"回归操作",可选择对全部请求重新测试、对出错请求重新测试及对所有漏洞重 新测试,弹出二次确认框,点击确定后,即可对相应请求进行回归操作。

回归测试 >	编辑 删除
全部请求重新测试	
出错请求重新测试	
所有漏洞重新测试	● 混洞数 ● 戸
	回归测试 > 全部请求重新测试 出错请求重新测试 所有漏洞重新测试

图表 55 回归操作

1.6.4.2 插桩类

展示当前项目的基础信息,其中可看到项目名称、项目模式、项目归属人、项目成员、 项目模板、项目语言、请求数、漏洞数(未修复数)、创建时间、项目描述、项目安全系数 及安全等级,并且可对项目进行检测控制、输出报告等操作。

- 注:安全系数为百分制,数值越低对应的安全等级越危险:0[~]60分高危,61[~]90中危,91[~]99低危,100分时暂无风险。
- ▶ 用户可对该项目进行编辑、删除、输出报告等操作。

当前位置: 应用管理 > benchmark_211	· 项目列表 > 项目详情 播桩模式				
0 安全系数	0 869 0 检测中 已检测 待检测	测试人员数: 创建日期: 项目归属人: 项目成员:	0 2022-01-05 12:29:14 chenlu 无	项目描述: -	项目控制 项目控制 主动方式暂停中 私动方式检测中
高危 安全等级	通 利数: 869 860 0 未修重 已修变	项目模板: 项目语言:	无 Java		编辑 副除 输出报告

图表 56 插桩类项目基础信息

 点击"编辑",可对项目信息进行编辑,如项目名称,项目语言,项目规则,项目成员, webhook,邮件通知,进行漏洞类型配置或主动扫描配置等。如果需要修改应用的关联 关系,也在此处修改。

		уу Г 🚅 Г 🕞
当前位置: 应用管理 > 项目详情 > 编辑项目 编辑项目		
3 1834年4月2月19日に	2 第日第中设置 级目前联合置	
1.384世初9937 ◆ 張臣名称 关联应用名称 ● 孤臣类型		
加速期に介加 通用語彙 第二日 同語 現 に の に の に の に の に の に の に の に の に の に の に の に の に の に の に の に の に の に の に に の に に の に に の に に の に に の に の に の に の に の に の に の に の に の に の に の に の に の に の の に の に の の に の の に の の に の の に の の に の の の に の の の に の の の に の の の の に の の の に の の の の に の の の の に の の の の の の の の の の の の の	: Java/Golang/NET Framework/NET Core/Node/ja/Python/PHP 语言开放的web/app简目,基于http/http/进行数据符单 基本回题间本整 环转的一种运行器 在20ken,件格动用,验证预导初重或机制 需要用来和显示的和显示。他延行目的计数组成,请求数据也,属用代码行数 比较像在磁泡组织服务器上起要求和更简值的Agent,若非能更,调先用trig [编程Agent] 页面,进行Agent下取印配更	
	К-9 (Х.Я.)	

图表 57 编辑插桩类项目

- 点击项目控制下"主动方式"控制按钮,停止或开启项目的主动检测(默认为开启)此 功能在项目语言为 Java 和 Goalng 时支持,.NET Framework、.NET Core、Node.js 和 Python 无此功能。
- 点击"被动方式"控制按钮,停止或开启项目的被动检测(默认为开启)此功能在项目
 语言为 Java、.NET Framework、.NET Core、Node.js、Python 和 PHP 时支持,Golang
 无此功能。
- 点击"删除",弹出二次确认提示框,点击"确定"后该项目即被删除,对应漏洞关联 删除。
- 点击"输出报告",输入报告名称、及选择日期区间。点击"确定"后,页面跳转至报告管理页面(详见当前文档 3.6 报告管理)。

输出报告		
项目名称:	benchmark_211	
报告名称:		
报告维度:⑦	漏洞类型	\vee
报告日期: 🥐	2022-01-05 - 2022-01-11	
	确定取消	

图表 58 插桩类项目输出报告

1.6.5项目概况

1.6.5.1 扫描类

扫描类项目概况由四部分组成:项目统计、漏洞列表、SITEMAP、扫描动态、爬虫动态组成。

0 安全系数	去重请求数:105 0 296 699 检测中 已检测 符检测	项目地址: 192.168.30.66:31180 请求数: 99 测试人员数: 0 创建日期: 2021-12-27 23:10:51	项目描述: -	项目控制
高危 _{安全等级}	漏洞数: 72 2 未停室 已停室	项目归属人: chenlu 项目成员: 无 项目模板: 无 用户凭证状态: 无法获取 (未设置过期页面 用	<mark>请</mark> 前往设置) 户凭证督换 逻辑漏网检测中 回归游试 ~	」 编辑 副除 输出报告
目鏡计 漏洞列計 星洞等级 電念	k sitemap 扫描动态 爬取动态	潮湖失控分布Top10 単始请求の強いSRPi 文件包括 SQL希前注入 田研祭理定 日始遊漢の	一股销售を設置 30 25 20 15 10 5 5	 ● 黒洞数 ● 已修复 ● 未修

图表 59 非鉴权模式项目概况

杭州默安科技有限公司

▶ 扫描动态:展示了该项目的扫描动态

按时间倒序排列(即最新检测的展示在最前面),动态内容包括检测时间、检测状态、检测的具体 URL、检测的具体漏洞类型、漏洞个数及耗时。

项目统计	漏洞列表	sitemap	扫描动态	爬取动态											
												扫描动态	Q	打包Excel	下载Excel
扫描时间]		扫描动态												
2022-04	-25 11:25:11		开始检查:	ttp://192.168	8.180.57:8071/init	ial/index.cgi?act=r	register 漏洞类型	型:CORS漏洞							
2022-04	-25 11:25:11		结束检测计	ittp://192.168	8.180.57:8071/init	ial/index.cgi?act=r	register 漏洞类型	말: X-XSS-Prot	otection配置	不当, 漏洞个数:0,	, 耗时: 0.01s				
2022-04	-25 11:25:11		开始检查:1	ittp://192.168	8.180.57:8071/init	al/index.cgi?act=r	register 漏洞类型	발:X-XSS-Prot	tection配置	不当					
2022-04	I-25 11:25 <mark>:</mark> 11		结束检测:1	ittp://192.168	8.180.57:8071/init	ial/index.cgi?act=r	register 漏洞类型	발: Content-Se	ecurity-Poli	cy配置不当, 識洞	个数:0, 耗时: 0.	01s			
2022-04	1-25 11:25:11		开始检查:1	ittp://192.168	8.180.57:8071/init	al/index.cgi?act=r	register 漏洞类型	발:Content-Se	ecurity-Polic	:y配置不当					
2022-04	1-25 11:25:11		结束检测:	ittp://192.168	8.180.57:8071/init	ial/index.cgi?act=r	register 漏洞类型	만:参数遍历, 源	漏洞个数:0, 非	眊时: 0.02s					
2022-04	1-25 11:25:11		开始检查计	ittp://192.168	8.180.57:8071/init	ial/index.cgi?act=r	register 漏洞类型	2:参数遍历							
2022-04	1-25 11:25:11		结束检测:	nttp://192.168	8.180.57:8071/init	al/index.cgi?act=r	register 漏洞类型	말: GET/POST?	「混合使用, 漏	调个数:0, 耗时: (0.00s				
2022-04	1-25 11:25:11		开始检查:†	ittp://192.168	8.180.57:8071/init	ial/index.cgi?act=r	register 漏洞类型	말:GET/POST)	混合使用						
2022-04	-25 11:25:11		结束检测计	ittp://192.168	8.180.57:8071/init	ial/index.cgi?act=r	register 漏洞类型	12: 不安全的资	2源加载, 漏洞	同个数:0, 耗时: 0.0	00s				
					共1243条	< 1 2	3 4 5	5 12	25 >	10 条/页 >	跳至	页			

图表 60 扫描动态

支持以 excel 导出,先点击"打包 Excel",等出现的提示框消失后再点击"下载
 Excel",即可将生成的 Excel 文件下载到本地。



图表 61 生成提示框

▶ 项目统计:展示了该项目的统计信息。

- 1) 漏洞等级分布图:统计该项目的漏洞等级及相应比例。
- 2) 漏洞类型分布图:统计该项目数量最多的十个漏洞类型及相应比例。
- 漏洞状态图:展示所有项目高危,中危,低危,提示类漏洞,漏洞数/已修复/未修 复的数量。
- ▶ 漏洞列表:展示该项目下所有漏洞记录,可自定义列表展示项。

漏洞列表默认按检测时间倒序排列(即最新检测的排在最前面),列表可选内容包括漏 洞地址、漏洞类型与等级、漏洞参数、测试人员、最后检测时间、首次发现时间、状态及操 作。

可根据漏洞等级、修复状态、漏洞类型进行查看,根据漏洞地址或测试人员进行搜索,可查看漏洞详情,JIRA及禅道同步情况或进行重新检测,并且可对漏洞进行批量忽略、恢复、分享和同步 JIRA、分享、同步禅道和导出漏洞操作(详见 3.4.3.1)。同时可以对漏洞进行

批量添加备注信息。

項目统计 <mark>議測列表</mark> sitemap 扫描动态 爬取动态			
状态 全部 ・ 等级 全部	▼ 类型 全部 ▼ 开放时长	全部 💌 漏洞地址/	测试人员
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	主动验证: • 未验证 测试人员: Iijxadmin	更新时间:2021-12-2822:56:37 发现时间:2021-12-2822:56:37	查看详情! ——
○ 軟穩页面浸露 未休息 192.168.30.66:31180/phpinfo.php 漏洞参数: -	主动验证: e 验证成功 测试人员: chenlu	更新时间:2021-12-28 19:47:21 发现时间:2021-12-27 23:23:30	查看详情丨检测中
○ 个安全配置 ※考照 192.168.30.66.31180/crossdomain.xml 濿洞参数: -	主动验证: e 验证成功 测试人员: chenlu	更新时间:2021-12-28 19:47:01 发现时间:2021-12-27 23:23:30	查看详情丨检测中
● 目录通历温润 法传觉 192.168.30.66:31180/config 温润参数: -	主动验证: e 验证成功 测试人员: chenlu	更新时间:2021-12-28 10:16:44 发现时间:2021-12-27 23:23:30	查看详情 重新检测
 ◎ 跨站脚本攻击(XSS) 美考室 192.168.30.66:31180/vulnerabilities/xss_r/ 逼词参数: name 	主动验证: • 验证成功 测试人员: chenlu	更新时间:2021-12-28 10:16:34 发现时间:2021-12-28 10:16:34	查看详情 重新检测

图表 62 漏洞列表

SITEMAP 默认按照网站目录结构排序,列表内容包括 URL、测试人员、漏洞数、最后检测时间、检测状态及操作。左侧标红代表此 URL 下无请求录入,标记感叹号代表此目录下请求含漏洞。

在初始页面可查看已知 URL 覆盖度及未覆盖 URL。

可根据检测状态进行查询,根据 ur1 地址进行搜索,可按照检测状态筛选请求,也可筛选有漏洞的请求,对有漏洞的 URL 进行点击查看请求详情及漏洞详情,或进行重新检测操作。

有漏洞的请求						urlitta		Q 导入日志接口
优先级 全部	检测状态	全部						
192.168.110.230	9 »							
D /	0	请求列表		检测状态	漏洞数	最后检测时间	测试人员	操作
🖃 api	0						The second second second	
🖃 auth		中级 192.168.110.230/api/config/v1/info		已检测	1	2022-04-25 14:15:45	dev_sec urity	添加漏洞 重新检测 展开▼
🖭 v1								
🖃 config	0	始而会选 沿 要 代生命						
E v1	0							
🗅 info	0							
🗅 log	0		共1条 <	1 >	10 条/页 >>			
🗅 login	0							

图表 63 扫描类项目 SITEMAP

点击添加漏洞后,提示选择漏洞类型,会在该 sitemap 的请求下添加一个新的漏洞。

0	去重请求数	10	-	项目地址: 清求数:	192.168.11 39	0.230	项目描述: -				项目控制 9 先許服入
安全新数				测试人员数: 创建日期:	添加漏洞						902748288 ()
古存	漏洞数: 7			项目归属人: 项目成员:	• 滴润类型:	1		Q			
安全等度	未施設	0 已候	复	项目模板:		跨站脚本攻击(XSS)					
				用户凭证状		SQL延时注入					
				1		文件上传			逻辑编词检测回归		輪棋 删除 输出报告
	1		diaman hade			命令现行					
项目软件 漏影列表	sitemap	加強制心	IIGHX403425			文(HBB) struts2漏洞					
有蕭何的清求						信息泄露					日本 日
优先级 全部		检测状态	255 •			URL重定向					
192.168.110.230		0 »									
D /		0	请求列表				检测状态	漏洞数	最后检测时间	测试人员	操作
i api i auth i v1		•	(192. 1	68.110.230/ap	pi/config/v1/ii	nto	已检测	1	2022-04-25 14:15:45	dev_sec urity	添加漏洞 重新检测 展开 ▼
Config		0	□ 单页全选	设置优先级							
D log		0					共1条 < 1 >	10条/页			

图表 64 添加漏洞

> 爬虫动态显示当前爬虫状态、爬虫运行日志以及爬虫控制按钮。

页目统计	漏洞列表	sitemap	扫描动态	爬取动态		
开始爬取	爬取状态	:: 爬取完成				
爬取时间	P.	爬取	动态			
						暂无数挑

图表 65 扫描类项目爬虫动态

可点击开始爬取,选择需要爬取的地址、User-Agent、爬取深度、用户凭据,点击开始 执行爬虫。

* HOST			~
User-Agent	Mozilla/5.0 (X11; Li	nux x86_64) Apple	WebKit/537.36 (KHTML, like Gecko) Ubuntu C
爬取深度	6 (深度	取值范围为1-15)	
用户凭据 🍞	凭据位置	字段名称	字段值
	HTTP header	Cookie	

图表 66 扫描类项目爬虫动态-开始爬取

爬虫开始后可以在动态中看到爬虫的动态。

项目统计	漏洞列表	sitemap	扫描动态	爬取动态
停止爬取	爬取状态	※ 正在爬取		
爬取时间		爬取	动态	
2020-03	-30 15:57:22	开始	爬取,站点ht	ttp://testphp.vulnweb.com
2020-03	-30 15:52:47	开始	爬取,站点ht	ttp://testphp.vulnweb.com
2020-03	-30 15:48:36	爬取	页面http://te	estphp.vulnweb.com/
2020-03	-30 15:48:36	爬取	页面http://19	92.168.120.24:55007/?ms_src_host=testphp.vulnweb.com
2020-03	-30 15:48:36	爬取	完成,站点ht	ttp://testphp.vulnweb.com
2020-03	-30 15:47:23	开始	爬取,站点ht	ttp://testphp.vulnweb.com

图表 67 扫描类项目爬取动态-正在爬取

1.6.5.2 插桩类

插桩类项目概况由六部分组成:项目统计、漏洞列表、sitemap、API发现、第三方库、 Agent 组成,若开启主动扫描模式,则额外新增扫描动态。

播桩模式			
0 检测中 已检测 待检测 漏洞数: 869 26 未停室 已停室	 測试人员数: 0 创建日期: 2022-01-05 12:29:14 项目均属人: chenlu 项目成员: 元 项目模板: 元 项目语言: Java 	项目描述: -	项目控制●
sitemap API发现 第三方库	Agent		編輯 删除 输出报告
	漏洞类型分布Top10	漏洞状态	🔵 漏洞数 🌑 已修复 😑 未修复
- 88.8	NHEiままり海(CSP) 不安生物(cook)e 海皮(日以) 命令执行 日泉穷結	350 300 250 150 150 年現由(XSS)	
	 通転儀式 ① 1 2000 (1000) 1 2000 (1000) 2 2000 (1000)	通知中 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	正確規定 第二人员整:0. 項目描述: - 「「「」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」

图表 68 插桩模式项目概况

- ▶ API 覆盖状态图:统计该项目的 API 已请求与未请求的比例。
- ▶ 漏洞类型分布图:统计该项目数量最多的十个漏洞类型及相应比例。
- ▶ 漏洞状态图:展示所有项目高危,中危,低危,提示类漏洞,漏洞数/未修复的数量。
- ▶ 漏洞列表:展示该项目下所有漏洞记录,可自定义列表展示项。

漏洞列表默认按漏洞类型归类排列,列表可选内容包括漏洞地址、漏洞类型与等级、漏 洞参数、测试人员、最后检测时间、首次发现时间、状态、主动验证结果及操作。

可根据漏洞等级、修复状态、漏洞类型、主动验证状态进行查看,可查看漏洞详情,JIRA 同步情况或进行漏洞验证,并且可对漏洞进行批量忽略、恢复、分享和同步 JIRA、分享、同 步禅道和导出漏洞操作(详见 3.4.3.2)。同时支持对漏洞进行批量添加备注功能。

项目统计 Mitrovity sitemap API发现 第三方库 Agent		
状态 全部 ・ 等級 全部 ・ 発型 全部 ・	主动验证 全部 🔹 开放时长 全部 🔹	漏洞地址/测试人员
○ 不安全的時越配置 已回照 ● 192.168.180.57:8079/ 漏過參数: - 汚点的行: -	主动验证: • 未验证 更新时间: 2022-04 测试人员: zhongbin 发现时间: 2022-04	-25 15:11:54
○ 不安全的JSP校置 已回照 ● 192.168.180.57.8079/ 漏回参数: - 巧应即行: -	主动验证:•未验证 更新时间:2022-04 测试人员:zhongbin 发现时间:2022-04	-25 15:11:53 - 查看评情 展示备注 -25 13:03:16
○ \$\$ \$\$#\$*\$\$\$ \$	主动验证: • 未验证 更新时间: 2022-04 测试人员: zhongbin 发现时间: 2022-04	-25 13:33:01 查看评情 测调验证 -25 13:03:43
● 路钻脚4-玫瑰(XSS) ●===== 192.168.1805.75/8079/taintwebapp/vulns/xss/ 篇詞参数: username 语点组织行:spService0@index_jspjava:188	主动验证: • 未验证 更新时间: 2022-04 测试人员: zhongbin 发现时间: 2022-04	-25 13:33:01 -25 13:03:43 -25 13:03:43
● 除结脚4-较点(XSS) ●==== 192.168.1805.75/8079/taintwebapp/vulns/xss/ 溯詞参数: username 符点组织行: jspService0@index_jspjava.219	主动验证: • 未验证 更新时间: 2022-04 测试人员: zhongbin 发现时间: 2022-04	-25 13:33:01 直侧详情 漏洞验证 -25 13:03:43
○	主动验证: • 未验证 更新时间: 2022-04	-25 13:33:01

图表 69 漏洞列表

▶ SITEMAP 默认按照网站目录结构排序,列表内容包括 URL、测试人员、漏洞数、最后检测

杭州默安科技有限公司

时间、检测状态及操作,标记感叹号代表此目录下请求含漏洞。

可查看当前项目有漏洞的 url 数和总 url 数,可根据 url 地址及 url 参数进行搜索(url 参数搜索不支持搜索 post 中的参数),可筛选有漏洞的请求,对有漏洞的 URL 进行点击查看请求详情及漏洞详情。

项目统计 漏洞列表 sitemap API发现	第三方库 Agent			
 有漏洞的清末 有漏洞的url数/总url数: 2/5 url地址 			● url参数	9入日志接口
□ 192.168.180.57:8079	请求列表	松沢状态 満 調数	最后检测时间 测试人员	操作
annwebapp ·	192.168.180.57:8079/taintwebapp/vulns/xss/	已检测 1	2022-04-25 13:03:43 zhongbi n	添加漏洞│展开▼
xss	192.168.180.57:8079/taintwebapp/vulns/xss/	已检测 1	2022-04-25 13:03:43 zhongbi n	添加漏洞 │ 展开▼
	192.168.180.57:8079/taintwebapp/vulns/xss/	已检测 1	2022-04-25 13:03:43 zhongbi n	添加漏洞 │ 展开 ▼
	192.168.180.57:8079/taintwebapp/vulns/xss/	已检测 1	2022-04-25 13:03:43 zhongbi n	添加漏洞 │ 展开 ▼
	192.168.180.57:8079/taintwebapp/vulns/xss/	待检测 0	- zhongbi n	添加漏洞│展开▼
	192.168.180.57:8079/taintwebapp/vulns/xss/	待检测 0	- zhongbi n	添加漏洞│展开▼
		共 6 条 〈 1 〉 10 条/页 〈		

图表 70 插桩项目 SITEMAP

点击添加漏洞后,提示选择漏洞类型,会在该 sitemap 的请求下添加一个新的漏洞。

ジ 雳 鉴・IAST 器 28 28 28 28 28 28 28 28 28 28 28 28 28		yy + 🚅 + 🖨
当前位置: 应用管理 > 项目列表 > 项目详情		
Linyueqing Line 20 Line Dian exists 20 Line Dian exists 20 Line Dian exists 20 Line Dian exists 20 Line Dian exists		
项目统计 凝闭列表 sitemap Agent 有强同的请求 有遇用的请求 有遇用的如何发行如何数之		
urithte		Curtexx
192.168.32.33:801	廣東列表 192.168.180.56/plkachu/wul/rce/rce ping.php? ・ 已結例	第1月数 最后地流程1月 第1法人员 編作 1 2022-08-31 09-44-36 hyq2 第15回第1 周开 *
Ophrapadmin phprayadmin pikachu index.php index.php index.php	共1条 く 1 >	10 %//2 ~
e vul 🛛 0		

图表 71 添加漏洞

➢ API 发现:展示该项目下 Agent 自动发现的 API 及对应请求情况。此功能仅项目语言为 Java、.NET Framework、.NET Core 和 Python 时支持。

默认按照 API 首字母字典顺序排序,列表内容包括请求方法、API 地址、方法签名、请 求状态、"忽略"操作,标记红色代表此目录下的 API 未请求。支持对请求"批量忽略"和 "批量恢复"。

可查看当前项目 API 覆盖率,可根据 API 地址进行搜索,筛选请求状态,对全部、已请

Tel: (+86) 400-0571-211

Email: market moresec.cn

求、未请求的 API 进行点击查看请求详情。

当某个 API 存在未授权访问漏洞时,会有标记进行展示。

项目统计 漏洞列表 sitemap API发现	第三方库 Agent				
API覆盖率: 0.94% 请求状态: 全部 未请求 已请求 已忽略			AP	地址	Q
 4e6bf391-09a8-3773-8731-d6c26a87bb sanitizer 	请求方法	API地址	方法签名	请求状态	操作
vulns /	GET	/DeserializationServlet	at.dallermassLap.security.taint.webapp.deserialization.DeserializationServlet.doGet(javax.servlet.http://ttpServletResponse)	未请求	忽略
DeserializationServlet Dom4jXML Encryptdata	POST	/DeserializationServlet	at.dallermassl.ap.security.taint.webapp.deserialization.DeserializationServlet.doPost(javax.serv let.http.HttpServletRequest.javax.servlet.http.HttpServletResponse)	未讀求	忽略
 GsonServlet HqlServlet HZbank 	2金选 忽略	恢复			

图表 72 插桩项目 API 发现

第三方库:展示该项目下所有第三方库记录。此功能在项目语言为 Java、golang、node. js 和 Python 时支持,.NET framework、.NET core、PHP 不支持。

第三方库列表默认按检测时间倒序排列(最新发现的第三方库展示在前面),列表内容 包括库名、引用路径、风险等级、当前版本号、最新版本号、开源许可证、最后更新时间及 操作,其中库名可按字典顺序排序,最后更新时间可正逆序排序。

注: 高、中、低危等级的第三方库均有漏洞,具体等级按其 CVE 漏洞的等级与数量而定, 提示等级的第三方库为无漏洞但非最新版本,无风险等级的第三方库为无漏洞且为最新版本。

项目统计 漏洞列表 sitemap API发现 扫描动态 第三方库 Agent							
有漏洞的第三方库 等级 全部 🔹						库名称	Q 导出excel
库名 🗘	引用路径	风险等级	当前版本号	最新版本号	开源许可证	最后更新时间 🗧	操作
xmi-apis	xml-apis-1.0.b2.jar	⑦ 无风险	1.0.b2			2021-08-27 17:26:29	库信息 详情
com.google.code.gson.gson	gson–2.8.5.jar 🛄	◎ 提示	2.8.5	2.8.6	Apache 2.0	2021-08-27 17:26:29	库信息 详情
net.bytebuddy.byte-buddy	byte-buddy-1.8.17.jar	◎ 提示	1.8.17	1.10.18	Apache 2.0	2021-08-27 17:26:29	摩信息 详情
commons-configuration.commons-configuration	commons-configuration-1.10.jar	⑦ 无风险	1.10	1.10	Apache 2.0	2021-08-27 17:26:29	库信息 详情
commons-fileupload.commons-fileupload	commons-fileupload-1.3.2.jar 🛄	高危	1.3.2	1.4	Apache 2.0	2021-08-27 17:26:29	库信息丨详情
antir	antir-2.7.7.jar 🗖	⑦ 无风险	2.7.7	—	-	2021-08-27 17:26:29	库信息 详慎
batik-css	batik-css-1.8.jar 📃	⑦ 无风险	1.8		1	2021-08-27 17:26:28	库信息丨详情
oom.fasterxml.jackson.core.jackson-databind	jackson-databind-2.9.7.jar	● 高危	2.9.7	2.12.0-rc2	Apache 2.0	2021-08-27 17:26:10	库信息 详情
commons-lang.commons-lang	commons-lang-2.4.jar	() 提示	2.4	2.6	Apache 2.0	2021-08-27 17:26:48	厚信息 详情
org.beanshell.bsh-core	bsh-core-2.0b4.jar	⑦ 无风险	2.0b4			2021-08-27 17:26:29	厚信息丨详情

图表 73 项目第三方库列表

可对第三方库进行忽略和恢复操作,忽略后的第三方库可查看忽略原因且不展示在报告上。

项目统计 瀛洞列表 sitemap API发现 扫描动态 第三方库 Agent	操作成功1						
◎ 有瀛洞的第三方库 等级 全部 •						库名称	Q 导出excel
库名 🗘	引用路径	风险等级	当前版本号	最新版本号	开源许可证	最后更新时间 🗘	操作
ml-apis	xml-apis-1.0.b2.jar	() 无风险	1.0.b2		-	2021-08-27 17:26:29	库信息丨详情
com.google.code.gson.gson	gson-2.8.5.jar 🔤	0 提示	2.8.5	2.8.6	Apache 2.0	2021-08-27 17:26:29	库信息丨详情
net.bytebuddy.byte-buddy	byte-buddy-1.8.17.jar 🗮	() 提示	1.8.17	1.10.18	Apache 2.0	2021-08-27 17:26:29	库信息丨详情
commons-configuration.commons-configuration	commons-configuration-1.10.jar	() 无风险	1.10	1.10	Apache 2.0	2021-08-27 17:26:29	库信息 详情
commons-frieupload.commons-frieupload	commons-fileupload-1.3.2.jar	() 高危	1.3.2	1.4	Apache 2.0	2021-08-27 17:26:29	库信息丨详情
antir	antir-2.7.7.jar	② 无风险	2.7.7		_	2021-08-27 17:26:29	库信息丨详情
batik-css	batik-css-1.8.jar 📃	⑦ 无风险	1.8		_	2021-08-27 17:26:28	库信息丨详情丨收回原因
操作人:admin 忽略原因:test							
com.fasterxml.jackson.core.jackson-databind	jackson-databind-2.9.7.jar 🔲	③ 高危	2.9.7	2.12.0-rc2	Apache 2.0	2021-08-27 17:26:10	库信息(详情
commons-lang.commons-lang	commons-lang-2.4.jar	() 提示	2.4	2.6	Apache 2.0	2021-08-27 17:26:48	库信息 详情
org.beansheil.bsh-core	bsh-core-2.0b4.jar	⑦ 无风险	2.064			2021-08-27 17:26:29	库信息 详情
○ 单页全选 ② 全选 ⑧ 幣 俠 复							

图表 74 项目第三方库忽略

可根据第三方库风险等级、第三方库是否有漏洞进行查看,可查看第三方库信息和第三 方库详情,可导出第三方库报告。

查看第三方库信息:点击操作-库信息,出现新页面,新页面为 maven 上该第三方库的页面,可以查看更多该第三方库的信息,还可以下载最新版本的第三方库。

ASPOSITOR I		Ŀ	Search for groups, artifacts, categories		Search	h	Categories Popular Contact
i Artifacts (13.4M)	Home »	org.springfram	ework » spring-webmvc				Ad closed by Google
/		Spring W	eb MVC				Stop seeing this ad
	spring	Spring Web M	IVC				Crop booming time to
/							Why this ad? ⊳
2019	License		Apache 2.0				
	Categor	ies	Web Frameworks				
Categories	Tags		spring mvc web framework				
riented	Used By	<i>.</i>	3,150 artifacts				
ameworks							
on Metrics	Central	(152) Atlassi	an 3rd-P Old (1) Spring Plugins (45) Spring Lib	M (1) Spring Milestones (2)	Geomajas (1)	Alfresco (7)	
ols	Cambrid	dge (1)					1
a Libraries			Version	Repository	Usages	Date	
nd Line Parsers		5.1.4.RELEASE		Central	16	Jan, 2019	
nd Line Parsers		5.1.4.RELEASE		Central	16 370	Jan, 2019 Nov, 2018	
nd Line Parsers nplementations imputing alvzers	5.1.x	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE		Central	16 370 35	Jan, 2019 Nov, 2018 Oct. 2018	
nd Line Parsers nplementations imputing alyzers ns	5.1.x	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE		Central Central Central	16 370 35 353	Jan, 2019 Nov, 2018 Oct, 2018	
nd Line Parsers mplementations omputing alyzers ns ation Libraries	5.1.×	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE 5.1.1.RELEASE		Central Central Central Central	16 370 35 353 27	Jan, 2019 Nov, 2018 Oct, 2018 Oct, 2018	
nd Line Parsers mplementations imputing alyzers ns ation Libraries ities	5.1.×	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE 5.1.1.RELEASE 5.1.0.RELEASE		Central Central Central Central	16 370 35 353 27	Jan, 2019 Nov, 2018 Oct, 2018 Oct, 2018 Sep, 2018	
nd Line Parsers nplementations ymputing alyzers ns ation Libraries ities I Time Utilities	5.1.×	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE 5.1.1.RELEASE 5.1.0.RELEASE 5.0.12.RELEASE	E E E E E	Central Central Central Central Central Central	16 370 35 353 27 24	Jan, 2019 Nov, 2018 Oct, 2018 Oct, 2018 Sep, 2018 Jan, 2019	
nd Line Parsers mplementations mputing alyzers ns ation Libraries litites i Time Utilities ncy Injection	5.1.x	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE 5.1.1.RELEASE 5.0.12.RELEASE 5.0.12.RELEAS 5.0.11.RELEAS	8) 8) 8) 8) 10) 10) 10) 10) 10) 10) 10) 10	Central Central Central Central Central Central Central	16 370 35 353 27 24 16	Jan, 2019 Nov, 2018 Oct, 2018 Oct, 2018 Sep, 2018 Jan, 2019 Nov, 2018	
nd Line Parsers mplementations omputing alyzers ns ation Libraries itities 1 Time Utilities ncy Injection rd SQL Databases	5.1.×	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE 5.1.1.RELEASE 5.1.0.RELEASE 5.0.12.RELEAS 5.0.11.RELEAS 5.0.11.RELEAS	E) E E E E E E E E E E E E E	Central Central Central Central Central Central Central	16 370 35 353 27 24 16 31	Jan, 2019 Nov, 2018 Oct, 2018 Oct, 2018 Sep, 2018 Jan, 2019 Nov, 2018 Oct, 2018	
nd Line Parsers mplementations omputing alyzers ns ation Libraries littles d Time Utilities ncy Injection d SQL Databases rsers	5.1.x	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE 5.1.1.RELEASE 5.0.12.RELEASE 5.0.12.RELEASE 5.0.11.RELEASE 5.0.10.RELEASE 5.0.9.RELEASE	8) 8) 9) 9) 9) 9) 9) 9) 9) 9) 9) 9	Central Central Central Central Central Central Central Central Central	16 370 35 353 27 24 16 31 47	Jan, 2019 Nov, 2018 Oct, 2018 Oct, 2018 Sep, 2018 Jan, 2019 Nov, 2018 Oct, 2018 Sep, 2018	
nd Line Parsers mplementations mputting alyzers ation Libraries litites d Time Utilities mry Injection rd SQL Databases rsers ants	5.1.x	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE 5.1.0.RELEASE 5.0.12.RELEASE 5.0.11.RELEASE 5.0.11.RELEASE 5.0.10.RELEASE 5.0.9.RELEASE 5.0.8.RELEASE	8) 8) 8) 9) 9) 90 90 90 9) 1)	Central Central Central Central Central Central Central Central Central Central	16 370 35 353 27 24 16 31 47 335	Jan, 2019 Nov, 2018 Oct, 2018 Oct, 2018 Jan, 2019 Nov, 2018 Oct, 2018 Sep, 2018 Jul, 2018	
nd Line Parsers mplementations omputing alyzers ns ation Libraries lities incy Injection of SQL Databases rsers ants ies	5.1.x	5.1.4.RELEASE 5.1.3.RELEASE 5.1.2.RELEASE 5.1.1.RELEASE 5.1.0.RELEASE 5.0.12.RELEASE 5.0.11.RELEASE 5.0.9.RELEASE 5.0.8.RELEASE 5.0.2.8.LEASE	8) 9) 9) 10) 10) 10) 10) 10) 10) 10) 10	Central Central Central Central Central Central Central Central Central Central	16 370 35 353 27 24 16 31 47 335 66	Jan, 2019 Nov, 2018 Oct, 2018 Oct, 2018 Sep, 2018 Jan, 2019 Nov, 2018 Oct, 2018 Sep, 2018 Jul, 2018 Jun, 2018	Ad closed by Google

图表 75 第三方库信息

查看第三方库详情:点击操作-详情,跳转至第三方库详情页,该页面中可见该第三 方库的风险等级、推荐版本、最新版本、关联项目名称、当前版本号、开源许可证 等自述信息,可知第三方库漏洞的漏洞名称、漏洞等级、公布时间、漏洞描述和参 考链接,可点击页面右侧关联项目名称跳转至该项目的管理页面查看信息。

祖件信息: Java / org.	mybatis.mybatis / 3.4.5						
中危风险等级		 推荐版本	\odot	3.5.6 最新版本	\odot	开源许可证信息 开源许可证: 许可证风险: 使用级权情况:	テレい日 test_gt qwcqw 8/19/test03/lhc
藏洞							
₽	漏洞名称			漏洞等级		公布时间	操作
	CVE-2020-26945			0 中危		2020-10-11	服开▼

图表 76 第三方库详情

2 選河				
编号	漏洞名称	漏洞等级	公布时间	操作
1	CVE-2020-26945	♥ 中危	2020-10-11	收起。
 羅明描述 MyBatis before 3.5.6 misha 参考链接 https://github.com/mybatis https://github.com/mybatis 	ndles desarialization of object streams. //mybatis-3/compare/mybatis-3.5.5mybatis-3.5.8 //mybatis-3/pull/2079			

图表 77 第三方库漏洞详情

- 导出第三方库报告:点击"导出 EXCEL",出现弹框后输入报告名称,选择导出内容后点击"确定",生成的报告可以在报告管理页面下载。
 - 注:选择第三方库信息,导出的内容有库名、风险等级、漏洞数、当前版本号、最 新版本号、开源许可证、引用路径;

选择第三方库漏洞,导出的内容有漏洞名称、漏洞等级、第三方库名、第三方库版本号、公布时间、引用路径。

输出报告	
报告名称:	
内容选择:	 第三方库信息 第三方库漏洞信息
	确定取消

图表 78 生成项目第三方库报告

▶ Agent: 展示该项目规则下的所有 Agent 列表。

Agent 列表默认按插桩 Agent 地址归类排列,列表内容包括名称、key、最近请求时间、 安装时间、项目名称、标签、状态及操作。 可根据 Agent 状态筛选,可根据名称、Agent 地址、key、备注和标签搜索。

状态 全部 运行中	暂停 高线							名称/Agentl地址/KEY/标签 Q
名称	插桩Agent地址	key 🕜	最近请求时间	安装时间 🗘	项目名称	标签	状态	操作
• testservice	192.168.32.40	ff1ff3ff-faf 🔤	2022-07-11 10:56:12	2022-07-11 10:28:11	test_yt_004 🔤	yjf-service	商线	—— 删除 数据同步 详情
• testxxxxxxxxx	192.168.32.40	b7afbd3f-fff 🔤	2022-07-11 14:02:06	2022-07-07 11:38:55	test_yt_004 🔤	yjfhosttttttttt	高线	—— 删除 数据同步 详情
○ 全选 ○ 单页全选	启动 暂停	批量研除						

共2条 < 1 > 10条/页 >

图表 79 项目 Agent 列表

▶ 扫描动态:展示了该项目的扫描动态

按时间倒序排列(即最新检测的展示在最前面),动态内容包括检测时间、检测状态、检测的具体 URL、检测的具体漏洞类型、漏洞个数及耗时。

打包Excel 下载Excel		扫描动态
扫描时间	扫描动态	
2020-08-31 16:00:08	停止检查:http://localhost.8080/taintwebapp//sonServlet, 原因:Options http://localhost.8080/taintwebapp//sonServlet: dial tcp: lookup localhost on 1	27.0.0.1:53: n
2020-08-31 16:00:08	停止检查:http://localhost.8080/taintwebapp/JsonServlet, 原因:Options http://localhost.8080/taintwebapp/JsonServlet: dial tcp: lookup localhost on 1	27.0.0.1:53: n
2020-08-31 16:00:02	结束检测http://192.168.30.77:8080/taintwebapp/vulns/json/ 漏洞关型: 目录遍历漏洞, 漏洞个数:0, 耗射: 1.97s	
2020-08-31 16:00:02	开始检查:http://192.168.30.77-8080/taintwebapp/vulns/json/	
2020-08-31 16:00:02	结束检测http://192.168.30.77-8080/taintwebapp/vulns/json/	
2020-08-31 16:00:02	开始检查:http://192.168.30.77-8080/taintwebapp/vulns/json/	
2020-08-31 16:00:02	结束检测http://192.168.30.77-8080/taintwebapp/vulns/json/ 漏洞狭型:不安全配置, 漏洞个数.1, 耗好: 0.01s	
2020-08-31 16:00:02	开始检查.http://192.168.30.77-8080/taintwebapp/vulns/json/	
2020-08-31 16:00:02	结束检测http://192.168.30.77-8080/taintwebapp/vulns/json/	
2020-08-31 16:00:02	开始检查.http://192.168.30.77-8080/taintwebapp/vulns/json/	

图表 80 主动模式扫描动态

支持以 excel 导出,先点击"打包 Excel",等出现的提示框消失后再点击"下载
 Excel",即可将生成的 Excel 文件下载到本地。

1.6.6逻辑漏洞检测(扫描类)

点击基础信息右侧的逻辑漏洞检测,用户需添加有效登录凭据,为保证准确性,最好添加一个高权限和两个低权限用户,选择 URL 后,即可进行测试。

1051: 192.168.180.105 *1	Q置用户凭据过期特征,请【前代	[设置]			ų¢,
告择测试url					
2 全选					
192.168.180.105/project	/edit/377				
2 192.168.180.105/安全定的	設模板文件.xlsx				
192.168.180.105/api/apj	proveTemplate/stage/add				
3 192.168.180.105/api/dep	partment/users				
192.168.180.105/api/apj	proveTemplate/setting/add				
192.168.180.105/api/app	proveTemplate/setting/info				
2 192.168.180.105/api/apj	proveTemplate/add				
192.168.180.105/api/api	proveMgr/planStage/securityF	ating/detail			
2 192.168.180.105/api/use	er/page				
192.168.180.105/api/rol	e/list				
2 192.168.180.105/api/dep	partment/usersPage				
192.168.180.105/api/dep	partment/info				
	* 35.750	.05 47 TH 46 46			
	E, MURULE MURANNE CAUPA	ILLIANDIN ES			
化据位置	学段名称		字段值		+
TTP header	Cookie				

图表 81 添加用户凭证权限

P10 为最大权限, P1 为最小权限, 角色名则为被测业务网站登录的账户名。

点击"开始检测"即可进行逻辑漏洞检测,检测过程中会展示扫描动态。每一个请求如果检测出错,会展示返回码,便于排查请求过程中发生的错误。点击取消会清楚此次扫描任务, 点击返回会返回至项目详情界面,本次扫描任务会在后台进行。



扫描动态	
扫描时间	目編為さ
2021-10-29 15:08:22	结束检测: http://192.188.30.93.8080/examples/ 編現党型: 预检测, 编译个数-0.011348 s 道田码: 506

图表 82 逻辑漏洞检测中

等检测完毕后便可看到结果,点击确定会清空此次扫描动态,点击返回会暂时返回至项目详 情界面,扫描动态内容仍会保留。

44000 (0400) - (04	## > 世知識明明的中
SWIR	Estat
2021-10-21 16:08:41	線漆地線: Http://192.185.30.558580/with/with 編詞批算: 例地場, 編詞个数.0, 純計: 0.076/154 s 編詞研: 955
2021-10-21 16:08:41	福田和山田: http://112.198.50.058560/samtwabaus/varias/al 福岡県語: 別社画, 南岡小松 0, 同社: 0.018575 5 道田田谷: 581
2021-10-21 16:08:40	総定総計 HTU-//92.198.30.59/950/1wrfwebaou/vwrs/log 運用定型: 研約法, 第時10.18662 s 道田前: 581

图表 83 逻辑漏洞检测完毕

回到项目管理页面即可看到漏洞具体详情

192.188.120.100.81/projects//ist 漏尽步数: -	膨祛人员:wufengjuan	发现时间: 2022-04-25 17:56:24	2019(FFI) 205(F2/3
●ppl能L1考究授(5)69 === == 192,168,12,0.1006/j.api/user/api/namelist 第26,68,12,0.1006/j.api/user/api/namelist 要定券型: - - -	主动验证:- 图述人员:wufengjuan	更新时间:2022-04-2517:56:09 发现时间:2022-04-2517:56:09	亚带洋情 重新检 测
● ppl版日未提校306间 ++==第二 192.168.120.1008//ap/detaill 度段参数: -	主动始证:- 调试人员:wufengluan	更新创词: 2022-04-25 17:55:54 发现时间: 2022-04-25 17:55:54	臺灣洋情(重新检測
● ppl能已未提现206间 ##1第 192.168.120.1008//ap/cover 黨員等数:-	主动绘证: - 贺武人员: wufengjuan	更新创词: 2022-04-25 17:55:39 发现时间: 2022-04-25 17:55:39	查看详情(重新绘测
● pp/IBT未規模KX6问 ###第 192158-130.1008//ep/kek 氣俗參数: -	主动物证:- 常述人员:wufengluan	更新时间: 2022-04-25 17:55:24 发现时间: 2022-04-25 17:55:24	查看详情!重新检测
● ppl能工来提取36间 ###第 1921-58-130.1008//ep/ap/list 度同参数: -	主动物证: - 附近人员:wufengluan	更新时间: 2022-04-25 17:55:09 发现时间: 2022-04-25 17:55:09	查看洋情(重新检测
● papi能已未提取56月 #**5年 1921-561120.1028//ap/index 黨段參数:-	主动触证:- 前述人员:wufengluan	更新时间:2022-04-25 17:53:38 发现时间:2022-04-25 17:53:38	臺灣洋情(重新检测
◆ppi度日未規反政府 →==== 192.168.12.0.10/8//api/user/power/register/info 集府參覧: -	主动给证: - 假试人员:wufengjuan	更新时间:2022-04-2517-53:23 发现时间:2022-04-2517-53:23	查看详情!重新检测
単原全法 会法 保注 修改状态 分享 重新地別 风地河か く 早出満用	共9条 < 1 > 10 象/页 ∨		兄】 🗌 【禅道問步情况】

图表 84 逻辑漏洞展示

1.6.7Sitemap(扫描类)

Sitemap 可清晰的知道该项目下 URL 的目录结构,以便于了解该项目下测试人员的点击 覆盖度,及对应的请求和测试人员,并查看到对应的漏洞,可对请求详情进行一键复制。

左侧列表中标红代表此 URL 下无请求录入,标记感叹号代表此目录下请求含漏洞。

项目统计	漏洞列表	sitemap	扫描动态	爬取动态		
()有黑雨) 优先级	的講求		检测状态	25 ×	unt地址	9、 导入日志接口
192.16	8.180.57:8071			● ≫ Ebauru要重成 <u>95.83%</u> 未搬蓝URL		
				192.168.180.57#071/ < 1 >		

图表 85 Sitemap 列表-URL 覆盖度

C REAL PROPERTY OF					ur	地毯址		- 导入日志
先级 全部 检测状态	全部	•						
192.168.180.57:8071	0 »							
D/	0	请求列表	检测状态	漏洞数	最后检测时间	测试人员	操作	
docs	0							
Introduction.html	•	Proc. 192.168.180.57:8071/docs/introduction.html	日检测	0	2022-04-25 10:51:01	xzm	流加病河「重	新检测丨收起▲
jasper-howto.html	0							
indi-resources-howto.html		请求详情 漏词详情						
security-howto.html		T (docc (introduction html HTTR/1 1						
🗅 setup.html	0	Host: 192.168.180.57:8071						
🗉 examples	0	User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KH	HTML, like Gecko) Chrome/37.0.2062.120 S	afari/537.3	36			
C) fffzzz		Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8						
🗅 index.jsp		Accept-Language: en.*						
index.php		X-Forwarded-For: 127.0.0.1						
🔃 initial								
1 jolokia								
🗉 manager								
i member								
phpmyadmin	1.1							
taintwebapp	•							
tittlesupp								

图表 86 Sitemap 列表-请求详情 1

右侧列表内容包括 URL、测试人员、漏洞数、最后检测时间、检测状态及操作。

可根据优先级和检测状态进行查询,根据 ur1 地址进行搜索,筛选有漏洞的请求,对有漏洞的 URL 进行点击查看请求详情及漏洞详情,或进行重新检测操作。

项目统计 過調列表 sitemap 扫描	动态 感激动	<u>څ</u>					
有混詞的请求					urtitet		◎ 导入日志接口
优先级 全部 检测线	迹 全部						
192,168,180,57:8071	0 %						
D/	0	请求列表	检测状态	漏洞数	最后检测时间	测试人员	操作
docs							
introduction.html	0	中级 192.168.180.57:8071/docs/introduction.html	已检测	0	2022-04-25 10:51:01	xzm	添加漏洞丨重新检测丨展开▼
jasper-howto.html	0						
jndi-resources-howto.html			已检测	1	2022-04-25 10:50:30	xzm	添加週洞 重新检测 展开▼
security-howto.html							
🗅 setup.html	0	单页全选 设置优先级					
🖽 examples	0						
fffzzz			共 2 条 < 1 > 10 条/页 >				
🗅 index.jsp							
🗅 index.php							
🗉 initial							
jolokia							
manager							
member							
phpmyadmin							
taintwebapp	0						
tttttest.jsp							

图表 87 SITEMAP 右侧列表 1

点击添加漏洞后,提示选择漏洞类型,会在该 sitemap 的请求下添加一个新的漏洞。

NUM: OTHER > OFFICE > SERVICE			法加速网	2					
(5) D (11)(11)(12)(12)(12)(12)(12)(12)(12)(12)		项目地址: 19 请求数: 28 刻试人员数: 0 创建日期: 20 项目归重人: fy 项目归重人: 无	+ 東京安臣 92.166.180 605 9 0022-06-31 11:06:06 9f 6	月払脚本攻击(XSS) SQL超射主人 文件上呼 命令所行 文件包含	q				改臣拉 知() ・ スメロート ・ 大田松田 ()
高范	1	项目模板: 无 用户凭证状态: •	6 无法获取 (未设置过期页)	SUUSERING 在意演器 URL重定问		nequena)	(214ARION) []]	3894 ×) [99.16 (B) /0: (A) /0: (B) /0:
Billit 2009 North Editions () (功态	项目模型: 无用户凭证状态: •	e Altra (figelingi	900520周期 信息流器 URL重定向		n-aina)	(BURNICH) (BU	2011 ×] [病紙 () () () () () () () () () () () () () () () () () () () ()
BALT READER	1 1	项目情報: 无用户凭证状态: •	6 无法获取 (未必置过期方)	1900年2月19 信息改進 URL重定向		NPALESSA)	(Jungan) (Br	38914 ×) (明明 開始 明 日の第2000 日の第2000
ВИВІТ ЖИКРИЗ Слима Слима ВИВІТ ЖИКРИЗ Голома БИВІЛО Г. ЖИКРИЗ Голома ВИВІЛО Г. ЖИКРИЗ КОЗА ВИВІЛО Г.	: :2)&: *	項目機能 天用户凭证状态。	5 无法获取 (朱公園过販売3	10000000 (信息注意 URL重定向		HP:stilling)	(THRANK) (B)) (× 1496	an Mai (maa) (maasa a)∧ Eatama Q
	(初志) (初志	項目構成: 元 用产気记状态: •	5 Alata (* Ga ima)	10000000 信息定意 URI重定向	1984/6	AD ¹² ALZANA MARK		villia state	RH (R) (N)55 0.136
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	项目惯数: 天 用户凭证状态: • 192.168.180.57:80	6 光法税款 (未必難以解表) 6079/	10 UTUALING 信息支援 URL重定向	松田水本 ・ 215月	HIPPOLENNA Mirtox 3	③2948年6月1日、 ●55日12月1日 2022-08-31 12:05:58	2 × 3186	18 (18 (18)) (18 (18)) → 13 (18) (18

图表 88 添加漏洞

导入日志接口支持用户将 web 日志导入雳鉴平台的 kafka 接口中, 雳鉴对 web 日志中的 请求进行扫描。使用时按照规定的格式向雳鉴的 kafka 接口导入日志即可。

导入日志接口	
1.kafka 接口为本机IP地址,端口为9092,topic为 sdl 2.数据样例为格式如下: {'host':"192.168.1.81", "client_ip":"", "cgi":"/", "header":'	"", "body":"",
"args":"", "key":"wjQs1gDSG"} 注意: -样例中的各个字段都必须要有的 -如果值为空,可以写空字符串	
-其中key键为校验身份所需要的,每台机器不一样,这里作host: 业务网站 WEB 日志中的记录的HOST client ip:业务网站 WEB 日志中记录的访问者的IP(若没有	直为wjQs1gDSG 有则为空字符串)
cgi:业务网站 WEB 日志中记录的URL路径 header:业务网站接收到请求的header(若没有则为空字 body: 业务网站接收到 POST 请求的body(若没有则为3	符串) 空字符串)
args:业务网站接收到请求的URL带的参数(若没有则为3	2字符串)
· · · · · · · · · · · · · · · · · · ·	

图表 89 导入日志接口

1.6.8Sitemap(插桩类)

Sitemap 可清晰的知道该项目下 URL 的目录结构,以便于了解该项目下测试人员已点击的 URL,及对应的请求和测试人员,并查看到对应的漏洞,可对请求详情进行一键复制。

左侧列表中标记感叹号代表此目录下请求含漏洞,其余目录为测试人员已点击但无漏洞的 URL。

] 有意同的请求 有漂洞的url数/总url数: 23/37					0	url参数	Q	导入日志接口
url地址	Q							
127.0.0.1:8080	0 »	2012-002	2010/01/02/02		I Income Statement Provide Automation			
WebGoat	0	请求列表	检测状态	漏洞数	最后检测时间	测试人员	操作	
WebGoatIntroduction.lesson.lesson XXE.lesson.lesson		127.0.0.1:8080/WebGoat/login	已检测	1	2022-04-26 15:40:03	lijiang	添加漏洞丨收起	•
🗅 login	0							
starture starture welcome.mvc welcome.mvc xxe xxe	0	Edit //wkbod/wcjogi HTTP/1.1 Cookie: jSESSIONID=V/0xAMeZbI38ol8DP/zJy89m_w4QA6wKHK8ts74b morresc-replay-mode: 1 Accept: text/html.application/html +xml.application/xmlcq=0.9.image/avftimage/webp.image/app Connection: texp=Jalee Referen: http://127.00.18808/WebGoat/start.rwc User-Agent Mcollids/0 (Macintoris): Intel Mac OS X 10_15_7) AppleWebKI/S37.36 (jK1TML, like Gec	g,*/*;q=0.8,applica ko) Chrome/100.1	ation/signer 0.4896.127	l-exchange;v=b3;q=0.9 Safari/537.36		-19	2M
		Sec-Fetch-Site: same-origin Sec-Fetch-Dest: document Host: 127.00.18000 Accept-Encoding gaip, deflate, br Sec-Fetch-Mode: navigate sec-ch-ua: Not Afrand'y=e*99, "Chromium'y="100", "Google Chrome'y="100" eec-ch-ua:-noble: ?0 Cache-Conten Afrand'y=e*99, "Chromium'y="100", "Google Chrome'y="100" eec-ch-ua:-noble: ?0 Cache-Conten Arganety=10 Sec-Chau-Pations: navege=0 Upgrade-insecure-Requests: 1 Sec-Chau-Pations: "nacOS" Caes.Satch-Liteer: ?1						Ţ
		Sec-Fetch-Site: same-origin Sec-Fetch-Site: document Host: 127.00.138080 Accept:Encoding gab.pdf sec-ch-ua: Not Adfand/y=*997, "Chromium"y="100", "Google Chrome"y="100" sec-ch-ua: platform" "macOs" sec-ch-ua: platform" "macOs" sec-ch-ua: Platform" "TacOS" 127.00.18800/WeGost//Ogin	已检测	1	2022-04-26 15:40:03	lijiang	添加網路!展开	

图表 90 SITEMAP 列表-请求详情 2

右侧列表内容包括 URL、测试人员、漏洞数、最后检测时间、检测状态及操作。

Email: market_moresec.cn

可查看当前项目有漏洞的 url 数和总 url 数,可根据 url 地址和 url 参数进行搜索 (url 参数不支持搜索 post 中的参数),可筛选有漏洞的请求,对有漏洞的 URL 进行点击查看请求 详情及漏洞详情。

项目统计 遭泻列表 sitemap API发现	第三方库	Agent						
有黨洞的请求 有漏洞的url数/总url数: 23/37						🗿 url∰ğ	R	日本接口 日本接口
url地址	Q							
127.0.0.1:8080	0 »							
E WebGoat	0	请求列表		检测状态	漏洞数	最后检测时间	测试人员	操作
WebGoatIntroduction.lesson.lesson								
XXE.lesson.lesson		127.0.0.1:8080/WebGoat/login		已检测	1	2022-04-26 15:40:03	lijiang	添加週期│展开▼
🗅 login	0			-				The second second
service		127.0.0.1:8080/WebGoat/login		己種調	1	2022-04-26 15:40:03	lijiang	添加織洞Ⅰ農汁▼
🗅 start.mvc								
welcome.mvc			共2条 < 1 > 10条	16/页 ∨				
🗄 xxe	0							
Iocalhost:8080	0							

图表 91 SITEMAP 右侧列表 2

点击添加漏洞后,提示选择漏洞类型,会在该 sitemap 的请求下添加一个新的漏洞。

	E ♪ 00 0 FA @ MANTER MIIIST MEAGENT MEMORIE MITER MEANE			w i 🚅 i 🕞
当前位置: 应用管理 > 项目列表 > 项目详情				
linyueqing 播發概式	添加満洞			
20 10 10 10 10 10 10 10 10 10 10 10 10 10	第二人员数: 0 前端日期: 2022-06-29 如音目編人: 9/92 第二日編人: 9/92	٩		项目拉利 《 就成方式检测中 《
高代 255年8 255年8	34日頃年: 売 36日道帝: PHP XAL55部実在主入 部务論構本の当(SSRF) SQL主入			
项目统计 漏洞列表 sitemap Agent				
有漏洞的请求 有漏洞的url数/总url数: 2/15				
			Q url#数	
192.168.32.33:801 w localhost:80 0	请求列表	检测状态 漏洞	國 最后检测时间 测试人员 操作	
C index.php C login.php	192.168.180.56/pikachu/vul/rce/rce_ping.php?	• 已检测 1	2022-08-31 09:44:36 lyq2 添加陽何	展开▼
pipinyaamin pikachu index.php pikachu		共1.条 < 1 > 10.条/页 >		
vul •				

图表 92 添加漏洞

导入日志接口支持用户将 web 日志导入雳鉴平台的 kafka 接口中, 雳鉴对 web 日志中的 请求进行扫描。使用时按照规定的格式向雳鉴的 kafka 接口导入日志即可。

Tel: (+86) 400-0571-211

Email: market_moresec.cn



图表 93 导入日志接口

1.7 漏洞管理

漏洞列表展示目前用户所有测试项目的情况。由概述和漏洞列表两部分组成。

💋 雳鉴·IAST		 (♠) (♣) (♣)		yy i 🚅 i 🖨
当前位置: 漏洞管理 > 漏洞列表				
既述				
197 项目数	534667 请求政	50 憲法人民	6049 漏问政	6014 未嫁复致
状态 全部	▼ 毎极 全部	 ★ 数型 全部 ★ 項目模式 請認择 	 主助強逆 全部 予約的 	* 全部 • 羅用地拉/項目名称/期試人员 Q
◎ 会话超时设置不当 → ペタ 192.168.32.105:8080/ 運用参数: 45 汚点执行: -			項目名称: java 項目模式: 描述模式 激武人员: fyf	主动验证: * 未验证 更新时间: 2022-09-01 10:15:23 重新详细 編詞验证 发现时间: 2022-08-31 14:04:28
◎ 会话超射设置不当 **** 192.168.32.105:8080/ 週間参数: 45 汚点执行: -			項目名称: 3333 項目儀式: 插班模式 測試人员: xzm	主动检证:+ 检证成功 重新时间:2022-09-0110.15:23 重要作编 画用检证 2930时间: 2022-09-3114-04:28
 ○ 不安全的JSP故置 未均支 192.168.32.105:8080/ 福利参数: - 汚点执行: - 			項目合称: 3333 项目模式: 網破模式 憲試人员: xzm	主动检证: + 检证成功 對新时间: 2022-09-01 10:15:23 重要排斥局 建物检证 2030时间: 2022-09-31 14:04:28
● 不安全的JSP故置 *** 192.168.32.105.8080/ 運得參数: • 汚成执行: -			项目名称:ywk_test 项目模式:通过模式 测试人员:ywk	主动验证:• 未验证 原则时间:2022-09-0110:1523 重新并简 運用验证 2规时间:2022-09-0110:15:23
 ▲ A Y + MA + M = T Y 単页全选 全选 会注 	(修改状态) 重新绘制 分 家	REM# V	10000	(JRA明步御況) [#編明史報況]



1.7.1漏洞列表

用于统计目前用户环境所有项目的漏洞情况,具体包括当前用户管理的项目数、测试请 求数、测试人员数、漏洞数量和未修复的漏洞数等。

概述				
104 项目数	2001694 请求数	14 第武人员	489 通问数	(1) 488 未修复数

含衣 90 扫油尖麻闸列衣隙灶	图表	95 扫描类漏洞列	表概述
-----------------	----	-----------	-----

1.7.1.1 漏洞展示列表及漏洞详情

1.7.1.1.1 扫描类

漏洞列表展示项可自定义配置,默认按漏洞发现时间倒序排列,列表可选内容包括漏洞 地址、漏洞类型与等级、漏洞参数、项目名称、项目模式、测试人员、最后检测时间、首次 发现时间、状态及操作。

可根据漏洞等级、修复状态、漏洞类型、项目模式进行查看,选择漏洞等级后漏洞类型 筛选下拉框内仅出现对应等级漏洞类型,可查看漏洞详情,JIRA 和禅道同步情况或进行 重新检测,并且可对漏洞进行批量忽略、恢复、分享、同步 JIRA、同步禅道、添加备注。

状态 全部 ▼ 等級 全部 ▼ 英型 全部 ▼ 項目機 开始対长 全部 ▼	t [调选择
● 日马穿越 #### 192.168.30.107:9999/taintwebapp/vulns/file-upload/ 源同参数: multipart filename 污点损行: jspService()@index_jsp.java:151	项目会称: test y1_004 主政验证: • 未验证 项目模式: 插钮模式 更称时间: 2022-07-07 17:19:17 查看评情 漏詞验证 测试人员: yutong_test 发现时间: 2022-07-06 19:29:59
○ ◆ 文件上传 〒##第 192.168.30.107.9999/Laintwebapp/vulns/file-upload/ 派陽巻数: multipart filename 污点形行: jspService0@index_jspjava:151	项目名称: test yt_004 主动验证: • 未验证 项目模式: 插纸模式 更新时间: 2022-07-07 17:19:17 查看评情 满时验证 测试人员: yutong_test 发现时间: 2022-07-06 19:29:59
● 日安邦 王三派 192.168.30.107:9999/taintwebapp/vulns/file-upload/ 顺阔察教: multipart filename 污点执行: _jspService()@index_jsp.java:151	项目名称: yǐhosttitttitti关联 主动验证: • 未验证 项目模式: 插扭模式 更新时间: 2022-07-07 17:19:17 查查當評價 調問验证 测试人员: spf 发现时间: 2022-07-06 19:29:59
○ 文件上传 ※※第 192.168.30.107:9999/taintwebapp/vulns/file-upload/ 瓶调参数: multipart filename 污点影响; jspService()@index_jsp.java:151	项目名称: yjfhostttttttt关联 主动验证: • 未验证 项目吸式: 插班模式 更新时间: 2022-07-07 17:19:17 查看評購 調時验证 测试人员: spf 发现时间: 2022-07-06 19:29:59
○ 於蛤蟆本攻击(XSS) / ●===================================	项目名称: test yt_004 主动验证: • 未验证 项目模式: 插机模式 更新时间: 2022-07-07 17:19:08 查看评情 酒時验证 测试人员: yutong_test 发现时间: 2022-07-06 19:29:53
□ ♥ 時始調本:坎抗(XSS)	项目名称: yihosttittittittittit 項目模式: 播紙模式 更新时间: 2022-07-07 17:19:08 宣誓评情 満時論证

图表 96 漏洞列表

- 选择需要添加备注的漏洞,点击备注按钮后,可以对漏洞批量添加备注。添加后的备注
 可以到漏洞详情中编辑或者删除。
- 选择需要修改漏洞状态的漏洞,点击修改状态按钮,可以对漏洞批量修改状态,可以修

改为忽略、误报、已修复、未修复。修改状态时需要填写相关备注信息。被手动修改过 的漏洞,在漏洞名称后会有红色叹号提醒,提示该漏洞已经被人工托管,系统不会自动 修改其状态。

- 选择需要重新检测的漏洞,点击重新检测按钮,可以批量对漏洞进行重新检测。但是只 对勾选的扫描类漏洞生效,插桩类漏洞不会重新检测。
- 点击"分享",当测试人员发现漏洞时,支持批量漏洞分享(一次上限为200个),高效快捷的将该漏洞信息以地址+密码的方式发送至安全人员,可以选择漏洞分享的有效时长为1天、3天、7天、15天、30天,默认为1天。



图表 97 漏洞分享

点击"查看详情",跳转至漏洞详情页,该页面中可见该漏洞的类型、等级、状态等自述信息,可知描述、危害、建议、细节,漏洞代码示例(JAVA/.NET/PHP),对于可通过安全组件修复的漏洞可下载安全组件并查看安全组件的使用方法,并可进行漏洞重新检测,演示及编辑操作。

🎲 雳鉴・IAST 🐰 🗇		w i 🚅 i 🕞				
当前位置: 漏洞管理 > 漏洞列表 > 漏洞详情						
淝闭详情						
低危 未修复 ^{編39948} 編893.5	 編開発生: 軟质可測型値 軟化効果時時: 2022-08-23 15:18:30 取目合称: 3716/036 使用性数式: 活動情報表式 規模構成式: 活動情報表式 規模構成式: 活動情報表式 規模 方f. 方f. 方f. 方f. 方f. 方f. 方f. 方方 点面 点面	(风处河歩 ∨) 重新公司				
判断依据 漏洞描述 修复方案 请求信息 历史动动						
Reference Reference <t< td=""></t<>						
	<i>n</i> .	4				

图表 98 漏洞详情

其中进行漏洞演示时,需单击'展示响应'按钮,右边有两个窗口'响应包'和'验证

杭州默安科技有限公司

结果'。响应包里面内容显示该漏洞页面的请求响应源码;验证结果是以 web 的形式展示漏

洞。如 SQL 延时注入漏洞,单击'验证结果'就会显示相关的数据信息,如图 82 所示。

利斯祝得 濕明描述 修复方案 防束信息 历史动态	
请求包 编纸资文	柳庭43. 检证结果
("code":100,"msg":"内部上下交论理错误")	
	展示地应
ĥ	h.

图表 99 漏洞演示及编辑一

响应包	验证结果	
jQuery1	102079923	3818863606_1562748045630({"q":"linux shezhi","p":false,"g":
[{"type":	"sug","sa":"	s_1","q":"linux 设置ip"},{"type":"sug","sa":"s_2","q":"linux 设置环境
变量"},{"t	type":"sug",	"sa":"s_3","q":"linux 设置终端快捷键"},
{"type":"	sug","sa":"s	_4","q":"linux 设置目录权限"},{"type":"sug","sa":"s_5","q":"linux 设
置网络"},	{"type":"sug	g","sa":"s_6","q":"linux 设置路由命令"},
{"type":"	sug","sa":"s	_7","q":"linux 设置用户密码"},{"type":"sug","sa":"s_8","q":"linux 设
置服务自	启动"},{"typ	e":"sug","sa":"s_9","q":"linux 设置栈大小"},
{"type":"	sug","sa":"s	_10","q":"linux 设置dns地址"}]})

图表 100 SQL 延时注入漏洞演示

进行漏洞编辑时,在页面上单击'编辑请求','编辑请求'内内容与'测试请求'内 默认内容相同,用户可根据需要对其进行编辑。单击'发送请求'按钮后,右边有两个窗口 '响应包'和'验证结果',响应包里面的内容显示该漏洞页面的实时请求响应源码,验证 结果中则是以 web 的形式展示漏洞。

判斷依据 漏洞描述 修复方案 请求组制 历史动态	
请求包. 编程请求	的应也。 验证现来
("code":100,"msg":"内部上下文处理描误")	
	发送掉不
	s // // // // // // // // // // // // //

图表 101 漏洞演示及编辑二

- 点击"重新检测",漏洞对应请求进入检测中,检测完成之后更新漏洞状态及信息。
- 点击"风险同步-同步 JIRA",可将用户选择的漏洞一键同步至 JIRA 平台上,用户需填 写 JIRA 系统的 URL 地址、用户名、密码。

判断依据	漏洞描述	修复方案	请求信息	历史动态
2022· - 漏洞被	-02-15 16:49:: 支首次发现	38		
1 漏洞初	支首次发现			

图表 102 漏洞历史动态

 点击"历史动态",显示出该漏洞不同时间下更新的漏洞状态,包括漏洞的首次发现、 漏洞被复测、漏洞状态的改变(已修复、未修复)、漏洞状态的手动改变(手动调整为 已修复、误报、忽略、恢复)。

* URL	请输入 JIRA 系统地址	
* 用户名	请输入 JIRA 系统用户名	
* 密码	请输入 JIRA 系统用户密码	R

图表 103 同步 JIRA - 填写 JIRA 系统账号信息

◆ 第一次进行同步需要填入对应账号信息后点击"同步配置", 雳鉴会从 JIRA 地址 同步项目和问题类型等信息。页面上方出现提示, 且弹框内实时展现同步进度。

_	auto-test-498 ⊘ JIRA 数据	流重信便模式。 居正在同步中,请稍等	test_it 争	20:2
<u>~</u>	auto-test-356	流量信使模式	test_lt	202 18:5
同步 JIRA	i ș			
* URL	http://192.168.180	.81:8080/		
* 用户名	admin			
* 密码				ø
	○ 正在同:	步中40% 隐藏		

图表 104 同步 JIRA - 同步配置

◆ 同步完成后,弹框内展示所有项目及对应字段信息。

杭州默安科技有限公司

	青,漏洞链接		
(需要权限账号),漏洞分享链接(不需要权限账号,2	4h有效期)		
项目 字段测试	\sim		
问题类型 缺陷	~		
值字段 111	111		
描述 \$description	\$description		
主题 Stype	\$type		
选择用户(单选) 雳鉴项目组 / wudi	雳鉴项目组 / wudi ∨		
select list (级联) select list (级联) 12 / select list	st (级联) 122		

图表 105 同步 JIRA - 弹框

◆ 弹框内默认仅展示项目下的必填字段,用户可点击右上角的"自定义字段"按钮选择非必填字段加入弹框后进行填写。

坦二、可大会的市场) Stupe - Slovel	全部 必选 非必选
靠小,可在子段內填 \$description、\$envir 为漏洞类型、漏洞等 (需要权限账号),	vorupe、siever、 ronment、\$envin 级、项目名称、\$ 漏洞分享链接(7	 数值字段 组选择器(单组) 文本框(单行) 文本框(多行)
项目	字段测试	 环境 标签 版本选择(单一版本选择)
问题类型	缺陷	□ 文本框 (只读) □ URL字段
故值字 段	111	版本选择(多版本选择)
描述	\$description	 组选择器(多组) 单选按钮 复选框 日期选择控件
主题	\$type	
。选择用户(单选)	雳鉴项目组 / wudi ∨	
select list (级联)	select list(级联)12 / select list(级联)122	
	记住本次同步的选	项及填写信息 -08
	确认	取消

图表 106 同步 JIRA - 自定义字段

◆ 在字段填写框内填入特殊字段, 雳鉴在同步漏洞至 JIRA 时会将该字段替换成对应的漏洞信息。如:在某个文本框类型中填入特殊字段 "\$environment", 同步至 JIRA
后会展示为该漏洞的漏洞链接。



图表 107 同步 JIRA - 自定义同步漏洞信息

◆ 弹框下方可选择是否记住本次同步的选项及填写信息,若选择记住,则下次点击"同

步 JIRA"按钮后弹框内会展示上一次本账号进行同步时的选项及填写信息。

	* Select list	(5反映)	select list	(级联) 12/	select lis	t (狘联) 122	
)8/config		🗹 记	住本次同步的	选项及填写	信息		-08
			确认	取消			
					_		

图表 108 同步 JIRA - 记住选项及填写信息

◆ 点击确认后漏洞会同步到用户 JIRA 系统中,可通过点击"查看 JIRA 同步情况复选
 框"查看漏洞是否同步完成,同步完成的漏洞标识为 JIRA 图标。

 ○ XML外部实体注入 未約1 127.0.0.1:8080/taintwebapp/XXEServlet 漏洞参数: - 污点执行: doPost()@XXEServlet.java:42 	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 🔷
● 文件上传 医短 127.0.0.1:8080/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp:31	项目名称:huan-weblogic-jndi测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 🔷
● 単页全选 全选 备注 修改状态 分享 重新检测 共66838条 < 1 2	风险同步 × 3 4 5 ···· 6684 > 10条/页 × 跳	☑ 【JIRA同步情况】 至 页	□ 【禅道同步情况】

图表 109 同步 JIRA - 查看同步情况

- ◆ 用户非第一次进行同步 JIRA 操作,点击"同步 JIRA"按钮会直接展示上次同步配置后的弹框(或上次记住漏洞同步信息的弹框)。
- ◆ 若修改了 JIRA 系统中的用户名密码或项目的配置,可点击弹框上方的"重新同步 配置"按钮,在新出现的弹框中核对信息后点击"同步配置"进行更新。



图表 110 同步 JIRA - 重新同步配置

* URL	http://192.168.180.81:8080/	
* 用户名	admin	
* 密码		

图表 111 同步 JIRA - 重新同步配置弹框

● 点击"查看 JIRA 同步情况",列表右侧展示漏洞是否已同步至 JIRA。展示了 JIRA 图标的表示已同步。

 \$ XML外部实体注入 	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengluan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 🔷
文件上传 未修复 127.0.0.1:8080/taintwebapp/vulns/file-upload/	项目名称:huan–weblogic–jndi测试 项目模式:插桩模式	主动验证: • 未验证 更新时间: 2022–01–12 18:14:44	查看详情 漏洞验证 🔷
漏洞参数: - 污点执行: service()@index.jsp.31 □ 单页全选 全选 备注 修改状态 分 享 重新检测	测试人员:wufengjuan	发现时间:2022-01-12 18:14:44 ✔ 【JIRA同步情况】	□ 【禅道同步情况】
共66838条 < 1 2	3 4 5 ··· 6684 > 10条/页 / j	兆至 页	

图表 112 漏洞列表 - 查看 JIRA 同步情况

点击"风险同步-同步禅道",可将用户选择的漏洞一键同步至禅道平台上,用户需填写
 禅道系统的 URL 地址、用户名、密码。

	nnnnnnn	H
同步禅道		
* URL	请输入禅道系统地址	
	例如:http://192.168.180.100:8081	
* 用户名	tang	
* 密码	••••	Ø
	同步配置取消	
_	坚权代理	

图表 113 同步禅道 - 填写禅道系统账号信息

◆ 第一次进行同步需要填入对应账号信息后点击"同步配置", 雳鉴会从禅道地址同步所属产品和 Bug 标题等信息。页面上方出现提示,且弹框内实时展现同步进度。

	🕑 禅道数据正在同步中	,请稍等	餐秋代理 模式	Pin
	hhhh	hhh	鉴权代理	Pin
同步禅道				
* URL	http://192.168.180.52:8082			
	例如:http://192.168.180.100:8081			
* 用户名	tang			
* 密码	••••			Ø
		四次 井下		
	(〕止在同步甲20%	隐臧		
			收 和半理	

图表 114 同步禅道 - 同步配置

◆ 同步完成后,弹框内展示所有项目及对应字段信息。

			1
	同步禅道 【重新同步]	記置】	◎ 自定义字段
ap			
s	提示:可在字段内填入\$ \$description、\$environ 洞类型、漏洞等级、所fi (需要权限账号),漏》	\$type、\$level、\$project、\$sub nment、\$environment-24h,景 属项目、开发人员、风险状态、》 同分享链接(不需要权限账号,2	mitter、\$status、 §鉴将会自动替换为漏 属洞详情,漏洞链接 24n有效期)
ar	* 所属产品	刃甲	×]
ar	* Bug标题		
	*影响版本		
s		记住本次同步的选项及填写信息	
ab		确认 取消	

图表 115 同步禅道 - 弹框

◆ 弹框内默认仅展示项目下的必填字段,用户可点击右上角的"自定义字段"按钮选择非必填字段加入弹框后进行填写。

Tel: (+86) 400-0571-211

Email: market_moresec.cn

同步禅道 【重新同	同步配置】	③ 自定义字段
		全部
提示:可在字段内均 \$description、\$en 洞类型 漏洞等级	真入\$type、\$level、\$prc vironment、\$environme 所属项目 开发人员	
(需要权限账号),	漏洞分享链接(不需要)	Bug标题颜色 截止日期
		🗌 关键词 📄 操作系统 📄 优先级
* 所属产品	刃甲	一 严重程度 📃 抄送给 🗌 所属模块
* Bug标题		所属项目 重现步骤
		□ 相关需求 □ 相关任务
* 於响版平		当前指派 ✓ 所属产品
	ᠵ 记住本次同步的选项	✓ Bug标题 ✓ 影响版本
	确认	//3 in_h _11

图表 116 同步禅道 - 自定义字段

◆ 在字段填写框内填入特殊字段, 雳鉴在同步漏洞至禅道时会将该字段替换成对应的 漏洞信息。如: 在某个文本框类型中填入特殊字段"\$environment", 同步至禅道 后会展示为该漏洞的漏洞链接。

bar	同步禅道	【重新同步配置】	② 自定义字段
S	提示:可在	字段内填入\$type、\$level、\$project、\$submitte	ter、\$status、
	\$descriptic	m、\$environment、\$environment–24h,雳鉴将	将会自动替换为漏
	洞类型、漏	洞等级、所属项目、开发人员、风险状态、漏洞前	详情,漏洞链接
	(需要权限	账号),漏洞分享链接(不需要权限账号,24h存	有效期)

图表 117 同步禅道 - 自定义同步漏洞信息

◆ 弹框下方可选择是否记住本次同步的选项及填写信息,若选择记住,则下次点击"同

步禅道"按钮后弹框内会展示上一次本账号进行同步时的选项及填写信息。

3	记住本次同步的选项及填写信息
b	确认取消

图表 118 同步禅道 - 记住选项及填写信息

◆ 点击确认后漏洞会同步到用户禅道系统中,可通过点击"查看禅道同步情况复选框" 查看漏洞是否同步完成,同步完成的漏洞标识禅道图标。

杭州默安科技有限公司

● 目录穿越 深修里 127.0.0.1:8060/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp.31	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: ● 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证
 ◇ XML外部实体注入 ※●更 127.0.0.1:8080/taintwebapp/XXEServlet 週洞参数: - 汚点执行: doPost()@XXEServlet.java.42 	项目名称:huan-jdk16-taintwebapp 项目模式:插纸模式 测试人员:wufengluan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 ⓒ
 ○ 文件上传 法参复 127.0.0.1:8080/taintwebapp/vulns/file-upload/ 溫洞参数: - 污点执行: service()@index.jsp:31 	项目名称:huan-weblogic-jndi测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 😡
 単页全选 全选 备注 修改状态 分享 重新检测 共66638条 < 1 2 	风险同步 ∨ 3 4 5 ··· 6684 > 10 条/页 ∨ 算	UIRA同步情况 至 页	】 🛛 【禅道同步情况】

图表 119 同步禅道 - 查看同步情况

- ◆ 用户非第一次进行同步禅道操作,点击"同步禅道"按钮会直接展示上次同步配置 后的弹框(或上次记住漏洞同步信息的弹框)。
- ◆ 若修改了禅道系统中的用户名密码或项目的配置,可点击弹框上方的"重新同步配置"按钮,在新出现的弹框中核对信息后点击"同步配置"进行更新。

			hhhhhhhh	Ping
	同步禅道	【重新同步配置】		③ 自定义字段
at				
	提示:可在 \$descriptic 洞类型、漏	字段内填入\$type、 on、\$environment 洞等级、所属项目	\$level、\$project、\$submitter、 、\$environment-24h,雳鉴将会自 、开发人员、风险状态、漏洞详情	\$status、 目动替换为漏 漏洞链接
	(需要权限	账号),漏洞分享	链接(不需要权限账号,24h有效期	月)

图表 120 同步禅道 - 重新同步配置

同步禅道		
* URL	请输入禅道系统地址	
	例如: http://192.168.180.100:8081	
* 用户名	tang	
* 密码	••••	Ø
	同步配置取消	

图表 121 同步禅道 - 重新同步配置弹框

 点击"查看禅道同步情况",列表右侧展示漏洞是否已同步至禅道。展示了禅道图标的 表示已同步。

 ● 目录穿越 ● 目录穿越 ● 127.0.0.1:8080/taintwebapp/vulns/file-upload/ ï漏洞參数: 一 污点执行: service()@index.jsp.31 	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022–01–12 18:14:44 发现时间: 2022–01–12 18:14:44	查看详情 漏洞验证
● XML外部实体注入 未9 127.0.0.1:6080/taintwebapp/XXEServlet 漏洞參数: - 污点执行: doPost()@XXEServlet.java:42	项目名称:huan-jdk16-taintwebapp 项目模式: 插纸模式 测试人员: wufengjuan	主动验证:• 未验证 更新时间:2022-01-12 18:14:44 发现时间:2022-01-12 18:14:44	查看详情 漏洞验证 🕞
 ◆ 文件上传 法考复 127.0.0.1:8080/taintwebapp/vulns/file-upload/ 溫洞参数: - 污点执行: service()@index.jsp:31 	项目名称:huan-weblogic-jnd)测试 项目模式:播桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情「漏洞验证 😡
 单页全选 全选 备注 修改状态 分享 重新检测 共66838条 < 1 2 	风险同步 > 3 4 5 ···· 6684 > 10 条/页 > 月	UIRA同步情况 五	】 🕑 【禅道同步情况】

图表 122 漏洞列表 - 查看禅道同步情况

同时选择"JIRA 同步情况"和"禅道同步情况"复选框,可同时查看漏洞同步 JIRA 和
 禅道的情况,列表右侧展示 JIRA 图标和禅道图标表示均已同步。



图表 123 漏洞列表 - 查看 JIRA 和禅道同步情况

1.7.1.1.2 插桩类

漏洞列表展示项可自定义配置,默认按漏洞发现时间倒序排列,列表可选内容包括漏洞 地址、漏洞类型与等级、漏洞参数(可多个)、项目名称、项目模式、测试人员、最后检测 时间、首次发现时间、状态、主动验证及操作。

可根据漏洞等级、修复状态、漏洞类型、项目模式、主动验证进行查看,选择漏洞等级 后漏洞类型筛选下拉框内仅出现对应等级漏洞类型,可查看漏洞详情,JIRA 和禅道同步 情况或进行漏洞验证,并且可对漏洞进行批量忽略、恢复、分享、同步 JIRA、同步禅道、 添加备注。

状态 全部 等级 全部 主动验证 全部 开放时长 全部	 ▼ 类型 全部 ▼ 項目機式 	播桩模式 ▼ 漏洞地址/项目名称/测试人员 Q
● ⑦ 加密發明硬編码 <u>●参集</u> localhost:8080/getinfo 漏洞参数: - 汚点执行: -	項目名称:huan-weblogic-jndi测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-11 15:48:50查看详情 漏洞验证 发现时间: 2022-01-11 14:39:45
① 加密發明硬編码 R01 localhost:8080/getInfo 満調参数: - 汚点执行: -	项目名称:huan-redis 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-11 15:48:50 查看详情 講詞验证 发现时间: 2022-01-11 14:39:45
● 配置文件弱密码 ★## localhost/ 漏洞参数: -	项目名称:huan-weblogic-jndi测试 项目模式:播桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-11 15:48:20查看详情 / 講房验证 发现时间: 2022-01-11 14:23:28
● 配置文件錄密码 ▶世年 localhost/ 漏洞参数: - 汚点执行: -	项目名称:huan-redis 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-11 15:48:20
◎ ② 加密秘钥硬编码 未移業	项目名称: huan-redis	主动验证: • 未验证

图表 124 插桩类漏洞列表

- 选择需要添加备注的漏洞,点击备注按钮后,可以对漏洞批量添加备注。添加后的备注
 可以到漏洞详情中编辑或者删除。
- 选择需要修改漏洞状态的漏洞,点击修改状态按钮,可以对漏洞批量修改状态,可以修 改为忽略、误报、已修复、未修复。修改状态时需要填写相关备注信息。被手动修改过 的漏洞,在漏洞名称后会有红色叹号提醒,提示该漏洞已经被人工托管,系统不会自动 修改其状态。
- 选择需要重新检测的漏洞,点击重新检测按钮,可以批量对漏洞进行重新检测。但是只 对勾选的扫描类漏洞生效,插桩类漏洞不会重新检测。
- 点击"分享",当测试人员发现漏洞时,支持批量漏洞分享(一次上限为200个),高效快捷的将该漏洞信息以地址+密码的方式发送至安全人员,可以选择漏洞分享的有效时长为1天、3天、7天、15天、30天,默认为1天。

Tel: (+86) 400-0571-211

Email: market moresec.cn

				<u>>→- == /</u>	
	分享漏洞				n
ain	分享地址				n
ain	提取密码				
					n
	有效时长	1天	^	生成链接并复制	- 1
ain		1天			n
		3天			
		7天		+=1>1++-+	
ain	twebapp	15天		抽性楔式	admin
		30天			
in	twohann		lvi11	乐粒档式	admin

图表 125 插桩类漏洞分享

- 点击"查看详情",跳转至漏洞概述页,该页面中可见该漏洞的类型、等级、状态等自述信息,可知描述、危害、建议、细节,漏洞代码示例(JAVA/.NET/PHP),对于可通过安全组件修复的漏洞可下载安全组件并查看安全组件的使用方法,可进行请求展示和编辑,并可查看详细数据流。
 - 在判断依据中可查看漏洞的代码片段、主动验证结果(仅针对开启了主动验证功能的漏洞)以及 Payload(仅针对开启了主动方式功能检测出的漏洞)。

🎷 雳 鉴・IAST 器 🗇 😑 🛆 ด 🗢 💷 民 @ 🗄	уу Т 🚅 Т 🕞
当 时位置 : 氟肟挖理 > 氟肟泮物	
现用许纳	
中信 未修复 項目名称: taintwebapp-20220830120955 豊富性調明得: 2022-08-30 12:10:56	
· 해외가신: 해외가신: 해외 · · · · · · · · · · · · · · · · · ·	ctionheader.jsp?type=0
题就人员: chenlu 开做时候: 0天	
	风险同步 >
▶ 第11 (1) (1) (1) (1) (1) (1) (1) (1) (1) (
🔕 मार्कारताव	
存在个人類結婚間差漏间检查讓非URL为127.0.0.18080/taintwebapp/vulns/providers/xxsprotectionheader/sp. 匹配影手起放燃/限報处谱的个人類結婚類: 127***0.10P) 建数据保存在地址中 经检测,该漏漏的存在地址反了(漏用数器保护条例(GDPR) 》和(支付卡行业数据安全标准(PCI DSS))标准。	
● 主动始征	
● 未始证	

图表 126 插桩类漏洞概述

杭州默安科技有限公司

其中进行漏洞验证时,在页面上单击'编辑请求','编辑请求'内内容与'测试请求'内默认内容相同,用户可根据需要对其进行编辑。单击'发送请求'按钮后, 右边有两个窗口'响应包'和'验证结果',响应包里面的内容显示该漏洞页面的 实时请求响应源码,验证结果中则是以 web 的形式展示漏洞。

科斯结婚 展彩面线 修理方案 或外所能 数据后期单 历史为态	
Image:	wide Boden
User-Agent PostmenRenerge 728.4 Foot localhostd000 connections of the second second second second second second connections coache	REEL
accepteronoding: gaip, deflate accepte 1° ('studentName'i'den1', 'studentNape''17')	
	h h

图表 127 漏洞演示及编辑二

在数据流信息中可查看漏洞的详细数据流(包括 TagRange)及栈调用等信息。在调用栈信息展示时,可以选择默认、所有堆栈、用户堆栈三种显示模式。用户代码的 堆栈会标红展示,以便于区分。

默认:展示前10条堆栈

所有堆栈: 展示所有堆栈信息

用户堆栈:展示用户代码的堆栈信息

利斯依据 潮南部	★ 修复方案 案次图表 数据14GB 历史动态	
🕗 污点疏入		
执行函数: 代码位置: 漏洞参数:	janalang String org papehe astalina.comeetos/Request/acade.get/Barameter(janalang.String) authors/Lany Niven	願开▼
60 #00511533		
执行函数: 代码位置: 漏洞参数:	boolean janalang String equals(janalang Clojet) Lany Nien	周开▼
🔵 海点傳播		
执行函数: 代码位置: 漏洞参数:	janalang SeringBuilder janalang SeringBuilder appendijanalang Sering) //Bookfauthorn"Lany Ninen	服开业
🔵 法应终播		
执行函数: 代码位置: 漏洞参数:	janalang Saring janalang Saring BuildentoSaring) //Bookfauthor="Lany Niem"}bildentoS	願幵▼
🛞 清点执行		
执行函数: 代码位置: 漏洞參数:	janaxumi.xparti.XPartiEspression org.apache.sparti.jap.XPartimpi.compiler.jap.alang.txing) //book(authors"Lany Mixeel/Mikel/hest)	展开▼
☆ 該論认漏洞存在		

图表 128 插桩模式漏洞详情-数据流信息

 点击"历史动态",显示出该漏洞不同时间下更新的漏洞状态,包括漏洞的首次发现、 漏洞再次上报、漏洞状态的改变(已修复、未修复、验证成功、验证异常、存在过滤)、 漏洞状态的手动改变(手动调整为已修复、误报、忽略、恢复)。

判断依据	漏洞描述	修复方案	清求信息	数据流信息	历史动态
2022 • 未验i	2-03-17 10:10: Œ	19			
2022 漏洞ī	2-03-17 02:39: 再次上报	24			
2022 潇河	2-03-17 02:35: 被首次发现	30			

图表 129 插桩模式漏洞详情-历史动态

 点击"Agent",显示出该漏洞关联的 Agent 列表,包含 Agent 名称、插桩 Agent 地址、 key、标签、状态和操作(查看详情)。

判断依据 漏洞描述	修复方案 请求信息 数据流信息	历史动态 Agent			
Agent密称	播桩Agent地址	key 🥥	标签	状态	攝作
—	10.244.0.188	713a6aa1-1b7d-31e7-b66b-fbb8401d07e9	taintwebapp_docker	 已暫停 	详情
		共1条 < 1 > 10条/页 <			

图表 130 插桩模式漏洞详情-Agent

点击"风险同步-同步 JIRA",可将用户选择的漏洞一键同步至 JIRA 平台上,用户需填写 JIRA 系统的 URL 地址、用户名、密码。

* URL	请输入 JIRA 系统地址	
* 用户名	请输入 JIRA 系统用户名	
* 密码	请输入 JIRA 系统用户密码	Ø

图表 131 同步 JIRA - 填写 JIRA 系统账号信息

◆ 第一次进行同步需要填入对应账号信息后点击"同步配置", 雳鉴会从 JIRA 地址 同步项目和问题类型等信息。页面上方出现提示,且弹框内实时展现同步进度。

-	auto-test-356	流量信使模式	test_lt	202
同步 JIRA	ñ			10
* URL	http://192.168.180	.81:8080/		
* 用户名	admin			
* 密码				Ø
		bcbx0% 降荷		

图表 132 同步 JIRA - 同步配置

◆ 同步完成后,弹框内展示所有项目及对应字段信息。

\$description、\$envi 为漏洞类型、漏洞等 (需要权限账号),	ACSTOPE、Stever、Sproject、Stester ronment、Senvironment-24h,需 级、项目名称、测试人员、漏洞详 漏洞分字链接(不需要权限账号,)	智、 整将会自动替换 情,漏洞链接 24h有效期)
项目	字段测试	~
• 问题类型	缺陷	~
数值字段	111	
* 描述	\$description	
* 主题	\$type	
∗选择用户(单选)	雳鉴项目组 / wudi	\sim
	(47 E) (2	(纪开) 122

图表 133 同步 JIRA - 弹框

◆ 弹框内默认仅展示项目下的必填字段,用户可点击右上角的"自定义字段"按钮选择非必填字段加入弹框后进行填写。

桿示· 可在字段内描	λ Styles Slavel	全部	必选	非必选
description、\$envir	onment, Senvir	✓ 数值字段	组选择	器 (单组)
为漏洞类型、漏洞等 (需要权限账号),	级、项目名称、3 漏洞分享链接(2	文本框 (身	約 🗌	文本框 (多行)
		环境	标签	
项目	字段测试	版本选择	(单一版本选持	圣)
问题类型	缺陷	文本框 (5	マ读) 🗌 し	JRL字段
值字段	111	版本选择	(多版本选择)	
		组选择器	(多组)	单选按钮
描述	\$description	复选框	日期选择	控件
主题	\$type			-00
选择用户(单选)	雳鉴项目组/	wudi		~
select <mark>list</mark> (级联)	select list(级	联)12 / select	list(级联)1.	22
		****		-08
i 🔽	己住本次同步的选	项及填写信息		100
	确认	取消		

图表 134 同步 JIRA - 自定义字段

◆ 在字段填写框内填入特殊字段, 雳鉴在同步漏洞至 JIRA 时会将该字段替换成对应的漏洞信息。如:在某个文本框类型中填入特殊字段 "\$environment", 同步至 JIRA 后会展示为该漏洞的漏洞链接。



图表 135 同步 JIRA - 自定义同步漏洞信息

◆ 弹框下方可选择是否记住本次同步的选项及填写信息,若选择记住,则下次点击"同

步 JIRA" 按钮后弹框内会展示上一次本账号进行同步时的选项及填写信息。

* Select IIS	t(奴昧) select list(级联)12 / select list(级联) 122
)8/config	✔ 记住本次同步的选项及填写信息	-08
	确认 取消	

图表 136 同步 JIRA - 记住选项及填写信息

◆ 点击确认后漏洞会同步到用户 JIRA 系统中,可通过点击"查看 JIRA 同步情况复选 框"查看漏洞是否同步完成,同步完成的漏洞标识为 JIRA 图标。

 ◆ XML外部实体注入 <a>5.5 127.0.0.1:8080/taintwebapp/XXEServlet 漏洞參数: - 污点执行: doPost()@XXEServlet.java:42 	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: ●未验证 更新时间: 2022-01-12 18:14:44 查看详情 運溯验证 ◆ 发现时间: 2022-01-12 18:14:44
 ◆ 文件上传 未移業 127.0.0.1:8080/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp:31 	项目名称:huanweblogic-jndi测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 查看详情【灑洞验证 ◆ 发现时间: 2022-01-12 18:14:44
 单页全选 全选 备注 修改状态 分享 里新检测 共66838条 < 1 2 	风脸同步 ∨ 3 4 5 ···· 6684 > 10 条/页 ∨ 1	 (JIRA同步情況) (禅道同步情況) (禅道同步情況) (第

图表 137 同步 JIRA - 查看同步情况

- ◆ 用户非第一次进行同步 JIRA 操作,点击"同步 JIRA"按钮会直接展示上次同步配置后的弹框(或上次记住漏洞同步信息的弹框)。
- ◆ 若修改了 JIRA 系统中的用户名密码或项目的配置,可点击弹框上方的"重新同步 配置"按钮,在新出现的弹框中核对信息后点击"同步配置"进行更新。

-				155555505	18:52:07
ig	同步 JIRA	【重新同步配置】	4	③ 自定	<u> </u>
ig	提示:可在 \$descriptio 为漏洞 类 型 (需要权限	字段内填入\$type、\$ n、\$environment、\$ 1、漏洞等级、项目名 1账号),漏洞分享链	ilevel、\$project、\$t \$environment-24h, 称、测试人员、漏源 i接(不需要权限账号	ester、 房鉴将会自动 可详情,漏洞锁 号,24h有效期	替换 接)
	图	表 138 同步、	JIRA - 重新同	司步配置	

* URL	http://192.168.180.81:8080/	
* 用户名	admin	
* 密码		Ø

图表 139 同步 JIRA - 重新同步配置弹框

 点击"查看 JIRA 同步情况",列表右侧展示漏洞是否已同步至 JIRA。展示了 JIRA 图标 的表示已同步。

● XML外部实体注入 無何里 127.0.0.1:8080/taintwebapp/XXEServlet 漏洞參数: 一污点执行: doPost()@XXEServlet.java:42	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 🔷
 ◆ 文件上传 未参算 127.0.0.1:8080/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp:31 	项目名称:huan-weblogic-jndi测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: ● 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 🔶
 单页全选 全选 备注 修改状态 分享 重新检测 共66838条 < 1 2 	<u>风险同步</u> ∨ 3 4 5 ···· 6684 > 10 条/页 ∨ 1	✓【JIRA同步情况】 現至 页	🗌 【禅道同步情况】

图表 140 漏洞列表 - 查看 JIRA 同步情况

杭州默安科技有限公司

点击"风险同步-同步禅道",可将用户选择的漏洞一键同步至禅道平台上,用户需填写
 禅道系统的 URL 地址、用户名、密码。

	nnnnnnn	
同步禅道		
* LIBI	· 请输入 逆道 系统 他 批	
OTIL	例如:http://192.168.180.100:8081	
* 用户名	tang	
* 密码	••••	Ø
	同步配置取消	
	<u> </u>	

图表 141 同步禅道 - 填写禅道系统账号信息

◆ 第一次进行同步需要填入对应账号信息后点击"同步配置", 雳鉴会从禅道地址同步所属产品和 Bug 标题等信息。页面上方出现提示,且弹框内实时展现同步进度。

		◆ 禅道数据正在同步中,请稍等 〈 ◆ 禅道数据正在同步中,请稍等 〈 ◆ 〈 ◆ ◆ ☆ 式	Pingce
	_	hbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb	Pinqce
	同步禅道		
bar	-		
	* URL	http://192.168.180.52:8082	
es		例如:http://192.168.180.100:8081	
	* 用户名	tang	
bar	* 密码	••••	Ø
bar		○ 正在同步中20% 隐藏	
		鉴权代理	

图表 142 同步禅道 - 同步配置

◆ 同步完成后,弹框内展示所有项目及对应字段信息。

				A 12	- IIIGC
	同步禅道	【重新同步配】	2]	0	自定义字段
aţ					
S	提示:可在字 \$description 洞类型、漏洞 (需要权限账	段内填入\$ty 、\$environn]等级、所属] (号),漏洞:	vpe、\$level、\$project、\$submitter、 nent、\$environment-24h,雳鉴将会 项目、开发人员、风险状态、漏洞详情 分享链接(不需要权限账号,24h有效;	\$st 自动 i,漏 期)	atus、 替换为漏 洞链接
at	* 所属产品		刃甲		V
at	* Bug标题				
ŀ	*影响版本				
s		🔽 记	住本次同步的选项及填写信息		
ab			确认 取消		ir

图表 143 同步禅道 - 弹框

◆ 弹框内默认仅展示项目下的必填字段,用户可点击右上角的"自定义字段"按钮选择非必填字段加入弹框后进行填写。

	同步禅道 【重新同步配置】	② 自定义字段	15:52:4
at	提示: 可在字码内值入\$type \$layel \$pre	全部 必选 非必选	2021-(
s	\$description、\$environment、\$environme 洞类型、漏洞等级、所属项目、开发人员、)浏览器 Bug类型	_(
	(需要权限账号),漏洞分享链接(不需要 [;]	Bug标题颜色 截止日期	2:0
ar	* 所属产品	● 关键词 ● 操作系统 ● 优先级	(7:5
ar	* Bug标题	 广里程度 抄运结 所属项目 重现步骤 	
	* 影响版本	□ 相关需求 □ 相关任务	4:0
s		□ 当前指派 🕢 所属产品	_(
	✓ 记住本次同步的选项	✓ Bug标题 ✓ 影响版本	1:1
ab	确认	in_h	2021–0 18:36:0

图表 144 同步禅道 - 自定义字段

◆ 在字段填写框内填入特殊字段, 雳鉴在同步漏洞至禅道时会将该字段替换成对应的 漏洞信息。如: 在某个文本框类型中填入特殊字段"\$environment", 同步至禅道 后会展示为该漏洞的漏洞链接。



图表 145 同步禅道 - 自定义同步漏洞信息

◆ 弹框下方可选择是否记住本次同步的选项及填写信息,若选择记住,则下次点击"同

步禅道"按钮后弹框内会展示上一次本账号进行同步时的选项及填写信息。

៖	己住本次同步的选项及填写信息	
b	确认 取消	n

图表 146 同步禅道 - 记住选项及填写信息

◆ 点击确认后漏洞会同步到用户禅道系统中,可通过点击"查看禅道同步情况复选框" 查看漏洞是否同步完成,同步完成的漏洞标识禅道图标。

● ① 不安全的readline方法调用	项目名称:huan–redis 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-11 15:43:53 发现时间: 2022-01-11 14:39:52	查看详情 漏洞验证
○ 不安全的readline方法调用 ★修算 Iocalhost:8080/login 漏洞参数: body 污点执行: getBodyString()@HttpHelper.java:30	项目名称:huan-weblogic-jnd测试 项目模式:播桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-11 15:43:53 发现时间: 2022-01-11 14:39:53	查看详情 漏洞验证
 ○ 時站脚本攻击(XSS) 注:7.0.0.1/taintwebapp/vulns/xss/ 漏洞参数: name 污点执行: jspService()@index_jsp.java:125 	项目名称:test-dubbo-ly3 项目模式:播桩模式 测试人员:llyun	主动验证: • 未验证 更新时间: 2022-01-11 15:18:01 发现时间: 2022-01-07 09:04:31	查看详情 漏洞验证 🕝
 ◎ 会话超时设置不当 未停复。 127.0.0.1/ 漏洞参数: 45 汚点执行: - 	项目名称:test-dubbo-ly3 项目模式:抓桩模式 测试人员:liyun	主动验证: • 未验证 更新时间: 2022-01-11 15:17:49 发现时间: 2022-01-07 09:03:46	查看详情 漏洞验证 🕞
 単页全选 全选 备注 修改状态 分享 重新检测 (共62210条 < 1 2 	风险同步 ∨ 3 4 5 ···· 6221 > 10 条/页 ∨ 3	〇【JIRA同步情况 跳至 页] 🕑 【禅道同步情况】

图表 147 同步禅道 - 查看同步情况

- ◆ 用户非第一次进行同步禅道操作,点击"同步禅道"按钮会直接展示上次同步配置 后的弹框(或上次记住漏洞同步信息的弹框)。
- ◆ 若修改了禅道系统中的用户名密码或项目的配置,可点击弹框上方的"重新同步配置"按钮,在新出现的弹框中核对信息后点击"同步配置"进行更新。





Contract (1997)	100000000000000000000000000000000000000	
同步禅道		
* URL	请输入禅道系统地址	
	例如:http://192.168.180.100:8081	
* 用户名	tang	
* 密码	••••	Ø
	同步配置 取 消	
	AII	-1

图表 149 同步禅道 - 重新同步配置弹框

 点击"查看禅道同步情况",列表右侧展示漏洞是否已同步至禅道。展示了禅道图标的 表示已同步。

◆ 不安全的readline方法调用 未修算 localhost:8080/login	项目名称:huan-redis 项目模式:插桩模式	主动验证: 更新时间:	● 未验证 20220111 15:43:53	查看详情	漏洞验证
漏洞參数: body 污点执行: getBodyString()@HttpHelper.java:30	测试人员: wufengjuan	发现时间:	2022–01–11 14:39:52		
◆ 不安全的readline方法调用 無修复 localhost:8080/login 漏洞参数: body 污点执行: getBodyString()@HttpHelper,java:30	项目名称:huan-weblogic-jndi测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: 更新时间: 发现时间:	● 未验证 202201-11 15:43:53 202201-11 14:39:53	查看详情	漏洞验证
 ◆ 時站脚本攻击(XSS) 連修更 127.0.0.1/taintwebapp/vulns/xss/ 漏洞参数: name 污点执行: _jspService()@index_jsp.java:125 	项目名称:test-dubbo-ly3 项目模式:抓妊模式 测试人员:liyun	主动验证: 更新时间: 发现时间:	● 未验证 2022-01-11 15:18:01 2022-01-07 09:04:31	查看详情	漏洞验证 🞯
 ◆ 会话認时设置不当 未作其 127.0.0.1/ 漏湯参数: 45 汚点执行: - 	项目名称:test-dubbo-ly3 项目模式: 插桩模式 测试人员:liyun	主动验证: 更新时间: 发现时间:	● 未验证 20220111 15:17:49 20220107 09:03:46	查看详情	漏洞验证 🞯
単页全选 全选 备注 (修改状态) 分享 (重新检测) (A 共62210条 < 1 2 3	脸同步 ∨ 4 5 ··· 6221 > 10 条/页 ∨ 跳	ن <u>ت</u>	【JIRA同步情况】	☑ 【祥	单道同步情况】

图表 150 漏洞列表 - 查看禅道同步情况

同时选择"JIRA 同步情况"和"禅道同步情况"复选框,可同时查看漏洞同步 JIRA 和
 禅道的情况,列表右侧展示 JIRA 图标和禅道图标表示均已同步。



图表 151 漏洞列表 - 查看 JIRA 和禅道同步情况

1.7.2数据安全漏洞

用于统计目前用户环境所有项目的数据安全漏洞情况,具体包括当前用户管理的项目数、 测试请求数、测试人员数、漏洞数量和未修复的漏洞数等。数据安全漏洞包括个人隐私数据 泄漏、个人隐私信息泄露、数据库连接弱密码、敏感页面泄露、SQL注入、NoSQL注入、api 接口未授权访问。



图表 152 数据安全漏洞列表概述

数据安全漏洞列表展示项可自定义配置,默认按漏洞发现时间倒序排列,列表可选内容 包括漏洞地址、漏洞类型与等级、漏洞参数、项目名称、项目模式、测试人员、最后检测时 间、首次发现时间、状态及操作。

可根据漏洞等级、修复状态、漏洞类型、项目模式进行查看,选择漏洞等级后漏洞类型 筛选下拉框内仅出现对应等级漏洞类型,可查看漏洞详情,JIRA 和禅道同步情况或进行 重新检测,并且可对漏洞进行批量修改漏洞状态、同步 JIRA、同步禅道、添加备注。

(注意 ・) 毎報 (注意 ・) 発致 (注意 ・) 項目儀式 (注)	an • ±3%20 25 • 7.000% 25 • 1.000%
○ ◆ 大利時45年1日開始 ● #### 1270.0.1880807Jahntwebapp/valns/providers/xxssprotectionhea 置 編明命載: - 予約時以行: -	短程名称: taintwebage-20220830120955 主法指定: * 未始正 項目相応: 論任相応 更新的可能: 2022-08-30 12:10:58 重新評論 (編示) 解成人品: cheniu 安規時時間: 2022-08-30 12:10:58
今 へ入時はKeiKEIEEEE ***** 1270.0.18090/taintwebapp/vulm/providers/xxssprotectionhea 編載時間に、・予防的以行・・	18日号(Sh: talhtwebapp-20220530120017 主法治定: 未治证 項目相応: 論任相応
 ◆ 个人场机低低能量 ×95% 127.0.0.130808/taihtwebapp/vulms/providers/sessionrewriting. 調明參載: - 汚過助行: - 	语目名将: taintweebapp-20220830120017 生动验证: 未动论证: 项目电优:: 编组优: 展频电优 展频电池: 2022-08-30 1210.57 重新计算 尾印 激励人员: chemlu 发现到词: 2022-08-30 1210.57
● ◆人移動紙時間源 ●000 127.0.0.18080(TalnitveEapp/vulns/providers/sessionrewriting. 編時參載: - 汚成形式: -	道臣名称: taintwebapp-20220830120955 注动始近: + 未始正 活臣戦死: 論地戦亡 夏勝時明記: 2022-08-30121057 重要許増 東府 勝武人員: chenlu 22現時時: 2022-08-30121057
◆ ◆人類は低低調査 ×800 1270.0.18808/1aintwebap/vulms/providers/httpauth/sp 順同参覧: - 汚点的以行: -	項目條何: taintwebapp-20220830120955 生动始近: 米地征 項目條何:: 接触病亡 原動時間: 2022-08-30 1210.56 重要決損 東府 動成人员: chemlu 22初時间: 2022-08-30 1210.56
◆ 今人為私知能理解 ●●●■■ 127.0.0.18080/taintwebapp/vulns/providers/httpauth.jsp 編明考試: - 可通用点:	短日名時: talitvebage-20220830120017 主法物任: 未発任: 高日朝史: 論約相応: 論約相応: 論約相応: 第時日 謝知ら人品: cheniu 22初回時: 2022-08-30 12:10:56 重新評論 (高時)

图表 153 数据安全漏洞列表

- 选择需要添加备注的数据安全漏洞,点击备注按钮后,可以对数据安全漏洞批量添加备
 注。添加后的备注可以到数据安全漏洞详情中编辑或者删除。
- 选择需要修改漏洞状态的数据安全漏洞,点击修改状态按钮,可以对数据安全漏洞批量 修改状态,可以修改为忽略、误报、已修复、未修复。修改状态时需要填写相关备注信 息。被手动修改过的数据安全漏洞,在漏洞名称后会有红色叹号提醒,提示该漏洞已经 被人工托管,系统不会自动修改其状态。
- 选择需要重新检测的数据安全漏洞,点击重新检测按钮,可以批量对数据安全漏洞进行 重新检测。但是只对勾选的扫描类数据安全漏洞生效,插桩类数据安全漏洞不会重新检 测。
- 点击"分享",当测试人员发现数据安全漏洞时,支持批量漏洞分享(一次上限为200个),高效快捷的将该漏洞信息以地址+密码的方式发送至安全人员,可以选择漏洞分享的有效时长为1天、3天、7天、15天、30天,默认为1天。



图表 154 漏洞分享

● 点击"查看详情",跳转至漏洞详情页,该页面中可见该漏洞的类型、等级、状态等自

杭州默安科技有限公司

述信息,可知描述、危害、建议、细节,漏洞代码示例(JAVA/.NET/PHP),对于可通过 安全组件修复的漏洞可下载安全组件并查看安全组件的使用方法,并可进行漏洞重新检 测,演示及编辑操作。

9雳	鉴·IAs	ST											99 i 😅 i 🔂
当前位置:	漏洞管理 > 1	屬阿列表 > 漏洞	洋情										
混闭详情													
高加	<mark>州)</mark> ^{與狠}	未修复 ^{編明状态}			漏泪 项E	同英型: 日名称: 日模式:	api接口未接 信使例此去 流量信使模	₩0访问 重-请求路径 式	印参数			首次发现时间 最后检测时间 漏洞地址:	2022-08-29 1434:31 2022-08-29 1642:04 GET 192:168:180:522:0000/wilnerabilities/xss_d//default=English7777777777777777788userkey=
					20	武人员:	xzm					开放时长:	
PORTAGE	漏洞描述	修复方案	请求信息	历史动态									
(3) #1866	衣掘												
存在	在漏洞的接口 过检测,该接	是http://192.16 口末做遊权措施	8.180.52:200 ,可能存在未挂	00/vulnerat 受权访问漏洞	oilities/xss_ 月。(提示:	_d/ 如果为业务:	本身需求/无需	接权接口,1	可以配置检测	黑名单处理证	RHR.)		
Paylo	ad												
GE	T												

图表 155 数据安全漏洞详情(扫描类)

其中进行漏洞演示时,需单击'展示响应'按钮,右边有两个窗口'响应包'和'验证结果'。响应包里面内容显示该数据安全漏洞页面的请求响应源码;验证结果是以 web 的形式展示漏洞。如 SQL 延时注入漏洞,单击'验证结果'就会显示相关的数据信息,如图 82 所示。

祝聞 漏同曲述 修复方案 前末(48) 历史动态	antra tetram	
code':100,"msg":"内部上下交处理错误"}		
	展示地位	

图表 156 漏洞演示及编辑

iOuerv1	10207992313818863606 1562748045630({"a"·"linux shezhi" "p"·false "a"·
[{"type"	"sug" "sa"·"s 1" "g"·"linux 没置ip"} {"type"·"sug" "sa"·"s 2" "g"·"linux 没置环境
	vpe"·"sug" "sa"·"s 3" "g"·"linux 设置终端性推键"}
/"tupe"."	sug" "sa":"s /" "g":"linux 设置(动顺)/定定)/
Type . 署网络"}	3ug, 3u · 5_4, q · mux 设置口承快限],[type · 3ug , 3u · 5_5 , q · mux 设 {"type"·"sug" "sa"·"s 6" "g"·"linux 设置路由命令"}
置网络"}	sug , sa : s_ 4 , q : linux 设置白泉仪限),(spe : sug , sa : s_ 5 , q : linux 设 {"type":"sug","sa":"s_6","q":"linux 设置路由命令"}, sug" "sa":"s_7" "g":"linux 设置田户密码"} {"type":"sug" "sa":"s_8" "g":"linux 设
置网络"} {"type":' 署昭冬白	sug", su : sug", "sa ::"s_6", "q":"linux 设置台家设设 [, (ype : sug , su : s_5 , q : linux 设 {"type":"sug", "sa":"s_6", "q":"linux 设置用户密码"},("type":"sug", "sa":"s_8", "q":"linux 设 巨动"\/("type":"sug" "sa":"s_9" "g":"linux 沿置#十小"\

图表 157 SQL 延时注入漏洞演示

进行漏洞编辑时,在页面上单击'编辑请求','编辑请求'内内容与'测试请求'内 默认内容相同,用户可根据需要对其进行编辑。单击'发送请求'按钮后,右边有两个窗口 '响应包'和'验证结果',响应包里面的内容显示该漏洞页面的实时请求响应源码,验证 结果中则是以 web 的形式展示漏洞。

判断依据	漏洞描述	修复方案	谢求信息	历史动态										
请求包	编播请求							响应包	脸证结果					
("code":1	00,"msg":"内)	部上下文处理	音涙")											
							发送请求							
						1.								11

图表 158 漏洞演示及编辑二

点击"历史动态",显示出该数据安全漏洞不同时间下更新的漏洞状态,包括数据安全漏洞的首次发现、漏洞被复测、漏洞状态的改变(已修复、未修复)、漏洞状态的手动改变(手动调整为已修复、误报、忽略、恢复)。

判断依据	漏洞描述	修复方案	请求信息	历史动态		
2022	-02-15 16:49::	38				
漏洞被	技首次发现					

图表 159 漏洞历史动态

● 点击"重新检测",漏洞对应请求进入检测中,检测完成之后更新漏洞状态及信息。

Ø	雳鉴・IA	ST													уу I 🚅 I 🕞
当前位	: 漏洞管理 >	漏洞列表 > 漏洞	洋情												
瀧闭详	ŧ.														
					漏》	●樊型:	个人隐私数	原泄漏					首次发现时间:	2022-08-30 12:10:58	
F	危	未修复			项目	8名称:	taintwebap	p-20220830	0120955				最后检测时间;	2022-08-30 12:10:58	
.05	94942	1001910-022			项目	目模式:	播柱模式						漏洞地址:	GET 127.0.0.1:8080/taintwebapp/vulns/providers/xxssprotectionheader.jsp?type=	=0
					Ria	t人员:	chenlu						开放时长:	0天	
															风险同步 >
P18563	漏洞描述	修复方面	请求信息	数据流信	他 历史	133次	Agent								
0 #	新依据														
	存在个人隐私道 127***0.1(IP), 经检测,该漏算	改振泄漏风险的清 该数据保存在# 同的存在违反了(球URL为127.0 1应中 通用数据保护部	1.0.1:8080/ta 분위 (GDPR)	intwebapp) 》和《支	o/vulns/pro 付卡行业数	viders/xxsspr 居安全标准(P	otectionhea CI DSS) 》 8	ider.jsp, 匹敵 眎進。	记到未经加密/	脱敏处理的1	下人隐私数据:			
() ±	动验证														
	 未验证 														

● 点击"数据流信息",可查看漏洞的详细数据流(包括 TagRange)及栈调用等信息。

判断依据	淝阀描述	修复方案	译本编剧 历史动态 Agent	
隐私数据(0		 ● 除私政策 	
- 127***0.	1(IP)		教授 : 127***0.1(IP)	
			(2) 范围位置(这次增长保存在地位中)	
			時行確認: void org.apache.jssper.unime.skpWitterimpLprint(java.lang.String) 代码位置: service(3)eHttps/BaseJava/20 編詞書数: https.br/aja&e/zf_&e/zf_12 ⁺⁺⁺⁰ 1.1&#s/aja8080&#zf_tainnebapp&#zf_tuins&#s/zf_providers&#zf_txxssprotectionheaderjapType=0</td><td>履开▼</td></tr></tbody></table>	

图表 161 插桩模式数据安全漏洞详情-数据流信息

 点击"Agent",显示出该漏洞关联的 Agent 列表,包含 Agent 名称、插桩 Agent 地址、 key、标签、状态和操作(查看详情)。

判断依据	漏洞描述	修复方案	请求信息	数据流信息	历史动态 Agent				
Agent名称		播	往Agent地址		key 🔵		标签	状态	攝作
		10	.244.0.188		713a6aa1-1b7d-31e7-b66b-fbb8401d	e9	taintwebapp_docker	 已留停 	详情
						共1 条 < 1 > 10 条/页 ∨			

图表 162 插桩模式数据安全漏洞详情-Agent

点击"风险同步-同步 JIRA",可将用户选择的漏洞一键同步至 JIRA 平台上,用户需填写 JIRA 系统的 URL 地址、用户名、密码。

* URL	请输入 JIRA 系统地址	
* 用户名	请输入 JIRA 系統用户名	
* 密码	请输入 JIRA 系统用户密码	Æ

图表 163 同步 JIRA - 填写 JIRA 系统账号信息

◆ 第一次进行同步需要填入对应账号信息后点击"同步配置", 雳鉴会从 JIRA 地址 同步项目和问题类型等信息。页面上方出现提示, 且弹框内实时展现同步进度。

-	auto-test-356	流量信使模式	test_lt	202
同步 JIRA	ñ			10
* URL	http://192.168.180	.81:8080/		
* 用户名	admin			
* 密码				Ø
		bcbx0% 降荷		

图表 164 同步 JIRA - 同步配置

◆ 同步完成后,弹框内展示所有项目及对应字段信息。

\$description、\$env 为漏洞类型、漏洞等 (需要权限账号),	a/Stype、Stever、Sproject、Stever ironment、Senvironment-24h, 雳 蜂级、项目名称、测试人员、漏洞详 漏洞分享链接(不需要权限账号,	er、 鉴将会自动替换 情,漏洞链接 24h有效期)
「项目	字段测试	\sim
* 问题类型	缺陷	V
数值字段	111	
* 描述	\$description	
* 主题	\$type	
•选择用户(单选)	雳鉴项目组 / wudi	\sim

图表 165 同步 JIRA - 弹框

◆ 弹框内默认仅展示项目下的必填字段,用户可点击右上角的"自定义字段"按钮选择非必填字段加入弹框后进行填写。

二, 可大会的内核) Etwas Elaval	全部	必选	非必选
description、\$envi j漏洞类型、漏洞等	ronment、\$envin 级、项目名称、\$	✓ 数值字段	组选择	器 (单组)
(需要权限账号),	漏洞分享链接(2	文本框((单行) 🗌 :	文本框 (多行)
而曰	之時御時	环境	标签	
	THEOSIN	版本选择	² (单一版本选持	圣)
可题类型	缺陷	文本框((只读)	JRL字段
直字段	111	版本选择	2 (多版本选择)	
		组选择器	(多组)	单选按钮
苗述	\$description	复选框	日期选择	控件
E <mark>题</mark>	\$type			-00
选择用户 (单选)	雳鉴项目组 /	wudi		~
elect <mark>l</mark> ist(级联)	select list(级	联)12 / selec	t list (级联) 1	22
_		15TL HERE		-08
	记住4次问步的远	坝及填与16息		1

图表 166 同步 JIRA - 自定义字段

◆ 在字段填写框内填入特殊字段, 雳鉴在同步漏洞至 JIRA 时会将该字段替换成对应的漏洞信息。如:在某个文本框类型中填入特殊字段 "\$environment", 同步至 JIRA 后会展示为该漏洞的漏洞链接。



图表 167 同步 JIRA - 自定义同步漏洞信息

◆ 弹框下方可选择是否记住本次同步的选项及填写信息,若选择记住,则下次点击"同

步 JIRA" 按钮后弹框内会展示上一次本账号进行同步时的选项及填写信息。

*	Select list (次地大	select list	(级联) 12 / sele	ect list(级联)122	
18/config		🖌 记住本次同步的	的选项及填写信息	E	-08
		确认	取消		

图表 168 同步 JIRA - 记住选项及填写信息

◆ 点击确认后数据安全漏洞会同步到用户 JIRA 系统中,可通过点击"查看 JIRA 同步 情况复选框"查看数据安全漏洞是否同步完成,同步完成的漏洞标识为 JIRA 图标。

● XML外部实体注入 <u>未</u> 便更 127.0.0.1:8080/taintwebapp/XXEServlet 漏洞參数: - 污点执行: doPost()@XXEServlet.java:42	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 🔶
● 文件上传	项目名称:huanweblogic-jndi测试 项目概式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 🔷
 单页全选 全选 备注 修改状态 分享 里新检测 共66838条 < 1 2 	风险同步 ∨ 3 4 5 6684 > 10 条/页 ∨ 5	✓【JIRA同步情况】 跳至 页	□【禅道同步情况】

图表 169 同步 JIRA - 查看同步情况

- ◆ 用户非第一次进行同步 JIRA 操作,点击"同步 JIRA"按钮会直接展示上次同步配置后的弹框(或上次记住漏洞同步信息的弹框)。
- ◆ 若修改了 JIRA 系统中的用户名密码或项目的配置,可点击弹框上方的"重新同步 配置"按钮,在新出现的弹框中核对信息后点击"同步配置"进行更新。

同步 JIRA	【重新同步配置】	ł	③ 自定义	(字段
提示:可在 \$descriptio 为漏洞类型 (需要权限	字段内填入\$type、\$ n、\$environment、\$ 1、漏洞等级、项目名 账号),漏洞分字链	ilevel、\$project、\$ Senvironment-24h, 称、测试人员、漏 接(不需要权限账	tester、 房鉴将会自动替 同详情,漏洞链接 号,24h有效期)	换 E
图	表 170 同步]	JIRA - 重新	司步配置	

* URL	http://192.168.180.81:8080/	
* 用户名	admin	
* 密码		Ø

图表 171 同步 JIRA - 重新同步配置弹框

 点击"查看 JIRA 同步情况",列表右侧展示数据安全漏洞是否已同步至 JIRA。展示了 JIRA 图标的表示已同步。

● XML外部实体注入 第127.0.0.1:8080/taintwebapp/XXEServlet 漏洞参数: - 污点执行: doPost()@XXEServlet.java:42	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: ● 朱验证 更新时间: 2022-01-12 18:14:44 查看详情 灑淵驗证 ◆ 发现时间: 2022-01-12 18:14:44
 ○ 文件上传 法修复 127.0.0.1:8080/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp:31 	项目名称:huan-weblogic-jnd测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: ● 未验证 更新时间: 2022-01-12 18:14:44
 单页全选 全选 备注 修改状态 分享 重新检测 共66838条 < 1 2 	_ 风陰同步 ∨ 3 4 5 ··· 6684 > 10 条/页 ∨ j	♥【JIRA同步情况】 ○【禅道同步情况】 減至 页

图表 172 漏洞列表 - 查看 JIRA 同步情况

杭州默安科技有限公司

点击"风险同步-同步禅道",可将用户选择的数据安全漏洞一键同步至禅道平台上,用
 户需填写禅道系统的 URL 地址、用户名、密码。

	nnnnnnn	P
同步禅道		
* 1 101	· 法 (1) 》 汕 治 玄 体 州 州	
ONL	明明(11)11年1月1日) 例如: http://192.168.180.100:8081	
* 用户名	tang	
*密码	••••	Ø
	同步配置 取 消	
_	华 权代理	_

图表 173 同步禅道 - 填写禅道系统账号信息

◆ 第一次进行同步需要填入对应账号信息后点击"同步配置", 雳鉴会从禅道地址同步所属产品和 Bug 标题等信息。页面上方出现提示,且弹框内实时展现同步进度。

		◆ 禅道数据正在同步中,请稍等 〈 ◆ 禅道数据正在同步中,请稍等 〈 ◆ 〈 ◆ ◆ ☆ 式	Pingce
	_	hbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb	Pinqce
	同步禅道		
bar	-		
	* URL	http://192.168.180.52:8082	
es		例如:http://192.168.180.100:8081	
	* 用户名	tang	
bar	* 密码	••••	Ø
bar		○ 正在同步中20% 隐藏	
		鉴权代理	

图表 174 同步禅道 - 同步配置

◆ 同步完成后,弹框内展示所有项目及对应字段信息。

同步禅道 【重新同步	配置】	◎ 自定义字段
提示:可在字段内填入; \$description、\$enviro 洞类型、漏洞等级、所 (需要权限账号),漏;	\$type、\$level、\$project、\$submitter. nment、\$environment-24h,雳鉴将会 属项目、开发人员、风险状态、漏洞详忙 洞分享链接(不需要权限账号,24h有效	、\$status、 ≿自动替换为漏 青,漏洞链接 y期)
* 所属产品	刃甲	~
* Bug标题		
*影响版本		
	记住本次同步的选项及填写信息	
	确认 取消	
	同步禅道 【重新同步 提示:可在字段内填入 \$description、\$enviro 洞类型、漏洞等级、所 (需要权限账号),漏 * 所属产品 * Bug标题 * 影响版本	 同步禅道 【重新同步配置】 提示:可在字段内填入\$type、\$level、\$project、\$submitter.\$description、\$environment、\$environment-24h, 雳鉴将会洞类型、漏洞等级、所属项目、开发人员、风险状态、漏洞详性(需要权限账号),漏洞分享链接(不需要权限账号,24h有效 * 所属产品 刃甲 * Bug标题 * 影响版本 ② 记住本次同步的选项及填写信息 确认 取消

图表 175 同步禅道 - 弹框

◆ 弹框内默认仅展示项目下的必填字段,用户可点击右上角的"自定义字段"按钮选择非必填字段加入弹框后进行填写。

ſ	同步禅道 【重新同步配置】	 ④ 自定义字段 	15:52:4
ar	担子・可左字段内植入をかって やしいつ やっ	全部 必选 非必选	2021-i 2:'
s	\$description、\$environment、\$environm 洞类型、漏洞等级、所属项目、开发人员、	。 ◎ 浏览器 Bug类型	
	(需要权限账号),漏洞分享链接(不需要	型 Bug标题颜色 截止日期	2:0
ar	* 所属产品	关键词 □ 操作系统 □ 优先级	(7-5
	* Bug标题	○ 严重程度 抄送给 所属模块	
ar			—(1:0
	* 影响版本	□ 当前指派 🕑 所属产品	_(
5	✓ 记住本次同步的选工	👿 🕑 Bug标题 🖌 影响版本	4:1
ab	确 认	ኪ //-	2021–0 18:36:3

图表 176 同步禅道 - 自定义字段

◆ 在字段填写框内填入特殊字段, 雳鉴在同步漏洞至禅道时会将该字段替换成对应的 漏洞信息。如: 在某个文本框类型中填入特殊字段"\$environment", 同步至禅道 后会展示为该数据安全漏洞的漏洞链接。

Tel: (+86) 400-0571-211

Email: market_moresec.cn



图表 177 同步禅道 - 自定义同步漏洞信息

◆ 弹框下方可选择是否记住本次同步的选项及填写信息,若选择记住,则下次点击"同

步禅道"按钮后弹框内会展示上一次本账号进行同步时的选项及填写信息。

s 🗸 🗸	已住本次同步的选项及填写信息
b	确 认 取 消 ir

图表 178 同步禅道 - 记住选项及填写信息

◆ 点击确认后数据安全漏洞会同步到用户禅道系统中,可通过点击"查看禅道同步情况复选框"查看数据安全漏洞是否同步完成,同步完成的漏洞标识禅道图标。

 ② 目录穿越 (未修覧) 127.0.0.18080/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp.31 	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证
 ◇ XML外部实体注入 <a> 127.0.0.18080/faintwebapp/XXEServlet 漏洞参数: - 污点执行: doPost()@XXEServlet.java:42 	项目系称: huan-jdk16-taintwebapp 项目模式: 插桩模式 测试人员: wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 🙃
◆ 文件上传 法修复	项目名称:huan-weblogic-jndi测试	主动验证: • 未验证	查看详情 漏洞验证 😡
127.0.0.1:8080/taintwebapp/vulns/file-upload/	项目模式:插桩模式	更新时间:2022-01-12 18:14:44	
漏洞参数: - 污点执行: service()@index.jsp.31	测试人员:wufengjuan	发现时间:2022-01-12 18:14:44	
○ 単页全选 全选 备注 修改状态 分享 重新检测	风险同步 ∨	〇 【JIRA同步情況] 🛛 【禅道同步情况】
共66833条 < 1 2	3 4 5 ··· 6684 > 10 条/页 ∨ §	挑至 页	

图表 179 同步禅道 - 查看同步情况

- ◆ 用户非第一次进行同步禅道操作,点击"同步禅道"按钮会直接展示上次同步配置 后的弹框(或上次记住漏洞同步信息的弹框)。
- ◆ 若修改了禅道系统中的用户名密码或项目的配置,可点击弹框上方的"重新同步配置"按钮,在新出现的弹框中核对信息后点击"同步配置"进行更新。





Contract (1997)	100000000000000000000000000000000000000	
同步禅道		
* URL	请输入禅道系统地址	
	例如:http://192.168.180.100:8081	
* 用户名	tang	
* 密码	••••	Ø
	同步配置 取 消	
	AII	-1

图表 181 同步禅道 - 重新同步配置弹框

 点击"查看禅道同步情况",列表右侧展示数据安全漏洞是否已同步至禅道。展示了禅 道图标的表示已同步。

 ● 目录穿越 (未参差) 127.0.0.1:8080/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp:31 	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证
● ② XML外部实体注入 派师算 127.0.0.1:8080/taintwebapp/XXEServlet	项目名称:huan-jdk16-taintwebapp 项目模式:插桩模式	主动验证: • 未验证 更新时间: 2022–01–12 18:14:44	查看详情 漏洞验详 😡
漏洞参数: - 污点执行:doPost()@XXEServlet.java:42	测试人员:wufengjuan	发现时间:2022-01-12 18:14:44	
 ○ 文件上传 未修理。 127.0.0.18080/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp.31 	项目名称:huan-weblogic-jndi测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证 ⓒ
□ 单页全选 全选 备 注 修改状态 分 享 重新检测	风险同步 >	□【JIRA同步情况	】 🛛 【禅道同步情况】
共66838条 < 1 2	3 4 5 ···· 6684 > 10条/页 / 1	第至 页	

图表 182 漏洞列表 - 查看禅道同步情况

同时选择"JIRA 同步情况"和"禅道同步情况"复选框,可同时查看数据安全漏洞同步
 JIRA 和禅道的情况,列表右侧展示 JIRA 图标和禅道图标表示均已同步。

● 目录穿越 ※#11 127.0.0.1-8080/taintwebapp/vulns/file-upload/ 濿洞参数: - 万点执行: service()@index.jsp:31	項目名称:huanjdk16-taintwebapp 項目模式:播桩模式 測试人员: wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详情 漏洞验证
◆ XML外部实体注入 (##9月) 127.0.0.1:8080/taintwebapp/XXESarvlet 溜洞参数: - 汚点抵行: doPost()@XXESarvlet.java.42	項目名称:huan-jdk16-taintwebapp 項目標式: 插紙模式 測试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详 漏洞验 情 □ 证
● 文件上传 亲考复 127.0.0.18080/taintwebapp/vulns/file-upload/ 漏洞参数: - 污点执行: service()@index.jsp:31	項目名称:huan-weblogic-jndi测试 项目模式:插桩模式 测试人员:wufengjuan	主动验证: • 未验证 更新时间: 2022-01-12 18:14:44 发现时间: 2022-01-12 18:14:44	查看详 漏洞验 情 证
 单页全选 全选 备注 修改状态 分享 重新检测 共66638条 < 1 2 	风险同步 ∨ 3 4 5 ··· 6684 > 10 条/页 ∨ 跳	☑ 【JIRA同步情况 至 页	】 🕑 【祥道同步情况】

图表 183 漏洞列表 - 查看 JIRA 和禅道同步情况

1.8 第三方库(插桩类)

第三方库管理页面展示目前用户所有测试项目的第三方库情况。由3部分组成:概述、 图表分析、第三方库列表。

	Agent WARFIEM MINISTER N	R O E TTI SARE EDTO						yy i 🚅 i 🕞
680 ##			19 A	<mark>57</mark> 项目数				591 METRO
N2019(2):4:8	送三方」を使用Top5 の見たいに、 congrages conflaters ionflaters iog5log6 0	10 20	30	40	第三方库版本	0.859布周	0	1885
和周阳が第三方本 語音 200 + 等級 200 库谷	* : RJ09918	项目名称	语言	当前版本号	最新版本型	开源许可证	#-58//0日58- 截5页##时间 :	C Ottexcel
org.springframework.spring-test	() 提示	test-ly1	Java	5.2.3.RELE ASE	5.2.22.REL EASE	Apache 2.0	2022-08-30 16:01:39	#CEB 1916
com.alībaba.fastjson	0 Rt	871f8527-5c62	Java	1.2.45	2.0.3.andr old	Apache 2.0	2022-08-30 16:01:39	库德密(详饰
com.fasterxml.jackson.core.jackson-core	② 无风险	auto_pro6_jdk1.9個년 訪日_1661234129	Java	2.9.7			2022-08-30 16:01:38	ANTER 1998

图表 184 第三方库管理

1.8.1概述

用于统计目前用户环境所有项目的第三方库情况,具体包括当前第三方库总数、所有使 用了第三方库的项目数、所有第三方库的漏洞数量。

<u>e</u>	2196 第三方库		225 涉及项目数	<u></u>	1058 演調政
		图表 18	35 第三方库概述		

1.8.2图表分析

图表分析由 3 部分组成:第三方库风险等级分布图、第三方库使用数量 TOP5、第三方 库版本状态分布图。

第三方库风险等级分布图:所有第三方库风险等级分布比例;

第三方库使用数量 Top5: 所有测试项目中使用次数最多的前五个第三方库;

第三方库版本状态分布图:所有第三方库版本状态分布比例。

风险等级分布图	第三方库破用Top5 第三方库额本状态分布图
88 #8	compage
- 57	antirantir
7.642	log4jog4
	tomcat-api
	0 30 60 90 120 150

图表 186 第三方库列表图表分析

1.8.3第三方库展示列表

第三方库列表默认按检测时间倒序排列(最新发现的第三方库展示在前面),列表内容 包括库名、风险等级、项目名称(关联多个项目时,点击右侧省略号可显示完全所有的项目 名称)、语言、当前版本号、最新版本号、开源许可证、最后更新时间及操作,其中库名可 按字典顺序排序,首次发现时间可正逆序排序。

注: 高、中、低危等级的第三方库均有漏洞,具体等级按其 CVE 漏洞的等级与数量而定, 提示等级的第三方库为无漏洞但非最新版本,无风险等级的第三方库为无漏洞且为最新版本。

有瀰洞的第三方库 语言 全部	等级全部						库名称/项目名称	Q 导出excel
库名	\$ 风险等级	项目名称	语言	当前版本号	最新版本号	开源许可证	最后更新时间 🕴	操作
org.apache.httpcomponents.httpclient	😲 中危	webgoat6.0.1 🔤	Java	4.5.3	4.5.13	Apache 2.0	2022-07-07 17:20:37	库信息丨详情
org.apache.httpcomponents.httpcore	◎ 提示	webgoat6.0.1 🔤	Java	4.4.6	4.4.15	Apache 2.0	2022-07-07 17:20:37	库信息 详情
com.fasterxml.jackson.core.jackson-annotations	0 提示	webgoat6.0.1 🔤	Java	2.9.7	2.13.3	Apache 2.0	2022-07-07 17:20:37	库信息丨详情
org.jboss.jandex	0 无风脸	webgoat6.0.1 🔤	Java	2.0.5.Final	-		2022-07-07 17:20:37	库信息 详情
xom	⑦ 无风险	webgoat6.0.1 🔤	Java	1.2.10	-	-	2022-07-07 17:20:37	库信思 详情
com.github.virtuald.curvesapi	⑦ 无风脸	yjfhosttttttttt关联 🔤	Java	1.04		-	2022-07-07 17:20:36	库信思 详情
org.apache.poi.poi-ooxml	😲 中危	yjfhosttttttttt关联 🔤	Java	3.17	5.2.2	Apache 2.0	2022-07-07 17:20:36	库信息 详情
batik-css	⑦ 无风险	yjfhosttttttttt关联 🔤	Java	1.8	·	-	2022-07-07 17:20:36	库信思丨详情
xml-apis-ext	⑦ 无风脸	webgoat6.0.1 🔤	Java	1.3.04			2022-07-07 17:20:36	库信思 详情
commons-httpclient.commons-httpclient	0 低危	webgoat6.0.1 🔤	Java	3.1	20020423		2022-07-07 17:20:36	库信息 详情
	共2196条 < 1	2 3 4 5 …	220 >	10条/页 >>	跳至]	Σ		

图表 187 第三方库列表

杭州默安科技有限公司

91

可根据第三方库风险等级、语言、第三方库是否有漏洞进行查看,可查看第三方库信息 和第三方库详情,可导出第三方库报告。

查看第三方库信息:点击操作-库信息,出现新页面,新页面为 maven 上该第三方库的页面,可以查看更多该第三方库的信息,还可以下载最新版本的第三方库。

MVN REPOSITORY		S	Search for groups, artifacts, categories		Search	1	Categories Popular Contact Us
ndexed Artifacts (13.4M)	Home »	org.springframe	work » spring-webmvc				Ad closed by Google
3449k		Spring We	b MVC				Stop seeing this ad
724k	spring	Spring Web M	vc				Why this ad2 D
0	License		Apache 2.0				Wity this du : to
2004 2019	Categor	ies	Web Frameworks				
pular Categories	Tags		spring mvc web framework				
pect Oriented	Used By		3,150 artifacts				
tor Frameworks							
oplication Metrics	Central	(152) Atlassi	an 3rd-P Old (1) Spring Plugins (45) Spring Lib M	M (1) Spring Milestones (2)	Geomajas (1)	Alfresco (7)	
uild Tools	Cambrid	ige (1)					
tecode Libraries			Version	Repository	Usages	Date	
mmand Line Parsers		5.1.4.RELEASE		Central	16	Jan, 2019	
iche Implementations		5.1.3.RELEASE		Central	370	Nov, 2018	
de Analyzers	5.1.x	5.1.2.RELEASE		Central	35	Oct, 2018	
llections		5.1.1.RELEASE		Central	353	Oct, 2018	
nfiguration Libraries		5.1.0.RELEASE		Central	27	Sep, 2018	
re Utilities		5.0.12.RELEAS	E	Central	24	Jan, 2019	
to and Time Utilities					16	New 2019	
te and Time Utilities pendency Injection		5.0.11.RELEAS	E	Central		1400, 2018	
te and Time Utilities pendency Injection 1bedded SQL Databases		5.0.11.RELEAS	e]	Central	31	Oct, 2018	
ate and Time Utilities ependency Injection nbedded SQL Databases IML Parsers		5.0.11.RELEAS 5.0.10.RELEAS 5.0.9.RELEASE	E E	Central Central Central	31 47	Oct, 2018 Sep, 2018	
ate and Time Utilities ependency Injection nbedded SQL Databases TML Parsers TTP Clients		5.0.11.RELEAS 5.0.10.RELEAS 5.0.9.RELEASE 5.0.8.RELEASE	e E)	Central Central Central Central	31 47 335	Oct, 2018 Sep, 2018 Jul, 2018	
late and Time Utilities lependency Injection mbedded SQL Databases TML Parsers TTP Clients O Utilities		5.0.11.RELEAS 5.0.10.RELEAS 5.0.9.RELEASE 5.0.8.RELEASE 5.0.7.RELEASE	ej	Central Central Central Central Central Central Central	31 47 335 66	Nov, 2018 Oct, 2018 Sep, 2018 Jul, 2018 Jun, 2018	Ad closed by Google

图表 188 第三方库信息

- 查看第三方库详情:点击操作-详情,跳转至第三方库详情页,该页面中可见该第三 方库的风险等级、漏洞数、关联项目数、关联项目名称、当前版本号、最新版本号、 开源许可证等自述信息,可知第三方库漏洞的漏洞名称、漏洞等级、公布时间、漏 洞描述和参考链接,可点击页面右侧关联项目名称跳转至该项目的管理页面查看信息。
- 第三方库信息在项目语言中能够支持识别的插桩语言有 Java、Golang、Node.js 和 Python。Java 和 Node.js 的第三方库会正常显示所有信息与风险, Golang 语言的第 三方库仅显示第三方库信息,不现实开源许可证或 CVE、CNVD、CNNVD 的漏洞。

◎ 组件信息:	Java / org.apache.httpcomponents.h	ttpclient / 4.5.3							
中危风险等级	٦	4.5.13 _{推荐版本}	\heartsuit	4.5.13 _{最新版本}	\odot	开源许可证信息 开源许可证: Apac 许可证风焓: ▲ 多 使用授权情况: 允许和	he 2.0 全 矿业集成目没有开源…	关联项目 	*
测测 编号 编号 书	漏洞名称					漏洞等级	公布时间	操作	·
4	CVE 2020 12056 CNVD 2021	24249 CNNUD 202010 27	2			A +4	2020 12 02	100 TT	

图表 189 第三方库详情



图表 190 第三方库漏洞详情

- 导出第三方库报告:点击"导出 EXCEL",出现弹框后输入报告名称,选择导出内容后点击"确定",生成的报告可以在报告管理页面下载。
 - 注:选择第三方库信息,导出的内容有库名、风险等级、项目名称、漏洞数、当前 版本号、最新版本号、开源许可证;

选择第三方库漏洞,导出的内容有漏洞名称、漏洞等级、第三方库名、第三方 库版本号、项目名称、公布时间。

输出报告	
报告名称: 内容选择:	 第三方库信息 第三方库漏洞信息
5	确定取消

图表 191 生成项目第三方库报告

1.9 插桩 AGENT (插桩类)

∮雳鉴·IA:	ST 58		☆ (金) (① 第三方岸 開始Agent (5:88)					yy i 🚅 i 🖨
前位置: 插桩Agent								
H柱Agent								
法 <u>118</u> 运行	中 暫停 南线 语言	全部	▼ 版本	合部 最新版 非最新版		各称/Agent地址/K	EY/标题	TrittAgent
名称	播艇Agent地址	key 😑	最近清求时间 🗘	安装时间 🗘	项目名称	标签	状态	操作
& —	192.168.20.134	5c647bd5-326 🚍	2022-08-31 16:53:32	2022-08-31 15:17:36	ProcessImpl	_	• 运行中	智停 详情
\$ —	127.0.0.1	c4a4e196-053 🔤	2022-08-31 11:54:50	2022-08-30 18:40:52	test_host_22	tag_bind	• 高統	
2 4	127.0.0.1	c992704c-294 🔤	2022-08-30 18:40:15	2022-08-30 18:37:15		c992704c-2944-bac2-2024-17a5234a5b47	。嬴浅	—— 删除 详情
\$ —	127.0.0.1	ad5d4655-8cc 🗖	2022-08-30 18:31:55	2022-08-30 18:30:04		ad5d4655-8ccf-2d9b-b5a6-1fd5690bd47d	• 南线	—— 删除 详情
۵-	192.168.20.94	16317054-1A1 🗖	2022-08-31 16:22:09	2022-08-30 18:17:30	php_groupbyleaktype6751719180755	default	• 南 线	—— 删除 详情
\$ —	127.0.0.1	31c705d1-7dc 🔜	2022-08-30 17:34:18	2022-08-30 17:33:15		31c705d1-7dce-f3f1-07ee-0e135ebaca56	• 陶纸	
∞—	192.168.180.56	CC043056-A67 🚍	2022-08-31 16:22:09	2022-08-30 17:24:07	php1-2 🔤	default	• 萬從	—— 翹除 洋橋
4 —	192.168.120.100	88ef986c-b3e 🔤	2022-08-30 17:24:56	2022-08-30 17:21:56	auto_pro7net播性项目_1661234130	88ef986c-b3ec-43af-2fc9-9db8eceb81c5	• 南线	—— 創除 洋情
£ —	172.17.0.5	b744a450-8c9 🔤	2022-08-31 16:53:32	2022-08-30 17:12:54	taintwebapp-20220830120955	taintwebapp_docker	• 运行中	暂停 —— 详情
<u> </u>	192.168.32.40	44е8с72с-сбс 🗖	2022-08-31 16:53:32	2022-08-30 17:09:00	jenkins_test	yjfhosttttttttt	• 运行中	留停 详博

图表 192 插桩 Agent 列表

插桩 Agent 页面提供对插桩 Agent 的下载和管理,当插桩 Agent 安装好后,会自动在该 页面生成一条记录,展示插桩 Agent 地址,key,最近请求时间,安装时间,项目名称,备注, 标签,状态,操作,同时在每一条 Agent 最前端还会通过图标展示当前 Agent 的语言类型。 支持 Agent 下载,支持根据 Agent 状态、语言和版本进行筛选,根据 Agent 地址,key,备注, 标签进行搜索。除此之外,还可设置离线 Agent 自动删除周期,默认为1周。可对 Agent 进 行批量启动、暂停和批量删除。

- 名称: Agent 复用时用来区分不同 Agent 之间的名称,自定义名称时需要在启动前加上 指定的-Dmoresec 参数。具体参数请参考帮助中心。
- 插桩 Agrnt 语言:每一条 Agent 记录都会在最前端展示语言所属图标
- 插桩 Agent 地址: 展示出 Agent 所安装的服务器地址;
- key:用于区分同一台机器上的 Agent,在 iast_agent.jar 中的 config.ini 中可以查看 该 Agent 的 key 值;
- 最近请求时间: Agent 最近一条请求上报的时间;
- 安装时间:展示 Agent 安装的时间;
- 项目名称:展示该 Agent 捕获的数据流所关联的项目名称;
- 备注:可自定义名称,区分 Agent;
- 标签: 取值自从 jvm 参数或者环境变量;
- 状态:分为离线,运行中,已暂停,已暂停状态为不上报数据流;

操作:操作分为开启,暂停,删除,详情。状态选择为离线,可对 Agent 进行批量启动、
 暂停和批量删除。

🗭 雳鉴・IAS	ST					(♠) 捕練∰Agent											· 🚅 · 🕞
曲射位置: ISREAgent > ISREAgent13物																	
播班Agent详情																	
*	运行中 Agentitit本		Agent地址: Agent Key: 最近清求时间: 安装时间: Agent版本:	192.168.2 5c647bd5 2022-08-: 2022-08-: 2.14.0	0.134 -3261-387 31 16:49:32 31 15:17:36	9-9faa-27aa	5178feb8			Age Age 確主 宿主	nt进程PID: nt绝对路径: 机CPU负载: 机内存占用:	2488 iast_agentjar = 0% 0%				Agenta	21) 2012 2012 2012 2014 2014 2014 2014 2014
应用详M API发现	漏洞列表	运油管理															
请求地址 localhost:8080						ह्य Se	/用名 ecurity_taint_	webapp_wa	u.				关联项目 → Process	Impl			

图表 193 Java 语言插桩 AGENT 详情

	🧭 雳鉴·IAST		●	yuying 🗉 😅 🖡 🖨
Agentității: 192,163,180.56 Agentității: 192,163,180.56 Agentității: 192,103,141 Agentității: Agentități: Agentități:	当前位置: 插桩Agent > 插桩Agenti半情 插桩Agenti半情			
成用時代 期時刊表 確求地述 算如目 192.168.180.56:9988 ・ golang host 繁合 ・ auto_pro@_golang語世語[1654152248 ・ auto_pro@_golang語世語[165465492 ・ auto_pro@_golang語世語[1654654990 ・ auto_pro@_golang語世語[1654650990	道 Agentitics	Agentibil: 192.168.180.56 Agent Key: 27(29986-1e69-663 最近實現時間: 2022-07-07 20:35:4 安誠時間: 2022-07-05 16:43:22 Agent版本: 0.1.1	Agent进程PD: 21968 a31633a6663 原用格径: hello 宿主町CPU负载 0% 宿主町JA存石田: 21%	Agentizās
演求地社 关联项目 192.168.180.56:9988 + golang host 聚合1 + golang host 聚合1 + audo gno6_golang/##世頃目_1654152248 + audo gno6_golang/##世頃目_16546522 + auto gno8_golang/##世頃目_1654654920	应用详情 漏洞列表			
	请求地址 192.168.180.56 .9 988		 実政毎日 golang host 聚合1 golang host 聚合 auto_pro8_golangi播校添員_1654152248 auto_pro8_golangi播校添員_1654654822 auto_pro8_golangi播校添員_1654660990 	

图表 194 Golang 语言插桩 AGENT 详情

🎲 雳鉴・IAST 📰		● □ FA ◎ □ Hent Makina Hintera Hintera		yy i 🚅 i 🕞				
出新位置: IBREAgent > IBREAgent评组								
播班Agenti详确								
NET 运行中 Agentit生	Agent地址: 192. Agent Key: 293 最近端字时间: 2022 安阔时间: 2022 Agent版字: 0.1.1	1683218 D1AF-4552-0847-8AAF-EC9547438E72 -08-31165192 -08-2518-4136	Agent温程PID: 24704 確正的CPU全部: 1% 確正的OPI在出现: 89%					
应用详纳 API发现 漏洞列表								
请求地址 localhost		<u>回</u> 师告 /	关助(第日 * avfo_pro7_net38(19888_1661234130 * azm-fra					

图表 195 . NET Framework 语言插桩 AGENT 详情

🇭 雳鉴・IAST						yuying I 😅 I 🕞
当前位置:插桩Agent > 插桩Agent	t详情	Agent地址: 1	192.168.32.18		Agent进程PIC	· 76
NET 离线 Agentitio	5	Agent Key: Fi 最近请求时间: 2 安装时间: 2 Agent版本:	10983D43-D184-0007-BD65-2B774G 2022-07-07 20:21:27 2022-06-30 14:10:26	F11261	宿主机CPU项i 宿主机内存占J	龙 0% 註 0%
成用锌荷 API发现 漏洞列的 请求地址 localhost	Ę		应用名 /		关联项目 + net core + net core	▲ 國際送≝+Host+丢弃 ////////////////////////////////////
					→ net core → net core → net core → net core → 相同host → net core → net core + net core + net core	期期定日 新合 Shhader的数 标记保证 参考 差并 五年 同時のt 20時 同時のt 20時 日日 一日 一日 一日 一日 一日 一日 一日 一日 一日

图表 196 .NET Core 语言插桩 AGENT 详情

🂅 雳 鉴・IAST 🐰 🗇 🖯	☆ □ ○ ○ ● □ ○ ○ ○ ○ □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	圓 yuying I 📫 I 😝
当前位置: 插班Agent > 插桩Agent详情		
插桩Agenti并情		
Agenti 高线 Agenti AgentitS: 最近到 友安勝到 Agentit	社: 192.168.180.57 メ434bba3-94cd-4198-8119-d32e61182b17 時時 2022-07-05 23x3x42 : 2022-07-05 19x4123 本:	Agent进程PD: 元 宿主机CPU负数 0% 宿主机内存占用: 0% 翻除
应用译情 漏洞列表		
遺式地社 192.168.180.57:8000	適用名 /	关联项目 → node+host +url 緊合 → node+host +url 鄂氏 → node#host +url 現限 → node∰/header313

杭州默安科技有限公司

Tel: (+86) 400-0571-211

96
图表 197 Node. js 语言插桩 AGENT 详情

デ	☆ ● ● ● FR ● ■ 第二方本 ■ ● ● ● ● FR ● ■ 第二方本 ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	🗐 yuying (🚅) 😝
<u>当前位置</u> : 插桩Agent > 插桩Agent详情		
播桩Agentu举情		
Age 高线 Age Agestitas 最近 安妮	MbbL: 192,168,180.57 KKy; 93b6672x6664x422b0511541a828569d Mp39; 2022-07-05 102428 Mp59; 2022-07-04 1754429	Agenti提醒PD: 元 電差机CPU负載 0% 電差机A存合用: 0%
2018年間 激励列表	(1964a)	
潮求地社 192.168.180.57.8004	政用名 /	关戦項目 - rongruo - pytho qingqiu - python 形合 - python 影響 - python意識(Sheader操設+host+url - 相同現意美術展開設) Host+調算の相合能調整合 - 自由文header傳動+調算設備



	C FR C FR C RATE REFERENCE MARK	yy I 😅 I 🏟
曲般位置。 据是Agent > 据是Agent译描 据是Agent译描		
Apertitiz 及行中 Apertitiz 和er	168,180,54 1686,56,677 - 4402-C02F-2C36D3C7352F 2-88-31 095047 2-88-30 1752407 0	AgentEIEF102 24078 電気的CPL2番目 19 電気的存在局 95%
<u> </u>		
傳來認証 localhoot	应用单 /	php1-2. ************************************

图表 199 PHP 语言插桩 Agent 详情

详情可显示支持的语言、Agent 状态、Agent 地址、Agentkey、最近请求时间、安装时间、 Agent 进程 PID、Agent 绝对路径(Java 语言 Agent)、应用路径(Golang 语言 Agent)、宿 主机 CPU 负载、宿主机内存占用、Agent 收到的所有请求的 host 以及 Agent 获取到的被测服 务器中的应用名(Java、Golang、.NET Framework、.NET Core、Node.js、Python、PHP 语 言 Agent)、Agent 所关联到的项目、Agent 自动发现的 api(Java、.NET Framework 和.NET Core 语言 Agent)、该 Agent 下的漏洞列表(Java、.NET Framework、.NET Core、Node.js、 Python、PHP 语言 Agent)、JVM 详情(Java 语言 Agent)、运维管理(Java 语言 Agent)、 日志下载(Java 语言 Agent)以及 agent 控制开关(Java 和 Golang 语言 Agent);

详情页面中,在线的 Agent 会显示版本号,当版本号不是最新版时,会标红展示。

Tel: (+86) 400-0571-211

Email: market_moresec.cn

Java 语言 agent 中的个人隐私开关用于解决将身份证号、密码、用户名、手机号等明文 保存到数据库、日志或者展示在响应中而泄露隐私的问题;请求收集开关用于主动插桩的流 量收集。

Java 语言的插桩 Agent 详情页面中,还会有 JVM 参数的 tab 页,用来展示 Agent 回传的 所在服务器的 JVM 参数。

插桩 AGENT 的安装方式见房鉴 IAST 帮助中心-插桩 Agent。

1.10 镜像扫描

1.10.1 镜像仓库

镜像仓库中记录了包括仓库地址、镜像总数、API 类型、危险镜像分布、上次扫描时间、 扫描状态等信息的镜像仓库列表。支持对仓库地址的搜索查找,支持批量地重新扫描和批量 删除。

ê.									
							Galifidade.	٩	#820/4
	命库地址	領像总数	API 美型	后脸镜像分布	上次扫描时间	扫描状态	操作		
	http://192.168.180.195	0	harbor api V1.x	0	2022-07-08 13:45:29	扫描完成	(年頃) 重新扫描 编辑	潮除	
	https://192.168.132.114/	7	harbor api V2.x	7	2022-07-08 11:45:29	扫描完成	译情 重新扫描 编辑	删除	
	http://192.168.20.66:380	1	harbor api V2.x		2022-07-05 12:38:26	扫描完成	(FO) (1997)]][[1] [1] [1] [1] [1] [1] [1] [1] [1] [898	
	https://harbor.moresec.cn	53	harbor api V1.x	53	2022-07-08 13:45:29	连續超时	(平衡) 重新扫描 编辑	删除	
	https://192.168.132.114/	6	harbor api V2.x	6	2022-07-04 15:57:29	扫描完成	(字傳) 重新扫描) 编辑)	部時	
	https://harbor.moresec.cn	48	harbor api V1.x	48	2022-07-08 09:45:29	连接超时	洋橋 重新扫描 编辑	删除	
	https://harbor.moresec.cn	47	harbor api V1.x	47	2022-07-04 21:00:22	归捕中	(#14) 110(12)) (644)	209	

图表 200 镜像仓库

- 点击"详情",进入镜像仓库详情。可查看镜像仓库基本信息、镜像风险趋势和镜像列表等信息。
- 点击"重新扫描",出现二次确认提示框,点击"确定"后该镜像仓库重新扫描,此时 扫描状态变为扫描中,且"重新扫描"、"编辑"和"删除"操作置灰不可点击。



Tel: (+86) 400-0571-211

Email: market_moresec.cn

图表 201 镜像仓库-重新扫描

点击"编辑"操作,可修改目录、排除目录、TAG、排除TAG,支持开启定时扫描,开启
 后可设置在上一次扫描结束时间后 6-72 小时自动进行扫描。

HOR	1: 销价归语 > 销价仓库					+ API 版本
tea						harbor api VI.x
						* 合厚地让
						http://192.168.180.195
	Amand	1000			i matumates	· 89
	计并记 上	确保已数	API 类型	際設備像分布	上次引播的间	as
	http://192.168.180.195	0	harbor api V1.x	-	2022-07-08 13:45:29	排除目录
						df
	https://192.168.132.114/	7	harbor api V2.x	1 () () () () () () () () () (2022-07-08 11:45:29	+ TAG
	http://192.168.20.66:380	1	harbor api V2.x		2022-07-05 12:38:26	899
						排IR TAG
	https://harbor.moresec.cn	53	harbor api V1.x	53	2022-07-08 13:45:29	bbb
	http:////02.158.522.514/	2	had as as 100 m		2022 07 04 15 57 20	* 用户名
	100527132.100.132.1149	0	Harbor aprives		2022-01-04 13.31 23	haha
	https://harbor.moresec.cn	48	harbor api V1.x	48	2022-07-08 16:45:29	* 武昭
	https://harbor.moresec.cn	47	harbor api V1.x	47	2022-07-04 21:00:22	♥ 开启定时扫描
		AN AVEC				每 6 小时扫描

图表 202 编辑镜像仓库

点击"删除",弹出二次确认提示框,点击"确定"后该镜像仓库即被删除,对应漏洞
 关联删除。



图表 203 镜像仓库-删除

支持新建仓库。需选择 API 版本,填写仓库地址、目录、排除目录、TAG、排除 TAG、用 户名和密码。支持开启定时扫描,开启后可设置在上一次扫描结束时间后 6-72 小时自动进行 扫描。

API 版本	
harbor api V1.x	~
仓库地址	
请输入	
目录	
支持正则匹配	
非除目录	
支持正则匹配	
TAG	
支持正则匹配	
非除TAG	
支持正则匹配	
用户名	
请输入	
密码	
请输入	
T ====+1-1#	
并启建的归拥	

图表 204 新建镜像仓库

点击"详情"操作,进入镜像仓库详情。可查看镜像仓库基本信息、镜像风险趋势和镜 像列表(包含镜像名称、TAG、漏洞数据、扫描结束时间、扫描状态),支持镜像风险等级 和扫描状态筛选,支持镜像列表的批量删除,支持镜像扫描报告导出。

	C) (i) (i) (i) (i) (i) (i) (i) (i) (i) (i		E E		yuying 🚅 🤅
自前位置 : 镜像扫描 > 镜像仓库 > https://harbor.moresec.cn					
https://harbor.moresec.cn					
编曲心体基本品品	更新的14 25 <u>来</u> 先:74	2022-07-1210:41:19 HR9AU 70 60 60 60 60 60 60 60 60 60 60 60 60 60	1839 	2022-07-09 2022-07-10	 現地・平地・低地・銀河・安全 2022-07-11 2022-07-12
操师级 请法师 • 林念 请法师 •				編像名称	Q 94838
續像各称	TAG	漏洞数据	扫描語年期計問	≎ 状态	攝作
harbor.moresec.cn/last/ls_web	2.12.0.0	8 5 2	2022-07-12 10:41:47	加速度	3年1期 1883年
harbor.moresec.cn/last/ls_user	2.12.0.0	5	2022-07-12 10:41:47	扫描完成	洋捕 目 翻訳
harbor.moresec.cn/last/ls_user2	2.12.0	5	2022-07-12 10:41:47	扫描完成	洋博 删除
harbor.moresec.cn/last/ls_web	2.12.0	10 5 2	2022-07-12 10:41:47	扫描完成	洋橋 翻除
harbor.moresec.cn/last/ls_task	2.12.0.0	5	2022-07-12 10:41:46	扫描完成	洋橋(副時
harbor.moresec.cn/last/is_task	2.12.0.0-test.1	2	2022-07-12 10:41:46	扫描完成	洋橋 删除

图表 205 镜像仓库详情

- 镜像仓库基本信息:可直观观察到不同漏洞等级的占比以及具体的数量。同时,可看到 最新更新时间;
- 镜像风险趋势:支持查看近七天内不同漏洞等级的镜像风险趋势;
- 批量删除:支持批量删除镜像。点击"批量删除"后,弹出二次确认提示框,点击"确定"后该镜像仓库即被删除,对应漏洞关联删除;

		0 2022-07-06	2022-07-07 2022-07-08 2022	-07-09 2022-07-10 2	022-07-11 2022-07-12
R12914 (1933) • 176 (1933) •	① 提示	111111			
領導名称	TAG	12510118F /	扫描结束时间	0 秋志	操作
harbor.moresec.cn/iast/is_web	2.12.0.0	46, 779	2022-07-12 10:41:47	扫描完成	洋博 删除
harbor.moresec.cn/last/is_user	2.12.0.0	5	2022-07-12 10:41:47	扫描完成	详博 删除
harbor.moresec.cn/last/is_user2	2.12.0	5	2022-07-12 10:41:47	扫描完成	洋橋 副除
harbor:moresec.cn/last/ls_web	2.12.0	10 5 2	2022-07-12 10:41:47	扫描完成	iff fig. () HEIDE
harbor:moresec.cn/last/is_task	2.12.0.0	5	2022-07-12 10:41:46	扫描完成	洋橋 細胞
harbor.moresec.cn/last/ls_task	2.12.0.0-test.1	2	2022-07-12 10:41:46	扫描完成	洋橋 删除
harbor.moresec.cn/last/is_task	2.12.0.0-zh	2	2022-07-12 10:41:46	扫描宛成	洋橋 創時
harbor.moresec.cn/iast/is_user	2.12.0	5	2022-07-12 10:41:46	扫描完成	详惯 目 删除
harbormoresec.cn/last/is_sync	2.12.0.0	2	2022-07-12 10:41:46	扫描完成	洋橋 删除
harbor.moresec.cn/last/is_sysconf	2.12.0.0	5	2022-07-12 10:41:46	扫描完成	详情 删除
○ 全造 単页全选 批量制除					
	共74条 < 1 2 3 4	5 … 8 > 10条/页	× 執至 页		

图表 206 镜像仓库-批量删除

 镜像详情:点击镜像列表的"详情"操作后,进入镜像详情页面。在镜像详情页面中, 可查看到镜像大小、漏洞数据、Digest、TAG、扫描结束时间信息。除此之外,支持看到 由漏洞编号、漏洞名称、影响组件、漏洞状态组成的镜像漏洞列表。

镜像大小: 197.4	2MB	潮洞政語: 8 5 2	Digest:	sha256:507059bb322238695676bde64 936430fc34	:69e8e7fc10d6b3fa0	6958cd5b62c8
TAG: 2.12.0	.0	扫描結束时间: 2022-07-12 10:41:47				
秋彩信の 组件包信	● 機像分层信息					
漏洞等级 请选择	▼ 漏洞状态 请选择 ▼				潮的病母	Q
混丙编号	履同名称			影响组件	濃雨状态	操作
© CVE-2022-2257	6 curl: OAUTH2 bearer bypass in connection re-use			libcurl	未忽略	详情丨忽略
© CVE-2022-2777	5 curl: auth/cookie leak on redirect			libcuri	未忽略	详情 忽略
O CVE-2022-2257	6 curl: OAUTH2 bearer bypass in connection re-use			curl	未忽略	详情丨忽略
O CVE-2022-2777	δ curl: auth/cookie leak on redirect			curl	未忽略	详情 忽略
0 CVE-2022-2777	5 curl: bad local IPv6 connection reuse			curl	未忽略	详情丨忽略
0 CVE-2022-2740	5 FreeType: Segementation Fault			freetype	未忽略	详情丨忽略
© CVE-2022-2740	5 Freetype: Segmentation violation			freetype	未忽略	详情丨忽略
© CVE-2022-2740	4 FreeType: Buffer Overflow			freetype	未忽略	详情丨忽略
OCVE-2022-1271	gzip: arbitrary-file-write vulnerability			xz-libs	未忽略	详情丨忽略
0 CVE-2022-2982	4 libxml2: integer overflows in xmlBuf and xmlBuffer lead	to out-of-bounds write		libxml2	未忽略	详情丨忽略

共15条 < 1 2 > 10条/页 × 跳至 页

图表 207 镜像详情

镜像详情页面支持通过选择漏洞等级和漏洞状态筛选漏洞,支持通过漏洞编号搜索漏洞。 点击"详情",右侧弹出该漏洞的漏洞详情信息。

	() () () () () () () () () () () () () (圓 殿中心	× CVE-2022-22576
当前位置: 镜像扫描 > 镜像仓库 > https://harbor.moresec.cn > harbor.moresec.cn/last/	is_web		(2) 漏洞描述
harbor.moresec.cn/iast/is_web			4 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
· · · · · · · · · · · · · · · · · · ·	氟间数据: 8 5 2	Digest: sha2 9364	● 修复方案
TAG: 2.12.0.0	扫描结束时间: 2022-07-12 10:41:47		
			参考性 按考 使
■ 2011年2011年8日 第1日年2011年8日 業務等級 第10555 ・ 業務状态 約3555 ・			https://curl.se/docs/CVE-2022-22576.html https://cve.mitre.org/cgl-bin/cvenamec.gi?name=CVE-2022-22576 https://hackerone.com/reports/1526328 https://security.netapp.com/advisory/intap-20220609-0008/
還用編号 通用名称			https://ubuntu.com/secunity/notices/Usix-5597-1
CVE-2022-22576 curl: OAUTH2 bearer bypass in connection re-use			
CVE-2022-27776 curl: auth/cookie leak on redirect			
CVE-2022-22576 curl: OAUTH2 bearer bypass in connection re-use			
CVE-2022-27776 curl: auth/cookie leak on redirect			
CVE-2022-27775 curl: bad local IPv6 connection reuse			
CVE-2022-27405 FreeType: Segementation Fault			
CVE-2022-27406 Freetype: Segmentation violation			
CVE-2022-27404 FreeType: Buffer Overflow			

图表 208 镜像详情-漏洞详情

点击"忽略",出现二次确认的弹框,点击"确定"后,出现"忽略成功"的提示,漏 洞置底显示,忽略后的漏洞可点击"恢复"取消忽略。



图表 209 镜像详情-忽略漏洞

点击可切换 tab 页查看镜像的组件包信息详情和镜像分层信息。

1.10.2 流水线任务

流水线任务中记录了包括任务名称、jenkins 任务地址、构建次数和风险概览的流水线任 务列表。支持通过风险等级和任务名称筛选任务。

雳鉴·IAST		u (③) [] [] [] [] [] [] [] [] [] [] [] [] []	る (③) 管理 系统配置			yuying I 🚅 I
位置: 續像扫描 > 流水线任务						
线任务						🖸 播件使用指南 📋 坐 播件
\$\$						任务名称 Q 合并任
任务名称	jenkins 任务地址			构建次数	风险概范	摄作
• 🔹 xzm	http://192.168.120.10:9999/job/xzm/			13	24 4	把1 99
						请输入 Build_number 【
Bulld_number	创场版中打印	÷	执行时间		機像扫描結果	操作
19	2022-07-04 20:23:50		20s		24 4	详细
29	2022-07-04 20:20:56		68s		6	详情
28	2022-07-04 20:19:42		0s		0	详惯
15	2022-06-30 18:05:29		43s		6	洋間
4	2022-06-30 17:41:45		0s		0	洋橋
14	2022-06-30 17:33:53		142s		0	详惯
3	2022-06-30 17:02:54		0s		0	详制
15	2022-06-30 16:17:09		30s			法情

图表 210 流水线任务

点击"合并任务"后,须选择主任务和被合并任务,点击确定后,被合并任务成功合并 到主任务里。

任怎会并后不可能	S合并后不可撤销,请谨慎操作				
125910771071-918	USE) PERENTE				
* 主任务					
				\vee	
* 被合并任务					
			v] [-	+	

图表 211 流水线任务-合并任务

点击"删除"操作,出现确定删除的提示框,点击"删除"后,该流水线任务即可被删

除。

0				
U :	是否删除	新生务 xzm。	2 ?	
ł	删除后需	要重新运行对	」应 Jenkins 项	i目恢复。
		町治		
		4人 /日	1009 Par	

图表 212 流水线任务-删除任务

点击"详情",进入构建详情页面。在构建详情页面中,顶部可看到镜像数量、风险概览、 执行时长和创建时间信息。左侧显示镜像列表,可通过 TAG 和镜像名称进行搜索。右侧显示 镜像名称、镜像大小、Digest、TAG、扫描结束时间信息。同时,可查看漏洞列表,支持通过 漏洞等级、漏洞状态和漏洞编号进行搜索。

勞雳鉴·IAST		① ① ③ ③ ③ ③ □						iying 🚅 🕞
当前位置: 镜像扫描 > 流水线任务 > 档	建洋情							
Build number: 19								
· · · · · · · · · · · · · · · · · · ·		风险概范: 24	4		执行时长: 20s			
创趣时间: 2022-07-04 20:23:50								
TAG/機能高額	摄像名称: 127.0.0.1:8000/m	is_auth	镜像大小: 22.22MB		Digest: sha2 e005	56:13ceebb608347a 2fdf823746e9f	497ac8d7af6ce4a5e4	44426068c953ea12
• 127.0.0.1:8000/ms_a	TAG: 3.0.2		扫描结束时间: 2022-	07-04 20:24:08				
3.0.2	20760 12(45/2/8	情像分层信息						
• 127.0.0.1:8000/is_sys	建同等 极 计选择	 通用状态 消流译 • 					派羽编号	Q
2.12.000	漏洞编号	漏洞名称				影响组件	漏洞状态	操作
	O CVE-2021-42381	busybox: use-after-free in awk apple the hash_init()	et leads to denial of service and	possibly code execution whe	en processing a crafted awk pattern in	busybox	未忽略	详情丨忽略
	OVE-2021-42380	busybox: use-after-free in awk apple the cirvar()	et leads to denial of service and	possibly code execution whe	en processing a crafted awk pattern in	busybox	未忽略	详情 忽略
	O CVE-2021-42379	busybox: use-after-free in awk apple the next_input_file()	et leads to denial of service and	possibly code execution whe	en processing a crafted awk pattern in	busybox	未忽略	详情丨忽略
	OVE-2021-42382	busybox: use-after-free in awk apple the getvar_s()	et leads to denial of service and	possibly code execution whe	en processing a crafted awk pattern in	busybox	未忽略	详情丨忽略
	O CVE-2021-42383	busybox: use-after-free in awk apple the evaluate()	et leads to denial of service and	possibly code execution whe	en processing a crafted awk pattern in	busybox	未忽略	详情 忽略

图表 213 流水线任务-构建详情

点击"详情",右侧出现漏洞详情弹窗,包含漏洞描述、修复方案、参考链接等信息。

Build number: 19					× CVE-2021-42381
鏡像数量:2		风险概范:	24 4	执行时长: 20s	[] 湯河描述
別離时间: 2022-07-04 20:23:50					
TAG/投發名称	镜像名称: 127.0.0.1:8000/	ms_auth	镜像大小: 22.22MB	c	修复方案
• 127.0.0.1:8000/ms_a	TAG: 3.0.2		扫描结束时间: 2022-07-04 20:24:08		
3.0.2	福同位則 絕件包信息	積像分层信息			https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42381
• 127.0.0.1:8000/is_sys 2.12.0.0	進同等级 请选择	▼ 蕭同状态 诱选择	v		https://jtrog.com/biog/unboxing-busybox-14-new-vulnerabilities- uncovered-by-claroty-and-jfrog/ https://lists.fedoraproject.org/archives/list/package-
	漏洞编号	漏洞名称			announce@ists.tedoraproject.org/message/61210/kB+1/GBMQ111W DSOAIQGP7WCPGV/ https://ists.fedoraproject.org/archives/list/package-
	CVE-2021-42381	busybox: use-after-free in aw the hash_init()	k applet leads to denial of service and possibly code e	xecution when processing a crafted awk	amounceenists.teobraproject.org/message/00x000wb1+w01v0- RKHZR34UMEHQBX5/ https://security.netapp.com/advisory/ntap-20211223-0002/ https://security.netapp.com/advisory/ntap-20211223-0002/
	O CVE-2021-42380	busybox: use-after-free in awl the clrvar()	k applet leads to denial of service and possibly code e	xecution when processing a crafted awk	ingegradamateungeeunghousearoan arrait
	OCVE-2021-42379	busybox: use-after-free in aw the next_input_file()	k applet leads to denial of service and possibly code et	xecution when processing a crafted awk	
	OCVE-2021-42382	busybox: use-after-free in awk the getvar_s()	k applet leads to denial of service and possibly code e:	xecution when processing a crafted awk	
	© CVE-2021-42383	busybox: use-after-free in aw the evaluate()	k applet leads to denial of service and possibly code e:	xecution when processing a crafted awk	
	O CVE-2021-42374	busybox: out-of-bounds read decompressed	in unizma applet leads to information leak and denial	of service when crafted LZMA-compres-	
	O CVE-2021-42384	busybox: use-after-free in aw the handle_special()	k applet leads to denial of service and possibly code e	xecution when processing a crafted awk	

图表 214 流水线任务-漏洞详情

点击"忽略",出现二次确定弹窗,点击"确定"后,出现"忽略成功"的提示,漏洞 置底显示,忽略后的漏洞可点击"恢复"取消忽略。



图表 215 流水线任务-忽略漏洞

点击可切换 tab 页查看镜像的组件包信息详情和镜像分层信息。

1.11 报告管理

1.11.1 报告列表

报告管理可以按照项目生成报告:选择关联的项目、输入报告名称、选择报告维度(漏洞的聚合展示维度,分为漏洞类型维度和URL维度)、选择报告日期(该时间段内的测试情况,可以从项目周期、本月、本周、今天四个维度快捷选择),输入完成后,点击'生成报告',在列表中会生成相应的报告。

根据项目进行选择生成报告时,可以选择多个项目,选择的项目名称会显示到筛选框内, 点击删除符号或者再次点击下拉框内项目名称可以取消选择项目。

🎲 雳鉴・IAST 🐰 🎯							
当前位置: 报告管理							
报告管理	生成报告						
自动清理 开 🔿 保留范围:近7天 🏚	• 关联项目	请选择关联项目					(生成报告)
报告名称	 报告目标 	请详细输入报告名称			创建日期	生成状态	操作
	* 报告维度 🔵 项目:java-webh	请详细输入报告名称			2022-08-30 15:31:29	 生成完成 	下载 在线查看 删除
ddd	 报告日期 项目:auto pro4 	开始日期	→ 結束日期	•	2022-08-30 15:30:27	 生成完成 	下載 在线查看 删除
项目id:236-报告-sqh1	项目:taintwebar	取消	确定		2022-08-30 12:10:57	• 生成完成	下载 在线查看 删除
项目id:235-报告-jiza	项目:taintwebapp-zuzzuosurzu	017(55921835)	2022-08-29~2022	-08-30	2022-08-30 12:01:22	• 生成完成	下载丨在线查看丨删除
192.168.132.114-1661776487463			_		2022-08-29 20:34:47	• 生成宛成	下载 删除
project_smoke_test-灑洞报告-1661776485552	漏洞导出		—		2022-08-29 20:34:46	• 生成宛成	下载 在线查看 删除
third_parts_1661776478	项目: auto_pro4_非鉴权代理项目_	_1661234128 的第三方库	_		2022-08-29 20:34:46	• 生成完成	下载! (删除
192.168.132.114-1661776458602			—		2022-08-29 20:34:19	• 生成完成	下载 删除
dadad	所有项目第三方库				2022-08-29 20:09:28	• 生成完成	下载
dddd	所有项目第三方库				2022-08-29 20:09:18	• 生成完成	下载
	共96条	< 1 2 3 4 5	10 > 10条/页 > 跳3	e 📃 🕱			

图表 216 选择报告目标

选择一个关联项目时,展示更多选项按钮,点击更多选项后显示请求地址,报告模板,漏洞信息,第三方库信息选项。请求地址可以对项目中所有的请求地址做筛选,只到处选中地址所对应的信息。报告模板可以选择使用 PCIDSS、GDPR、OWASP TOP 10 或者不使用,当不实用模版时,可以选择想要导出的漏洞类型。漏洞信息和第三方库信息可以通

过勾选决定导出报告中所包含的内容。

- ▶ 开启自动清理报告功能。开启后,保留范围可选:近7天,近14天,近30天,并删除 该时间范围外的报告。
- ▶ 报告维度选择默认为漏洞类型,选择后将相同漏洞类型的 URL 展示在一起;报告维度选择 URL,选择后将相同 URL 的漏洞类型展示在一起;
- 注:报告列表按照生成时间倒序排列(最新生成报告展示在前面),列表内容包括报告 名称、报告目标、报告日期、报告创建时间、生成状态及操作。(多个项目的报告目标 需要在操作内点击"在线查看",在报告信息内的报告目标查看)

🦻 雳 鉴・IAST 🐰 🗇	日 ① ④ ④ ① R ④ 日 現物監理 第三方庫 請使Agent 後後日語 第四面理 系句監理 系統配置 報知				уу I 🚅 I 🕞
当前位置:报告管理					
报告管理					
自动清理 开 保留范围:近7天 🔅				报告名称	(生成报告)
报告名称	报告目标	报告日期	创建日期	生成状态	操作
ш	项目:java-webhook(摘柱模式)	2022-08-24~2022-08-30	2022-08-30 15:31:29	• 生成完成	下载 在线查看 删除
ddd	项目:auto_pro4_非鉴权代理项目_1661234128(非鉴权代理模式)	2022-08-23~2022-08-30	2022-08-30 15:30:27	• 生成完成	下载 在线查看 删除
项目Id:236-报告-sqh1	项目:taintwebapp-20220830120955(描柱模式)	2022-08-29~2022-08-30	2022-08-30 12:10:57	• 生成完成	下载 在线查看 删除
项目Id:235-报音-Jiza	项目:taintwebapp-20220830120017(調性模式)	2022-08-29~2022-08-30	2022-08-30 12:01:22	• 生成完成	下载 在线查看 删除
192.168.132.114-1661776487463		-	2022-08-29 20:34:47	• 生成完成	下载 删除
project_smoke_test-漏洞报告-1661776485552	灑闷号出		2022-08-29 20:34:46	• 生成完成	下载 在线查看 删除
third_parts_1661776478	项目: auto_pro4_非鉴权代理项目_1661234128 的第三方库	_	2022-08-29 20:34:46	• 生成完成	下载 删除
192.168.132.114-1661776458602			2022-08-29 20:34:19	• 生成完成	下载 删除
dadad	所有项目第三方库	_	2022-08-29 20:09:28	• 生成完成	下载 删除
dddd	所有项目第三方库	_	2022-08-29 20:09:18	• 生成完成	下载
	共96条 < 1 2 3 4 5 … 10 >	10 条/页 > 就至 页			

图表 217 报告管理

▶ 点击下载之后可以选择格式: PDF/WORD/EXCEL/JSON (EXCEL 格式中仅包含漏洞信息)。

下载报告	
报告名称 sktest	1
报告格式 PDF	× .
	- 朔 定

图表 218 报告下载

1.11.2 检测报告

PDF/WORD 格式报告由六部分组成:报告信息、综述、图表分析、漏洞列表、漏洞详情、

参考标准。

- ▶ 报告信息:包括名称、编号、日期、目标、类型、生成时间作为展示;
- 综述:展示报告的安全评分及安全等级,包括项目名称、项目模式、项目模板、创建时间、测试人员、漏洞数(高/中/低/提示数),若为插桩模式项目报告还包含第三方库数 (高/中/低/提示/无风险);若导出的是单个项目,则在报告中显示项目归属人和项目 成员。
- 图表分析:包括漏洞趋势、漏洞修复统计、漏洞类型分布图、漏洞等级分布图,若为插 桩模式项目报告还包含第三方库风险等级分布图、第三方库版本状态分布图;
- 漏洞列表:若选择导出报告的维度为漏洞类型,分类展示该报告中的漏洞类型,并标识漏洞地址、发现时间及修复状态;若选择导出报告的维度为URL,分类展示该报告中的漏洞地址,并标识漏洞类型、安全等级、发现时间及修复状态;
- ▶ 漏洞详情:分类展示该报告中的风险项,并对其漏洞进行展示及描述等详细信息;
- 第三方库列表及详情: 仅插桩模式项目报告包含此项,展示了第三方库信息及第三方库 漏洞信息;
- ▶ 参考标准:报告末尾进行漏洞等级,第三方库等级及项目安全等级的说明。

EXCEL 格式报告由十六部分组成:项目名称、项目危险等级、项目模式、漏洞类型、漏 洞风险等级、漏洞地址、漏洞参数、发现时间、测试人员、状态、攻击细节、漏洞描述、漏 洞危害、修复建议、测试请求、数据流信息,其中数据流信息仅插桩模式项目的报告包含。 项目代码安全检测报告

报告信息

报告名称: 项目id:490-报告-5as7 报告编号: LJ-2021-04-13-700333 报告日期: 2021-04-12 00:00:00---2021-04-19 23:59:59 报告类型: 单个项目报告 牛成时间: 2021-04-13 15:46:09

杭州默安科技有限公司

1.综述





项目名称:	benchmark-1618300048(插桩模式)
创建时间:	2021-04-13 15:46:01
测试人员:	0
项目归属人:	admin
项目成员:	
漏洞数:	2 (高危:0 中危:0 低危:1 提示:1)
第三方库数:	21 (高危: 4 中危: 1 低危: 1 提示: 10 无风险: 5)

2.图表分析



漏洞修复统	ìt			
漏洞等级	漏洞数	已修复数	待修复数	修复占比
高危	0	0	0	0.00
中危	0	0	0	0.00
低危	1	0	1	0.00
提示	1	0	1	0.00
总计	2	0	2	0.00





杭州默安科技有限公司

108

	必钥健编码	(漏洞数:1)					♥ 漏洞等级:低
导	漏洞地	址				发现时间	修复状态
	192.16	8.201.100:30002/bench	mark/crypto-00/E	enchmarkTest000	19	2021-04-13 15:46:09	未修复
不安全	全的加密(漏洞数:1)					● 漏洞等级:提
导	漏洞地	址				发现时间	修复状态
	192.16	8.201.100:30002/bench	mark/crypto-00/E	enchmarkTest000	19	2021-04-13 15:46:08	3 未修复
漏洞详情	青						
加密和	泌钥硬编码	(漏洞数: 1)					👽 漏洞等级:低
漏洞	描述						
当	开发者将密 时如果软件	钥保存在源代码中,在f 在外流传,攻击者即可道	、码投入使用之后 通过反编译等手段	除非对软件进行 直接获取密钥等相:	修补,否则将无法 关信息。	更改密钥。	
漏洞	危害						
п	岩老无注修						
π.	X H /L/APS	以密钥, 同时以击者可以	人通过反编译获取	到硬编码的密钥。			
π .	74 201	· 风密钥,回时以击者可以	《通过反编译获取	到硬编码的密钥。			
修复	建议	(Q 密 研, 回 时 以 古 者 可 b	人通过反编译获取:	到硬编码的密钥。			
开. 修复 不:	建议 建议 将密钥硬编	^成 做研, 回时 攻击者 可比 码于程序中。	认通过反编译获取 :	到硬编码的密钥。			
开. 修复 不:	建议将密钥硬编	^成 盆钮,回时攻击者可比 码于程序中。	认通过反编译获取 :	到硬编码的密钥。			
开. 修复 不: 风服	建议 将密钥硬编 险地址:192	成	《通过反编译获取 nchmark/crypto	创硬编码的密钥。 -00/BenchmarkTe	*st00019		
 ポ. 修复 不: 风服 攻击 	建议 将密钥硬编 ^{险地址} :192	IX	↓通过反编译获取 nchmark/crypto 文件DESKeySpe Iden];	创硬编码的密钥。 -00/BenchmarkTe c.java(类:javax.cry	est00019 pto.spec.DESKey:	Spec)中,	
 ボ. 修复 不: 风限 攻击 请対 	建议 建议 将密钥硬编 <u>逾地址</u> :192 击详情 求	成金額,回時以広者可以 码于程序中。 2.168.201.100:30002/be 开发者将密钥硬编码于 private byte[] key= [hic POST /benchmark/cry content-length: 37 postman-token: c609i User-Agent: Postmani host: 192.168.201.100 content-type: text/pla connection: keep-alive cache-control: no-cac accept-encoding: gzig accept: */*	↓通过反编译获取 hchmark/crypto 文件DESKeySpe iden]; pto-00/Benchma 8c75-a72e-4db5- Runtime/7.26.2 :30002 n a he he , deflate, br	创硬编码的密钥。 -00/BenchmarkTe c.java(类:javax.cry rkTest00019 HTTF ac10-911c7dc9bd	est00019 pto.spec.DESKey 7/1.1 31	Spec)中,	
 ボ・ 修复 不: 风 风 丸 す す ボ 	建议 建议 将密钥硬编 造地址:192 击详情 求 全的加密() 描述	成金額,回時以広者可以 码于程序中。 2.168.201.100:30002/be 开发者将密钥硬编码于 private byte[] key= [hic POST /benchmark/cry content-length: 37 postman-token: c609i User-Agent: Postman host: 192.168.201.100 content-type: text/pla connection: keep-alive cache-control: no-cac accept-encoding: gzig accept: */*	↓通过反编译获取 hchmark/crypto 文件DESKeySpe iden]; pto-00/Benchma 3c75-a72e-4db5- Runtime/7.26.2 :30002 n a he , deflate, br	创硬编码的密钥。 •00/BenchmarkTe c.java(类:javax.cry rkTest00019 HTTF ac10-911c7dc9bd	est00019 pto.spec.DESKey 1/1.1 31	Spec)中,	〕漏洞等级:提示

e	修复建议		
	建议使用安全	的加密算法,例如AES-256、SHA-512	
1	风险地址:192	2.168.201.100:30002/benchmark/crypto-00/BenchmarkTest00019	
	攻击详情	应用在:BenchmarkTest00019.java:52处调用了不安全的加密算法: javax.crypto.Cipher javax.crypto.Cipher.getInstance(java.lang.String)	
	请求	POST /benchmark/crypto-00/BenchmarkTest00019 HTTP/1.1 content-length: 37 postman-token: c6098c75-a72e-4db5-ac10-911c7dc9bd31 User-Agent: PostmanRuntime/7.26.2 host: 192.168.201.100:30002 content-type: text/plain connection: keep-alive cache-control: no-cache accept-encoding: gzip, deflate, br accept: */*	
5.第3	三方库列表及详情		
-	org.apache.tomc	at.tomcat-juli(漏洞数:0)	🕑 安全等级:提示
	当前版木 号・ 05	34	
	コェリル(本ら・ 0.5) 見新版本品・ 10	0.0 M2	
	取利加水 与・10.	0.0-103	

1618300048"]

- org.apache.tomcat.tomcat-jasper-el (漏洞数: 0)

关联项目: ["dubbo_test1","is_filter","chenlu_test2","benchmark-

关联项目: ["dubbo_test1","is_filter","chenlu_test2","benchmark-

- com.sun.jersey.jersey-servlet (漏洞数: 0)

开源许可证: Apache 2.0

1618300048"]

当前版本号: 8.5.34 最新版本号: 10.0.0-M5 开源许可证: Apache 2.0

当前版本号: 1.19.4 最新版本号: 1.19.4 开源许可证: CDDL 1.1 关联项目: ["is_filter","benchmarkd","Bbenchmark","peload","repload","bench_mark","benchmark_tag","benchmark_tag12","bench_markoff","java_baihe","benchmark-1618300048"]

 $d"," chenlu_test_active1"," benchmark_active"," benchmark_active2"," chenlu_test1"," chenlu_test5"," chenlu_test3"," chenlu_29_taint"," benchmark_active2"," chenlu_test1"," chenlu_test3"," chenlu_29_taint"," benchmark_active2"," chenlu_test1"," chenlu_test3"," chenlu_$

 $d","chenlu_test_active1","benchmark_active","benchmark_active2","chenlu_test1","chenlu_test5","chenlu_test3","chenlu_test2.9_1","chenlu_test3","chenlu_tes$

Tel: (+86) 400-0571-211

Email: market_moresec.cn

安全等级:提示
 提示

安全等级:无风险

6.参考标准

漏洞等级

漏洞等级	危害说明
高危	攻击者可以远程操作系统文件、读写后台数据库、执行任意命令或进行远程拒绝服务供。
中危	攻击者可以利用WBE网站攻击其他用户,读取系统文件或后台数据库。
低危	攻击者可以获取某些系统、文件的信息或冒用身份。
	攻击者可以获取到系统的或应用的一些提示性信息。

第三方库等级

高危	攻击者可通过CVE漏洞进行远程命令执行、读写数据库、操作系统文件或拒绝服务攻击。
中危	攻击者可通过CVE漏洞攻击其他用户、修改数据信息、读取任意文件。
低危	攻击者可通过CVE漏洞攻击系统获取敏感信息、进行钓鱼攻击。
	第三方库为非最新版导致可能有潜在的安全隐患。

项目等级

项目等级	对应评分	说明
高危	评分<60	暂无
中危	60<评分<=90	暂无
低危	90<评分<100	暂无

图表 219 检测报告

1.12 帐号管理

1.12.1 用户管理

用户管理页面:可以看到当前登录账户的信息,并可以编辑资料(可修改姓名、角色、 部门、邮箱、电话)、修改密码。

测试用户可以申请角色升级为项目经理,管理员权限可以管理所有的账号,项目经理和 安全人员可以管理自己的账号并查看所有账号的信息。

🍠 雳鉴・IA:	ST							EA KSER						yy I 🚅 I 🕞
当前位置: 账号管理 >	用户管理													
NPGB	用户名: 姓名: 联系电话:	уу Үу1@123 ——	4			用户角色。	: 管理!	8			00007/8): #X7:	2022-08-24 11:42:28 RK\ATEN]		《编辑资料
用户角色全部用户	•	所履部门	全部部门	44-77	-			ncaaa	III Chefrig	21.0777088	NENG	Automatic A	用户名/姓名/邮箱/电	活 Q 新潮用户
HP-6				8940	EN 1			用户测型	PH2P-HEPHE	WAEDR	联系地语	ERSWER3161	MELT MERCH JINJ	SRTF
xh_ xmjl					默认部门			管理员	-	xzm(ldap)	_	2022-08-31 11:03:03	_	皖赣资料 ——— ——
honeypot					联认部门			管理员	_	xzm(ldap)	_	2022-08-31 11:03:03		編攝資料
tong cheng					默认部门			管理员	123@qq.com	xzm(ldap)	13325411111	2022-08-31 11:03:03	-	编编资料
xzmtest1 xzmtest1					默认部门			管理员	-	xzm(ldap)	-	2022-08-31 11:03:03		编编资料
admin					默认部门			管理员	-	xzm(ldap)	-	2022-08-31 11:03:03	-	编编资料
xlazhangmin				夏彰敏	xzm-ladp			管理员		xzm(ldap)		2022-08-31 11:03:03	2022-08-31 11:03:21	编辑资料
hj					默认部门			管理员	-	xzm(ldap)	_	2022-08-31 11:03:03	_	编辑资料
user1					默认部门			管理员	-	xzm(ldap)	-	2022-08-31 11:03:03	-	编辑资料
test3					默认部门			管理员	-	xzm(ldap)	16666666661	2022-08-31 11:03:03	_	编编资料
-														

图表 220 用户管理

点击"编辑资料",进入编辑资料页面,可以修改部门、邮箱、电话。并且控制该用户
 是否允许登录以及使用鉴权代理录入流量。点'确定'即可修改成功。
 允许登录:控制用户是否可以登录产品或使用 api。

允许鉴权代理:控制用户是否可以使用此账户进行鉴权代理的录入。

用户名	chenyi		
认证源	Local		
姓名	支持中英文、数字及符号		
*角色	管理员	V	
* 部门	默认部门	V	【新增部门】
邮箱	请输入邮箱		
电话	输入手机号码或座机		
允许登录 🕜	允许 金许鉴权代理 ② () ×	闭

图表 221 编辑资料

● 点击"修改密码",进入修改密码页面,新密码和确认新密码保持一致,输入管理员账

杭州默安科技有限公司

号的密码并输入正确的验证码后点击"确定"即可修改成功。需要注意的是通过 LDAP

同步过来的账号无法修改密码。

用户名	chenyi	
新密码	輸入新密码	ø
确认新密码	再次输入新密码	ø
* 密码确认	请输入当前管理员账号的密码	ø
* 验证码	验证码	-64957

图表 222 修改密码

 点击"新增用户",进入新增用户页面,输入用户名、姓名、密码、确认密码(密码和确认密码保持一致)、选择角色(管理员、安全人员、项目经理、测试人员、审计人员、新增加的角色)、部门、邮箱、电话、选择是否允许登录和是否允许鉴权代理之后点击 '确定'即可在列表中看到新增的用户。

* 用户名	支持英文、数字及下划线	
姓名	支持中英文、数字及符号	
* 密码	支持中英文、数字及符号	
* 确认密码	请再次输入密码	
* 角色 🥜	「请选择角色」 ∨	
* 部门	「清选择部门」 ∨	【新增部门】
邮箱	请输入您的电子邮箱	
电话	请输入您的手机号或座机	
允许登录 🥑	☆ 分许鉴权代理 ② ●	XØ

图表 223 新增用户

- 管理员权限可以管理所有的账户,在用户列表中可以看到用户名、部门、用户角色、用户邮箱、联系电话、创建时间、最近登录时间、操作(可以对除当前账号外所有账号进行编辑资料、修改密码、删除操作);
- ▶ 编辑资料可修改子账户的信息及角色权限。

用户名	chenyi	
认证源	Local	
姓名	支持中英文、数字及符号	
*角色	管理员	V
* 部门	默认部门	∨【新增部门】
邮箱	请输入邮箱	
电话	输入手机号码或座机	
允许登录 🥜	允许 公开 公开 经 人 计 鉴权 代理 👔 📿	关闭
	取消 确定	

杭州默安科技有限公司

114

图表 224 编辑资料

▶ 修改子账号的密码时需要输入当前登录的管理员密码。

用户名	chenyi	
* 新密码	输入新密码	ø
* 确认新密码	再次输入新密码	Ø
* 密码确认	请输入当前管理员账号的密码	ø
* 验证码	验证码	34990

图表 225 修改密码

点击"删除",弹出删除提示框,点击'确定'即可删除该用户。需要注意的是通过 LDAP
 通过过来的账号无法删除。

0	提示 确认删除该用户?
4	确定取消
	图表 226 删除用户

1.12.2 部门管理

点击"账号管理"-"部门管理",进入部门管理页面,可以查看用户部门,支持批量修改用户部门。

🇭 雳鉴・IAST	88 69 89 69 60 第日总法 应用管理 編明管理 第二方库 調性Age	①		■ 助中心			yy I 🚅 I 🖨
当前位置: 账号管理 > 部门管理							
音时门管理							
 」 就认問「」 ユzm-ladp 	用户名	部门	用户角色	用户邮箱	联系电话	包括整合力间	
 ceshibumenming 34 	xh_xmjl	默认曾印门	管理员			2022-08-31 11:03:03	
 xzm-ad f级识撒大大 	honeypot	服从目的门	管理员		—	2022-08-31 11:03:03	
d d	 tong cheng 	默认部门	管理员	123@qq.com	13325411111	2022-08-31 11:03:03	
(C) (80.000-900-900-90	xzmtest1 xzmtest1	RGA 85(7)	管理员			2022-08-31 11:03:03	
	admin	默认問门	管理员			2022-08-31 11:03:03	
	🗆 hj	RK认用517	管理员			2022-08-31 11:03:03	
	user1	默认問门	管理员		—	2022-08-31 11:03:03	
	test3	10%从1867	管理员		16666666661	2022-08-31 11:03:03	
	test2	新ti人用5门	管理员		15988843085	2022-08-31 11:03:03	
	school	服从目的门	管理员		_	2022-08-31 11:03:03	
	单页全选 全选 更改部门						
		共66条	< 1 2 3 4	5 6 7 > 10 条/3	瓦 v 與 至 页		

图表 227 部门管理

*更改部门	请选择要更改的部门	\sim

图表 228 修改用户部门

点击左侧部门条目,会浮现新增、删除、编辑按钮,可对部门进行增删改操作,删除部 门后,部门中的人员会归类到默认部门下,默认部门不运行进行编辑或删除操作。



图表 229 部门管理-编辑部门

1.12.3 角色管理

管理员可以在角色管理中查看管理员的权限,可配置测试人员、安全人员及项目经理的

权限。

管理员可以在角色管理中新增角色,并对新增的角色进行重命名和删除操作,新增的角 色可配置权限与测试人员相同。

😴 雳鉴 · IAST 👘			уу I 🚅 I 🕞
当前位置: 账号管理 > 角色管理			
角色管理			
角色列表 + 新谐角色	通用漏洞操作		
		◎ 重新检测	
8 -			
-	项目总览		
	◎ 項目自定		
· 项目经理	应用管理		
	应用列表		
	2 22 (8) 574 (0) 572	(c) scal	
(/) 期試人员		☑ 359	
	项目列表		
	2 22 0 MH () HH	12 新田	
	😪 曲編 🛞 所有 🔘 所属	◎ 田時 ● 所有 ○ 所属	
	😨 项目控制 🔍 🛞 所有 🔘 所篇		
D 0	项目模板		
S 12	🕞 11 🛞 MR 🔘 MR	(1) 新加速	
Ŀ	國 新闻 ⑧ 所有 ◎ 所属	☑ 曲時 ● 所有 ◎ 所属	
0	漏洞管理		
test_yt_001	☑ 韋時列表		

图表 230 角色管理

ダ 雳 鉴・IAST 88			
当新位置: 东弓管理 > 角色管理			
角色繁建		重命名角色	
角色列表 + 新潮角色	通用漏洞操作	角色名称 12	
		•董章各各称 请输入角色名称	
8 ***	项目总统		
		取用 青定	
Lines	应用管理 应用列表		
	2 前音 ⑧ 所有 〇 所至		
(/) 期試人员	8 mm 8 mm 0 mm	Res Record	
	项目列表		
	N BE B NR O NE		
Co sels	※ 總統 第 所有 〇 所置	Sme su Onz	
	S NUMER • · · · · · · · · · · · · · · · · · ·		
E B	項目機械		
8 12			
	National Contraction	N 200 @ 6-12 U MS	
0	漏洞管理		
B test yt_001			

图表 231 角色管理-重命名

雳鉴·IAST 🔤			
【: 账号管理 > 角色管理			
2		提示	
A + 新電角色	通用瓶洞操作 19 miz	是四副粉丝的角色? 取 测 取 测	
8 ***	项目总览 197 第四日元		
iner and	廠用管理 应用列表		
()) 期成人员	 ※ ※ ※ ※ ○ ※ ※ ※ ※ ※ ○ ※ ※ 	⊗en» ⊛n∺ Onz	
Q. 2018		≥ 53 2 50	
_@			
8 12	回 前有 ※ 所有 ○ 所属 図 前有 ※ 所有 ○ 所属	N ma N ma () an () an	
8 test_yt_001	蒸洞管理		

图表 232 角色管理-删除

1.12.4 权限审批

管理员可以在权限审批中管理是否开启用户注册功能,关闭后,无法通过登录页面自助

注册。

当前位置:账号管理> {	又限管理									
用户注册 🔽 开启用户	P注册功能 (开启后用户可以通过	春景页面注册成为刻试人员)								
权限审批							历史审批记录			
用户姓名	861)	用户角色	申请角色	用户邮箱	联系电话	tuismer (m	操作			
ceshi		测试人员	项目经理			2020-03-31 11:34:29	同意丨驳回			
	共1条 < 1 > 10 条/页 > 載至 页									

图表 233 用户注册控制

测试人员可以通过申请角色升级变为项目经理,申请记录会在权限审批列表中,管理员 权限可以审批申请是否通过(同意和驳回)。

当前位置:账号管理> {	反限管理						
用户注册 🔽 开启用户	注册功能(开启后用户可以通过	登录页面注册成为测试人员)					
权限审批							历史审批记录
用户姓名	部门	用户角色	申请角色	用户邮箱	联系电话	创建时间	操作
ceshi	一级部门	测试人员	项目经理			2020-03-31 11:34:29	同意 驳回
			<u>#</u> 1	★ < 1 > 10 %	/页 🗸 跳至 📃 页		

图表 234 权限审批

历史审批:可看到所有审批的历史记录,记录列表记录用户名、部门、当前角色、申请 角色、用户邮箱、联系电话、审批人、审批时间、审批结果。

当前位置:账号管	理 > 权限审批 > 历史审	制记录						
历史审批记录								
用户姓名	音阶门	当前角色	申请角色	用户邮箱	联系电话	审批人	审批时间	审批结果
song	默认部门	智无	测试人员	@qq.com	150000	admin	2019-10-10 14:38:11	申请通过
pm	测试部	项目经理	项目经理	@163.com	15000	admin	2019-10-10 14:34:21	申请通过
pm	测试部	项目经理	项目经理	@163.com	15000	admin	2019-10-10 14:34:00	申请驳回
				共3条 < 1 > 10	●条/页 ∨ 跳至 页			

图表 235201 审批记录

1.12.5 认证源

支持接入LDAP、AD域和CAS系统,可以快速同步企业内部已经有的账号信息,将LDAP、 AD域或CAS中的账号同步至雳鉴中。减少产品接入企业内部时账号创建的压力。

🗭 雳鉴・IAST						FA NGBR						99 (🚅 (🖨
当前位置: 账号管理 > 认证源												
从证源管理												
創用状态 全部 🔹	以证类型 <u>全部</u>	LDAP	AD ist	CAS								清加认证意 👻
认证名称	认证类型			启用状态		最后更新	时间		13	创建时间	\$ 操作	
xzm	LDAP (via BindDN)					2022-08-	31 11:03:03			2022-08-31 11:03:03	编辑(图称	
					<u></u> ب	1 🛱 <	1 >	10 奈/页 ∨				

图表 236 认证源

1.12.5.1 认证源管理

对已经添加的认证源进行管理,展示认证名称、认证类型、最后更新时间以及创建时间。 支持管理认证源是否启用,以及对认证源进行编辑、删除操作。

认证源管理							
启用状态全部	▼ 认证类型 全部	LDAP AD 域 CAS					添加认证源 🔻
认证名称	认证类型	启用状态	最后更新时间	¢	创建时间	÷	操作
121212	CAS		2022-07-07 14:23:20		2022-07-06 14:09:31		编辑丨删除
xzm	LDAP (via BindDN)		2022-07-06 12:42:00		2022-07-05 14:15:59		编辑丨删除
XZM AD	AD城		2022-07-07 20:57:24		2022-07-05 12:14:03		编辑丨删除
6	CAS		2022-07-07 14:23:25		2022-06-30 16:21:33		编辑丨删除
5	CAS		2022-06-30 16:21:20		2022-06-30 16:21:20		编辑丨删除
4	CAS	(原用)	2022-06-30 16:21:04		2022-06-30 16:21:04		编辑丨删除
cas_zm	CAS		2022-06-30 14:27:44		2022-06-30 14:27:44		编辑丨删除
		共	7条 < 1 > 10条/页 >				

图表 237 认证源管理

> 打开启用开关可以在登录时选择此认证源。关闭反之。

杭州默安科技有限公司

▶ 点击"编辑"按钮,可以进入编辑界面,对已有的认证源信息进行编辑修改。

🍠 雳鉴・IAS	ST 双目日達 包形智慧 副部分 素 通告方案 前日Agent 現象日間 日本 系列) (Acimi 83	E) E Silit Albr) Rů	yuying I 🚅 I 🕞
当前位置:账号管理 > 1	认证题 > 编唱 AD域 认证题				
编辑 AD域 认证原					
*认证名称	XZM AD				
1. 基本设置					
* 主机线社	Idap://192.168.180.19:389	銀短	EDN	CN=Administrator,CN=Users,DC=moresec,DC=cn	
律定面码	·····································				
2. 用户同步设置					
* 用户搜索基金	OU=iast,DC=moresec,DC=cn				
* 用户过滤规则	(objectClass=user)				
*用户漏性	a				
用户邮箱编性	mail				
用户电域曙性	mobile				
* 默认分配角色	● 智慧思 - 項目経歴 - 別成人間 - 安全人間 - text role yit - text role - 初期時式 123 - 初期時交別成 - youn - text role.yt2 - text role.zzc_1 - text11 - test_zzc_role_2 - test_role_zzc_3 - test_role_4 - 222 - 空空				
	xzmi认正原 / ad				
允许登录 🕤	<u>88</u>				
定期間步振号	1det ×				
	<u>桃田</u> 取消				

图表 238 编辑认证源

▶ 点击"删除"按钮,需要在弹窗中填写当前账号的密码,校验后才能删除认证源。

输入当則账尸 删除后该认证 是否删除该认	'密码后,点击确定即可删际对应 源同步的所有用户信息将被删除 、证源?	¥1入证源。 余,请确认
* 确认密码	请输入当前用户密码	Ģ
	藤 寺 取 消	
	确定 取消	

图表 239 删除认证源

1.12.5.2 添加认证源

点击"添加认证源"按钮,填写相关信息后即可完成认证源添加。

添加认证源 🔻
LDAP
AD 域
CAS

图表 240 添加认证源

4射位置:并弓首注 >	认证图 > 原加 LDAP 认证题			
RIE LOAP WERE				
• 认证名称	清晰人认证名中			
基本设置				
* 主机物社	[dap(s)//[ip]s(port)	创定DN	ng.cn=Search.dc=myDornain.dc=com	
类是面积	a asimelukunin.Arenas - 575500000			
用户同步设置				
* 用户搜索基准	n.g. au=Userudc=myDomain,dc=com			
*用户过读明到	(objectClass=posisAccount)			
* 用户雇性				
用户邮箱围性	eg.mal			
用中电话慢性				
* 默认分配角色	1 新規長 7 田田辺 ● 第51人気 全全人気 12 test yt_001 cerecerecereced 50 Z M 233 sec test_audit test_yt_002 yy 形式反映形式用 xzm			
• 默认分配部门	新い初门 、			
允许登录 😦				
定期局步所导	×1 (大)			

图表 241 添加认证源-LDAP

勞 雳鉴・IA:	ST 28 0 E 10 0 0 E E S			w 1 🚅 1 🔂
当前位置:所写答理 >	以证理 > 该组 ADM 认证题			
過加 ADIg 认证题				
- 认证名称	3867/72534			
1. 基本设置				
* 主机线社	ldap(s)//ījp)(port)	御宠DN	n.g. cn=linarch.dc=myDornain,dc=com	
卖定面得	· · · · · · · · · · · · · · · · · · ·			
2. 用户同步设置				
* 用户搜索基准	ng, au=Usen,dc=myDomain,dc=com			
×用户过途规则	[objectClass=posis/ccount]			
* 用户属性				
用户邮稿围性	e.g. mail			
用中电话懂性				
* 默认分配角色	● 智道長 「 項目回理 ● 第三人员 「 安全人员 12 test yt_001 eccence eccenced 50 Z 林 233 ecc test_audit test_yt_002 yy 高規原目反限 xzm			
* 款认分配部门	2018/2019			
允许登录 😦	88			
定期局步所导	(現)			
- 更新方式 🔵	更新电话、邮箱信息			
	R in			

图表 242 添加认证源-AD 域

₿ 房 盤・IAS	50 €1 € 0 € 0 € R 5000 FERR REAL MALE RANGE FERR REAL MALE F	(2) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	w 1 🗭 1 🔂
当前位置: 排写管理 > 1	以证度 > 添加 CAS 以正應		
ISTO CAS LAIER			
•认证名称	対応入いて名称		
1. 基本设置			
* CAS 认证 URL	消除入	* CAS Ticket始結 URL 前部心	
2. 用户同步设置			
- 默认分配角色	 ・		
* 数以分配的门	85.891 V		
允许登录 0	8# O		
	的业 取())		

图表 243 添加认证源-CAS

1.12.6 AK/SK

AK/SK页面:可以看到用户、AccessKey、SecretKey、状态和创建时间。可对 AK/SK 进



行状态的筛选和批量删除。

😚 雳鉴・IAST		 ① ① ② ① ③ ③ ○ ③ ④ ○ ○ ○ ○ ○ ○<th>a sett ret sat ant</th><th></th><th>yy i 🚅 i 🕞</th>	a sett ret sat ant		yy i 🚅 i 🕞
1前位置:账号管理 > AK/S	ĸ				
ik/sk					
K@ 1818.18 🔹				查費認用	的 生成AK/SK
甩户	AccessKey	SecretKey	状态	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	
УУ	630dd786a882e989c557e301 🤇	******	Ø 已启用	2022-08-30 17:25:26	(体用)删除
● 单页全选	P\$t				
			共1条 < 1 > 10条/3		

图表 244 AK/SK

点击"眼睛图标"出现"查看 SecretKey"弹窗,密码验证成功后即可查看 SecretKey。

验证成功之后,	5分钟内查看SecretKey无需再输入	密码
确认密码	请输入当前用户密码	ø
验证码	请输入	61782
300 AT A P	· 请捆人	onor

图表 245 AK/SK-查看 SecretKey

点击编辑操作,进入 AK/SK 的编辑页面,可编辑对应 AK/SK 的接口权限:

99 雳盗							ER Nette				🚅 ! 🕞	
当前位置: ※	母管理 > AK/SK > 编码A	AK/SK										
账号管理	92 ST/W18											
用户管理	音雅用户列表		•	新總用户	【可用角色】							
	於 改用 户 配置	【可用角色】		的用户								
项目控制	图包、调整成用		9	elf-st-Alto	101							
派司管理	10 au			K)R								
	图 6年											
应用管理	會看应用列表	 新 	有〇前	R								
	新建应用											
	😋 曲時成用	• 所	有〇丽									
	☑ 编辑应用	 所 	商〇所									
项目管理	🕑 新建項目											
	日鄭秋陽 💟	 所 	有〇府	R.								
	🖸 编辑项目配置	 If 	海 〇 肋									
	2 查看以目列表	• #i	有一册									
仓库镇僚	☑ 查看台库列表		•	后讓合库								

图表 246 AK/SK 编辑页面

1.12.7 登录安全设置

登录安全设置中,可进行登录过程中有关安全的自定义设置,包含登录失败设置、密码

有效期设置、token 有效期设置、密码复杂度设置。



图表 247 登录安全设置

1.13 系统配置

1.13.1 系统信息

系统信息由 6 部分组成:包括总体描述、服务信息、设备信息、系统状态、系统日志、 系统重置,如图所示。

- ▶ 总体描述:版本、支持项目数、当前项目数;
- ▶ 服务信息:展示设备上服务状态是否正常以及所有服务的名称、状态、运行时间。
- ▶ 设备信息:设备 ID、设备 IP、标签、设备状态、扫描网段;
- ▶ 系统状态:网络流通速度、CPU负载、内存占用;
- ▶ 系统日志:打包日志,下载系统日志;
- ▶ 系统重置: 只保留管理员账号并清空所有数据信息;

Tel: (+86) 400-0571-211

Email: market_moresec.cn

ジ 房盤・IAST 88 日 日 公 の の 四 ゴロテル 血が用意 東川市寺 東田市道 第		w + ⊯ + (+
当前位置: 系统配置 > 系统面积		
49年頃後 1812年: IAST VZ.15.0 支持疫目数: 20000 魚根将目数: 192 软件杂情		
副務協会 脱券状态:正常		東戸19倍 +
28年金倉 説祭(D: as4be-d4b- 説祭(P: - 外部時記: 192.168.120.200 説祭代志: 田行中		
系统状态		
PRE-Base S-20th/f0	27%	51%
扫描节点镜度		
2010 0-00000000 (12日):13510025102 (102) (102) - 10810 (12日)(12日)(12日)(12日)(12日)(12日)(12日)(12日)		
网络西弗里	CPU58	ляжая () 31%
日間も二位度 明治10-547-4.544.0 明治10-102-158180 C7 新潟・0124557899875543210 (2011) 明治11-1-7-241-1 日田昭和・1 へ 紀電		
Nikkas		

图表 248 系统信息

1.13.2 授权配置

授权配置包含设备指纹、安装环境、产品到期时间,维保到期时间、产品序列号,用户 可联系默安科技获取产品序列号用于配置更改,使用期限更改等操作。

🗭 雳鉴・IAST									豪 系統配置			yuying 🚅 🕞
当前位置:系统配置 > 授权配置												
设备相纹 b95fe32dbdab20c923b;	23a62a5029a	38							安装研	К IД L		
产品到期时间 无限期									维保至 2024-	期时间 07-11 18:31	:41	
产品序列号												
qP687gibMhrKRPHxnOS6GWSdUT	ZPmwGfDnp YX0KPmIdN	ghztYn/al+3 3QyqwpDl2i	gqb6fKhxO9 n6fwqoph1a	Sm2p9mc+f VfuzinaTCfr	2CIDjWoMJk IGD3w60EX6	p/qOBLussj c3/wlbotpN	tWj5wY3oLM 1IVU43RaTIr	dd4Njfjw67I	EDd+4+9pg		*******	*******************************
若产品即将到期,请联系服务提供商家	取最新序列号	1										
编辑序列号												



1.13.3 请求黑白名单(扫描类)

黑白名单分为站点黑名单、源 IP 黑名单、源 IP 白名单、请求特征黑名单和代理黑名单 五种。

 站点黑名单是用户根据实际情况,将不需要扫描的站点加入黑名单,设置后的站点流量 不进行录入与扫描。在列表显示包含 host、是否包含子域名、path、匹配方式、说明、 操作(编辑和删除),可根据 host 或 path 进行搜索。

当前位置:系统配置 > i	请求黑白名单							
站点黑名单 🕖	源IP黑名单 🥑	源IP白名单 🕐	请求特征黑名单 🕐	代理黑名单 🥝				
							host/path	Q 添加
host	是否包含子域名	path			匹配方式	说明		操作
192.168.180.56	是	/abc			后缀匹配			编辑丨删除
kirito.org.cn	否	/			前缀匹配	12test		编辑计量
				共2条 <	: 1 >			

图表 250 站点黑名单

点击"添加",可添加站点黑名单,输入host时直接输入根域名【如:www.test.com】
 或者 IP 地址【如:192.168.0.100】,项目地址可以勾选是否包含子域名;在 path 输入
 路劲【如:/test】),path匹配规则有前缀匹配、后缀匹配和正则匹配,添加描述(可以不选)确认填写准确之后点击"确定"即可完成添加站点黑名单,新增站点黑名单会更新至列表中。

* Host		包含子域名
path	/whitelist	前缀匹配 🗸
描述	描述文字	

图表 251 新增站点黑名单

2) 源 IP 黑名单是用户根据需求将其他扫描器等不需要录入请求的来源 IP 加入黑名单中, 设置后列表中 IP 的流量不进行录入与扫描。在列表显示 IP、说明、操作(编辑和删除), 可根据 IP 或说明进行搜索。

当前位置:系统配置 > 1	青求黑白名单						
站点黑名单 🕜	遼IP服名单 🔵	濟P白名单 💿	请求特征服名单 📀	代理黑名单 🕜			
						IP/说明	Q 添加
IP					1004月		操作
192.168.1.2					test		编辑丨删除
192.168.31.73							编辑丨删除
					共2条 < 1 >		

图表 252 源 IP 黑名单

 点击"添加",可添加源 IP 黑名单,确认填写准确之后点击"确定"即可完成添加,新 增源 IP 黑名单会更新至列表中。

* 源IP地址	
描述	
生效模式	☑ 鉴权/非鉴权代理、VPN

图表 253 新增源 IP 黑名单

3) 源 IP 白名单设置后,仅有列表中的 IP 发起的请求会被录入,主要用于流量信使、流量 镜像模式下,扫描请求脏数据过多的问题。在列表显示 IP、说明、操作(编辑和删除), 可根据 IP 或说明进行搜索。

当前位置:系统配置 >	黑白名单				
站点黑名单 🕜	源IP黑名单 🥑	源IP白名单 🕖	请求特征黑名单 🥑	代理黑名単 👩	
添加					IP/JE8B
IP				说明	操作
192.166.1.1				test	編編 删除
			共1条	< 1 > 跳至 页	

图表 254 源 IP 白名单

点击"添加",可添加源 IP 白名单,输入源 IP 地址及描述确认填写准确之后点击"确定"即可完成添加,新增源 IP 白名单会更新至列表中。

_	

图表 255 新增源 IP 白名单

 请求特征黑名单是用户根据需求对扫描器等不需要录入的请求,将请求头中的特征串加 入黑名单中,设置后符合列表中请求特征的流量不进行录入与扫描。即请求头字段中, 包含该特征字符串,则认为匹配命中,加入黑名单。在列表显示请求头字段、内容特征 串、说明、操作(编辑和删除),可根据请求头、特征串或说明进行搜索。默认填入开

源常用扫描器请求特征串。

当前位置:系统配置 > 请求黑	自名单					
站点黑名单 🥹 👔	和P黑名单 😗 濟IP白名单 😏	请求特征服名单 🖉 代理黑名单 💡				
						请求头/特征串/说明
请求头字段	内容特征率				说明	操作
User-Agent	.*acunetix-wvs-test-for-some-inexistent-file	<i>.</i>			awvs	编辑(删除
User-Agent	.*by_wvs.*				awvs	编辑 最佳
User-Agent	.*acunetix_wvs_security_test.*				awvs	编辑(删除
User-Agent	.*acunetix_wvs.*				awvs	编辑(删除
User-Agent	.*acunetix_test.*				awvs	编辑(删除
Acunetix-Aspect-Passwo rd	1				awvs	编辑 计最短令
Cookie	acunetixCookie				awvs	编辑 计最同论
Location	acunetix_wvs_security_test				awvs	编辑(最终
X-Forwarded-Host	acunetix_wvs_security_test				awvs	编辑 删除
X-Forwarded-For	acunetix_wvs_security_test				awvs	编辑 删除
		共445	k < 1 2 3 4 5	> 跳至 页		

图表 256 请求特征黑名单

 点击"添加",可添加请求特征黑名单,其中内容特征串需要填写正则表达式,确认填 写准确之后点击"确定"即可完成添加,新增请求特征黑名单会更新至列表中。

内容特征串	请填写正则表述	迂之	
描述			

图表 257 新增请求特征黑名单

5) 代理黑名单设置后的站点流量将不再经过"雳鉴"代理,不进行录入与扫描,需要输入 IP 及对应端口进行添加。在列表显示 IP、端口、操作(删除),可根据 IP 进行搜索。

当前位置:系统配置 >	黑白名单						
站点黑名单 🕜	源IP黑名单 🕜	源IP白名单 🥱	请求特征黑名单 🍞	代理黑名单 🕖			
添加						IP	Q
IP					通	擾	作
192.168.120.140					81	题	除
			共1条	< 1 > 跳至	页		

图表 258 代理黑名单

● 点击"添加",可添加代理黑名单,输入 IP 及对应端口确认填写准确之后点击"确定"

即可完成添加,新增代理黑名单会更新至列表中。

* ID			
* IF			
端口			
	确亲	取治	

图表 259 新增代理黑名单

1.13.4 消息通知

1.13.4.1 邮件通知

💋 雳鉴・IA	ST 88	6 8 	3 ① (4 网读 第三方库 插标/)	D FA 1919 Hussie	(1) 系统配置	日 日本申计	副総合	yuying 📫 😝
当前位置:系统配置 >	海思通知								
邮件通知	webhook 📀								
* 邮箱发送者用户名	1780975714@qq.com								
* 发送密码									
* 服务器地址	smtp.qq.com								
* 服务機端口	587		QQ邮输端口:587						
* 发件人	1780975714@qq.com								
	測试 保存	重置							

图表 260 邮件通知设置

对发件邮箱进行相关配置,即可对项目进度实时邮件通知(当填写 QQ 邮箱时,请使用

杭州默安科技有限公司

587 端口)。点击"测试"按钮可以检测填写内容的连通性。点击"保存"按钮可以保存当前填写项目,并应用于邮件发送。点击"重置"按钮,会清空当前填写的内容,同时取消邮件发送功能。

1.13.4.2 webhook

webhook 页面展示当前添加的所有 webhook 列表,包括名称、webhook ur1、添加日期、 创建人以及编辑、删除操作。点击编辑可以对已经添加的信息进行修改,点击删除会有弹窗 提示,点击确认后会删除一条 webhook 记录。

9雳鉴	·IAST							@ 5:0222				yuying 🚅 🕞
当前位置:系统	配置 > 消息通知											
邮件通知	webhook 💿											
												添 加
名称	Webhook URL									添加日期	创建人	操作
yapi-test	in the second	 	-	 -		-	-			2022-06-02 14:43:25	admin	编辑丨删除
yapi-test										2022-06-08 10:38:51	admin	编辑 删除
yapi-test		-		 	-	-				2022-06-08 10:41:09	admin	编辑丨删除
yapi-test		 		-		-	-			2022-06-08 12:05:30	admin	编辑丨删除
hyk-test					-		-			2022-06-28 15:58:36	zhangmeng	编辑丨册幹
222	parse fail									2022-07-04 17:31:16	xzm-safe	编码 册除
					共6券	ŧ < 1) > 1	0条/页 ∨				

图表 261 消息通知-webhook

点击添加按钮,可以添加 webhook,填写此条 webhook 的名称以及请求包内容。可在请 求包填写框内填入: \$id、\$name、\$status、\$owner、\$level 变量, 雳鉴在发送 webhook 时 将会自动替换为:项目 id、项目名称、项目状态、项目归属人、安全等级。最后,点击测试 可以对请求进行发送测试,点击保存即可保存此 webhook 信息。

提示,可在 \$level变量 称、项目和	王海水包填与框闪填入,Sid、Sidane、Status、Sowner、 2。雾鉴在发送webhook时将会自动替换为:项目id、项目名 术态、项目归属人、安全等级
名称	webhook名称
* 请求包	POST /aaaa/bbbb/cccc HTTP/1.1 Accept: */* Connection: keep-alive Host: aaaa.com Accept-Encoding: gzip, deflate Content-Length: 195 Content-Type: application/json X-schema: https {"msgtype": "text", "text": {"content":"项目扫描完成"}}

图表 262 消息通知-添加 webhook

1.13.5 网络配置

▶ 网络测试:输入地址测试,并进行结果输出

M-3-MIX3kFU	DNS配置	HOST配置		
ping	\vee			
IP 地址或域名	地址		测 试	
结果				

图表 263 网络配置-网络测试

▶ DNS 配置/Host 配置:进行 DNS 或 Host 配置,Host 配置支持无后缀的域名地址,当 DNS

杭州默安科技有限公司

和 Host 同时配置时,优先使用 Host 配置。

当前位置:系统配	置 > 网络配置			
网络测试	DNS配置	HOST配置		
请输入DNS		添加		
DNS列表				操作
192.168.120.1				刑邸余
192.168.1.1				册卿余
192.168.20.1				册卿余
192.168.20.1				删哪余

图表 264 网络配置-DNS 配置

当前位置:系统配置 > 网络配置		
网络测试 DNS配置 HOST配置		
Lot AL		
HOST	P	操作
www.last.on	192.168.160.72	删除
mmm.cn	192.168.120.66	删除
lijian.iast.com	192.168.100.208	BIR:
baidu.com	192.168.100.22	删除
moresec	192.168.1.1	删除
800	192.168.25.233	删除
2www2.dd2.dd	192.168.12.12	删除
www	192.168.12.12	用印象
a	192.168.123.255	册目录
C	192.168.123.255	#153

图表 265 网络配置-HOST 配置

以换行分隔每条香	置,IP与HOS	T间使用空格隔	开, 例:
192.168.160.72 w	ww.iast.cn		
192.168.160.63 w	ww.iasttest.cn		

图表 266 网络配置-HOST 配置-添加弹框

1.13.6 系统升级

定期进行系统升级会加强系统的兼容性、稳定性,使用户体验到更多的实用功能,或提高扫描效率、修复可能的软件漏洞等多种功能。



具体操作步骤如下:

- 1. 点击系统配置-系统升级;
- 2. 选择更新补丁文件并上传升级。
- ▶ 注:升级历史可从历史版本中进行查看

当前位置:系統	充配置 > 系统升级				
系统升级					
	当前系统版本 全新升级,一路相护 选择文件	雳鉴IAST V2.11.0		Ĵ,	
ID	升级版本	升级时间	状态	操作人员	操作
4	2.10.1–2–l4j2	2021-12-14 17:04:27	正在升级中	admin	详情
3	2.2.0-2	2021-03-17 15:30:25	正在升级中	admin	详情
2	2.8.0	2020-11-17 10:42:22	正在升级中	admin	详情

图表 267 系统升级

如果当前产品超过了序列号中定义的维保到期时间,升级功能将无法使用。请联系公司 售后服务人员。

😚 雳鉴・IAST					(日本1811) 日本1811			admin	1 [4
当前位置: 系统配置 > 系统升级									
系统升级									
当自	前系统版本 ⅠA\$	ST V2.10.0		1	1000		Ą		
11(#3)	间已到,无法遗行产品升载	8、调联系服务提供商进(7世保線期	<u>o</u> r		i	1		

图表 268 维保时间到期提示

1.13.7 流量信使(扫描类)

流量信使客户端用于测试人员较多,配置代理沟通成本较大,网络情况复杂的情况下, 通过在被测业务服务器上安装流量信使 agent,测试人员无需任何额外操作和配置,正常进 行功能测试,流量信使 agent 开放源代码,采用嗅探的方式收集流量,与正常业务并联,无 数据安全风险,不影响正常业务。
在【系统配置】---【流量信使】中,页面可查看流量信使 agent 的 IP 信息,最近收集到 请求的时间,最近请求的 Host 以及流量信使 agent 的状态,设置监听端口,还可对其添加标 签及进行操作。

9 雳	鉴·IAST 問 项目的发 d		D R				yy i 🚅 i 🕞
当前位置: 3	系统配置 > 流量信使						
流量信使							
"流量信便	Agent部署在业务机器上,开放源代码,通过	过虞探收重流量,无任何数据安全风险,不影响正常业务"					
秋志 11	部 运行中 暫停 离线					流量信使印/标签	Q 流量信使下载
派集	動電使IP	最近清求时间	最近请求目的地址	状态	板签	监听端口〇	操作
192	2.168.180.52	2022-08-31 12:08:28	192.168.180.52:20000	 运行中 	-2	20000 🜌	暂停丨卸载丨详情
192	2.168.32.196	-	-	• 高 线	-2	80 🗹	
192	2.168.120.200	-	-	 商线 	-2	80 🗹	
192	2.168.120.200	-	-	• 南 技	-2	80 🗹	
192	2.168.120.200	-	-	• 商线	-12	80 🗹	
192	2.168.120.200	-	-	。离线	-2	80 🗹	
192	2.168.120.200	-	-	• 高 线	-0	80 🗹	
192	2.168.120.200	-	-	• 陶 祛	-2	80 🗹	
192	2.168.120.200	-	-	 商线 	-0	80 🜌	
192	2.168.120.200	-	-	。淘祛	-2	80 🗹	
全选	单页全选 启动 暂停	HL REAL PROVIDENT					

图表 269 流量信使查看页面

- 可根据流量信使状态进行查看,根据流量信使 IP 或标签进行搜索,列表默认按最近请求 时间倒序排列。
- 鼠标点击列表上对应流量信使标签栏的修改按钮,点击修改后保存,标签即修改成功。

	标签
	项目组1 📝
	图表 270 流量信使-标签
标签	
项目组1	保存取消

图表 271 流量信使-修改标签

● 鼠标点击列表上对应流量信使监听端口栏的修改按钮,即可设置监听端口(多个端口请 使用逗号分隔)。

80,8008	
80,8008	
图表 272 流量信使-监听端口	
监听端口?	
80,8008 保存 取消	

图表 273 流量信使-修改监听端口

- 点击"暂停"或"批量暂停",运行中的项目进入已暂停状态。
- 点击"启动"或"批量启动",暂停状态的 Agent 进入运行模式。

1	提示				
	是否启动	已选Agent?		_	
		取消	确定		

图表 274 流量信使-启动

- 点击"删除"或"批量删除",离线的流量信使会被删除。
- 点击"卸载",运行中或已暂停的流量信使被卸载,该条记录自动删除。

7	提示 卸载该流量信使后,该条记录将自动删除,请确认 是否卸载?
	确定取消

图表 275 流量信使-卸载

 点击"详情",页面跳转至流量信使详情。流量信使详情页显示流量信使 IP、Agent 状态、流量信使占用资源和流量信使服务器总性能。除此之外,还显示请求列表和黑白名单。(流量信使占用资源及服务器性能达到设定的阈值时将会发送站内示警及邮件通知, 详见 3.8.9.3)

🧭 雳鉴·IAST	- 188 日 - 188 項目が近 血用管理 運用管		● ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	w I 🚅 I 🖨
当前位置:系统配置 > 流量信使	> 流量信使详情			
流量信使详情				
192.168.180.52 流量信使P	运行中 Agentttl态	泥量倍使占用资源 CPU负载:0% 内存占用:100kb	近量偏使服务器总性能 CPU负载:8% 内存占用:76%	H 4
請求列表 黑白名单				
				HOST
最近请求HOST			御近川海 寺日1日	
192.168.180.52:20000			2022-08-31 12:08:28	
192.168.180.52:20000			2022-08-31 12:08:25	
192.168.180.52:20000			2022-08-31 12:08:25	
192.168.180.52:20000			2022-08-31 12:08:25	
192.168.180.52:20000			2022-08-29 20:01:51	
192.168.180.52:20000			2022-08-29 20:01:51	
192.168.180.52:20000			2022-08-29 20:01:50	
192.168.180.52:20000			2022-08-29 20:01:50	
192.168.180.52:20000			2022-08-29 20:01:50	
192.168.180.52:20000			2022-08-29 20:01:50	

图表 276 流量信使-详情

点击"删除",当前列表中的离线流量信使信息将被删除,但不会删除已经安装在服务器中的流量信使程序。

⑦ 居	提示 删除后,安装在服务器中的流量信使程序不会自动 删除,只删除本记录,是否删除?
	确定取消

图表 277 流量信使-删除

▶ 在右上角"流量信使下载"提供两种安装方式(流量信使依赖C标准库)

		\bigcirc		
curl http://	192.168.120.62:81,	/api/api/agent_install	复制执行	点击下载
1.请先对被测 2.直接复制cu 体请至【帮助 3.安装完毕后	业务创建一个"流量 1命令到被测业务机 中心】-【流量信仰 ,可返回至本页面:	建信使模式"的项目 仉器上执行命令,或者 吏】【文件安装方法】 查看流量信使客户端划	下载后进入目录, 查看 术态	运行make, 具

图表 278 流量信使下载

1.13.7.1 流量信使文件安装方法

您也可在图 100 点击下载中下载安装压缩包,压缩包中含有两个安装包, raw_socket_sniffer.zip为未编译的安装包,tcp_sniffer.zip为编译完成的安装包。

1.13.7.1.1 源码编译安装方式

源码编译安装方式如下:

1. 使用 unzip 解压传输的 zip 文件

2. 进入解压后的文件路径 cd agent

3. 使用 unzip 解压源码文件 unzip raw_socket_sniffer.zip

4. 进入源码文件的路径 cd raw_socket_sniffer, 执行 make

5. make 成功后, 生成 tcp_sniffer 执行程序, 执行 bash run. sh install

6. 进入配置文件路径 cd /usr/local/sdl_sniffer

7.设置接收流量的地址,执行 ./tcp_sniffer -o ip:port,例: ./tcp_sniffer -o 192.168.199.212:9003

8. 完成配置后重启服务,执行 service tcp_sniffer_service restart

1.13.7.1.2 复制内容安装方式

点击"复制内容"后直接复制 curl 命令到被测业务机器上执行命令即可。

1.13.7.2 流量信使配置文件

1.13.7.2.1 配置文件说明

压缩包内的 run. sh 会生成/usr/local/sdl_sniffer 目录,内含配置文件 sdl_agent. ini 和可执行程序 tcp_sniffer, 服务名称为/etc/init. d/tcp_sniffer_service。

1.13.7.2.2 sdl_agent.ini 文件格式

port=81 #port 代表流量监听端口,多个端口以逗号分隔,例: port=80,81,8080

out=192.168.199.212:9003 #out 代表收集流量的服务器,一般是雳鉴机器的 ip:9003。

1.13.7.2.3 tcp_sniffer 执行方法

/usr/local/sdl_sniffer 目录下: ./tcp_sniffer --help 可查看该命令帮助 ./tcp_sniffer -s 关闭程序 ./tcp_sniffer -o ip:port #设置接收流量的地址 ./tcp_sniffer -a port #添加收集本机端口的流量 例: tcp_sniffer -a 8080 tcp_sniffer -o 192.168.199.212:9003 该操作会修改本目录下的 sdl_agent.ini 配置文件, 修改后需要 service tcp_sniffer_service restart.

1.13.7.2.4 如何启动/关闭/查看状态/重启服务

可以使用 service tcp_sniffer_service start|stop|status|restart 对服务进行操作。

Tel: (+86) 400-0571-211

Email: market moresec.cn

1.13.7.3 流量信使安装成功示例及常见错误排查

1.13.7.3.1 安装成功示例

Classes/../log.h:31:9: warning: no return statement in function returning non-void [-Wreturn-type] Classes/../log.h: In member function 'void* Log::async_write_log()': Classes/../log.h:51:9: warning: no return statement in function returning non-void [-Wreturn-type] g++ -g -Wall -DBUILD=20180706 -Dmoresec=vai_moresec raw_socket.o log.o data_parser.o data_send.o mac xInteger.o main.o -o tcp_sniffer -lstdc++ -lpthread -DBIG_EDIAN -I. 请使用root用户或管理员权限运行该脚本 程序已经安装到/usr/local/sdl_sniffer/目录下,配置文件为/usr/local/sdl_sniffer/sdl_agent.ini Note: This output shows SysV services only and does not include native systemd services. SysV configuration data might be overridden by native systemd configuration. If you want to list systemd services use 'systemctl list-unit-files'. To see services enabled on particular target use 'systemctl list-dependencies [target]'. netconsole 0:off 1:off 2:off 3:off 4:off 5:off 6:off 1:off 2:on 3:on 4:on 0:off 1:off 2:off 3:on 0:off 6:off network 4:on 5:on tcp_sniffer_service 5:on 4:off 6:off 已经將程序加入开机服务中,如果报chkconfig命令错误,请确认该机器是否支持该命令! 请前往/usr/local/sdl_sniffer目录下配置sdl_agent.ini,并且启动tcp_sniffer服务 设置收集流量的服务器地址: 192.168.1.214:9003 设置地址成功! 每次只支持添加一个端口: 80 添加端口成功! service tcp_sniffer_service start ... start tcp_sniffer.... start tcp sniffer end.... tcp_sniffer process status..... root 1922 _1 0 01:59 ? 00:00:00 /usr/local/sdl sniffer/tcp sniffer root [root@localnost ~]#

图表 279 流量信使安装成功样例

安装完毕后最后一行会查询 tcp_sniffer 的状态,若有结果返回,则说明进程已启动,可返回至流量信使页面查看流量信使客户端状态。此时客户端 IP 对应的状态为运行中/已暂 停即说明安装成功。

在雳鉴上对被测业务创建一个"简单模式"的项目,在任意 PC 上成功请求被测网站即可录入请求。

1.13.7.3.2 常见错误及解决方法

常见错误1:

Tel: (+86) 400-0571-211

Email: market_moresec.cn

<pre>[root@localhost ~]# curl http://192.168.1.214:81/api/agent_install sh</pre>
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 332 100 332 0 0 7511 0::: 7720
######################################
sh: line 2 unzip: command not found
sh: line 3: cd: agent. No such file or directory
sh: line 4: unzip: command not found
sh: line 5: cd: raw_socket_sniffer: No such file or directory
make: *** No targets specified and no makefile found. Stop.
sh: line 7: ./run.sh: No such file or directory
sh: line 8: cd: /usr/local/sdl_sniffer/: No such file or directory
sh: line 9: ./tcp_sniffer: No such file or directory
sh: line 10: ./tcp_sniffer: No such file or directory
service tcp_sniffer_service start
Redirecting to /bin/systemctl start tcp_sniffer_service.service
Failed to start tcp_sniffer_service.service: Unit not found.

图表 280 流量信使安装常见错误1

此报错为未安装 unzip, 使用 yum install unzip 安装 unzip 后再次执行安装即可。

常见错误2:



图表 281 流量信使安装常见错误 2

此报错为未安装 gcc 组件导致的,首先查询与系统匹配的组件:

Tel: (+86) 400-0571-211

Email: market_moresec.cn



图表 282 流量信使安装常见错误 2 g++

之后安装 gcc-c++. x86_64 组件,安装完成之后重新安装流量信使即可。



图表 283 流量信使安装常见错误 2 g++安装

1.13.8 规则列表

1.13.8.1 规则列表-扫描类

用户可以在扫描类规则列表中自定义扫描规则,安全人员也可以独立添加漏洞。

县朝位置 : 苏州沿置 > 规则管理								
扫描类自定义规则	播桩类自定义规则 摄	H任类自动发现规则 个人隐私数据港	國规则					
等级高中低县	提示 状态 全部 在	线 离线 规则类型 全部	▼ 漏洞类型 全部	•		规则名称/创建入		
规则名称	规则类型	漏洞类型	规则状态	风险等级	更新时间 ⇔	创建人	操作	
cds	检测规则	用户自定义漏洞	0255	< 2 提示	2021-06-11 16:48:09	admin	编辑丨删除	
test	检测规则	敏感页面泄露	œtt 💽	0低危	2021-06-09 11:12:57	chenlu	1981 1 111 12	
struts2_001	检测规则	命令执行	(##)	● 高危	2021-05-07 16:30:16	lluchuanxing	18111 19123	
textarea检测规则	检测规则	跨站脚本	(#H)	〇 中危	2021-01-26 19:59:17	chenwentao	编辑 删除	
dddddd	检测规则	跨站脚本	(##	〇 中危	2021-01-20 23:50:29	dabingtest	58198) #1928	
234	过滤规则	SQL布尔注入		● 高危	2020-11-23 15:29:10	admin	199111 1993	
dabing	过滤规则	SQL布尔注入		● 高危	2020-11-23 15:29:08	dabingtest	188115 19153	
<script>alter(x)</script>	过滤规则	SQL布尔注入		●高危	2020-11-23 15:29:07	admin	1921E 19128	

杭州默安科技有限公司

140

1.13.8.1.1 添加规则

点击"添加规则"按钮,填入规则名称,选择规则类型和漏洞类型,对照规则模板填入 新增规则,点击确定即规则被添加成功。也可用测试规则模块在添加前对规则的填写进行测 试(仅检测规则可用)。

当前位置:系统配置	> 规则列表			
编辑扫描类规则				
1. 规则信息				
规则名称	dabign_test			
规则类型	检测规则			
漏洞类型	信息泄露			
新增規則	\d+	規则機板 <<	(#operation:代表payload版入的位置初版入的方法 #loc代表版入的公置 #'args'代表ged数中 #'post_args'代表post参数中	Î
2. 测试规则	,	6	#op:代表版人的方法 #*append"代表在原件数据后面追加payload #femburet和P##MMF##MP#heredowd	
请求包		扫描日志		
		测试规则		
		图表 285 済	忝加规则	

- ▶ 规则信息:规则名称、规则类型、漏洞类型、新增规则和规则模板四部分组成。
 - 1) 规则类型:分为检测规则和过滤规则两种。
 - 漏洞类型:检测规则分为跨站脚本、SQL 延时注入、文件包含及命令执行等十九种, 过滤规则分为信息泄露和 SQL 布尔注入两种。
 - 新增规则:检测规则对照右侧规则模板向其中填入新增规则,过滤规则按照需求 填写规则。
 - 4)规则模板:给出左侧相对应新增规则类型的模板及对应注释,点击新增规则和规则模板中间箭头按钮,新增规则模块中会出现相应模板。请对照右侧规则模板中 注释进行修改(过滤规则不展示规则模板)。
- 测试规则:请求包和扫描日志两部分组成。
 向请求包框中填入请求包内容,点击测试规则按钮后,扫描日志框内标红的部分则为
 设置的规则测试出的漏洞。



图表 286 测试规则

1.13.8.1.2 规则管理

规则列表默认按更新时间倒序排列(最新添加的规则展示在前面),列表内容包括规则 名称、规则类型、漏洞类型、规则状态、风险等级、更新时间、创建人及操作。

▶ 可根据规则风险等级、规则状态、规则类型进行查看,可对规则进行编辑或删除。

4前位置: 系统定置 > 规则管理								
扫描类自定义规则	播桩类自定义规则	播桩类自动发现规则 个人隐私数	摆泄露规则					
等级高中低	提示 状态 全部	在线 离线 规则类型 全部	▼ 漏洞类型 全部	5		规则名称/创建人	Q 添加规则	
规则名称	规则类型	羅河类型	规则状态	风险等级	更新时间 👙	创建人	操作	
cds	检测规则	用户自定义漏洞		② 提示	2021-06-11 16:48:09	admin	18111 #IR\$	
test	检测规则	敏感页面泄露	(#11 O	〇低危	2021-06-09 11:12:57	chenlu	59458 MIR	
struts2_001	检测规则	命令执行	(£15)	●高危	2021-05-07 16:30:16	lluchuanxing	1921E 2018	
textarea检测规则	检测规则	跨站脚本	œis O	0 中危	2021-01-26 19:59:17	cheriwentao	编辑(删除	

图表 287 规则列表

点击编辑,跳转至编辑规则页面,进入页面后对需要编辑的部分进行相应的修改。

当前位置:系统配置	> 规则列表	
编辑扫描类规则		
1. 规则信息		
规则名称	dabign_test	
规则类型	检测规则	
漏洞类型	信思泄露	
新增规则	\d+	规则模板
2. 测试规则		#operation:代表payload插入的位置和插入的方法 #loc:代表插入的位置 #'args'代表包含数中 #'post_args'代表包含数中 #opr代表插入的方法 #'append'代表在原有数据后面追加payload #temploce/fait#MMMATEMMATEMANDAL
请求包		扫描日志
		986490M
		图表 288 编辑规则

点击删除,在弹框中进行二次确认后该规则被删除。

杭州默安科技有限公司

(?)	提示			
	是否确认删除	规则?		
		确定	取消	

图表 289 删除规则

1.13.8.2 规则列表-插桩类

用户可以在规则列表中自定义设置适用的过滤或验证函数至插桩规则中以减少误报。满 足在不重启应用和 agent 状态下生效新的过滤函数,且插桩类规则列表中的规则对全局生效。

当前位置:系统配置 > 规则管理					
扫描美自定义规则 植枝类自定	义规则 插桩类自动发现规则	个人隐私数据泄露规则			
规则状态 全部 在线 离线	規则类型 全部 🔹				规则名称/创雄人 Q 漆加规则
规则名称	规则类型	规则状态	更新时间 ≑	創建人	操作
myFakeSanitizer	过滤函数(sanitizer)		2021-06-18 16:46:52	yangjingfeng	编辑 删除
ogni_test	过滤函数(sanitizer)	(##)	20210618 00:48:15	chenlu	40.110 EH/23
WebGoat8.1_XSS_SINK	污点源函数(source)	(#15)	2021-06-17 20:25:24	wufengjuan	编辑(删除
header_sanitize	过滤函数(sanitizer)	在地	2021-06-17 14:52:35	chenlu	40.10 MIR:
chenlu_test	过滤函数(sanitizer)	(##)	2021-06-16 14:24:26	chenlu	102111 20173
0000	过滤函数(sanitizer)		2021-06-16 14:20:24	llyun	编辑目目

图表 290 插桩类规则列表

1.13.8.2.1 添加规则

管理员或安全人员可以进行规则添加,点击"添加规则"按钮,填入规则名称,选择规则类型,按规定格式填入 API 或 XML,选择适用的漏洞类型,点击保存后,前后端对新增加的自定义规则进行校验,校验不通过则前端展示错误提示,校验通过则规则被添加成功。

增加播桩类规则 📀			
* 规则名称	現則名称		
* 规则类型 🕜	过途函数(sanitizer) ~		
* API 📀	请输入API		
	例如: com.moresec.demo.Sanitizer(java.lang.String)		
	"播桩自定义规则填写规范及使用场景说明调至【帮助中心】-【播桩Agent】-【播桩自定义规	则填写规范及使用场量说明】中查看	
* 污点过滤目标 🕜	运动过渡目标		
参数黑名单	参数值置		
生效 Agent	可透透透频 * 选择为空时默认全局生效	已选选项	
			Q
	22项	0项	一键清空
	82218a51-dd7c-339d-a8b2-25e39577ba1b		
	b744a450-8c97-38e9-ab9b-0c4130dac58e		
	D983D43-D184-0007-BD65-2B774CF11261	暂无数据	
	AF5853A9-A22C-2C75-4229-8A2D92263378		
	c3b4a4df-9d70-3b7b-94cb-d6c26a87bb43		
	93b667ca6e6a4c22b0511541a828569d		
	7abd3182-d399-37bd-9a19-a9ffa1af1d74		
	67c01310-bbc5-360f-a3b3-d21447abbbb1		

图表 291 添加插桩类规则

- ▶ 规则名称:填写自定义的规则名称。
- ▶ 规则类型:分为验证函数、过滤函数与污点函数三种。
- API: Java API 必须包含方法名称和参数,请使用完全限定类型,并使用'*'字符标记 要验证或过滤的参数,用于过滤函数(validation)、过滤函数(sanitizer)和过滤函数(dubbo)。
- ➤ XML:必须包含 method 条目或 event 条目,请按照 XML 模板填写,用于污点源函数(source)、 污点传播函数(propagate)和污点检测函数(sink)。
- ▶ 适用漏洞类型:选择此规则适用的漏洞类型,仅过滤函数(validation)、过滤函数 (sanitizer)和污点检测函数(sink)展示。
- ▶ 生效 Agent: 勾选可选选项中的 Agent 后,被选中的 Agent 会自动进入已选选项。点击 "确定",被选中 Agent 生效。

1.13.8.2.2 规则展示

规则列表默认按更新时间倒序排列(最新更新的规则展示在前面),列表内容包括规则 名称、规则类型、规则状态、关联项目、更新时间、创建人及操作。

▶ 可根据规则状态、规则类型进行查看,可对规则进行编辑或删除。

当时位置: 永远的意义 知识管理					
扫描类自定义规则 播枝类	自定义规则 播植类自动发现规则	个人隐私数据泄露规则			
规则状态 全部 在线 离线	規则类型 全部 🔻				规则名称/创建人 Q 添加规则
规则名称	规则类型	规则状态	更新时间 💠	创建人	操作
myFakeSanitizer	过滤函数(sanitizer)		2021-06-18 16:46:52	yangjingfeng	192117 1921178
ognl_test	过滤函数(sanitizer)	(## D)	2021-06-18 00:48:15	chenilu	編編 删除
WebGoat8.1_XSS_SINK	污点源函数(source)	(Ell)	2021-06-17 20:25:24	wufengjuan	编辑 一副除
header_sanitize	过滤函数(sanitizer)	Ett	2021-06-17 14:52:35	chenlu	編編 删除
chenlu_test	过滤函数(sanitizer)	任线	2021-06-16 14:24:26	chenlu	编辑 删除
aaaa	过滤函数(sanitizer)		2021-06-16 14:20:24	liyun	编辑:图称
dabingtest	中断区(deadzone)		2021-06-16 14:04:11	dabingtest	編輯 删除

图表 292 插桩类规则列表

● 点击编辑,跳转至编辑规则页面,进入页面后对需要编辑的部分进行相应的修改。

编辑插桩类规则 🥥			
* 规则名称	31313		
* 规则类型 💡	过步奉记载(sanitizer) ×		
* API 👩	at.dallermassl.ap.security.taint.webapp.Sanitizer.encodeJs(java.lang.String)		
	例如: com.moresec.demo.Sanitizer(java.lang.String)		
	*播桩自定义规则填写规范及使用场景说明请至【帮助中心】-【播桩Agent】-【播桩自定义规则填写规	吃友使用场景说明] 中 查看	
* 汚点过渡目标 💡	R		
参数黑名单	参数位置		
生效 Agent	可透透现 " 选择为空时默认全局生效	已透透烦	
			Q
	22项	21项	一键清空
	82218a51-dd7c-339d-a8b2-25e39577ba1b	27c29986-1e69-663a-3532-3a31633a6663	0
	S b744a450-8c97-38e9-ab9b-0c4130dac58e	b52cffe3-af7f-3fff-bfef-3d7bd5e276ad	0
	G F0983D43-D184-0007-BD65-2B774CF11261	67c01310-bbc5-360f-a3b3-d21447abbbb1	Ô.
	AF5853A9-A22C-2C75-4229-8A2D92263378	7abd3182-d399-37bd-9a19-a9ffa1af1d74	0
	C3b4a4df-9d70-3b7b-94cb-d6c26a87bb43	93b667ca6e6a4c22b0511541a828569d	0
	93b667ca6e6a4c22b0511541a828569d	c3b4a4df-9d70-3b7b-94cb-d6c26a87bb43	0
	7abd3182-d399-37bd-9a19-a9ffa1af1d74	AF5853A9-A22C-2C75-4229-8A2D92263378	0
	G7c01310-bbc5-360f-a3b3-d21447abbbbb1	F0983D43-D184-0007-BD65-2B774CF11261	0
	52cffe3-af7f-3fff-bfef-3d7bd5e276ad	b744a450+8c97-38e9+ab9b+0c4130dac58e	0
	27c29986-1e69-663a-3532-3a31633a6663	82218a51-dd7c-339d-a8b2-25e39577ba1b	0
		< 1 / 3 >	< 1 / 3 >

图表 293 编辑插桩类规则

点击删除,在弹框中进行二次确认后该规则被删除。

?	提示 是否确认册	删除规则?		
		确定	取消	

图表 294 删除插桩类规则

1.13.8.3 插桩类自动发现规则

插桩模式下, agent 会将自动发现的过滤函数上报,并支持直接应用指定规则,同时将 发现的过滤函数展示在数据流中,解决使用雳鉴的人存在对场景中的过滤函数不了解的情况, 从而检测出较多误报漏洞的问题。

🧭 雳 鉴・IAST 88 🗂 吕 ♪	 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		yuying 🚅 😝
当前位 置: 系统配置 > 规则管理			
扫描英自定义规则 描桩英自定义规则 播柱英自动发现规则	入總私數讓泄靈規則		
			Agent key/這該函数
过述函数	Agent key	操作	
at.dallermassl.ap.security.taint.webapp.SanitizecencodeforHtml(Java.lang.Str ing)	7abd3182-d399-37bd-9a19-a9ffa1af1d74 💼	应用规则 忽略规则 展示源码	
at.dailermassl.ap.security.taint.webapp.Sanitizer.encode/s(java.lang.String)	7abd3182-d399-37bd-9a19-a9ffa1af1d74 🚍	应用规则 忽略规则 展示源码	
at.dallermassl.ap.security.taint.webapp.Sanitizer.validateXss(java.lang.String)	7abd3182-d399-37bd-9a19-a9ffa1af1d74 🚍	应用规则 忽略规则 展示源码	
org.jgroups.JChannel.checkClosed()	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 氟示源码	
org.jgroups.JChannel.checkClosedOrNotConnected()	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 展示源码	
com.arjuna.ats.Internal.jta.recovery.arjunacore.SubordinateAtomicActionRec overyModule.validatePosition()	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 展示源码	
org.xnio.loUtils.safeClose(Java.lang.AutoCloseable)	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 展示透明	
org.xnio.loUtils.safeClose(java.io.Closeable)	82218a51-dd7c-339d-a8b2-25a39577ba1b	应用规则「忽略规则」展示源码	
org.xnio.loUtils.safeClose(Java.lo.Closeable[])	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 展示源码	
org.xnio.loUtils.safeClose(java.net.Socket)	82218a51-dd7c-339d-a8b2-25a39577ba1b	应用规则 忽略规则 展示源码	
会选 单页全选 忽略规则 R7所忽略			

图表 295 插桩类自动发现规则

1.13.8.3.1 应用规则

点击"应用规则"按钮,会自动跳转至增加插桩类规则页面,刚刚发现的过滤函数会自动填充在"API"一栏中,规则名称、规则类型以及适用漏洞类型需要手动填写。填写完毕后,规则即可生效。点击"取消"按钮,会返回插桩类自动发现规则界面。

	规则名称			
20	过滤函数(sanitizer)			
	at.dallermassl.ap.security.taint.webapp	.xpath.XpathServlet.deadzone(java.lan		
	例如: com.moresec.demo.Sanitizer(java	.lang.String*)		
	*插桩自定义规则填写规范及使用场景说明;	青至【帮助中心】【插桩Agent】【插桩自定义规则	填写规范及使用场景说明】中查看	
屬洞类型	全部类型			
屬洞类型	 全部类型 跨站脚本 	○ 命令执行	URL 重定向	XML外部实体注入
福洞类型	 全部类型 跨站脚本 服务镭请求伪造 	 □ 命令执行 □ LDAP注入 	URL 重定向 xpath注入	□ XML外部实体注入 □ SQL注入
漏洞类型	 全部类型 時站脚本 服务端请求伪造 LOG注入 	命令执行 LDAP注入 表达式注入攻击	URL重定向 path注入 HOL注入	 XML外部实体注入 SQL注入 违反信任边界
扁洞类型	 全部英型 弊站脚本 風务端请求你遠 LOG注入 不安全的反序列化 	 命令执行 LDAP注入 表达式注入双击 目気穿越 	URL重定向 xpath注入 HGL注入 SMTF邮件注入	 XML外部支体注入 SQL注入 透反信任辺界 不安全的XML解析
漏洞类型	 金部英型 	 命令执行 LDAP注入 表达式注入攻击 局家穿越 NoSGL注入 	URL重定向 xpath注入 HGL注入 SMTP邮件注入 不安定的readine方法调用	 XML外部実体注入 SGL注入 违反信任辺界 不安全的対象系統
漏洞类型	全部英型 弊法据本 服务擁请求伪造 LOG注入 不安全的反序列化 Java反射注入 个人隐私数据逻辑	命令执行 LDAP注入 表达式注入攻击 目录穿越 NoSGL注入 充值金額任置修改	URL重定向 xpath注入 HQL注入 MTUBM注入 不安全的readline方法调用 Authentication Bypasses	XML分部实体注入 SQL注入 速反信任边界 不安全的河北朝析 不安全的河北转发 cwr-NewVulnTest

图表 296 应用规则

1.13.8.3.2 忽略规则

点击"忽略规则"按钮,即可忽略对应的过滤函数。在此点击"取消忽略"即可消除忽略状态。支持批量选择规则进行"忽略规则"和"取消规则"。

扫描描目示文规则 播拍描目示文规则 播拍描目动观别规则	入場所設計版計版目標		
			Agent key/stide#88
过速函数	Agent key	操作	
at.dellermassl.ap.security.taint.webapp.Sanitizer.encodeforHtml(javalang.String)	7abd3182-d399-37bd-9a19-a9ffa1af1d74 🗰	应用规则 忽略规则 展示原码	
at.dallermassl.ap.security.taint.webapp.Sanitizer.encodeJs(java.Jang.String)	7abd3182-d399-37bd-9a19-a9ffa1af1d74 🚍	应用规则 忽略规则 黑于源的	
at dallermasslap.security.taint.webapp.Sanitizer.validateXss(java.lang.String)	7abd3182-d399-37bd-9a19-a9ffa1af1d74 🔤	应用规则 加速规则 展示源码	
orgjgroupsJChannel.checkClosed()	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽喻规则 展示源码	
org.jgroups.JChannel.checkClosedOrNotConnected()	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 展示源码	
com.arjuna.ats.internal.jta.recovery.arjunacore.SubordinateAtomicActionRec overyModule.validatePosition()	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 展示原则	
org xnio.loUtils.safeClose(java.lang.AutoCloseable)	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 重于源词	
org.xnio.loUtils.safeClose(java.io.Closeable)	82218#51-dd7c-339d-#8b2-25#39577b#1b	应用机制 加速机制 加于调制	
org.xnio.loUtils.safeClose(java.io.Closeable[])	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 展示源码	
org.xnio.loUtils.safeClose(java.net.Socket)	82218a51-dd7c-339d-a8b2-25e39577ba1b	应用规则 忽略规则 展示源明	
▲法 单页金法 (308.602) 10(6598)			
	共35条 < 1 2 3 4 > 10% 页 / 颠至 页		

图表 297 忽略规则

1.13.8.4 个人隐私数据泄漏规则

个人隐私数据检测支持检测内容自定义,可手动开启、关闭以及新增检测项,使得检测 项可以根据用户需求自行定义。

当前位置:系统配置 > 规则管理					
扫描类自定义规则 插桩类自定义规则	则 插桩类自动发现规则	个人隐私数据泄露规则			
启用状态 全部 👻					规则名称/创建人
规则名称	规则类型	启用状态	更新时间	创建人	操作
qqqq	手动滚加		2021-06-16 17:10:19	admin	编辑 [图]38
5555	手动添加	<u>房用</u>	2021-06-11 15:19:23	admin	编辑 计删除
信用卡号正则	手动源加	度用	2021-06-11 00:42:45	chenlu	mate i mint
555	手动源加	(8冊)	2021-06-15 15:08:18	admin	9838 I 1978
liuc	手动滚加	商用	2021-06-10 19:29:47	lluc	50.400 I 19930
信用卡号	手动源加		2021-06-11 10:45:57	chenlu	anta i mito
测试01	手动液加		2021-06-10 11:37:00	yangjingfeng	aga 11 图12年

图表 298 个人隐私数据泄漏规则

1.13.8.4.1 添加规则

点击"添加规则"按钮,在弹窗中填写规则名称以及规则内容,点击确定即可生效。规则内容为正则表达式。

人隐私数据泄露	添加个人隐	私数据泄露检测规则	
	* 规则名称	请输入规则名称	
	* 新增规则	[1-9]\d{15}(?!\d)	
用状态			
言用 🔵		确 定 取 消	
言用 ●			

图表 299 个人隐私数据泄漏添加规则

1.13.9漏洞类型

用户可以根据需要自定义漏洞等级、漏洞描述、漏洞危害、修复建议,可新增插桩类漏 洞的漏洞类型。

注:若为扫描类 IAST,则列表仅展示扫描类漏洞,若为插桩类 IAST,则列表仅展示插桩 类漏洞,二者皆有则全部展示。若漏洞类型列有两种类型,则为共有类型漏洞。

🎲 雳鉴・IAST 🤐 🗂	日 ♪ ④	● □ FA nt Nakalin 报告管理 账号管理	(後) 系統和第二 幕前中心		yyı 🚅 i 😝
当前位置:系统配置 > 漏洞类型					
派羽英型					
				漏洞名称	() 新営美型
漏洞名称	漏洞等级	漏洞类型	更新时间	⇒ 最近更新人	攝作
auto_test_1661775420	♥ 高危	插桩樂	2022-08-29 20:17:11	cmtest	網細
auto_test_1661766340	• 高忠	插桩类	2022-08-29 17:45:47	cmtest	编辑
auto_test_1661762376	0 高度	播桩类	2022-08-29 16:39:44	cmtest	编辑
auto_test_1661742922	◎ 高危	播桩类	2022-08-29 11:15:30	cmtest	皖播
auto_test_1661738824	◎ 高危	插桩类	2022-08-29 10:07:12	cmtest	编辑
跨站脚本攻击(XSS)	◎ 高危	插桩类,扫描类	2022-08-26 16:42:11	xzm	编辑
xzm潮記	0 高地	扫描类	2022-08-26 15:36:32	xzm	網網
不安全的跨域配置	🗘 低危	播桩类	2022-08-26 15:15:16	xzm	1931E
12	() 高度	播桩类	2022-08-23 17:19:01	ZX	编辑
auto_test_1661237049	() 高度	播桩类	2022-08-23 14:44:15	cmtest	编辑
	#	41条 < 1 2 3 4 5	… 15 > 10 祭/页 ∨ 載至 页		

图表 300 漏洞信息自定义

- 可根据漏洞等级、漏洞类型进行筛选,根据漏洞名称进行搜索,根据更新时间进行正序 或倒序排列。
- ▶ 操作:点击编辑后出现弹框(自定义的插桩漏洞类型可修改漏洞名称,系统设定的扫描

类和插桩类漏洞不可修改漏洞名称)。

漏洞名称	任意文件删除
漏洞类型	插桩类
漏洞等级	高 v *文字换行请使用 标
漏洞描述	应用在处理文件删除时未对目标文件名做合法性校验,导致攻击者可以删除应用所在服务器的任意文件。
漏洞危害	攻击者可通过该漏洞删除应用所在服务器的任意文件,导致应用及服务器可用性被破坏。
修复建议	对将要进行删除操作的文件名进行校验,禁止对系统敏感文件进行删除操作
	保存 返回 恢复默

属洞类型	
	插桩类
漏洞等级	低 ×文字换行请使用
漏洞描述	当开发者将密钥保存在源代码中,在代码投入使用之后,除非对软件进行修补,否则将无法更改密钥。 时。 目时如果软件在外流传,攻击者即可通过反编译等手段直接获取密钥等相关信息。
扇洞危害	开发者无法修改密钥,同时攻击者可以通过反编译获取到硬编码的密钥。
多复建议	不将密钥硬编码于程序中。 br>
	保存返回

图表 301 编辑漏洞信息

漏洞等级可以在高/中/低/提示四种漏洞等级中选择,漏洞描述、漏洞危害及修复建议进行直接编辑时的换行需要用
标签代替,编辑后点击保存即可自定义成功。

点击"恢复默认"按钮可以使弹框内漏洞信息恢复雳鉴设置的默认值,然后点击保存即 可使漏洞信息恢复默认。

1.13.10 web/Idaplog 查询

🇭 雳鉴・IAST	88 11 項目总流 应用管理	auren a	☆ ④ 三方庫 請桩Agent) FA 200 M9200	() Right H	日期	yy I 🚅 I 🕞
当前位置:系统配置 > web/ldaplo	g查询						
web/idaplog查询							
调输入履机数		查询					
结果							
payload示例: weblog: http://192.168.120.200 ldaplog: ldap:/192.168.120.200 以以g4J2为例: \$[jndiid mi: rmi;//192.168.120.2007000 以Llg4J2为例: \$[jndiirmi;//	7000/7data=moresectes 7000/moresectdaptest ap://192.168.120.200700 /moresecrmitest 192.168.120.2007000/mc	0/moresecidaptes resecrmitest}	it)				

图表 302 web/ldaplog 查询

用户在 web/ldaplog 的输入框中输入随机数,点击查询,即可查询 weblog 或者 ldaplog 中的信息。

1.13.11 自定义设置

1.13.11.1 页面自定义

用户可以根据需要将页面 logo、icon 及页面关键词进行自定义设置。

页面及报告自定义	机器性能阈值自定义	证书自定义	检测自定义	项目风险值自定义	k8s webhook部署自定义	用户登录控制 😗
1. 自定义LOGO						
登录页LOGO	上传PNG 图片文件240pp	к*170рх				
	雳鉴·IAS	т				
主页面LOGO	上传PNG 图片文件204p:	x*54px				
	₿ 雳鉴・IAST					
主页面ICON	上传ICON 支持的图片大	小32px * 32px、48p	x*48px, 64px*64px			
	52					
报告LOGO						
PDF、WORD报告	上传PNG 图片文件140pz	x*42px				
	₿ 閉 盤 · IAST					
在线查看报告	上传PNG 图片文件160pt	x*40px				
	₿					
		图表	き 303 页面	「自定义		

杭州默安科技有限公司

151

- 自定义LOGO:用户单击上传按钮后,弹窗浏览本机文件,选择需要的logo文件或icon 文件,点击确定后,若符合要求即提示上传成功,在框内显示上传文件的缩略图。
 - 登录页 LOGO 图片格式要求为 PNG, 上传图片要求为 240px*170px 大小
 - 主页面 LOGO 图片格式要求为 PNG, 上传图片要求为 204px*54px 大小
 - 页面 ICON 图片格式要求为 ICO, 上传图片要求为 32px*32px、48px*48px 或 64px*64px 大小
 - PDF、WORD 报告首页 logo 格式要求为 PNG, 大小为 140px*42px
 - 在线查看报告首页 logo 格式要求为 PNG, 大小为 160px*40px
- ▶ 设定页面关键词:在输入框内输入需要的关键词(不超过 20 个字符),对页面内"IAST" 字段进行替换。

点击保存后提示更新成功。

1.13.11.2 机器性能阈值自定义(扫描类)

用户可以根据需要自定义流量信使的 CPU 负载及内存占用阈值、流量信使所在服务器的 CPU 负载及内存占用阈值、IAST 服务器的 CPU 负载及内存占用阈值。

当机器性能检测连续三次达到设定的阈值时,发送站内示警及邮件通知。 在流量信使阈值配置中,若流量信使占用 CPU 负载或占用内存连续三次达到阈值时,除发送 站内警示及邮件通知外,还将触发流量信使自动暂停功能。流量信使暂停 5 分钟后自动重启 流量信使。

在插桩 Agent 阈值配置中,若 Agent 所在系统 CPU 负载或占用内存连续三次达到阈值时, 除发送站内警示及邮件通知外,还将触发插桩 Agent 自动暂停功能。Agent 暂停后,若连续 3 次检测未超过设定阈值后自动重启 Agent。(该功能仅对 Java 语言插桩 Agent 起效)

🗭 雳鉴・IAST	88 政治目前		♪ ④ ! 第三方库 描桩Agen	 () 	FA 🚳	■ 幕助中心		yy I 🚅 I 🕞
当前位置:系统配置 > 白定义配置								
页面及报告自定义 机器	性能調查自定义	证书自定义	检测自定义	项目风险值自定义	k8s webhook部層自這	2. 用户登录控制 😑		
* 当机器性能检测连续三次达到设定 在流星信使调值配置中,若流星信 在插桩Agent阈值配置中,若Age	的阈值时,发送站 便占用CPU负载或 nt所在系统CPU负	的示警及邮件通知。 2占用内存连续三次达3 载或占用内存连续三次	则阈值时,除发送站内容示 (达到阈值时,除发送站内)	及邮件通知外,还将触发流 警示及邮件通知外,还将触	量信使自动暂停功能。流量的 发播桩Agent自动暂停功能。	i便暫停5分钟后自动重启流量信使。 Agent暫停后,若连续3次检测未超过设	设定简值后目动重启Agent。(该功能仅对Java语言搞桩Agenti	2M)
IAST服务器CPU负载				-	- 74%			
IAST服务器内存占用				•	90%			
IAST服务器硬盘占用	-				94%			
流量信使占用CPU负载	-				100%			
流量信便占用内存					00%			
流量信使服务器CPU负载	-				100%			
流量信使服务器内存占用					00%			
Agent所在系统CPU负载					100%			
Agent所在系统占用内存					100%			
告答周期	10 /9	钟 🙁						
	保存							

图表 304 自定义机器性能阈值

杭州默安科技有限公司

152

1.13.11.3 证书自定义(扫描类)

用户可以上传服务器证书以进行 Https 协议项目检测,适用于鉴权代理模式、非鉴权代理模式及 VPN 模式的项目检测。在列表内包含域名/IP、操作人、操作时间、标签及操作。

注: 请使用 Tomcat/Apache 的证书格式。

当前位置:系统配置 > 白拉	文配置									
页面及报告自定义	机器性能阈值自定义	证书自定义	检测自定义	项目风险值自定义	k8s webhook部署自定义	用户登录控制 💿				
										上街证书
域名/IP		操作人 握			摄作日时间				操作	
moresec.cn		huyk			2022-07-05 13:02:30 test 🖉 👹 🖗					
					共1条 < 1 >	10 条/页 ∨				

图表 305 自定义证书

▶ 点击"上传证书"按钮,在弹框内填入所传服务器证书的域名/IP,添加标签(可不填), 选择本地证书文件后点击"确定",校验域名/IP与所选证书相符后即可上传成功,新 增证书会更新至列表中。

上传证书	
* 域名/IP	192.168.120.62
标签	test
	选择证书
	<u>商</u> 之 取当
	441 元 以 /月

图表 306 自定义证书-上传证书

▶ 点击列表上对应证书标签栏的修改按钮,点击修改后保存,标签即修改成功。

标签		
test	保存	取消

图表 307 自定义证书-修改标签

▶ 点击列表上操作栏的删除按钮,在弹框中点击"确定",即可删除成功。



图表 308 自定义证书-删除证书

1.13.11.4 检测自定义(插桩类)

用户可在此开启 Agent 应用场景、CSRF 检测增强模式、Response 检测、Json XSS 检测、 API 覆盖率计算方法和 Java Agent 全局参数。

页面及报告自定义	机器性能阈值自定义	证书自定义	检测自定义	项目风险值自定义	k8s webhook部署自定义	用户登录控制
垂桩 横式						
Agent 应用场景	正常模式 推荐 检测效果与性能均衡。		性能模式 追求极致性能的场	景使用,可能会导致漏报。	高检出模式 提高罵問检出率,但可能会产 麵。	生误报以及性能问
CSRF检测增强模式						
Response检测						
son XSS检测						
API覆盖率计算方法	🔽 不计算中间件API 🛛 🛃	不区分同一接口的不同请:	求方式			
ava Agent 全局参数 😗	谓输入Agent参数 例: ("moresec.iast.enable":"tr	ue",				
	"moresec.trace.ttl.max":" }					

图表 309 检测自定义

- ▶ 为了降低 CSRF 误报率,可在此开启 CSRF 检测增强模式。
- 为了降低 Agent 的资源消耗, 雳鉴未开启全部检测点, 可在此开启更全面的 Response 检测。
- ▶ 为了可以正常检测出 json 响应格式的 xss 漏洞,可在此开启 Json XSS 检测。
- > API 覆盖率计算方法:用户可选择不计算中间件 API 和不区分同一接口的不同请求方式。
- ➢ Java Agent 全局参数:用户可设置 Java Agent 全局参数, Agent 下一次启动时参数配置 生效。

1.13.11.5 项目风险值自定义

用户可以自定义高危、中危、低危、提示漏洞的单个扣除分数和最多扣除分数。

页面及报	告自定义	机器性能阈值自定义	证书自定义	2 检测自定义	项目风险值自定义	用户登录控制 🕗
高危漏洞:	单个扣除分数	40	最多扣除分数	100		
中危漏洞:	单个扣除分数	10	最多扣除分数	40		
氏危漏洞:	单个扣除分数	3	最多扣除分数	20		
是示漏洞:	单个扣除分数	3	最多扣除分数	20		

图表 310 项目风险值自定义

▶ 点击保存,该自定义的风险值将被应用于保存后创建的项目风险值计算。

▶ 点击重置,各风险值将被重置为雳鉴的初始风险值。

1.13.11.6 k8s webhook 部署自定义

用户可在此界面编辑插桩 Agent 标记位置(namespace、labels)和插桩 Agent 启动参数(jvm 参数),点击保存后生效

9 雳鉴	·IAST	项目总览	应用管理 满词管理	第三方库 插桩Agent	續像扫描 报告管理		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		уу ' 🚥 ' (=>
当前位置: 系统	統配置 > 自定)	2.0200							
页面及报告的	自定义	机器性能阈值自定义	证书自定义	检测自定义	项目风险值自定义	k8s webhook部署自定	<u>×</u>	用户登录控制 🕗	
插桩 Agent 标	记位置								
namespaces	autotest								
labels	请输入								
播桩 Agent 启	动参数								
jvm参数	调输入								
	(Q 77								
	PK 17								

图表 311 k8s webhook 部署自定义

1.13.11.7 用户登录控制

用户可以在此界面开启用户登录控制功能,开关打开后,只有列表中的白名单 IP 允许访问产品。其余地址均无法访问产品的页面与 api。列表中展示源 IP、描述以及编辑、删除操作。编辑可以对己有信息进行修改,点击删除后会弹出对话框,确认是否删除。

当前位置:系统配置>自3	主义配置							
页面及报告自定义	机器性能調值自定义	证书自定义	检测自定义	项目风险值自定义	用户登录控制 \Theta			
用户整要控制								nt &
IP			描述				操作	
					10	无政语		

图表 312 用户登录控制

点击添加按钮,可以添加源 IP 信息。填写描述以及源 IP 地址段后,点击保存即可。

定义	项	新增登录白名	单	
		描述	请填写描述	
		*源IP地址段	请填写IP地址段,例如:172.16.1.1/24 或者 172.16.2.1/32	
			确定取消	
			李云	
			陈路	

图表 313 新增用户白名单

1.13.12 流量镜像管理(扫描类)

💋 雳鉴 · IAST						⑧ 系統配置				yy i 🚅 i 🕞
当前位置: 系统配置 > 流量	國命管理									
流量損像服务管理	流量铸像请求信息									
流量機像服务器IP			标签				状态	操作		
192.168.180.202							 运行中 	Re	名単 扁开 ▼	

图表 314 流量镜像管理

流量镜像管理页面可让用户对流量镜像进行管理,流量镜像服务器安装好后,会自动出现一条记录,展示出流量镜像 IP,标签,状态,操作。

- 流量镜像 IP: 代表流量镜像服务器的 IP
- 标签:用户可以添加标签来对流量镜像进行标识
- 状态:分为离线和在线,在线为正常状态,离线为异常状态

 操作:详情:展示流量镜像服务器的性能和收包个数;黑白名单:用户可查看该流 量镜像下的黑白名单列表

1.13.12.1 流量镜像请求信息

对流量镜像中最近请求 HOST 进行排布与展示

当前位置:系统配置 > 流量镜像管理		
流量铁像服务管理 流量铁像请求信息		
最近请求HOST		最近请求时间
-		2021-06-18 13:56:56
zta-jira.moreseo.com.cn:8443		2021-06-17 15:31:36
wc.qlogo.cn		2021-06-17 15:31:36
www.zjarmyy.cn		2021-06-17 15:31:36
www.qq.com		2021-06-17 15:31:36
szextshort.weixin.qq.com		2021-06-17 15:31:36
extshort.weixin.qq.com		2021-06-17 15:31:36
dns.weixin.qq.oom		2021-06-17 15:31:36
btrace.q.com		2021-06-17 15:31:36
alpha-cloud-log.cn-hangzhou.log.allyuncs.com		2021-06-17 15:31:36
	井145条 1 2 3 4 5 … 15 > 10条/页 排页	a

图表 315 流量镜像请求信息

1.13.13 日志审计

日志审计主要用于对雳鉴用户的操作日志做存储记录,方便后续对日志进行审计,帮助 系统管理人员发现异常操作,及时告警。日志模块记录了登录用户、登录 IP、事件类型、审 计时间、事件结果和具体的事件详情,并且支持通过登录用户、登录 IP 及事件类型进行搜索 筛选。支持日志全量下载导出和查询结果过滤导出。

😚 雳鉴·IAST					w 1 🚅 1 G
48位置: 系统定置 > 日志中计					
10401					
12.276 ¹⁴	220	aneti Esa			下載日志
登录用户	世界で	專件类型	·新计时间	春件活用	操作
ywk	192,168,30.19	编辑项目	2022-08-31 16:57:02	28225	8220 ×
專件例型:编编项目 原約环络:用户 ywk 编编项目。 舉約结果:成功	. 项目名称: ms_proxy (页目站: [241])				
ywk	192,168.30.19	编辑项目	2022-08-31 16:53:36	成功	篇开・
ywk	192.168.30.19	暂停拉用	2022-08-31 16:50:11	<i>1</i> 8230	展开▼
ywk	192.168.30.19	解停检测	2022-08-31 16:49:58	16281	龍井▼
yutong	192.168.32.54	聖景	2022-08-31 16:45:43	成功	展开▼
lyq	192,168.102.121	创建角色	2022-08-31 16:41:11	成功	親田 *
admin	192.168.32.48	用户-更新用户	2022-08-31 16:37:32	78737	職件 *
admin	192.168.32.48	型录	2022-08-31 16:36:38	15(2)	銀行 *
zhangżc	192.168.32.48	間当	2022-08-31 16:36:27	10,770	龍开▼
vwk	192,168.30.19	编编项目	2022-08-31 16:23:32	1820	展开▼

杭州默安科技有限公司

157

1.14 帮助中心

帮助中心主要用于介绍雳鉴的关键使用流程和对用户可能碰到的问题进行答疑,由15部分组成:证书配置、代理配置、逻辑漏洞检测、插桩Agent、流量信使、规则管理、第三方插件、Jenkins pipeline、k8s webhook部署、忘记密码、角色升级、系统升级、用户手册下载、产品 API 文档查看、安全组件、安全编码规范参考。

位置:帮助中心					
中心					
证书配置	* 測试配置				
代理配量 逻辑漏洞检测			5 配置检测		
插桩Agent 流量信使	常用功能				
观则管理 第三方插件	· 224年2388376月台2315	♀ 流量信便	规则管理	↓ 插桩Agent	
enkins pip <mark>el</mark> ine	第三方插件				
8s webhook部署 封己密码	S M M M M M M M M M M M M M	镜像扫描Jenkins插件			
他升级	Lauffer also fine				

图表 317 帮助中心

1.15 消息中心

消息中心会对项目进度、项目状态变动、账号升级、服务器告警及流量信使告警等进行 通知。

SHUTSLAN	88+0		
息中心	5451魚米读		
	标题	接收在时间	操作
	权限审批總國	2019-07-24.11:19:18	④ 删除:
	账号: sktest 的注册申请需要您审批通过	2019-07-24.11:17/21	◎Ⅰ删除
账号:	ktest 的注册申请需要您审批通过请到 账号管理-权限审批 查看, 通过后该账号才可以正常	使用	
	服务器告部	2019-07-11 17:44:22	
您好,	§务購192.168.199.55系統內存负載已到法设定的简值:1%,请及时处理。		
	服务器告誓	2019-07-11 17:43:21	④ 删除
	銀券録告誓	2019-07-11 17:42:20	④ 删除
	服务醫告答	2019-07-11 17541/20	④ 删除
	服务器告望	2019-07-11 17:40:19	利用 ④
	服务耦告管	2019-07-11 17:39:19	金●●
	服务器告答	2019-07-11 17:38:18	④ 删除
	服务器告誓	2019-07-11 17:38:18	④ 删除
	质全选 会选 标记已读 量除新选		
		共6237条 < 1 2 3 4 5 … 624 > 跳盔 页	

杭州默安科技有限公司

158

1.16 第三方插件(扫描类)

1.16.1 漏洞扫描插件

Jenkins 是当今使用最常用的开源持续集成(CI)工具之一,开发团队可以使用 Jenkins 完成整个自动化管理构建过程。 房鉴生成的 Jenkins 插件是一个将房鉴与 Jenkins CI 项目 集成的工具,可以让您在 Jenkins 中轻松配置房鉴项目并查看结果。房鉴 IAST 通过与 Jenkins pipeline 工作流框架的集成,将自动化安全测试融入到 pipeline 测试流程中,实现 DevSecOps 目标。

1.16.1.1 漏洞扫描插件使用步骤

🗭 雳鉴・IAST										日 「「「」 「「」」 「」」		yy I 🚅 I 🖨
当前位置:帮助中心												
帮助中心												
证书配置		漏洞扫	描Jenkins뒘	消下载: 🛒	油下戰							
代理配置			1					4			6	
逻辑漏洞检测		安	装插件	进行全	局设置	新增项目		配置项目	构建口	 页目	查看扫描结果	
插桩Agent		1.在帮助	助中心第三	方插件-Jenk	ins插件中,下	载Jenkins播	14					
流量信使			.	8		ER.	() Filter					
规则管理			cinios de	and the second	27700 INC. 19	at sponted	. spostar	C. Distanti	HEADER-CO			
第三方插件												
灑洞扫描插件		T	ienkios i 649	TR: 007								
镇像扫描插件		1	1		- 2							
Jenkins pipeline			安装播	14 进	行全局设置	新增项	8	配置项目	和10101页目	1 1		
k8s webhook部署			1.在帮助中。	心-第三方插件	- Jenkins插件中,	下舰Jenkins制	94					
忘记密码	-	2.打开」	lenkins,点	击左侧导航相	三中的"系统管	理",选择"插	件管理。					-

1) 在帮助中心-第三方插件-Jenkins 插件中,下载 Jenkins 插件

图表 319Jenkins 插件下载

2) 打开 Jenkins, 点击左侧导航栏中的"系统管理",选择"插件管理"

🧶 Jenkins	
Jenkins 🔸	
音 新建任务	
🌯 用户列表	
>构建历史	
🔅 系统管理	
& 我的视图	
Section Lockable Resources	
👰 凭据	
新建视图	
构建队列	-
队列中没有构建任务	
构建执行状态	-
1 空闲 2 空闲	



3) 在"插件管理"中选择"高级(Advanced)",在上传插件处选择在雳鉴帮助中心内下 载的插件文件上传。

Senkins Jenkins) 插件管理		
▲ 返回工作台	可更新 可选插件 已安装 高数	
· 更新中心		
	満口	
	用户名 admin	
	密码	
	不通过代理的主机	
	殿	
	上1支1田1十 您可以通过上传一个.hpi文件来安装插件。	
	文件. 选择文件 未选择任何文件	

4) 安装插件完成后,打开 Jenkins-系统管理-系统设置进行全局配置

🙆 Jenkins		
Jenkins 🔸		
🕋 新建任务		
🌯 用户列表		管理Jenkins
≥ 构建历史		
🔅 系统管理		系统设置 全局设置和略经
44 我的视图		ALL THRETHING
Section Lockable Resources		
条 凭据		Jenkins安全,定义谁可以切问或使用杂税。
📄 新建视图		凭据配置 配置凭据的提供者和类型
构建队列	-	
队列中没有构建任务		全局工具配置 工具配置,包括它们的位置和自动安装器
构建执行状态	-	一 读取设置
1 空闲 2 空闲		▶ 放弃当前内存中所有的设置信息并从配置文件中重新读取 仅用于当您手动修

5) 在"系统设置"内找到"IAST 全局配置"

Tel: (+86) 400-0571-211

AST服务器地址	http(s)://domain:port	
AST系统用户名		
AST系统密码		
		连接测试
3描任务超时时间(minutes)	120	
I描任务超时本次任务状态·	失败 ● 不稳定	
和洞超基线时本次任务状态	◎ 失败 ◉ 不稳定	
后温洞基线:	1	
中危漏洞基线:	1	
危漏洞基线:	100	
2.程源词其样。	100	

6) 按提示格式填入 IAST 服务器地址,填入管理员、项目经理或安全人员角色的 IAST 系统用户名密码,点击连接测试按钮可以测试填写信息是否正确。

IAST全局配置		
IAST服务器地址	http://192.168.120.62:81	
IAST系统用户名	admin	0
IAST系统密码		
	用户名/应码正确 连接测试	at 🛛

7) 设置"扫描任务超时时间"与"扫描任务超时本次任务状态",当扫描时间超过设定值后,任务的构建状态将为设定的超时任务状态;设置"漏洞基线"及"漏洞超基线时本次任务状态",当扫描到的任一等级漏洞数大于或等于设定的基线值时,任务的构建状态将为设定的超基线任务状态。

扫描任务超时时间(minutes)	120
扫描任务超时本次任务状态: 漏洞超基线时本次任务状态:	 ○ 失败 ● 不稳定 ○ 失败 ● 不稳定
高危漏洞基线: 中危漏洞基线:	1
低危漏洞基线:	100
提醒漏洞基线:	100

- 8) 配置完成后点击保存使全局配置生效
- 9) 在 Jenkins 左侧导航栏中点击"新建任务"

🧕 Jenkins	
Jenkins 🕨	
쯜 新建任务	
🌯 用户列表	
📂 构建历史	
🔅 系统管理	
🌯 我的视图	
Section Lockable Resources	
👰 凭据	
▶ 新建视图	
构建队列	
队列中没有构建任务	
构建执行状态	
1 空闲	
2 空闲	

10) 输入名称,选择"构建一个自由风格的软件项目",点击确定

IAST	项目一
必填项	
	构建一个自由风格的软件项目 这是Jenkins的主要功能.Jenkins将会结合任何SCM和任何构建系统来构建你的项目,甚至可以构建软件以外的系统。
w)	流水线 精心地组织一个可以长期运行在多个节点上的任务。适用于构建流水线(更加正式地应当称为工作流),增加或者组织难以采用自由风格的任务类型。
	构建一个多配置项目 适用于多配置项目,例如多环境测试,平台指定构建,等等。
)	GitHub 组织 扫描一个 GitHub 组织(或者个人账户)的所有仓库来匹配已定义的标记。
6)	多分支流水线 根据一个SCM仓库中检测到的分支创建一系列流水线。
	文件夹 创建一个可以嵌套存储的容器,利用它可以进行分组。 视图仅仅是一个过滤器,而文件夹则是一个独立的命名空间, 因此你可以有多个相同名称的 的内容,只要它们在不同的文件 夹里即可,
编员	一个已经存在的任务创建,可以使用这个选项

eneral 源码管理 构建航发圈 构建环境 得建 构建后操作	
1 2日1月7月4年	0
轮间 SCM	0
9建环境	
Delete workspace before build starts	
Use secret text(s) or file(s)	0
Abort the build if it's stuck	
Add timestamps to the Console Output	
With Ant	Ø
回建	
9建 增加地址非微 ▼ Execute Python script	
增加附级进步微 • Execute Pythan script Invoke Ant	
増加時報経行版 ・ Execute Python script Invoke Ant Invoke Gradie script	
増加時期経済版 ・ 増加時期経済版 ・ Execute Pythan script Invoke Ant Invoke Gradle script Run with timeout	
P建 I項加速法が識 ・ Execute Python script Invoke Ant Invoke Gradle script Run with timeout Set build status to "pending" on GitHub commit	
増加時転送炉煤 ・ Execute Python script Invoke Ant Invoke Gradie script Run with timeout Set build status to "pending" on GitHub commit 倒硬IAST顶目(時在測版的段之前確立IAST顶目)	
項加納加諾炸價 ▼ Execute Python script Invoke Ant Invoke Gradie script Run with timeout Set build status to "pending" on GitHub commit 创建IAST项目(请在测试阶段之前建立IAST项目) 执行 Windows 批处理命令	
增加附加证券價 ▼ Execute Python script Invoke Ant Invoke Gradie script Run with timeout Set build status to "pending" on GitHub commit 创建IAST项目(请在测试阶段之前建立IAST项目) 执行 Windows 批处理命令 执行 shell	

12) IAST 项目名称默认填入 Jenkins 任务名称,也可自行修改,填写完成后点击"项目 名称测试"按钮以测试项目名称是否已占用,若显示可用即可进行下一步,否则需要对项目 名称进行修改; (被测站点地址可以填入域名或 IP 地址;最大扫描并发量默认 50,用户可 根据需要进行修改,修改范围为 1[~]500)

创建IAST项目(请	在测试阶段之前建立IAST项目)	
IAST项目名称	Jenkins项目—	
	项目名称可用	顶目名称测试
被测站点地址	域名或ip地址	
最大扫描并发量	50	

13) 在"增加构建步骤"内选择自动化测试步骤并进行配置

14) 在"增加构建步骤"内选择"执行 IAST 扫描"(在执行扫描前需要在测试业务服务器上安装流量信使并且配置完成自动化测试步骤)

	Execute Python script
	Invoke Ant
	Invoke Gradle script
	Run with timeout
	Set build status to "pending" on GitHub commit
	创建IAST项目(请在测试阶段之前建立IAST项目)
	执行 Windows 批处理命令
	执行 shell
Γ	执行IAST扫描(请先在测试业务服务器上安装流量信使,且在测试阶段之后执行IAST扫描
	调用顶层 Maven 目标

15)执行 IAST 扫描内配置默认与全局配置中相同,可以根据需要进行修改,设置"扫描 任务超时时间"与"扫描任务超时本次任务状态",当扫描时间超过设定值后,此任务的构 建状态将为设定的超时任务状态,设置"漏洞基线"及"漏洞超基线时本次任务状态",当 扫描到的任一等级漏洞数大于或等于设定的基线值时,此任务的构建状态将为设定的超基线 任务状态。

170856163163(1001006)	
扫描任务超时本次任务状态	◎ 失敗 ● 不稳定
漏洞超基线时本次任务状态	◎ 失败 ● 不稳定
高危漏洞基线:	1
中危漏洞基线:	1
低危漏洞基线:	100
提醒漏洞基线:	100
加构建步骤 🔻	

配置完成后点击保存。

16) 在配置项目完成后点击保存,进入项目页面,在左侧导航栏中选择"立即构建"

🧕 Jenkins		
Jenkins > Jenkins项目—	E.	
 ▲ 返回面板 Q 状态 ジ 修改记录 		工程 Jenkins项目一
 ■ 工作空间 ② 立即构建 ③ 删除工程 ③ 配置 ○ 重命名 		工作区 量新修改记录
Build History	构建历史 =	相关链接
find	х	
S R.	SS 全部 <mark>돐</mark> RSS 失败	

17) 在左侧导航栏下方可以查看构建状态

🧕 Jenkins	
Jenkins → Jenkins项目— →	
 ▲ 返回面板 Q 状态 ご 修改记录 	工程 Jenkins项目一
 ■ 工作空间 	
→ Build History 均建历史 = find x → #3 2018-11-30 下午2:33 ∞ ∞ #3 2018-21-30 下午2:33 ∞ ∞ #3 2018-21-30 ∞ ∞ ∞ ∞ ∞	伯大链接

18) 构建完成后点击此次构建进入此次构建页面

🧕 Jenkins		
Jenkins > Jenkins项目—)		
┢ 返回面板		工程,lenkins项目—
🔍 状态		
🥏 修改记录		
┣ 工作空间		
🔊 立即构建		工作区
◎ 删除工程		0000000
🔅 配置		✓ 最新修改记录
🔁 重命名		相关链接
Build History	构建历史 =	 最近一次构建(#1),32 分之前 最近成功的构建(#1),32 分之前
find	х	 最近不稳定的构建(#1),32 分之前 最近未成功的构建(#1),32 分之前
🥥 #1 2018-11-30 下午2:37		• 最近完成的构建(#1),32 分之前
RS	<u>S 全部 🔊 RSS 失败</u>	

19) 在左侧导航栏内点击"扫描结果"

🧶 Jenkins	
Jenkins → Jenkins项目— → #1	
摿 返回到工程	
Q. 状态集	🥥 构建 #1 (2018-11-30 14:37:38)
🔁 变更记录	
🔄 控制台输出	000000
🔁 编辑编译信息	2 没有变化。
◎ 删除本次生成	
12 扫描结果	之 启动用户admin

20) 查看扫描结果

🔮 Jenkins			《《土北	② admin (注约
nkins → Jenkinsīģ⊟— → #1 →	日福靖県			北日南部市
返回到工程				
(状态集	IAST扫描结果			
*#)5 3	扫描摘要			
控制台输出		3.828 Courses	and a second	100
律祖律洋信息	A	18	28	28
開除本次生成	1.0	信求数	温可致	未修复
扫描结果				
	漏洞等级分布		漏洞类型分布TOP10	
				- ITANE A
	- R		spring@Willi	Carter
		-**	softers	- Helder States
			任双文件 卜载 ——————	
	118		SQL MENTLY.	
	漏洞状态			
	😑 😹 Raz 💿 🗆 AZ 🗮 😑 + AZ 🗮			
	246			
	12			

1.16.1.2 Jenkins pipeline 脚本使用步骤

1) 在帮助中心-Jenkins pipeline-Jenkins pipelin 脚本下载中,下载 Jenkins pipeline 脚本

🗭 雳鉴・IAST	田	уу Т 🚅 Т 🕞
当前位置:帮助中心		
帮助中心		
证书起置 代理起量 逻辑顺向检测 播在Agent 消瘟倍使	Jenkins pipeline脚本下载:点击下载 1 2 3 3 获取程序 参数说明 集成元例 1.下载Jenkinspipeline载诗井上传至Jenkins缓务器中(这里做在/var/fib/jenkins/workspace/指径下)。	
规则管理		
第三方插件		
Jenkins pipeline		
k8s webhook部署		
忘记密码		
角色升级		
系统升级	,	

2) 使用说明

[root@m	ereces just test. It should be so lipuy tool
LLOOLGIN	oresec-rast-test ~]# childu +x go-thiux-toot
[root@m	oresec-last-test ~]# ./go-linux-tool -h
Usage o	f ./go-linux-tool:
-b st	ring
	warn, low, mid, high (default "warn")
-conf	string
	if mode 1, conf is host; if mode 2, conf is your web appname
- d	if true, pipeline will delete project when pipeline stop.
- h	this help
-ip s	tring
	sdl ip addr
-mode	int
	1 unauthorized project mode 2 IAST project mode (default 1)
-port	int
	sdl web port (default 81)
-t st	ring
	it will force pipeline to stop when localtime is deadline.

杭州默安科技有限公司

168
-b:告警级别(提示、低级、中级、高级;默认提示)
-conf:如果是1则是主机地址 如果是2则为应用名
-d:如果为 true 当 pipeline 停止时则删除项目
-h:显示帮助命令
-ip: IAST 的 Web 应用地址
-port: IAST 端口,默认为 81
-mode:1为非鉴权代理项目(默认) 2为插桩项目
-t: Pipeline 停止时间

3) 在 192.168.120.62:81 上创建一个非鉴权代理项目,项目地址为 www.baidu.com, 11.03

分自动停止

[root@moresec-iast-test ~]# ./go-linux-tool -b low -conf www.baidu.com login successfully creat project successfully, please start sending your request tool will wait until end deadline, that -t XXXXXX	-ip 192.168.120.62 -mode 1 -t "2020-07-21 11:03:00"

4) 在雳鉴 iast 的项目管理-项目列表中可以看到创建成功的项目

www.baidu.com-Zs21		公 回
项目模式: 非鉴权代理模式		
项目状态:已完成	0	安全
项目归属人: admin	漏洞数	安全等级
请求数:0	1	暂停检测
漏洞修复占比: 0.00 ▼当前测试进度0.00%		

5) 创建项目成功后可以手动录入请求,也可以编写自动化脚本录入请求

[root@moresec-last-test ~]# date
2020年 07月 21日 星期二 11:02:24 CST
[root@moresec-iast-test ~]# ./go-linux-tool -b low -conf www.baidu.com -ip 192.168.120.62 -mode 1 -t "2020-07-21 11:03:00"
login successfully
creat project successfully, please start sending your request
tool will wait until end deadline, that -t XXXXXX
wait sdl project end
base line is low
creat project report successfully. You can log in to view
pass the baseline: low, exit 0[root@moresec-iast-test ~]#

6) 点击进入项目详情页查看扫描结果

and an an and an a	· 项目列表 > 项目详细								
ijianquan	金校(C进稿云)								
0 *****	<u>去職論学校:767</u> 10月中 日記和 時代和	項目地址: 11 請求数: 11 例は人员数: 0 创建日期: 2	92.168.180.57:8079 3739 922-08-23 15:33:57		项目描述:	1jq			适日控制 0
高危	震時数: 25 中容量 已感觉	项目归属人: 5) 项目级员: 元 项目模板: 5) 用户凭证状态: •	f 	助往设置)					
							用户关注数件	Restor - stat	B R MURE
NAST ALLOWA	sitemap Halliads RRRads							a a a a a a a a a a a a a a a a a a a	
BiAtt 45977	sitemup 13組込ち 税取込ち ・ 等級 会応	×	80	 开始时任 主当 	+		APSENA BARRE		RHUL/RAAR
 100017 100017	Stemup BBBibs R05255 • 098 === (055) eec applyLatinebapy/valss/log/ oon		82 55	• Rithtic 100	٠	主动的证: - 物成人品: fyf	1 2 2 2 2 2 2 2 2 2 2	9999149; 2022-08-31 00:07;21 1889149; 2022-08-29 16:02:33	AND AND A CONTRACT OF AN AND AND AND AND AND AND AND AND AND

杭州默安科技有限公司

169

1.16.2 镜像扫描插件

1.16.2.1 镜像扫描插件使用步骤

1) 下载镜像扫描 Jenkins 插件。

00 项目总览	日本市管理	周調管理	♪ 第三方库	(∲) 插桩Agent		[]] 报告管理	日本 「東雪吉理		日 日 日 日 日 日 日 日 日 日 日 日 日 日	
	5 m									
-	镜像扫	描Jenkins插	件下载: 点	陆下载						
2) 打	开 Jenki	ns, 点击	左侧导射	<u> </u>	系统管理	<u>!</u> ",选择	"插件管理	里"。		
	Dashboard * >		玄俠配署							
			不知日じ且 系統配置 配置全局设置和	腾径	全局工具配置 工具配置,包括它	们的位置和自动安装器	▲ 可用更新	成启用Jenkins功能扩展插		
			节点管理 添加、删除、招 点。	放制和监视系统运行任务的节						
			安全							
				定义谁可以访问或使用系	Manage Crede Configure creder	entials ntials	凭据配置 配置凭据的提供者	和类型		
			管理用户 创建、删除或格	設 Jenkins 用户	In-process Sc Allows a Jenkins proposed scripts which run inside so could bypass	ript Approval administrator to review (written e.g. in Groovy) the Jenkins process and security restrictions.				
			状态信息							

3) 在"插件管理"中选择"高级(Advanced)",在上传插件处选择在帮助中心内下载的插件文件上传。

織交	高级
上传插件	
您可以通过上传一个.hpi文件来安装插件。	
文件: 浏览	
E16	
升级站点	
URL https://updates.jenkins.jo/update-center.json	
建 文	
	21小时之前获取了更新信息

4) 安装时勾选"重启" Jenkins。

Dashboard · 更新中心					
● 道图工作台 登 程度 Jonkins 表 磁件管理	安装/更新 ^{演奏} messec-itacsame 演奏 重記 Jenkins ● (通知意所使用已社) ● 配安英方成前意品	插件中中 ① 開作moresec-itscsanne已经安装元度、Jert - Checking internet connectivity - Checking update center connectivity - Success - Gorgen - 保好的紹行 enkint(空)時計)	kins 重应后才能生效。		

5) 安装好插件,等待 Jenkins 重启后在点击系统管理-系统配置。

系统配置				
系统配置 配置全局设置和路径	X	全局工具配置 工具配置,包括它们的位置和自动安装器	ŧ	插件管理 添加、删除、禁用或启用Jenkins功能扩展插件。 ▲ 可用更新
节点管理 汤加、删除、拉制和监视系统运行任务的节点。				
安全				
全局安全配置 Jenkins 安全,定义谁可以访问或使用系统。	%	Manage Credentials Configure credentials	Å	凭据配置 配置凭据的提供密和类型
管理用户 创建、删除或得改 Jenkins 用户	2	In-process Script Approval Allows a Jenkins administrator to review proposed scripts (written e.g. in Groovy) which run inside the Jenkins process and so could bypass security restrictions.		
状态信息				
系统信息		系统日志	-	负载统计

6) 搜索 Moresec IscScanner,在其中配置相关服务器地址以及端口、认证账户信息(均

为 IAST 的地址 ip)。		
Dashboard [,] 配置		
	Moresec IscScanner	
	服务器地址	0
	http://192.168.120.100:81	
	Access Key	0
	62b7c43df80db364da31761d	
	Secret Key	0
	Concealed	Change Password

7) AK/SK 认证账户信息可以在 IAST:账号管理-AK/SK 中找到。

約位置: 医弓管道 > AK/SK	用户管理	
K/SK	10177世3世	
方 通過第 ▼	角色管理	查看使用说明 生成AK/SK
	权限审批	
用户 AccessKey SecretKey	NUER C RECENT	0 Mg/¥
yy 630dd786a882e989c557e301 0 ********	AX/SK 2022-08-30 17:25:26	9548 (F.H.) (H.H.)
0 mm (要求 安全设置	
带闪王达 <u>22.84世纪</u>		

8) 在项目构建中增加构建步骤,选择 Moresec IscScanner,扫描方式选择镜像扫描, 可设置风险阈值。

General 源的管理 利進脫及盛 利進汴渠 19鐘 能直扫描力式 配直扫描力式 配直扫描力式 利進后條下 4h2a
199速
Moresec IscScanner
配置扫描方式
 ① 扫描初始化 ○ 扫描結束
○ 扫描镌像
Moresec IscScanner
配置扫描方式
○ 扫描初始化
存在该风险等级源洞时,创建失败
High v
扫描喷像名称

9)项目构建完毕后可在控制台进行查看输出结果。

返回到项目	Console Output
状态	Started by user admin
变更历史	[Pipeline] Start of Pipeline [Pipeline] node (hide)
Console Output	Running on Jenkins in /var/jenkins_home/workspace/ywk_maoyan_1 [Pipeline] {
View as plain text	(PipeLine) { (Init) (PipeLine) { (Init) (PipeLine) sh
编辑构建信息	+ echo Init Init
删除构建 '#1'	[Pipeline] iscScanner [Morese: IscScanner] cmd: /var/jenkins_home/plugins/moresec-iscsanner/scanner/isc_client_linux devsecops init jenkins
从指定阶段重新运行	
回放	检测结果:通过 (Pipelinel)
流水线步骤	[Pipeline] // stage [Pipeline] stage
Workspaces	(Pipeline) { (Scan Image) (Pipeline) sh + echo' scan image' scan image Pipeline istScanner
	[Morsex: IsrScanner] cmd: /war/jenkins_home/plugins/moresec-isrSanner/scanner/sc_Client_linu: scan image —image_nomerit27.e.0.10800#xyg01c5.717.

10) 也可以直接在 IAST web 页面的镜像扫描部分查看对应任务结果。

🧭 雳鉴·IAST					yy 1 🚅 1 🕞
当前位置: 镜像扫描 > 流水线任务					
版水线任务					🖸 操作使用描述 👘 🛓 播件下载
风险等级 语选择					任务名称 () 合并任务
任务名称	jenkins 任务地址		构建次数	风险概述	摄作
▼ ♥ xzm	http://192.168.56.101:8080/job/xzm/		1	19 18 8	田和金
					i的输入 Build_number
Build_number	创建的加利	\$ 执行时间	i) (自像扫描结果	操作
3	2022-08-29 10:13:56	182s	-	19 18 3	17 fm
		共1条 く 1 3	10 条/页 ∨		
		共1条 < 1 3	10 奈/页 🗸		

2 附录:配置证书及代理说明(扫描类)

2.1 为什么要设置代理

需鉴的扫描方式与传统扫描产品的扫描方式最大的区别在于: 传统的扫描产品是通过爬 取的方式获取 URL 链接,并对其进行扫描,这种扫描方式对于一些孤岛 URL 是爬取不到的。 而需鉴的扫描方式是在研发和测试阶段,研发、测试人员在进行功能测试等操作时,通过代 理将请求流量复制到需鉴系统中进行安全检测。

2.2 对正常功能测试影响

雳鉴代理模式如下图所示,是将浏览器或者 APP 发起的业务请求数据复制一份到雳鉴系统中进行安全检测,正常数据请求仅仅是通过代理模式转发流量,对研发和测试人员在进行功能测试等操作时基本不会造成影响。



图表 320 雳鉴代理模式工作流程

2.3 设置证书步骤

注:对 Https 协议项目检测时,请上传服务器证书或者信任证书并安装后才可进行检测。 上传服务器证书请见本文档 3.8.9.4。以下为配置客户端证书方法。

2.3.1PC 端配置

以 windows 谷歌浏览器为例, 雳鉴的 http/https 证书设置如下: (其他版安装方式请前往雳鉴帮助中心-测试配置查看。)

1) 选择设置,拖到最下面,选择高级

沿署				G	A-1A-IRI -L-MARIN
汉旦				4	土以直中投东
☑ 询问是否保?	存您在网页上输入的	密码。管理密码			
网络内容					
字号:	中	▼ 自定义:	字体		
网页缩放:	100%	•			
网络					
您的网络代理设	置是由扩展程序管理	187.			
更改代理服务	器设置				
语言和输入设 ✓ 询问是否翻述	置 译非您所用语言的网	页。管理语言			
下戰內容保存位	置: C:\Users\1562	3\Downloads	更改		
📄 下载前询问	每个文件的保存位置		\square		
HTTPS/SSL 管理证书					
Google 云打印					
设置或管理"Goo	ogle 云打印"中的打印	印机。了解连情			

2) 然后点击管理证书,选择其中的受信任的颁发机构

财妇的(N):	<所有>					~		140 AV
人 其他人 中间	证书颁发机构受信	任的根证书	的质发机构	受信任的发布者	未受信任的发	定布者	xssi过滤的测量	C php连接Mysql的增量
颁发给	颁发者	截止日	友好名称			^		在设置中搜索
Acunetix WV	Acunetix WVS	2027/	<无>					
Acunetix WV	Acunetix WVS	2026/	<无>					
AddTrust Ext	AddTrust Exte	2020/	The USER	т				
ALIPAY_ROOT	ALIPAY_ROOT	2019/	<无>					
Baltimore Cy	Baltimore Cyb	2025/	DigiCert I	3a				
Certification	Certification A	2039/	WoSign					
	Certum CA	2027/	Certum T					
Class 2 Publi	Class 2 Public	2029/	VeriSion	-1				
DigiCert Ass	DigiCert Assur	2020/	DigiCert					
						~		
							18	
导入(I)	导出(E)	删除(R)				高级(A)		
出的预期目的								
<所有>								
					1	查看(V)		
						关闭(())	6-	
						关闭(C)		

3) 点击导入,选择下载好的证书,而后一直点击下一步即可,最后点击完成

ĒΒ			× iqi ×	(转-收集) ×	: <	127.0.0.1/in
预期目的(N):	<所有>		~			
个人 其他人 中间道 感发给 ■Acunetix WV ■AddTrust Ext ■AddTrust Ext ■ALIPAY_ROOT ■Baltimore Cy	E书読技机构 S	证书导入向导 要导入的文件 指定要导入的文件。			× php使用sessi	on来保 🕤 I
GCertification GCertum CA GCertum CA GCertum CA GCIAss 3 Publi DigiCert Ass りigiCert Ass ほよ的预期目的 <所有>	Certification A Certum CA Certum Truste Class 3 Public . DigiCert Assur	文件名(F): C:\Users\15623\Downloads\ca.cer 注意:用下列指式可以在一个文件中存 个人信息交换-PKCS #12 (.PFX,P 加密消息语法标准-PKCS #7 证书(Microsoft 系列证书存储(.SST)	诸多个证书: 12) .P78)	说理起(R)		
	下载内容(下载用 HTTPS/SSI			下一步(N)	取消	

杭州默安科技有限公司

2.3.2移动端配置

以 Android 版为例, 雳鉴对 App 进行安全检测前需要设置的代理步骤如下:

1) 与 Ios 版一致, 需进入帮助中心-测试配置中的代理及证书配置环节, 点击下载证书

A https://192.168.199.212/help/
 选择PAC代理后,仅存在项目中的请求会经过雳鉴代理服务 *使用PAC配置时,新建项目和编辑项目后需重启浏览器更新 PAC文件 Mac chrome版 Mac Firefox版 (Windows Firefox与Mac版一致) Windows Chrome版 App检测:项目及任务创建后,需设置代理,Android、iOS均有不
同的代理设置 <u> </u>
 2. 证书配置:对Https协议项目检测时,请信任证书并安装后才可进行检测 * 证书下载地址(适用于Web及App检测点此下载 * Web证书配置 Mac chrome版 Mac Firefox版(Windows Firefox与Mac版一致)
下载提示
文件名 : moresec.crt <i>Q</i> 大小 : 1.2K ♥ 安全
立即下载
取消

²⁾ 进入设置-更多设置,进行系统安全调整

-	设置	The set
A	锁屏、密码和指纹	•
c	通知和状态栏	×
	桌面与最近任务	•
ð	手机分身	Þ
Ø	防打扰	•
D	电量和性能	k
e	存储空间	Þ
	更多设置	•
帐号		
mi	小米帐号	chengable 🕨
8	其他帐号	Þ
应用管	理	
88	系统应用	۲
	田夕高田	
◆更多	设置	24
日期和	时间	Þ
语言和	输入法	Þ
系统安	全	•
悬浮球	t	Þ
截屏		Þ
呼吸灯	r	•
耳机和	音效	Þ
按键		Þ
单手模	式	Þ
无障碍		Þ
备份和	重置	Þ
一键换	机	Þ

3) 点击"从存储设备安装",进行证书安装

▲系统安全	- 24
设备管理	
设备管理器 查看或停用设备管理器	•
未知来源 允许安装来自未知来源的应用	
位置信息	×
通知使用权	10 个应用可以读取通知 🕨
凭据存储	
存储类型 硬件支持	
信任的凭据 显示信任的CA证书	
从存储设备安装 从存储设备安装证书	
清除凭据 删除所有证书	
SIM卡锁定方式	
中国移动	•

4) 安装证书时,凭据用途请选择"VPN和应用"

21:53 0.	40K/s 🗇	察 .all	移动 4G HD	移动 🚺	439
〈 系统安全					
设备管理器 查看或停用设备管理器					
未知来源 允许安装来自未知来#					•
为证书命令	Ś				
证书名称:					
 凭据用途: VPN和应用				-	
该数据包包含: 一个用户证书					
			取消	确定	
从存储设备安装 从存储设备安装证书					
清除凭据 删除所有证书					

5) 安装成功后,前往更多设置-系统安全进行证书信任凭据查看

▲ 系统安全	- 724
设备管理	
设备管理器 查看或停用设备管理器	•
未知来源 允许安装来自未知来源的应用	
位置信息	•
通知使用权	10个应用可以读取通知 🕨
凭据存储	
存储类型 硬件支持	
信任的凭据 显示信任的CA证书	
从存储设备安装 从存储设备安装证书	
清除凭据 删除所有证书	
清除凭据 删除所有证书 SIM卡锁定方式	

6) 新任凭据中发现"moresec"证书,即代表证书安装成功



2.4 设置代理步骤

不论是 web 还是 App 进行安全检测前,都需要先设置代理及证书。

配置分为三种: PC 端、移动端、浏览器插件。

注: PC 端代理分为 Http/https 配置、PAC 配置两种(任选其一),移动端分 APP-VPN 配置、APP 代理配置两种(任选其一),推荐使用浏览器插件方式(详见雳鉴 IAST 帮助中 心-代理配置-浏览器插件)。

2.4.1PC 端配置

方法1: http/https 代理配置

以 windows 谷歌浏览器为例, 雳鉴的 http/https 代理设置如下: (其他版安装方式请前往雳鉴帮助中心-测试配置查看。)

1)选择设置

打开新的	标签页(T)		Ctrl+T
打开新的	窗口(N)		Ctrl+N
打开新的	隐身窗口(I)	Ctrl+	Shift+N
历史记录	(H)		Þ
下载内容	(D)		Ctrl+J
书签(B)			•
缩放		100% +	
打印(P)			Ctrl+P
投射(C)			
查找(F)			Ctrl+F
更多工具	(L)		Þ
修改	剪切(T)	复制(C)	粘贴(P)
设置(S)			
帮助(E)			Þ
退出(X)		Ctrl+	Shift+Q

2)拖到最后,选择高级-->打开代理设置-->局域网设置

	ernet 雇	性			-				?
岘	安全	隐私	内容	连接	程序	高级			
-	》 要	设置 Int	ernet 连	度,单i	击"设置"	•		设置	<u>U</u>)
发号	引和虚拟	同网络	设置		-				
0	校园网							添加(<u>D</u>)
								添加 VP	N(<u>P</u>)
								删除(<u>R</u>)
如	果要为连	接配置代	建服务器	鲁 , 请 送	择"设置	ť.		设置	(<u>S</u>)
局均	或网(LAN	l)设置							
局地し面	或网(LAN AN 设置 前"设置	1)设置 不应用到 "按钮。	拔号连接	。对于	拔号设计	f[,单击」	E	局域网谈	建(1)
局はし面	或网(LAN AN 设置 前的"设置	0)设置 不应用到 "按钮。	拨号连接	、对于	拔号设	置,单击」	E	局域网诊	注重(L)
局地	或网(LAN AN 设置 前的"设置	1)设置 不应用到 "按钮。	拨号连接	、对于	拔号设计	〖 ,单击」	E	局域网诊	2置(L)

3) 勾选为 LAN 使用代理服务器,选择高级

A DECK THE REAL	盖手动设置。要确保使用手动设置,请禁用自动配置。
自动检测设	置(A)
使用自动配	置脚本(S)
地址(R)	http://127.0.0.1:1080/pac?t=2017080
为LAN使	I代理服务器(这些设置不用于拨号或 VPN 连接)(X) 端口(T): 80 高级(C)
地址(E):	

4)将从雳鉴中获取的 http 代理 IP 和端口、https 代理 IP 和端口,分别填入上留下两个框内(任务管理模块中可查看 IP 和端口),然后点击确定即可。

1000	N.4 7711			
4	类型	要使用的代理服务器地址	端口	÷
			:	
	安全(S):			
	ETP(F):			
	套接字(C):	~	:	
	□对所有	か议均使田相同的代理服务器(11)		
51/AL	□对所有	办议均使用相同的代理服务器(U)		
9J91	□ 对所有的 对于下列字	办议均使用相同的代理服务器(U) 在符开头的地址不使用代理服务器(N):		
列外 【1	□ 对所有的 对于下列字	办议均使用相同的代理服务器(U) ■符开头的地址不使用代理服务器(N):		
6491 S	□ 对所有能 对于下列字	か议均使用相同的代理服务器(U) □符开头的地址不使用代理服务器(N):	Ŷ	

方法 2. PAC 代理配置(适用于当前雳鉴设备无法连接外网)

以 windows 谷歌浏览器为例, 雳鉴的 PAC 代理设置如下: (其他版安装方式请前往雳鉴帮助中心-测试配置查看。)

1) 点击设置

\$ S			
打开新的标签	页(T)		Ctrl+T
打开新的窗口((N)	(Ctrl+N
打开新的隐身間	窗口(I)	Ctrl+S	hift+N
历史记录(H) 下载内容(D)			Ctrl+J
书签(B)			
缩放	1044	100% +	53
打印(P)			Ctrl+P
投射(C)			
查找(F)			Ctrl+F
更多工具(L)		(0
修改 剪	雪切(T)	复制(C)	粘贴(P)
设置(S)			
帮助(E)			
退出(X)		Ctrl+S	hift+Q

2)拖至最下方,并展开高级选项-->打开代理设置

Google 云打印 设置云打印设备 , 无範碍 添加无障碍功能 打开 Chrome 网上应用店 2 系統 关闭 Google Chrome 后继续运行后台应用 • 使用硬件加速模式 (如果可用) ● 打开代理设置 ② 就设置由"Proxy SwitchySharp"控制 停用 配 ● 打开代理设置 ③ 就设置由"Proxy SwitchySharp"控制 ● 電置 将设置还原为原始默认设置	印	
法臨尋 添加无障碍功能 打开 Chrome 网上应用店 SK 关闭 Google Chrome 后继续运行后台应用 使用硬件加速模式 (如果可用) 使用硬件加速模式 (如果可用) 打开代理设置 ② 此设置由"Proxy SwitchySharp"控制 摩置 将设置还原为原始默认设置()	Google 云打印 设置云打印设备	×
添加无障碍功能 打开 Chrome 网上应用店 系统 关闭 Google Chrome 后继续运行后台应用 使用硬件加速模式(如果可用) 打开代理设置 打开代理设置 び 此设置由"Proxy SwitchySharp"控制 停用 框置 将设置还原为原始默认设置、	无障碍	
系统 关闭 Google Chrome 后继续运行后台应用 使用硬件加速模式(如果可用) 使用硬件加速模式(如果可用) 打开代理设置 び 此设置由"Proxy SwitchySharp"控制 摩囲 将设置还原为原始默认设置、	添加无障碍功能 打开 Chrome 网上应用店	
关闭 Google Chrome 后继续运行后台应用 ● 使用硬件加速模式(如果可用) ● 打开代理设置 ● ● 此设置由"Proxy SwitchySharp"控制 停用 重置 将设置还原为原始默认设置() ●	系统	
使用硬件加速模式(如果可用) ● 打开代理设置 ② ③ 此设置由"Proxy SwitchySharp"控制 停用 重置 将设置还原为原始默认设置()	关闭 Google Chrome 后继续运行后台应用	-
打开代理设置 此设置由"Proxy SwitchySharp"控制 停用 重置 将设置还原为原始默认设置	使用硬件加速模式(如果可用)	
此设置由"Proxy SwitchySharp"控制 停用 重置 有设置还原为原始默认设置()	打开代理设置	Z
重置	🜏 此设置由"Proxy SwitchySharp"控制	停用
重置 将设置还原为原始默认设置、 [┣] ┓	重置	
÷	重置 将设置还原为原始默认设置 [m]	۶

3)选择局域网属性

Inte	rnet 属	性							?	>
朝规	安全	隐私	内容	连接	程序	高级				
-	要	设置 Int	ernet 连	接 , 单i	击"设置"	•		设	髶(<u>U</u>)	
拨号	和虚拟词	专用网络	设置		_					
6	校园网							添加	ם(<u>D</u>)	
								添加、	/PN(<u>P</u>)	
								删降	余(<u>R</u>)	
如馬	果要为连	接配置任	代理服务	器,请送	择"设置		1	设	置(<u>S</u>)	
局域 LA 面	如(LAN N 设置 的"设置	U)设置 不应用到 "按钮。	拨号连拍	度。对于	拨号设置	重,单击	£	局域网	↓ 〕 设置(L)	
					确定		取消	ž	应用	l(<u>A</u>)

4) 勾选使用自动配置脚本, 地址填写雳鉴 PAC 文件地址, 随后点击确定即可

司动配置会覆盖手动设置	^置 。要确保使用手动设置,请禁用	自动配置。
]自动检测设置(A)		
使用自动配置脚本(S)		
地址(R)		
里服务器		
为 IAN 使田代理服务	、器(这些设置不用干拨县或 VPN)	车接)(X)
	端口(T): 80	高级(C)
地址(E):		2.2.0.06.04

注:对 HTTPS 协议项目检测时,请先 <u>下载证书</u>并导入(安装成功后才可进行正常检测)

▶ Mac chrome 版安装证书方式如下,其他版安装方式请前往雳鉴帮助中心-测试配置查看。

1) 打开设置,拖至最下方,选择高级

O Chrome chrome://sett	ings		X
	Q、 在设置中探索		
	NO REPORT OF THE OWNER OF THE OWN		
	借助联想查询服务,帮您在地址栏中自动填充未输完的搜索字词和网址		
	使用联想查询服务更快递地加载网页		
	自动向 Google 发送某些系统信息和网页内容,以帮助检测危险应用和网站		
	保护您和您的设备不受危险网站的侵害		
	溶使用情况统计信息和崩溃报告自动发送给 Google		
	随浏览流量一起发送"不跟踪"请求		
	使用网络报务帮助解决拼写错误 将您在浏览器中输入的内容发送给 Google,以便提供更智能的拼写检查功能		
	管理证书 管理 HTTPS/SSL 证书和设置		
	内容设置 控制网站可使用的信息以及可向您显示的内容	*	
	清徐浏览数据 清除词览记录、Cookie、缓存及其他数据		

2) 点击管理证书,选择左下角的加号添加证书

🔒 系统 📴 系统根证书	▲ 此证书尚未经过第	三方验证	
	名称	^ 种类	过期时间
	com.apple.kerberos.kdc	证书	2037年2月15日 07:35:1
	📴 com.apple.kerberos.kdc	证书	2037年2月15日 07:35:1
	com.apple.systemdefault	证书	2037年2月15日 07:35:1
	mitmproxy	证书	2020年7月23日 21:14:4
	moresec	证书	2027年7月22日 20:50:
	MoreSecCA	证书	2027年7月18日 10:56:3
种类	PortSwigger CA	证书	2037年3月17日 14:06:3
 除 所有项目 ※ 密码 安全备注 到 我的证书 ♀ 密钥 	PortSwigger CA	证书	2037年6月12日 21:37:5
🔁 证书			
	1 拷贝		8 项

3)选择下载的证书,点击确定

1	moresec	证书	2027年7月22日 20:50:18	系统	
	moresec	ī <mark>.</mark> 书	2027年7月22日 10:45:33	系统	
	MoreSecCA	北书 図	则导入的证书027年7月18日 10:56:33	系统	
	PortSwigger CA	证书	2037年3月17日 14:06:36	系统	

4) 然后在证书上,点击右键,选择显示简介

新建证书偏好设置
拷贝"moresec" 删除"moresec"
导出"moresec"
显示简介 评估"moresec"

5)展开信任一栏,使用此证书时选择始终信任

	moresec
Certificate २००१ २००१ २००१ 回行签名的 过期时间: ▲ 此证书尚 ▼ 信任	;)根证书 2027年7月22日 星期四 中国标准时间 10:45:33 前未经过第三方验证
使用此证书时	: 始终信任 📀 ?
加密套接字协议层 (SS	iL) 始终信任 ◇
安全邮件 (S/MIM	E) 始终信任 📀
可扩展认证协议 (EA	P) 始终信任 📀
IP 安全 (IPse	b) 始终信任
代码签	名 始终信任 📀
时间	戳 始终信任 ◇
X.509 基本策	略 始终信任 📀
▼ 细节	
签发者名称	
国家/地区 CN	
省/市/自治区 ZJ	
所在地 HZ	
40 40 means	

2.4.2移动端配置

注: 1. 项目及任务创建后,需设置代理, Android、Ios 均有不同的代理设置;

2. 手机端登录雳鉴会提示有风险,需点击继续才可正确访问雳鉴-帮助中心。

方法1: APP-VPN 配置(推荐使用)

* 需先安装并信任证书后,才可正常连接 VPN,否则可能会导致 VPN 连接不成功

以Android 版为例,步骤如下:

① 进入系统设置,选择 VPN 进行添加设置

Tel: (+86) 400-0571-211

Email: market_moresec.cn

	我的设备	MIUI 8.5 稳定版 8.5.7.0(NDECNEF)	۲
网络和	连接		
D	双卡和移动网络		۲
((:-	WLAN	moresec-dev-5G	×
*	蓝牙	已开启	×
0	个人热点	已关闭	۲
VPN	VPN	未开启	•
	更多连接方式		•

② 添加 VPN 时,按要求依次填写信息,类型需选择 Hybrid 模式,而后点击确定保存

又消	添加VPN	确定
名称	SDL测试	
类型		
IPSec H	-lybrid RSA Hybrid 模式	>
服务器地	址 192 214	
PSEC CAi	正书	
morese	^C 选择先前安装过的证书	>
PSEC 服务	器证书	
(来自服	(务器)	>
	超级选项	
用户名	testcheng 房鉴的账号密	四
密码		

③ 此时该 VPN 还需被开启,点击开启后显示"已连接"则表示设置成功

开启VPN	
配置	
SDL测试 已连接	÷.

方法2: APP 代理配置

以 Android 版为例, 雳鉴对 App 进行安全检测前需要设置的代理步骤如下:

需下载检测插件 Postern. apk 至手机并安装, <u>http:sdsd</u>

① 打开 Postern,并添加代理服务器

15:00		3.97	K/s * (3 ? .	ⅆ 移动	4G HD	⊿⊪ 移动	50%
P	Poste	ern						
服务器	名称:							
服务器	地址:							·
服务器	端口:							
代理类	型							
SSH	2							
用户名								
密码								2
88	<u>1111</u>	٢	4	> -	(š)	Q		\sim
1 q	² W	1 E		i t	6 y l	, L	⁸ i	p p
	1	@	#	%	Ľ	8	*	?
ã	S	d	1	g	<u> </u>	J	ĸ	<u> </u>
á ↑	S Z	d x	t C	g v	b	J n	m n	

② 任意自定义服务器名称,代理类型选择"HTTPS/HTTP CONNECT",输入其他内容后点击保存

15:02	••• 2.17K/s *	9	att	修动 4G	HD⊿nd	移动 🛄	€50%
≣ <mark>∕</mark> Post	tern						
肥久思之致。							
adl app							
sul_app							
服劳茜吧亚:	100.04						
192.168.	199.34						
服务器端口:							
3128							
代理类型							
HTTPS/H	TTP CONNI	ЕСТ					
用户名							
test							
密码							
加密类型							
rc4							
一次性	认证(OTA)						
		保ィ	字				
		取	肖				
		0.011	~				
		删	F				

③ 点击左侧导航栏-配置规则,并进行规则添加



④ 匹配类型选择"匹配所有地址",动作选择"通过代理连接",代理/代理组勾选前面添加的代理服务器

15:06		1.05K/s	6	۰	a	移动	4G	HD	at	医动	48%
≣ <mark>₽</mark> P	Postern										
匹配类型											
匹配所	有地址										- 24
动作											
通过代	理连接										
代理/代码	粗										
test - 1	92.168	.199.3	4:30	000	0						
□ 开启	自抓包										
目标地址											
			仔	 R 存	Ŧ						
			Ę	又洋	Ĭ						
			H	制陶	È.						

5. 查看手机通知栏,当推送通知 "Postern 已激活 VPN"则代表代理设置成功



杭州默安科技有限公司

2.4.3浏览器插件配置

共有 Firefox 版, Chrome 版(67 版本以下), Chrome 版(67 版本及以上)三种配置可选,具体教程详见雳鉴 IAST 帮助中心-代理配置-浏览器插件。

2.5 配置检测环节

请进入雳鉴 IAST 帮助中心-配置检测进行检测。

注:

- 1. 验证是否正确配置雳鉴的代理及证书,且仅对 Http 环境配置有效。
- 2. 若无法打开页面,则代表用户未正确配置代理,请重新设置。