默安科技
企业信赖的安全伙伴

雳鉴 IAST 管理员使用手册

产品技术部

领先的第三方云计算安全服务商
AI驱动的下一代企业安全体系

版权声明

目 录

插图目录

1 概述

1.1 产品概述

雳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：

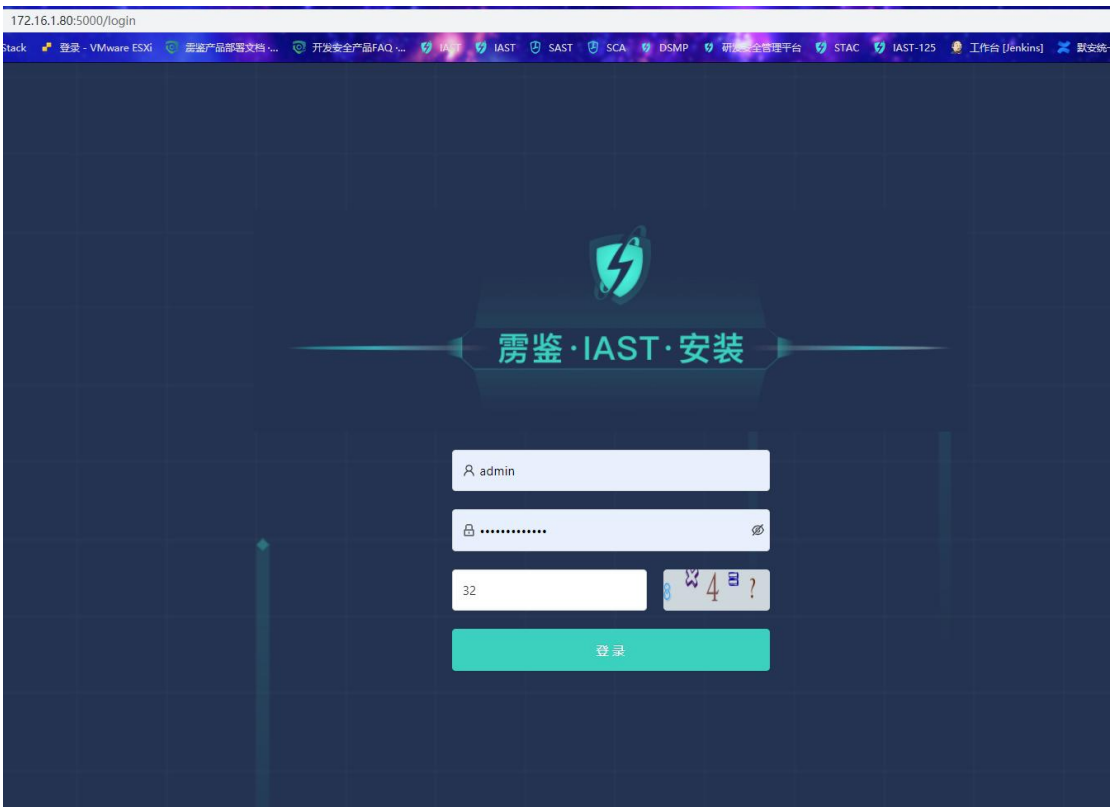
1. 提供一个 IP 地址。
2. 需要提供 DNS 和网关地址。
3. 防火墙策略保障预留的物理机 IP 之间网络连接。
需要开放的端口：

序号	源地址	目的地址	开放端口	协议	用途	描述
1	管理员地址段	雳鉴地址	22	TCP	SSH（远程管理）	可自定义
2			443	TCP	web 管理	
3			81	TCP	web 管理	
4			5000	TCP	程序安装端口	
5	测试终端地址段	雳鉴地址	9000	TCP	代理端口	鉴权代理
			9002	TCP	代理端口	非鉴权代理
6	目标服务器	雳鉴地址	8989	TCP	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

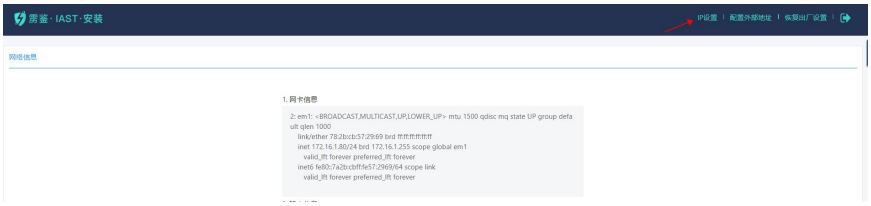
初次拉起 IAST 镜像后，可能需要进入后台配置地址信息，IAST 产品安装在 ubuntu20.04 操作系统上，请先配置*/etc/netplan* 下的网卡文件，确保 IAST 跟外部能联通再进行以下初始化操作

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



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



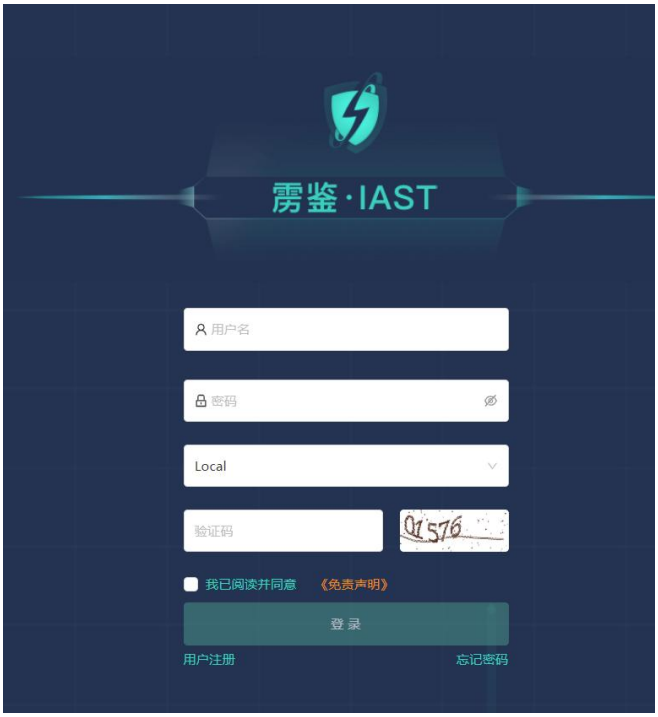
填写相应的 IP 地址信息，掩码，网关，DNS 信息后，点击确定保存

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

杭州默安科技有限公司

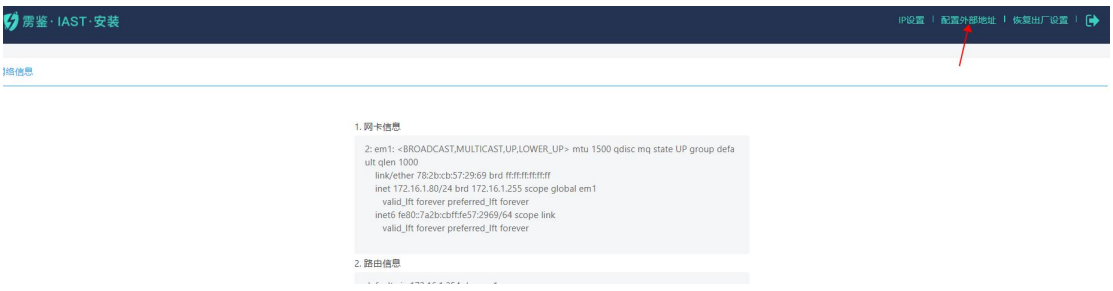
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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



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



杭州默安科技有限公司

Tel：（+86）400-0571-211　　Email：market_moresec.cn　　Web：www.moresec.cn

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。

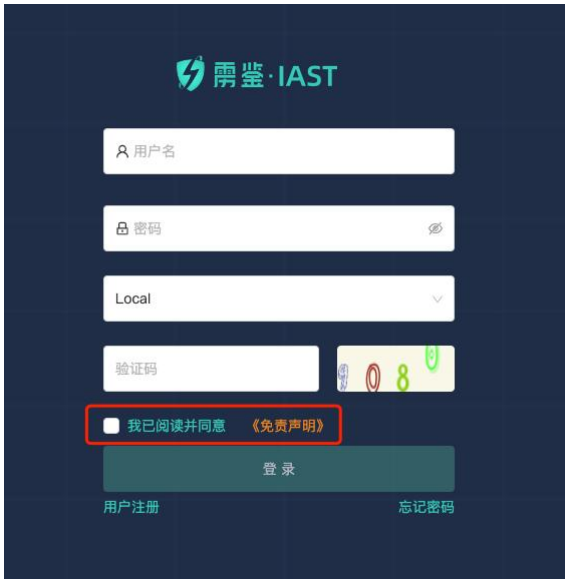
2) 打开浏览器 Google Chrome（支持以下浏览器：Google Chrome、Firefox、IE10、IE11、safari）

   - 用 HTTP 方式连接雳鉴的 IP 地址，如：http://192.168.199.80:81
   - 用 HTTPS 方式连接雳鉴的 IP 地址，如：https://192.168.199.80

3) 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。

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。



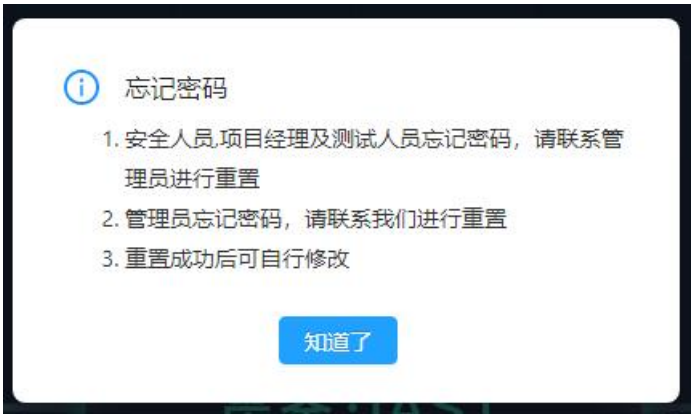
图表 2 登录-同意免责声明

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。



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。

图表 6 用户注册

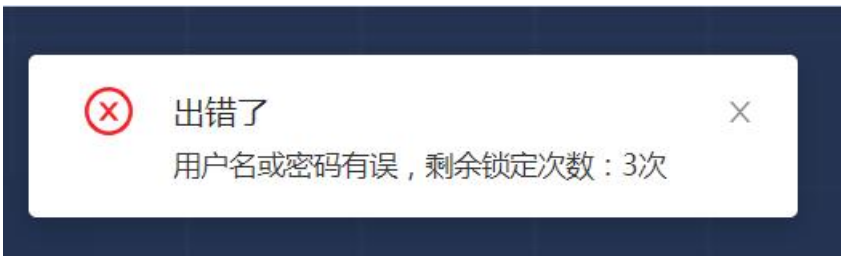
杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

图表 7 角色升级

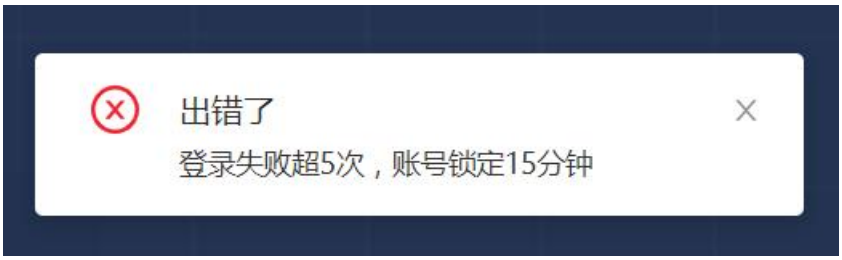
4) 账号防暴力破解。

- 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。



图表 8 登录失败

- 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

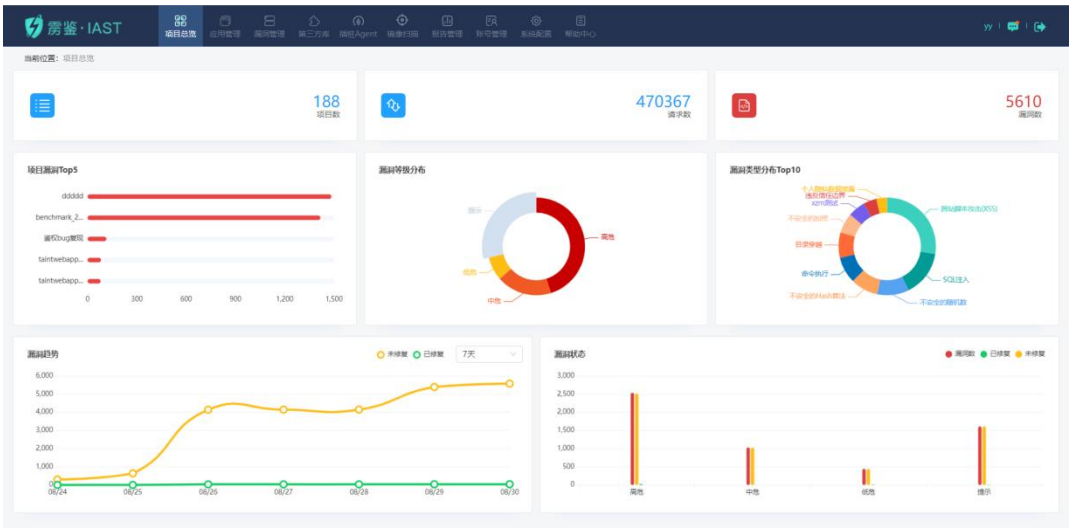
杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。



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

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

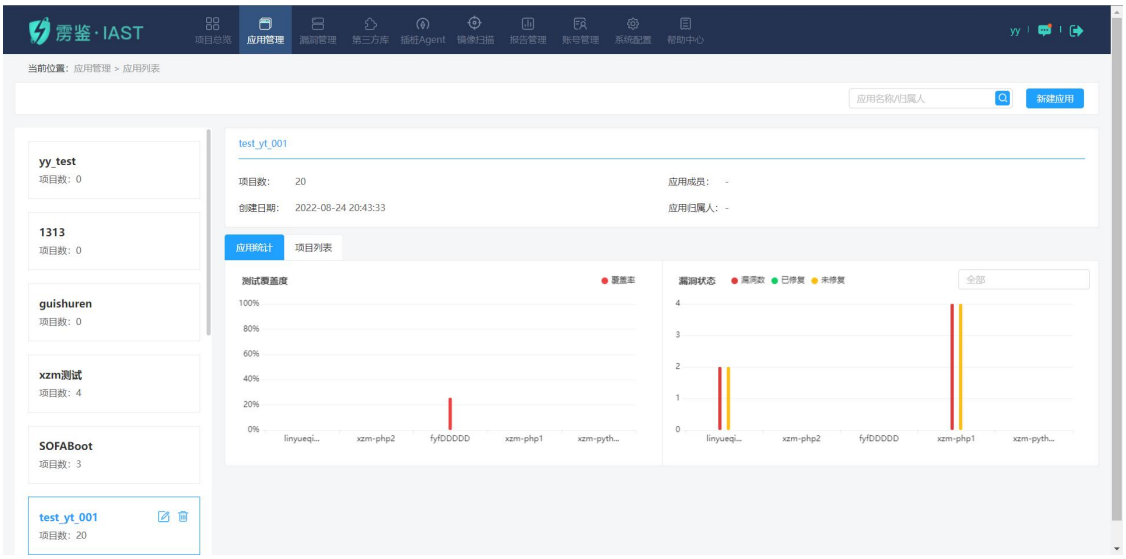
由 2 部分组成：漏洞趋势、漏洞状态。

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。



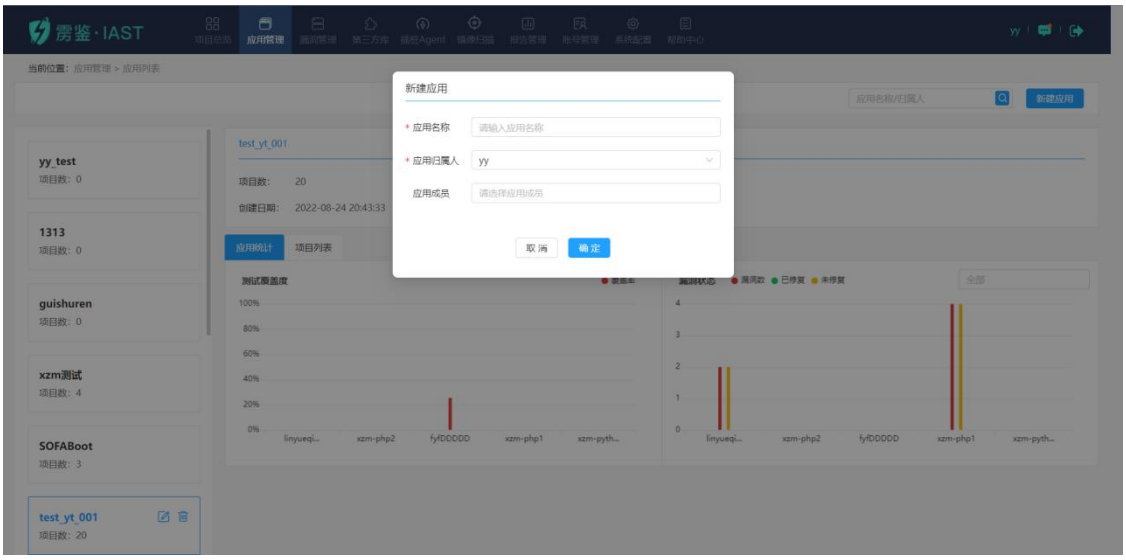
图表 13 应用管理

杭州默安科技有限公司

Tel：（+86）400-0571-211　　Email：market_moresec.cn　　Web：www.moresec.cn

1.5.1新建应用

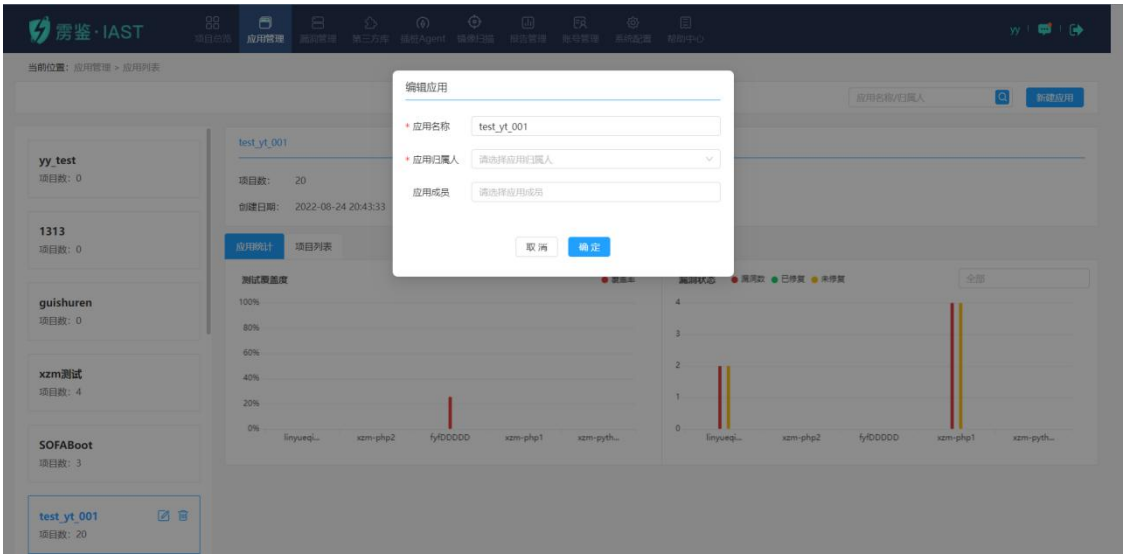
点击新建应用按钮，填写应用名称和应用归属人即可以进行新建操作，应用归属人默认为当前用户。应用成员属于非必填项。如需关联项目至应用中，可至 3.4.3.1 和 3.4.3.2 中查看。



图表 14 新建应用

1.5.2编辑应用

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。



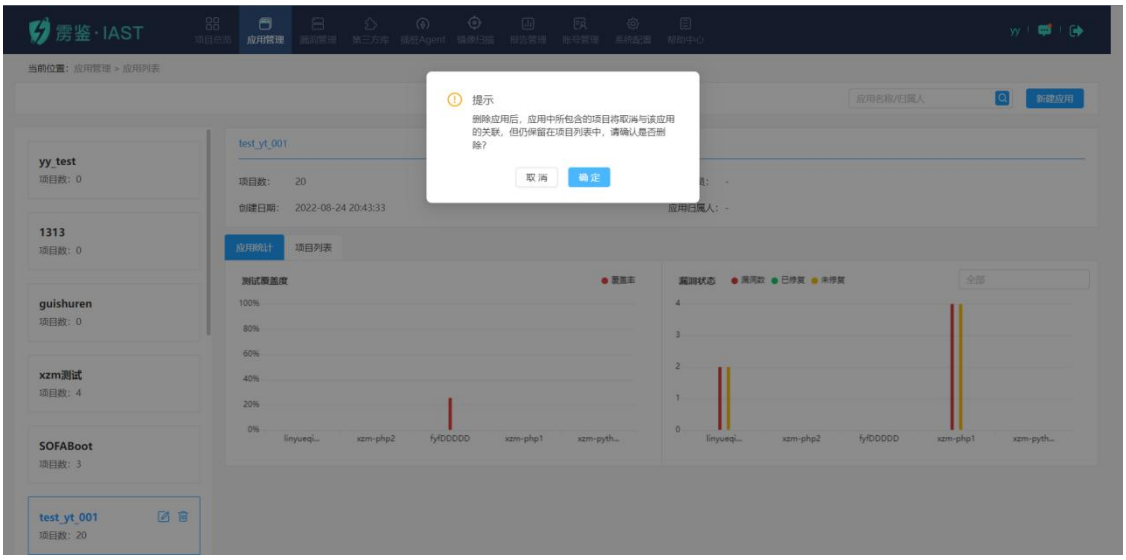
图表 15 编辑应用

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

1.5.3删除应用

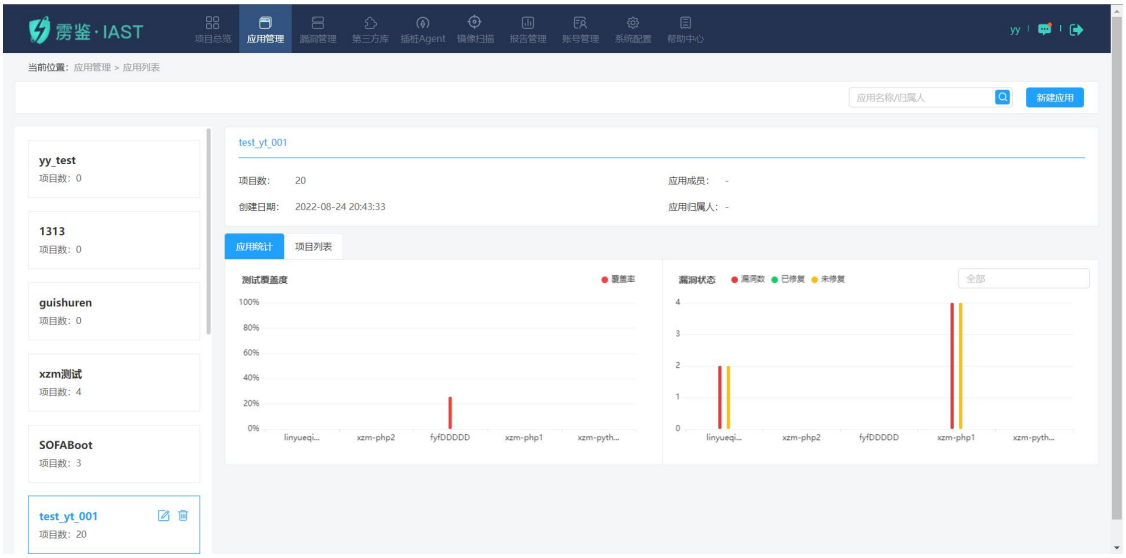
点击删除应用，弹出确认窗口后，可以删除已经创建好的应用。删除应用后，项目设置中所关联的应用选项将清空。



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。



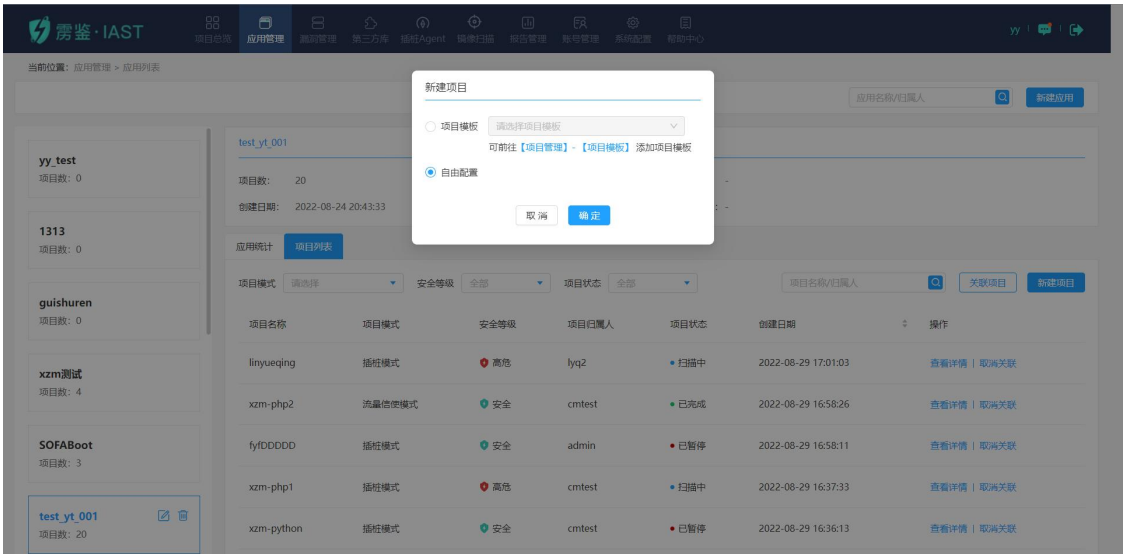
图标 17 应用详情

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

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

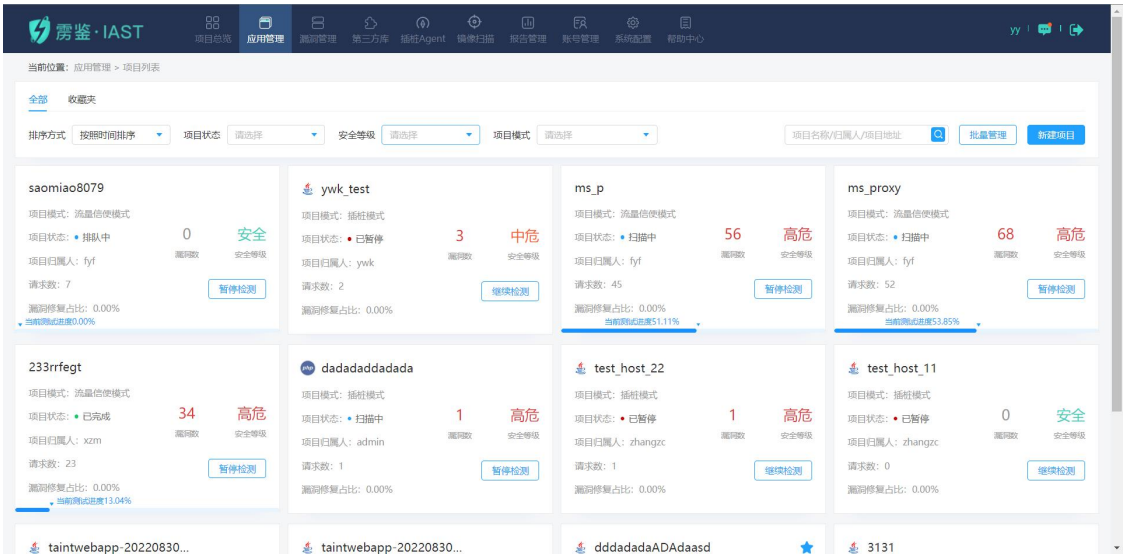
的项目，也可点击“关联项目”按钮进行批量项目关联应用。



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。



图表 19 项目管理

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

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

图表 20 项目模板列表

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)。

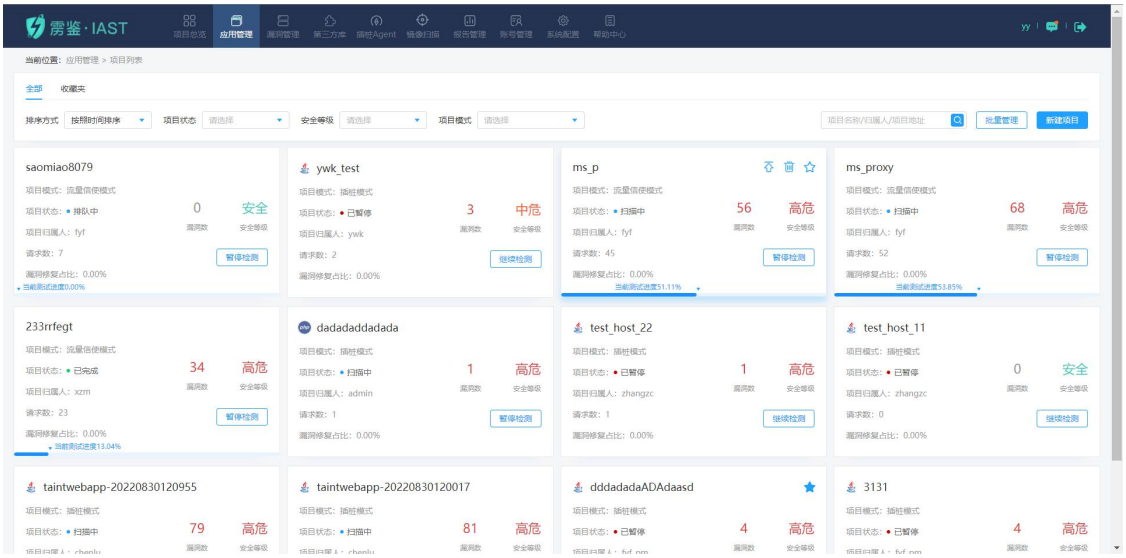
图表 22 新建项目模板

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、

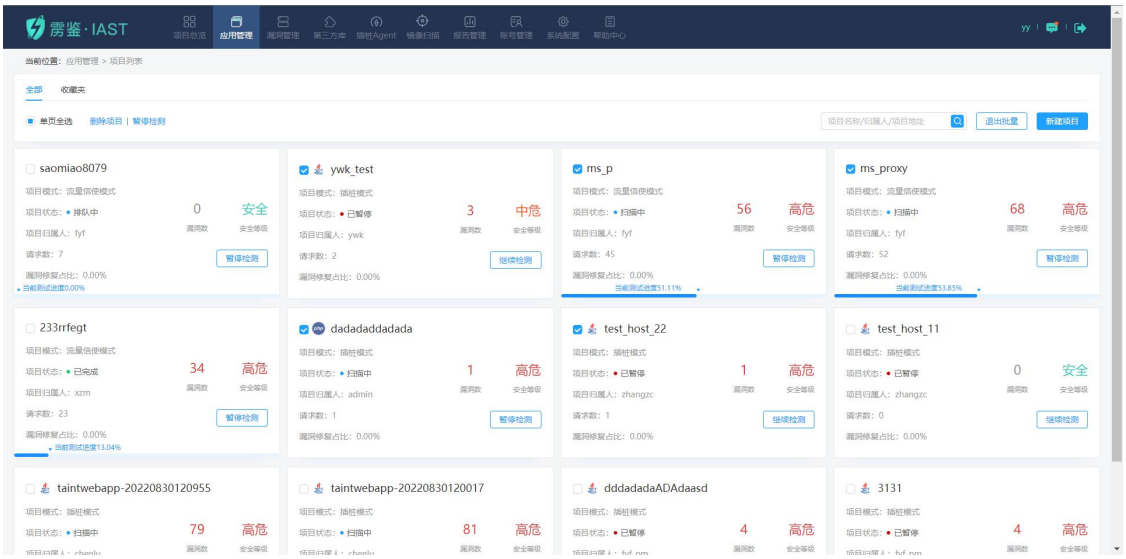
项目安全等级、项目状态、项目测试进度、请求数、漏洞修复占比、漏洞数、项目归属人。

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。



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。



图表 24 项目批量管理

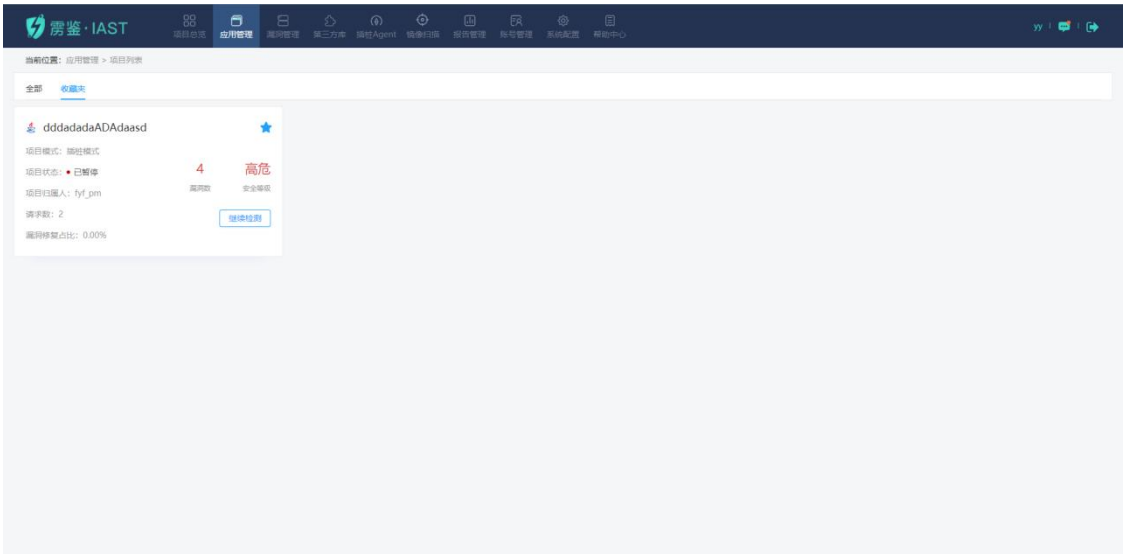
- 可以根据排序方式、项目状态、安全等级、项目模式对项目进行筛选，可以根据项目名称、归属人、项目地址进行搜索。

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。

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。



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。

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

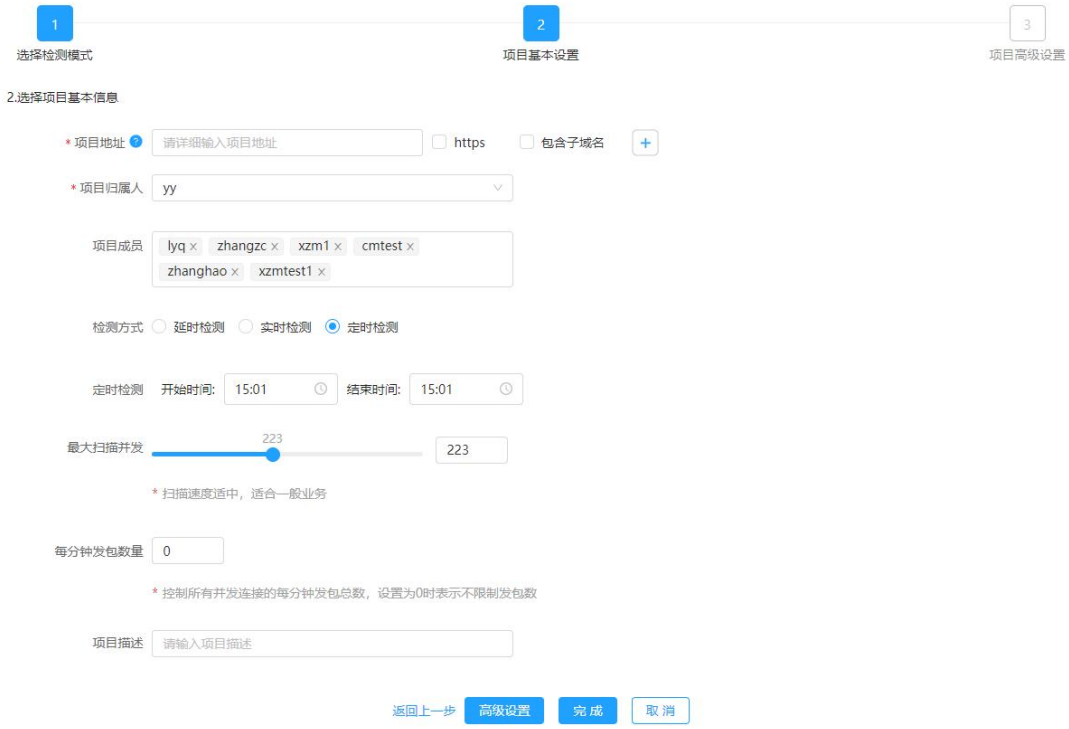
选择检测模式中，项目名称必填，检测模式从模板中继承且不可编辑。

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。

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。

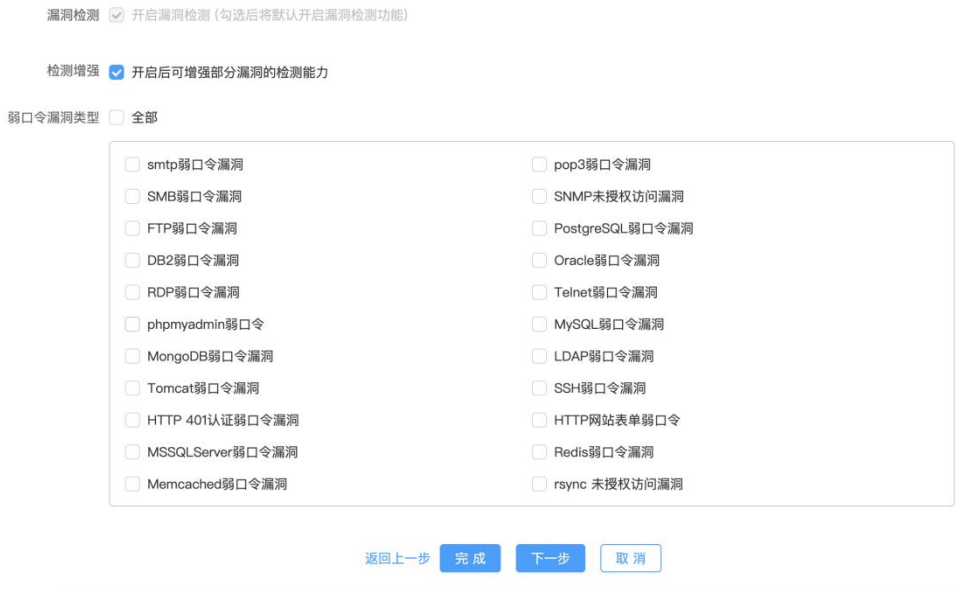


图表 30 新增项目-使用模板-扫描类-项目基本设置

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。

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。

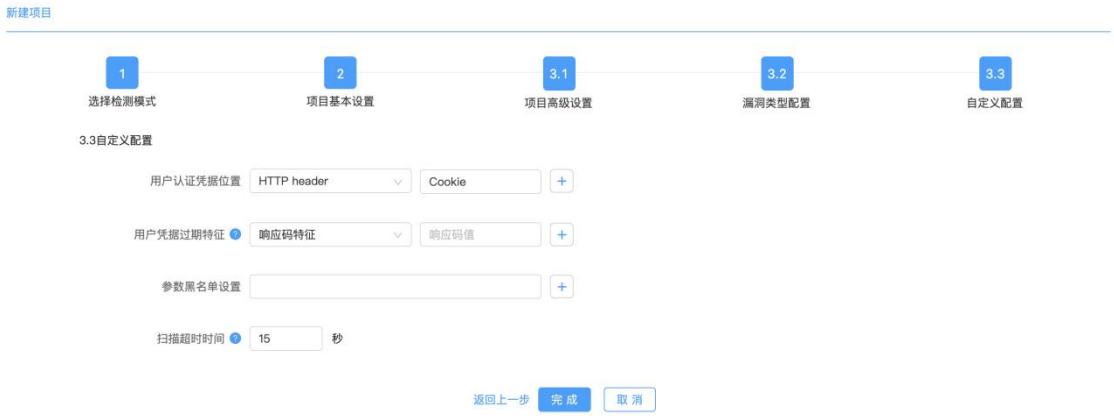


图表 32 新增项目-使用模板-扫描类-项目高级设置-开启检测增强

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。

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。



图表 34 新增项目-使用模板-扫描类-自定义配置

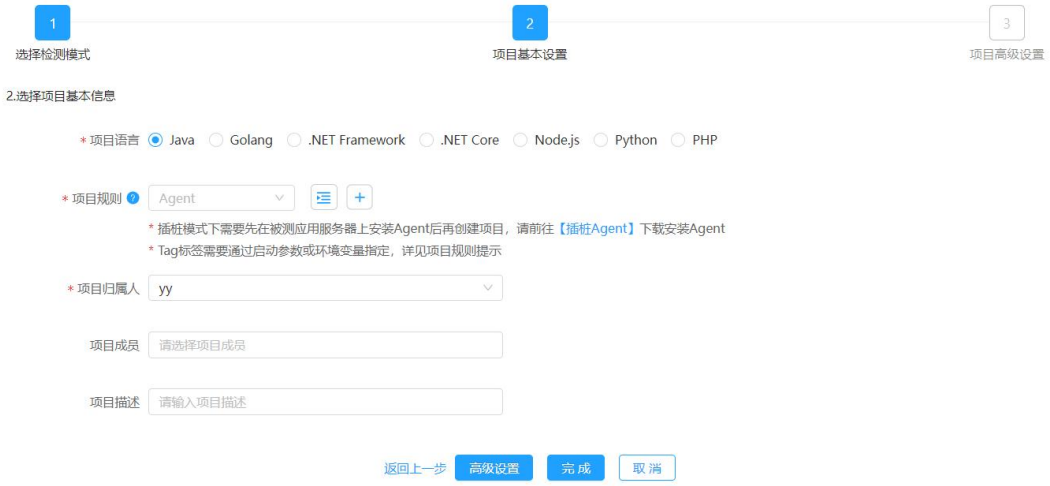
1.6.3.1.2 插桩类

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。

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。



图表 36 新增项目-使用模板-插桩类-项目基本设置

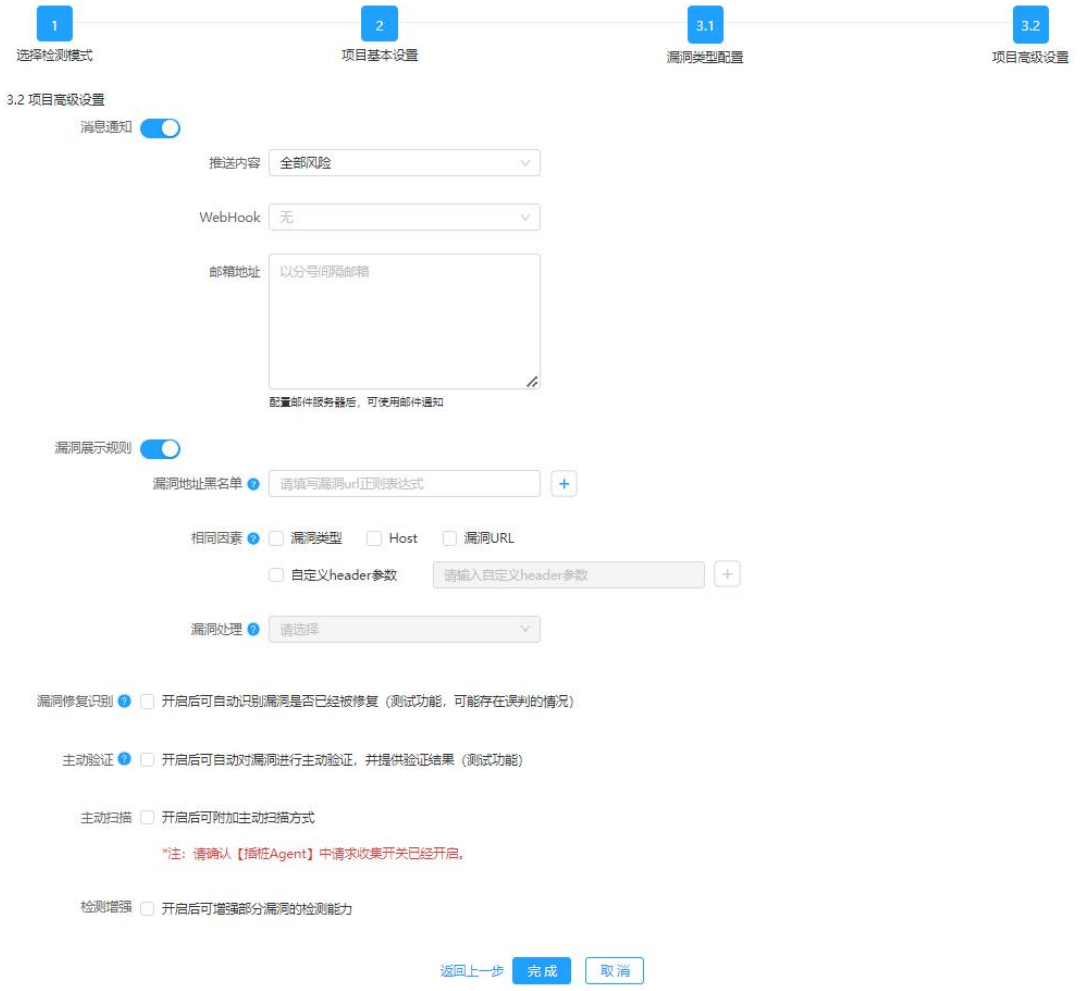
项目高级设置中，若模板为解锁状态，则可进行配置；若模板为锁定状态，则不可进行自由配置。在此处自行勾选需要检测的漏洞类型。

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。



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。

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。

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。

  1） 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。

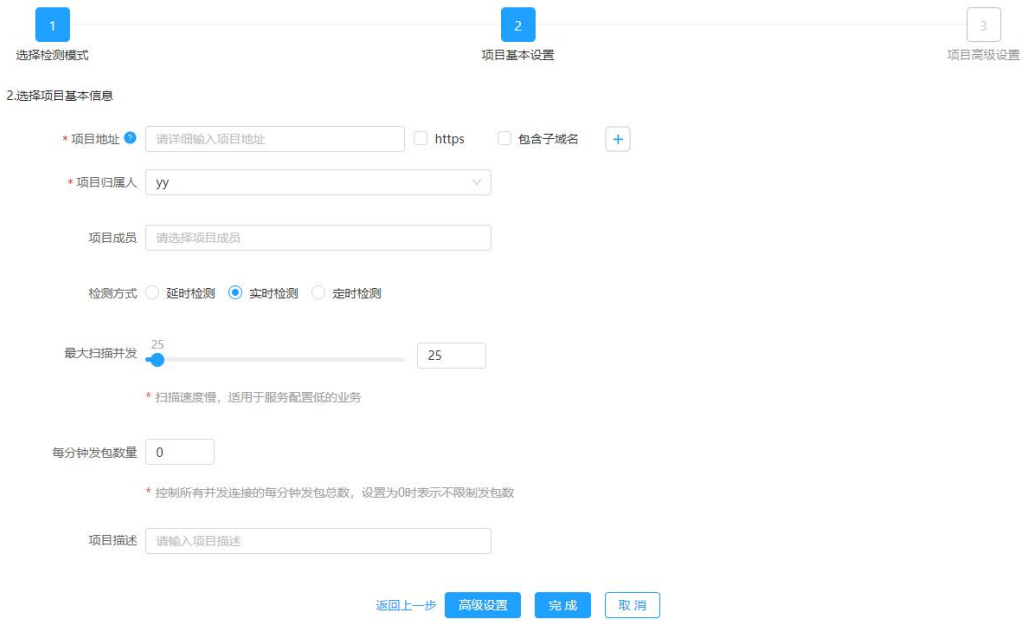
  3） 项目归属人：可选一人，默认为当前用户。

  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。



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。

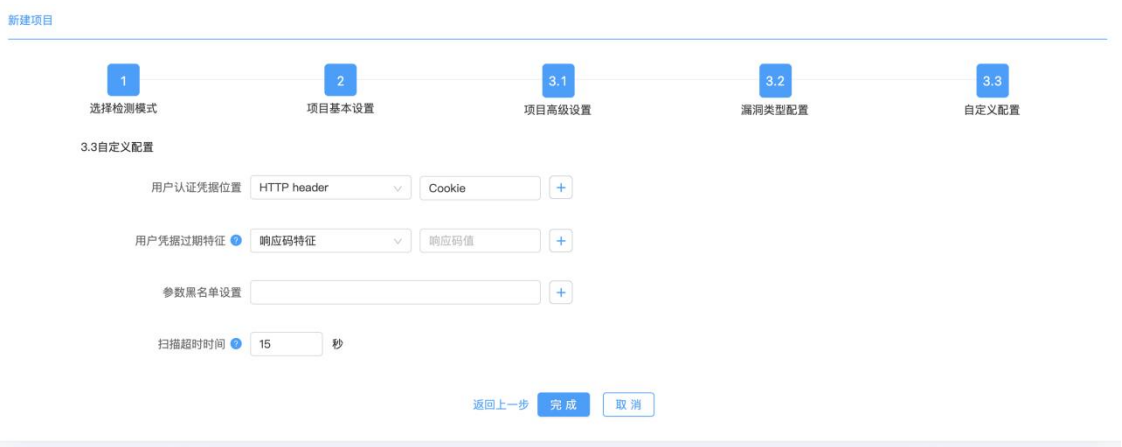
- webhook：选择此项目需要推送的 webhook 地址，具体添加方法，请参照 3.10.4.2 部分

图表 42 项目高级设置

图表 43 项目高级设置-漏洞类型

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



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

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、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 OOB 带外检测，用户根据自身的情景去配置 OOB 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 OOB 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

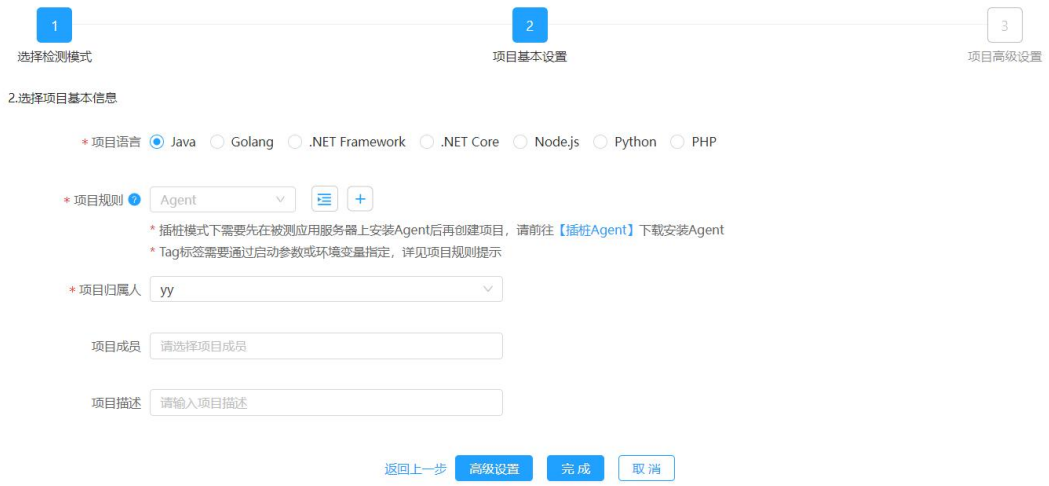
管理员、安全人员及项目经理可进行项目创建，点击“新建项目”按钮，输入项目名称填写项目基本信息包括项目语言、项目规则，项目成员，项目描述，此时项目归属人为当前登录人员，点击完成即项目被创建成功，此时会自动为成员分配对应任务。若有需要可点击高级设置，选择检测漏洞类型，进行主动扫描（Active IAST）配置等。

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。

图表 45 新增项目插桩类-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，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。



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。

1) 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。

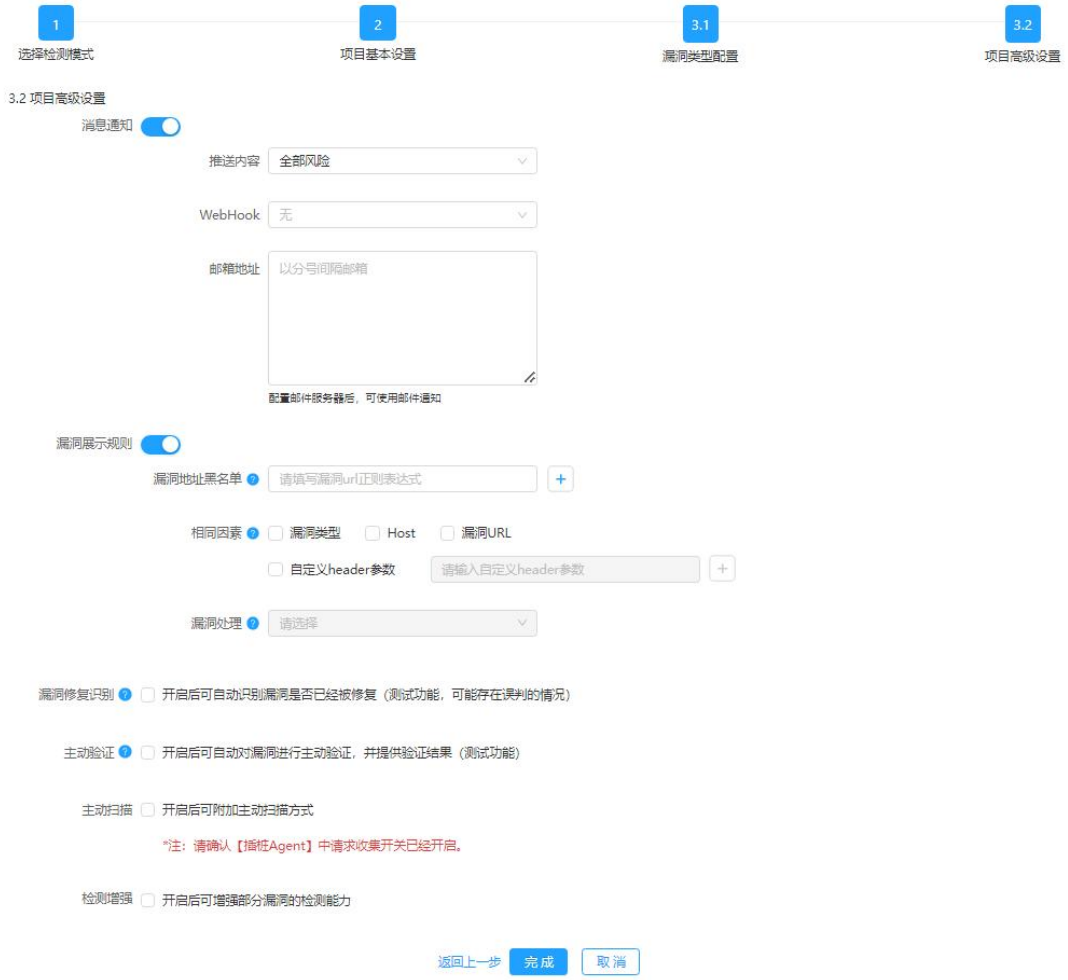
4) 项目成员：将需要进行测试的项目成员添加进来，而后会自动为该项目成员分配检测任务。

5) 项目描述：为项目添加描述，150 字以内。

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

图表 47 插桩类项目高级设置-漏洞类型



图表 48 插桩类项目高级设置

图表 49 插桩类项目高级设置-主动 IAST

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、

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。

6) 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。

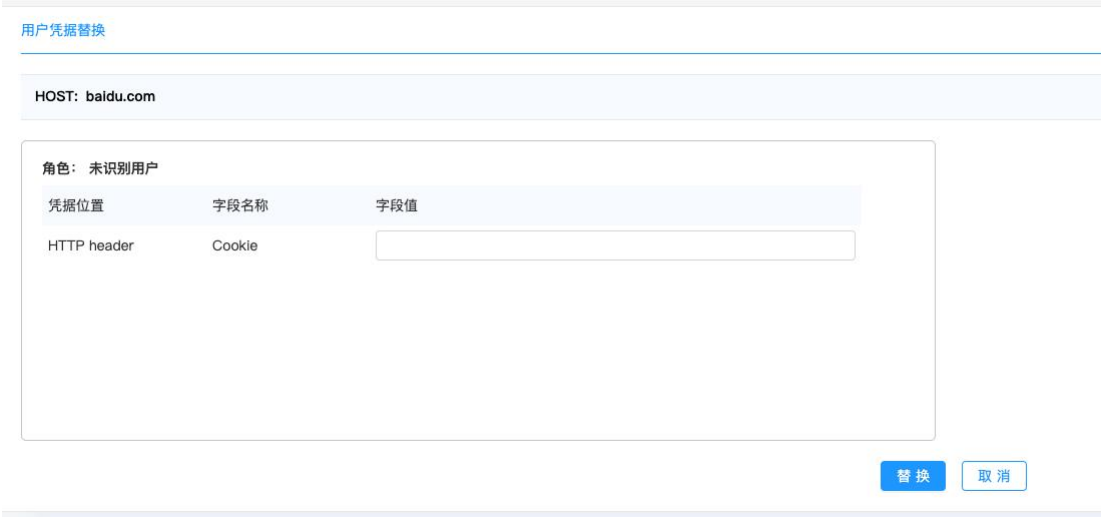
- 注：安全系数为百分制，数值越低对应的安全等级越危险：0~60 分高危，61~90 中危，91~99 低危，100 分时暂无风险。
- 用户可对该项目进行编辑、删除、输出报告、回归操作、检测逻辑漏洞、用户凭证替换等操作。

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。

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。



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）。

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。

图表 55 回归操作

1.6.4.2 插桩类

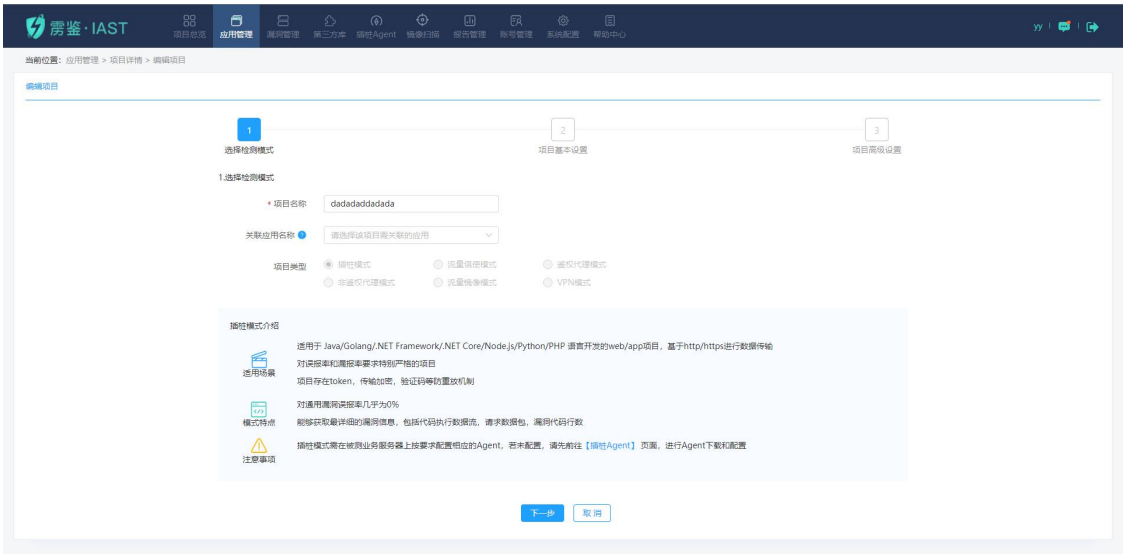
展示当前项目的基础信息，其中可看到项目名称、项目模式、项目归属人、项目成员、项目模板、项目语言、请求数、漏洞数（未修复数）、创建时间、项目描述、项目安全系数及安全等级，并且可对项目进行检测控制、输出报告等操作。

- 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。

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。



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）。

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。

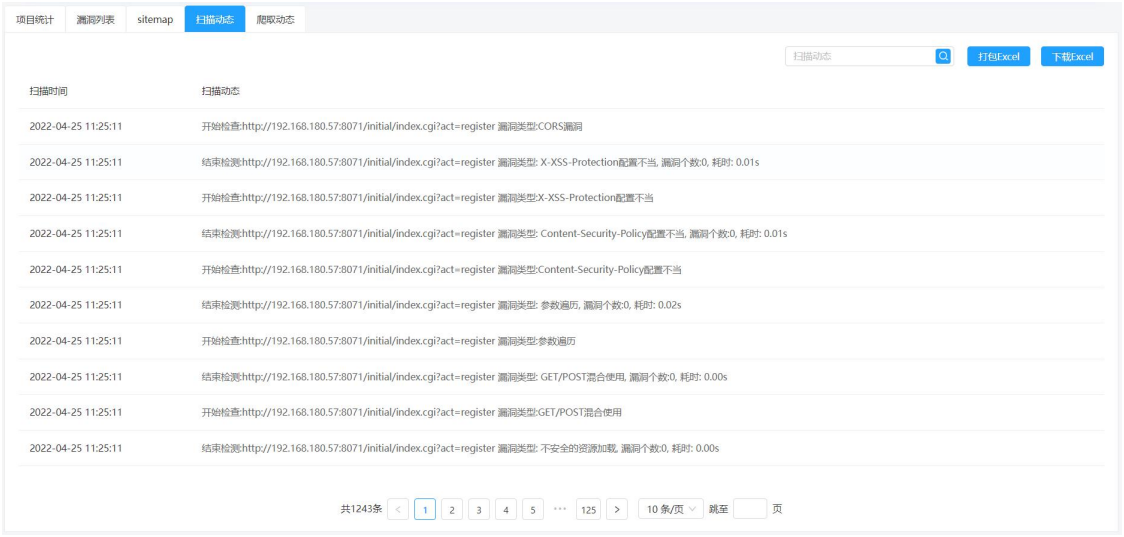
图表 59 非鉴权模式项目概况

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

➢ 扫描动态：展示了该项目的扫描动态

1） 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。



图表 60 扫描动态

2） 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。

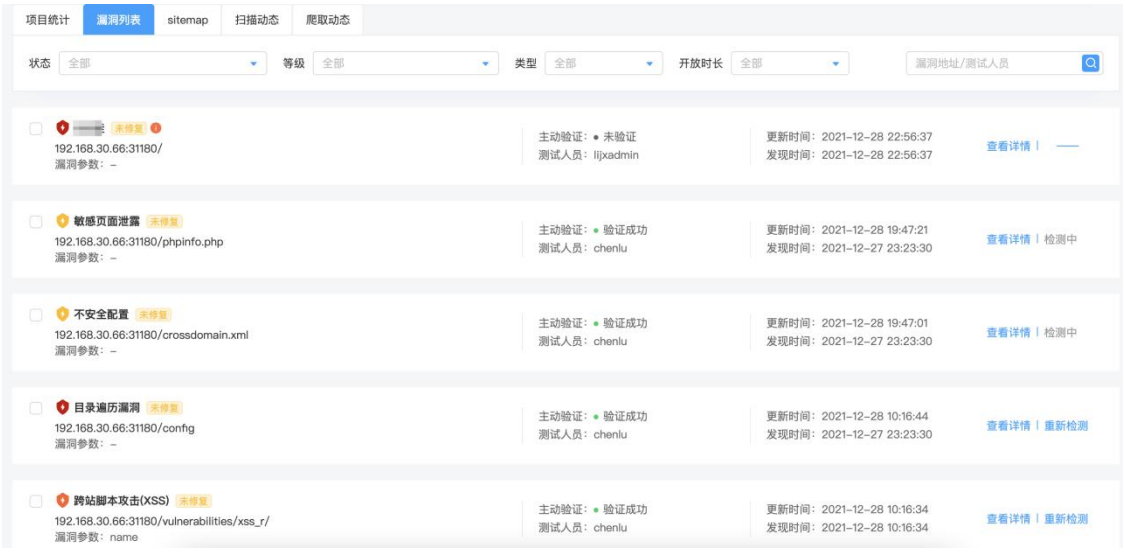
3） 漏洞状态图：展示所有项目高危，中危，低危，提示类漏洞，漏洞数/已修复/未修复的数量。

➢ 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。

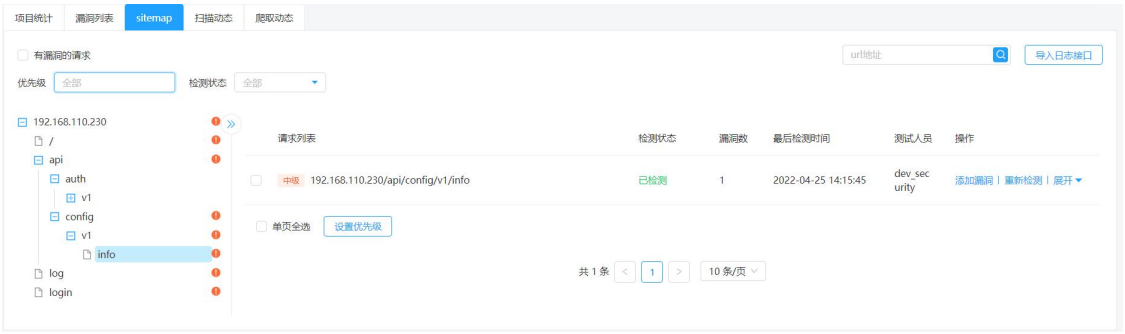


图表 62 漏洞列表

- 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。

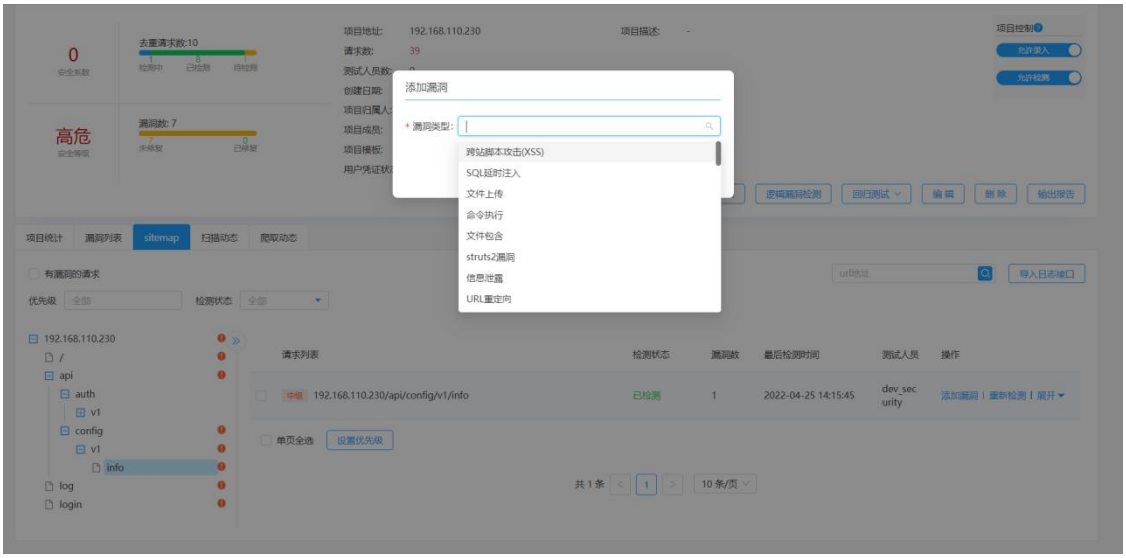
  在初始页面可查看已知 URL 覆盖度及未覆盖 URL。

  可根据检测状态进行查询，根据 url 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。



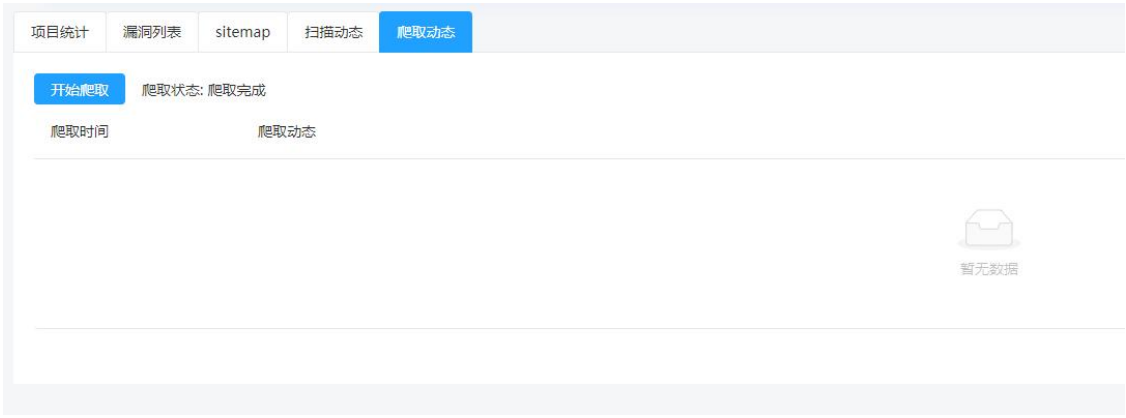
图表 63 扫描类项目 SITEMAP

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。



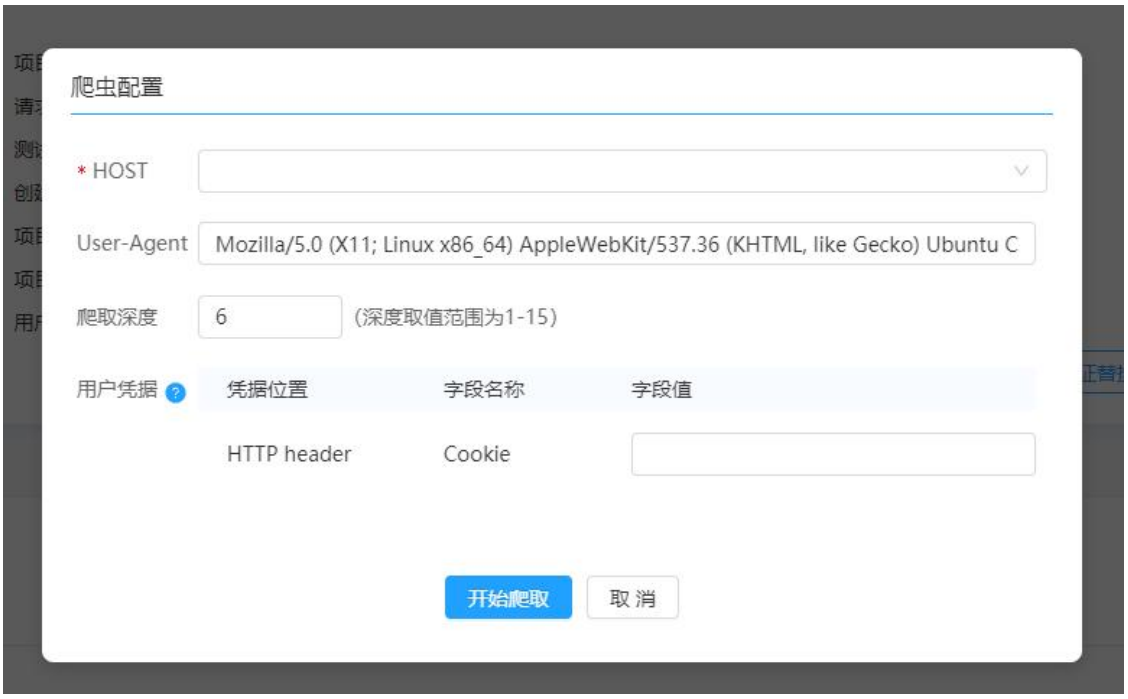
图表 64 添加漏洞

➢ 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。



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。



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。

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。

杭州默安科技有限公司

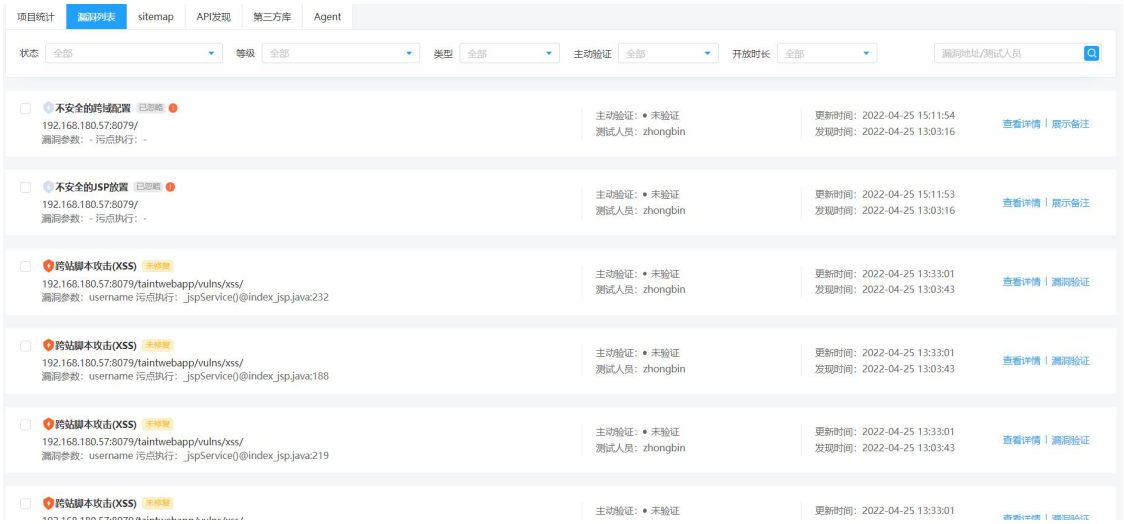
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

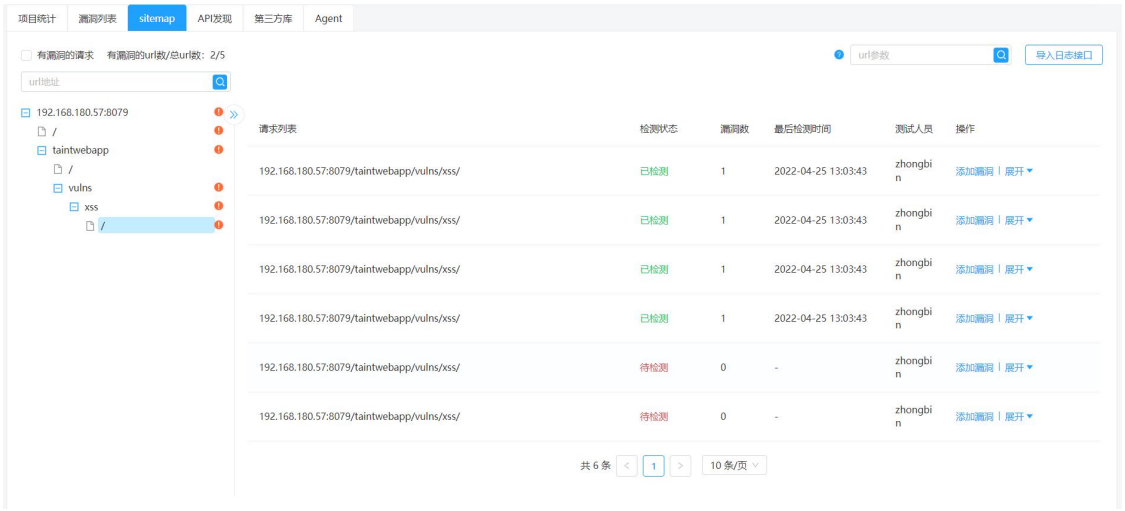


图表 69 漏洞列表

- 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

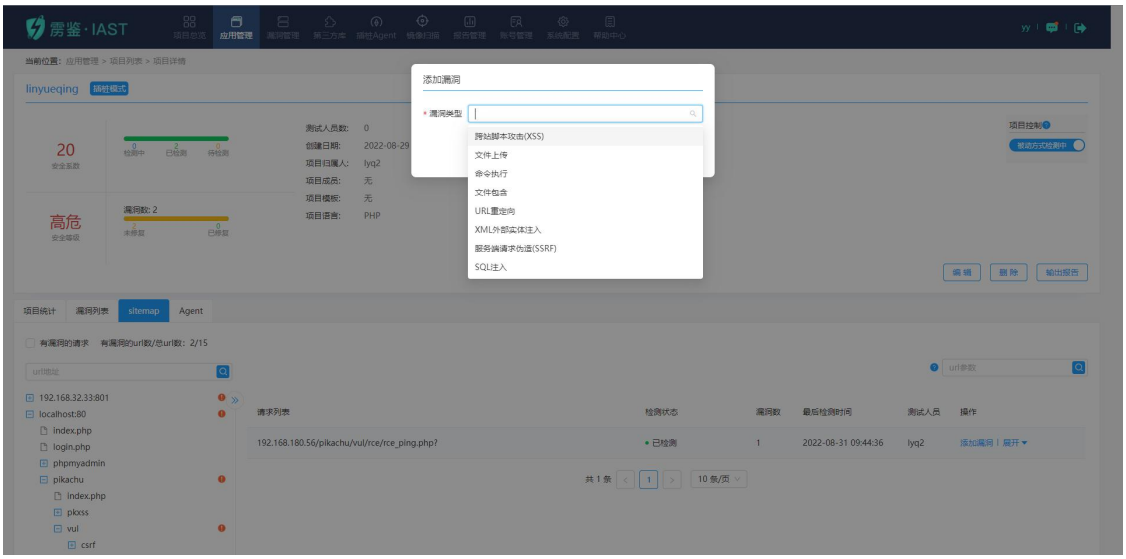
时间、检测状态及操作，标记感叹号代表此目录下请求含漏洞。

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。



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。



图表 71 添加漏洞

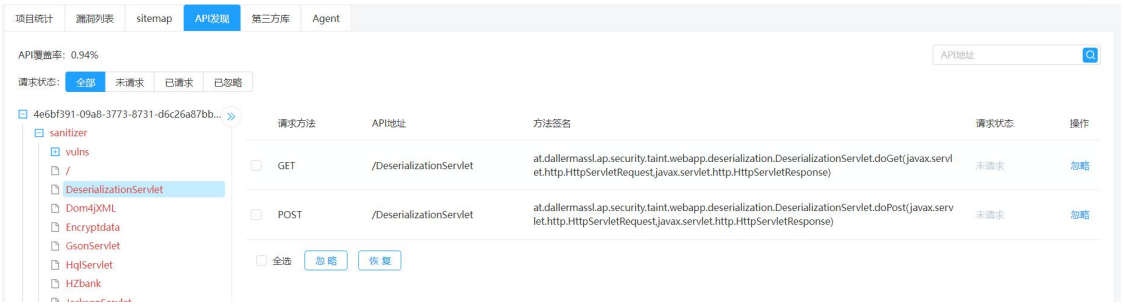
➢ API 发现：展示该项目下 Agent 自动发现的 API 及对应请求情况。此功能仅项目语言为 Java、.NET Framework、.NET Core 和 Python 时支持。

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

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。

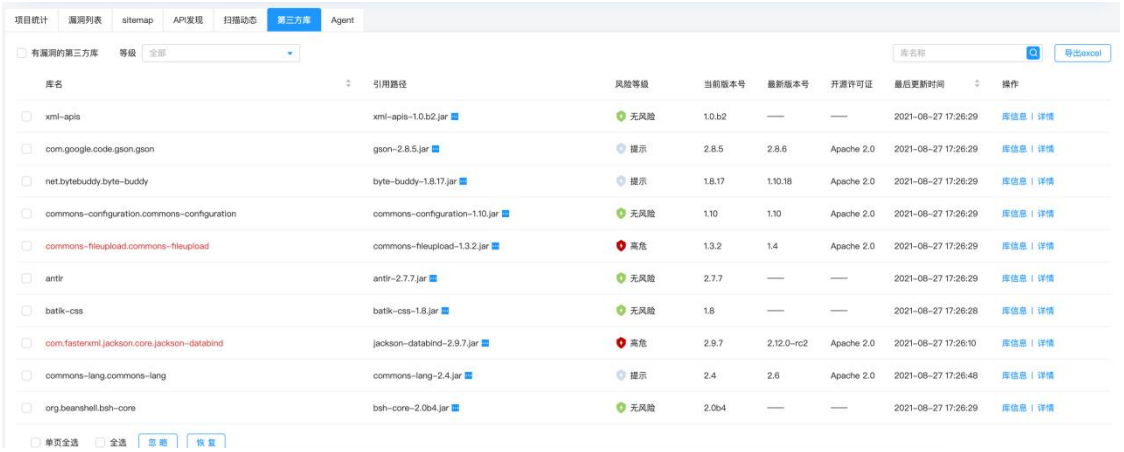


图表 72 插桩项目 API 发现

➢ 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。

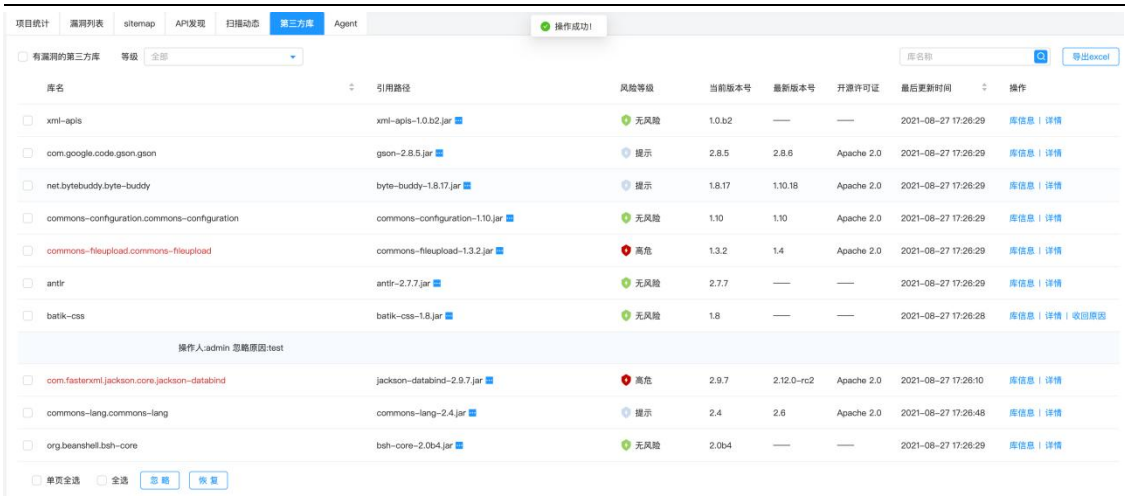


图表 73 项目第三方库列表

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。

杭州默安科技有限公司

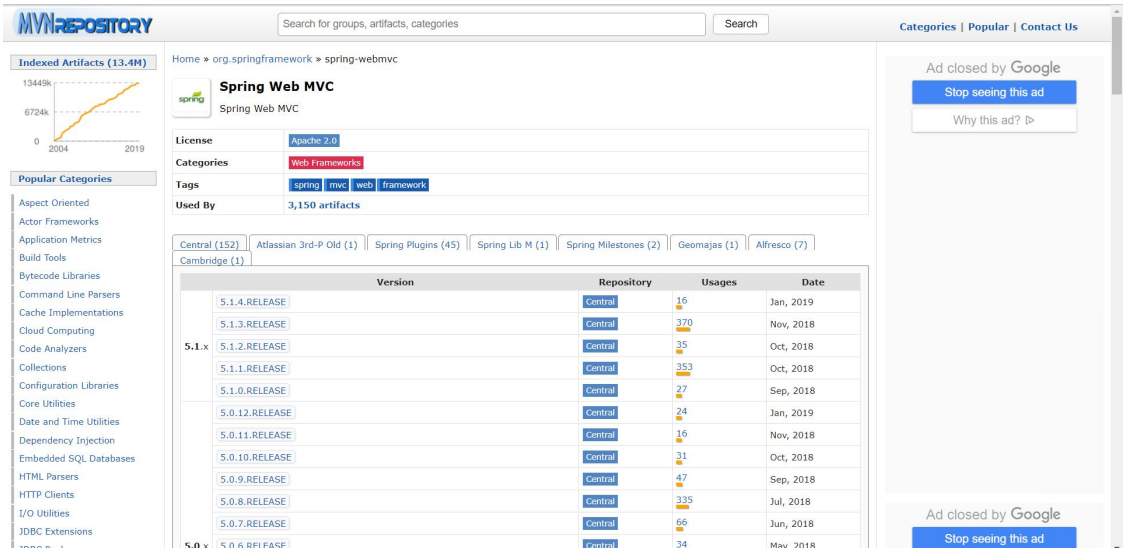
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



图表 74 项目第三方库忽略

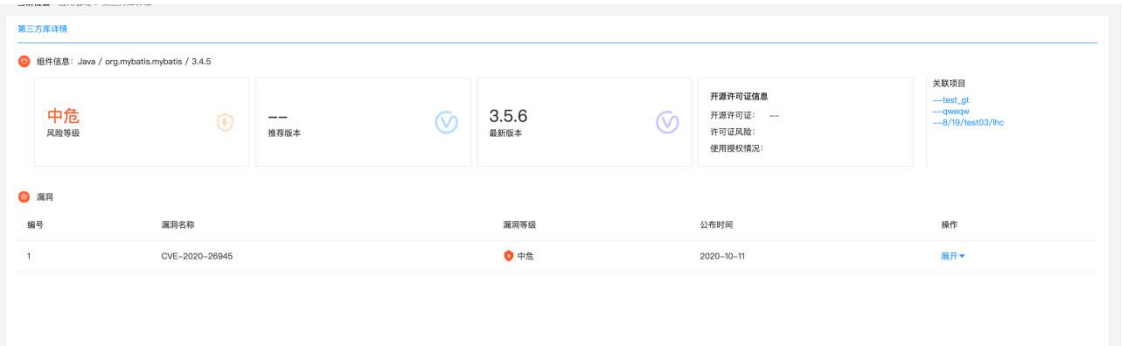
可根据第三方库风险等级、第三方库是否有漏洞进行查看，可查看第三方库信息和第三方库详情，可导出第三方库报告。

- 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。



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。



图表 76 第三方库详情

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。

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。

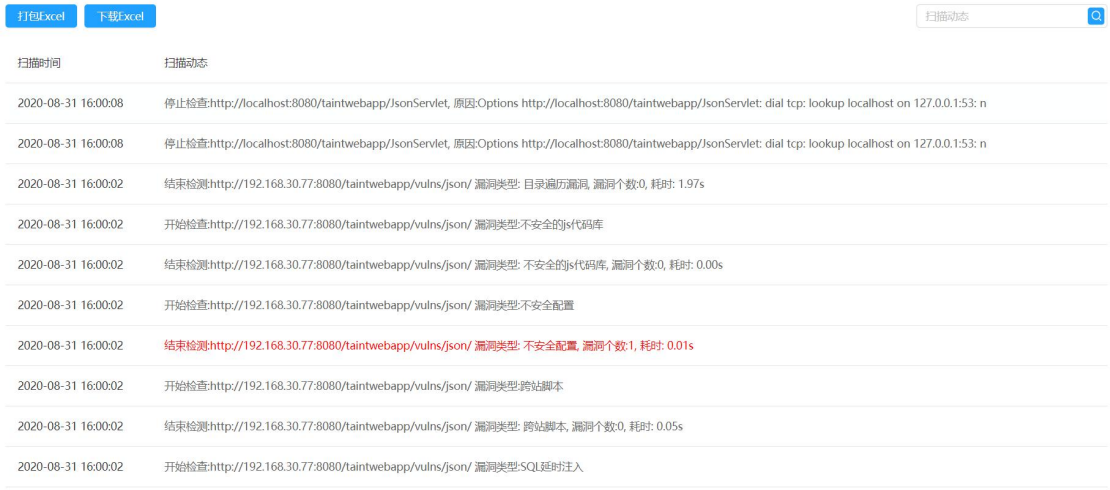
Agent 列表默认按插桩 Agent 地址归类排列，列表内容包括名称、key、最近请求时间、安装时间、项目名称、标签、状态及操作。

可根据 Agent 状态筛选，可根据名称、Agent 地址、key、备注和标签搜索。

图表 79 项目 Agent 列表

➢ 扫描动态：展示了该项目的扫描动态

1) 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。



图表 80 主动模式扫描动态

2) 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。

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。

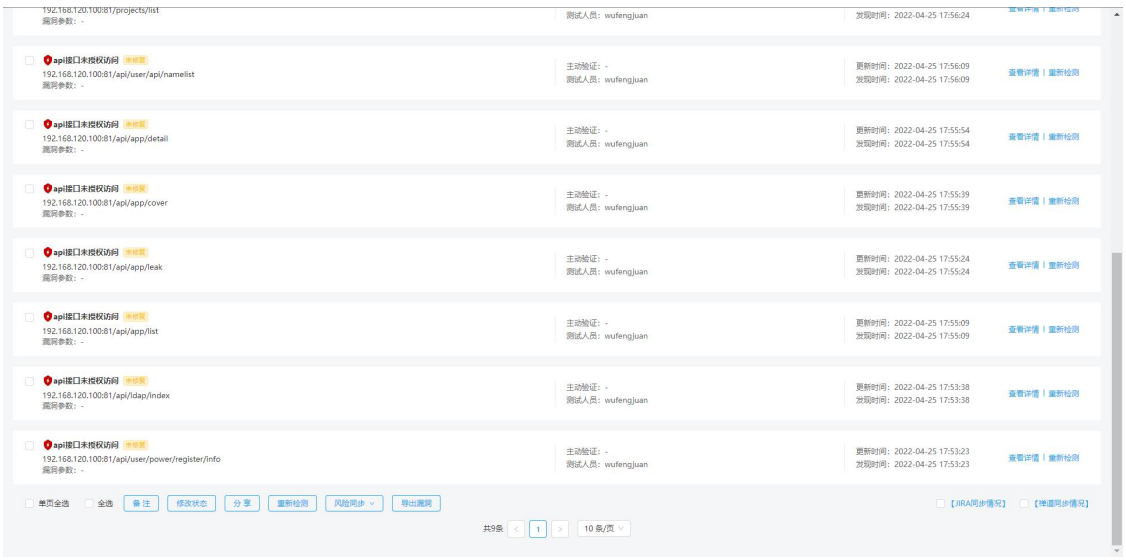
点击“开始检测”即可进行逻辑漏洞检测，检测过程中会展示扫描动态。每一个请求如果检测出错，会展示返回码，便于排查请求过程中发生的错误。点击取消会清楚此次扫描任务，点击返回会返回至项目详情界面，本次扫描任务会在后台进行。

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。

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

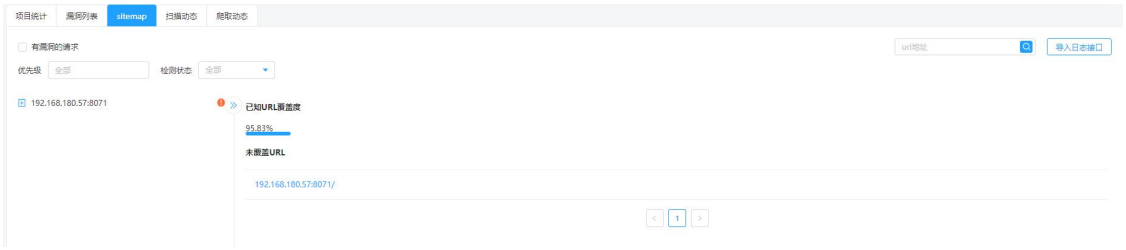


图表 84 逻辑漏洞展示

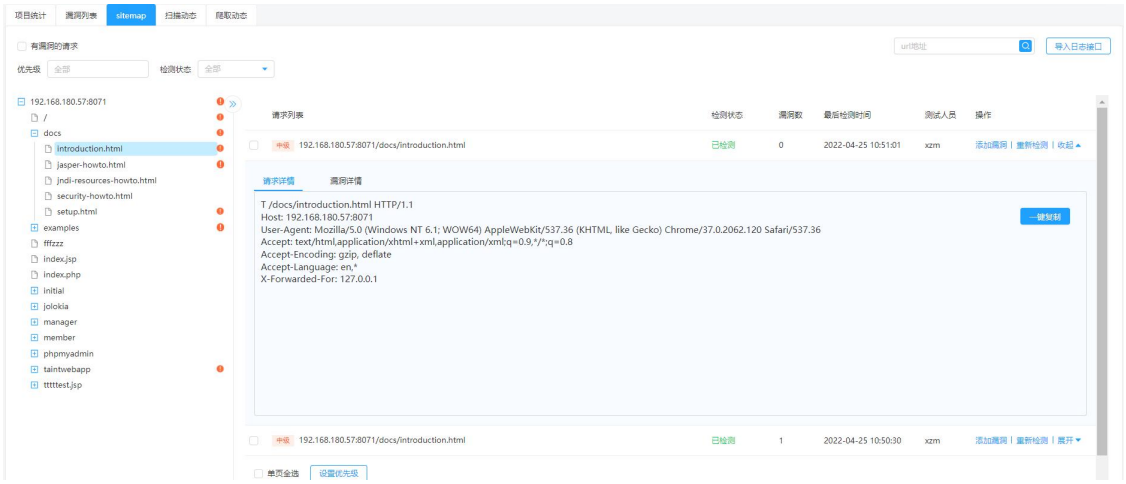
1.6.7Sitemap（扫描类）

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。



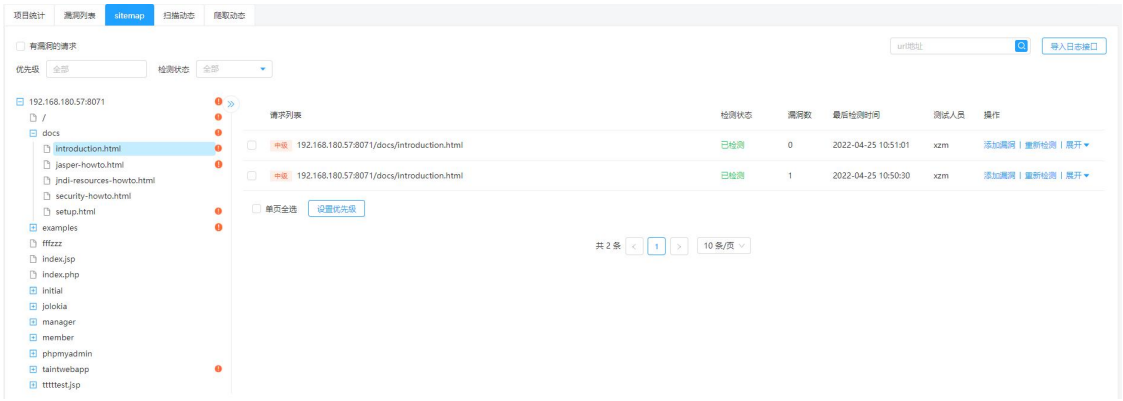
图表 85 Sitemap 列表-URL 覆盖度



图表 86 Sitemap 列表-请求详情 1

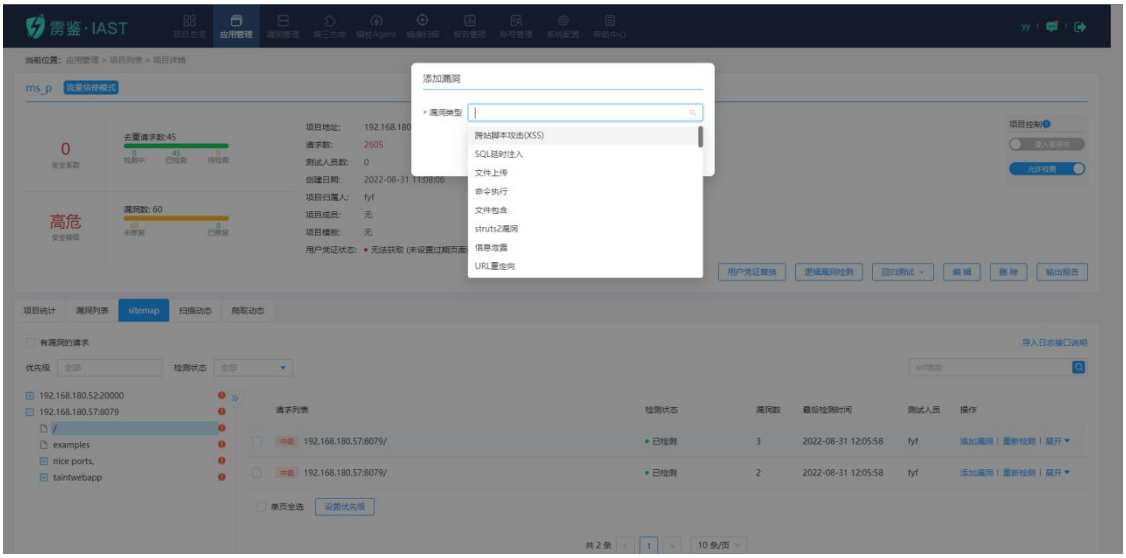
右侧列表内容包括 URL、测试人员、漏洞数、最后检测时间、检测状态及操作。

可根据优先级和检测状态进行查询，根据 url 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。



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。



图表 88 添加漏洞

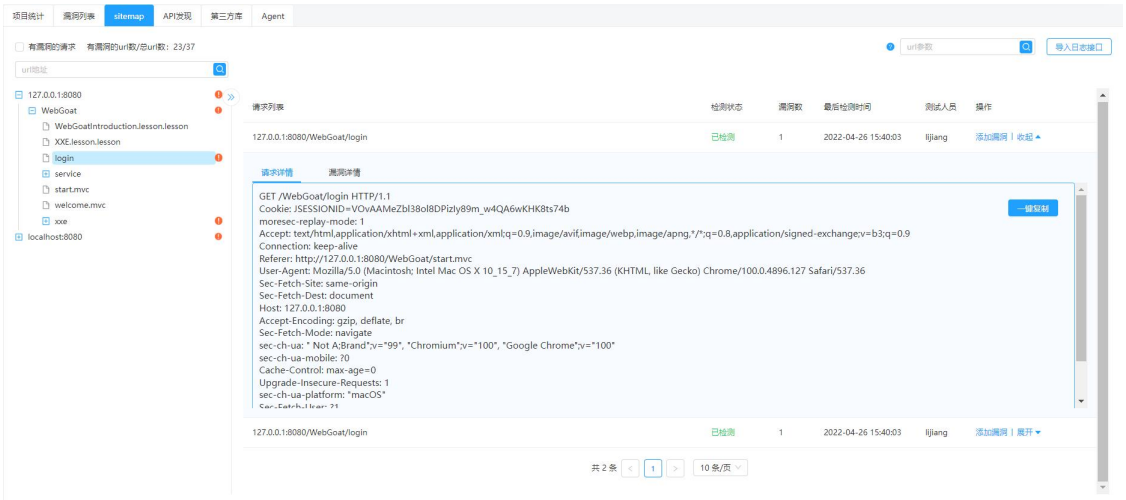
导入日志接口支持用户将 web 日志导入雳鉴平台的 kafka 接口中，雳鉴对 web 日志中的请求进行扫描。使用时按照规定的格式向雳鉴的 kafka 接口导入日志即可。

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。

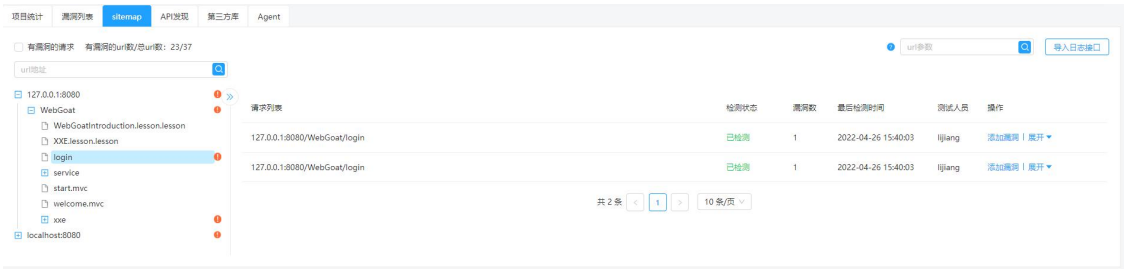
左侧列表中标记感叹号代表此目录下请求含漏洞，其余目录为测试人员已点击但无漏洞的 URL。



图表 90 SITEMAP 列表-请求详情 2

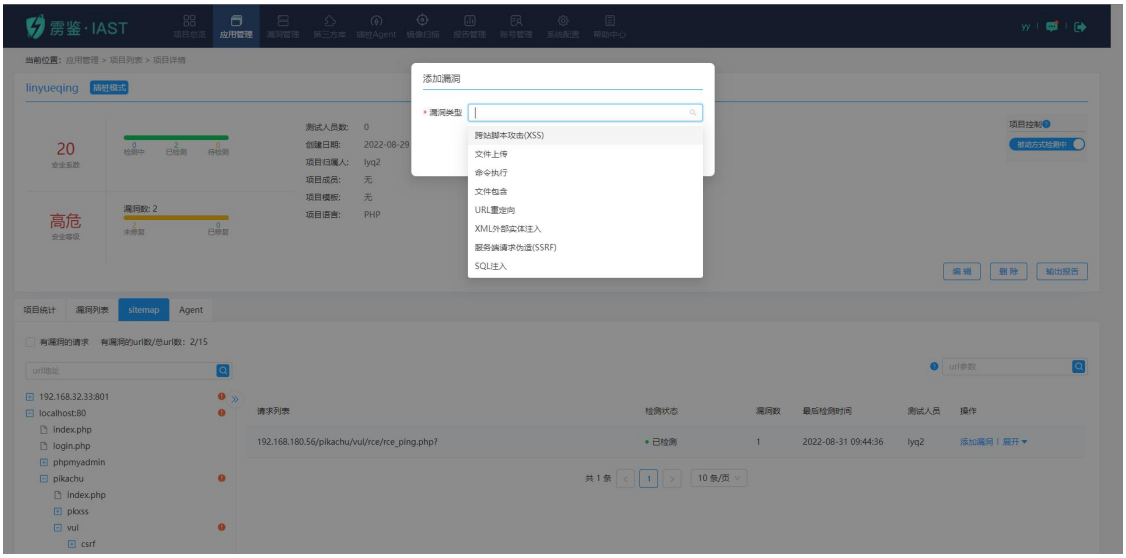
右侧列表内容包括 URL、测试人员、漏洞数、最后检测时间、检测状态及操作。

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。



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。



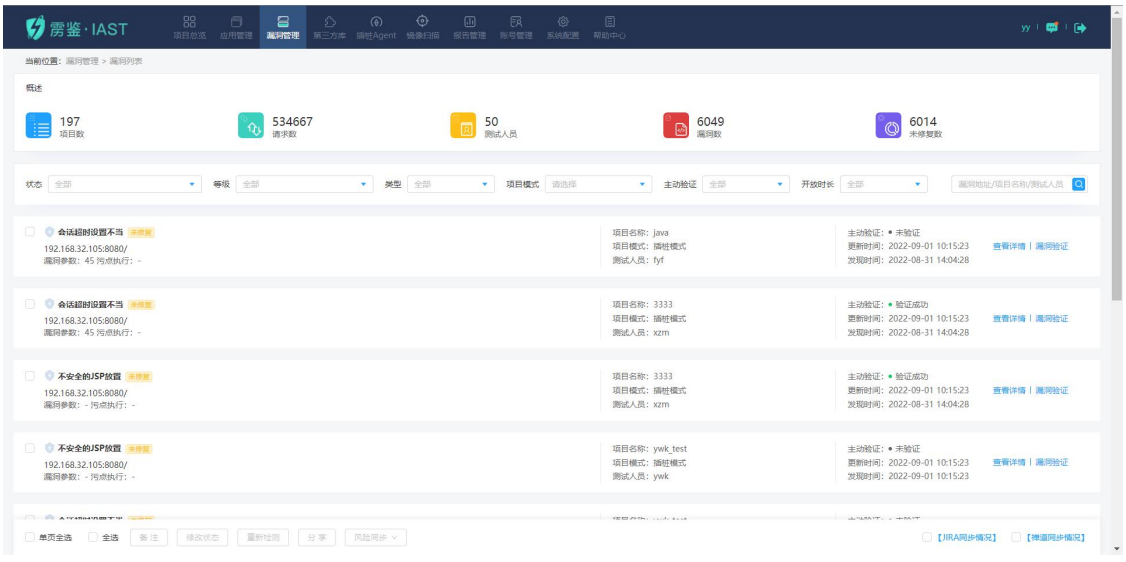
图表 92 添加漏洞

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。

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。

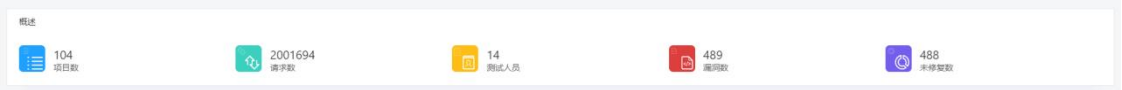


图表 94 漏洞列表

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。



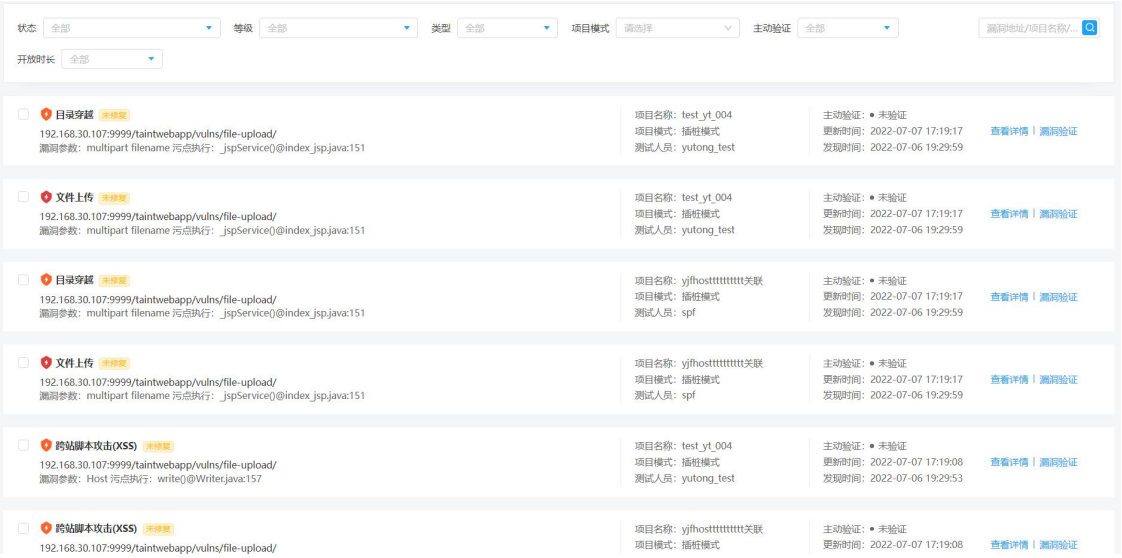
图表 95 扫描类漏洞列表概述

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。



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

杭州默安科技有限公司

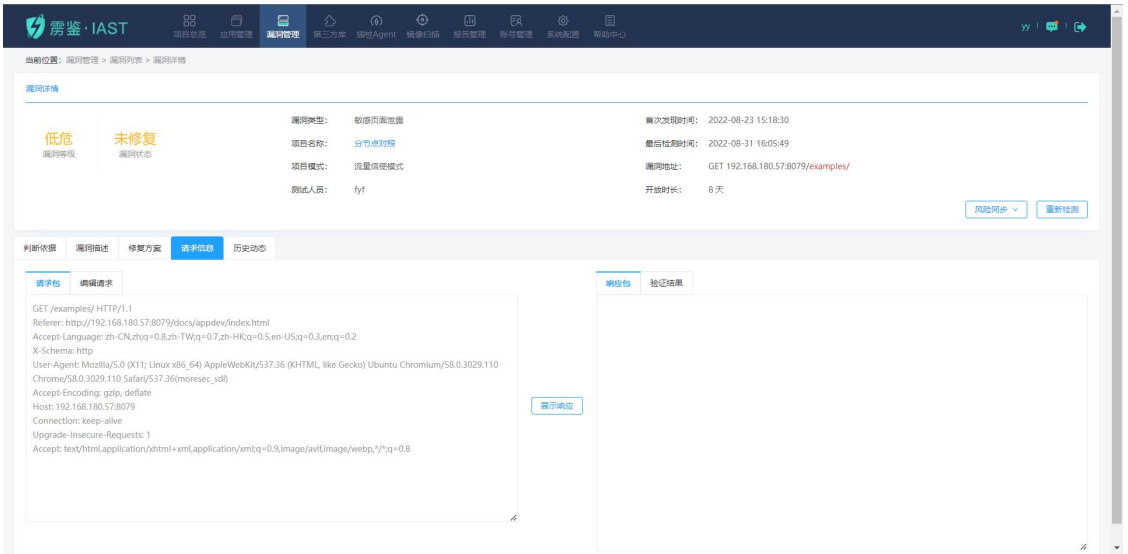
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。



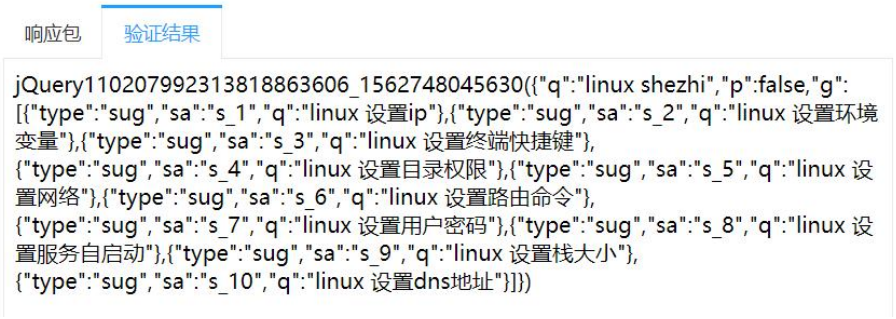
图表 98 漏洞详情

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
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

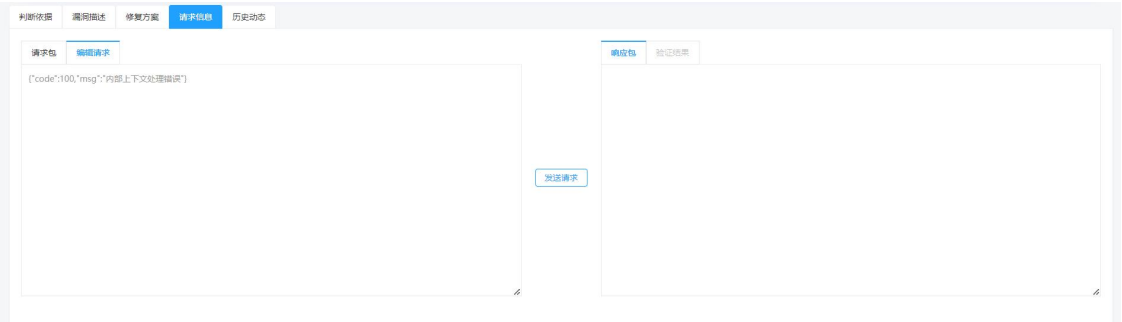
结果’。响应包里面内容显示该漏洞页面的请求响应源码；验证结果是以 web 的形式展示漏洞。如 SQL 延时注入漏洞，单击‘验证结果’就会显示相关的数据信息，如图 82 所示。

图表 99 漏洞演示及编辑一



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。



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。

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）。

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。

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。

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。

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。

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。

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

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

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。

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。

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。

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。

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。

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。

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。

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。

图表 120 同步禅道 – 重新同步配置

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。

图表 122 漏洞列表 - 查看禅道同步情况

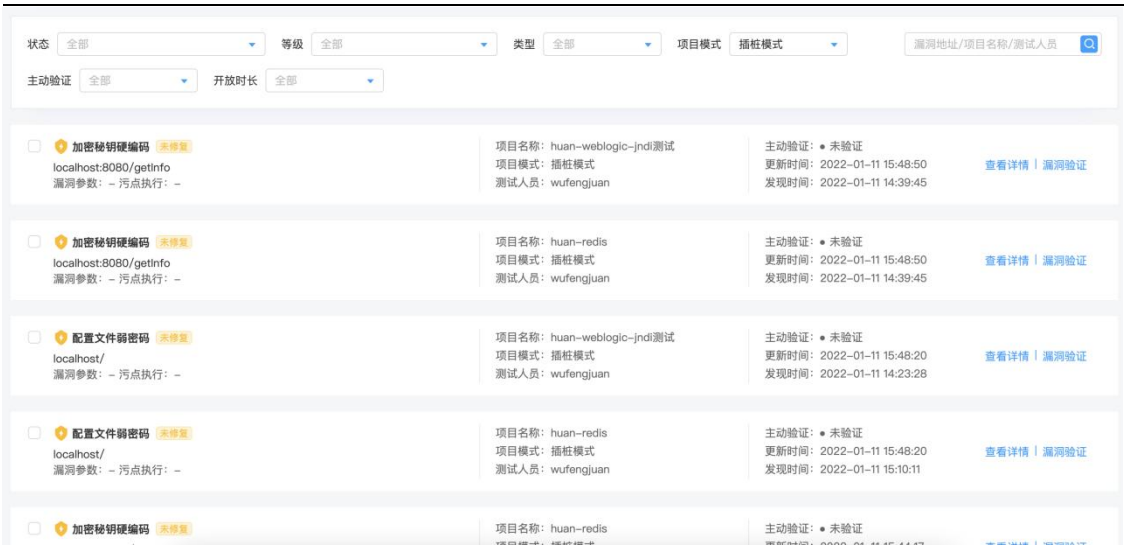
- 同时选择“JIRA 同步情况”和“禅道同步情况”复选框，可同时查看漏洞同步 JIRA 和禅道的情况，列表右侧展示 JIRA 图标和禅道图标表示均已同步。

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。

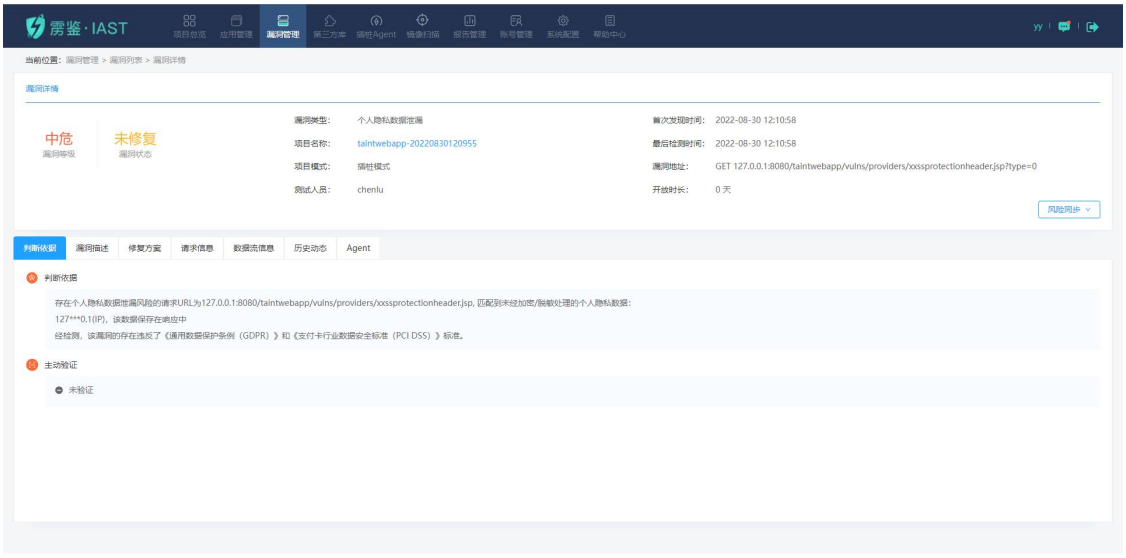


图表 124 插桩类漏洞列表

- 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。

图表 125 插桩类漏洞分享

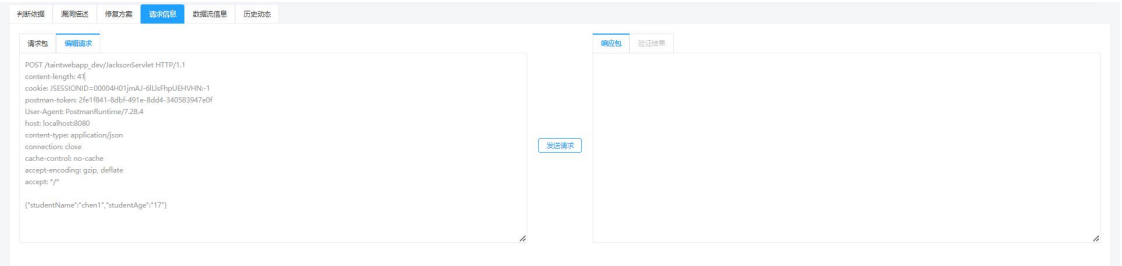
- 点击“查看详情”，跳转至漏洞概述页，该页面中可见该漏洞的类型、等级、状态等自述信息，可知描述、危害、建议、细节，漏洞代码示例（JAVA/.NET/PHP），对于可通过安全组件修复的漏洞可下载安全组件并查看安全组件的使用方法，可进行请求展示和编辑，并可查看详细数据流。
  - 在判断依据中可查看漏洞的代码片段、主动验证结果（仅针对开启了主动验证功能的漏洞）以及 Payload（仅针对开启了主动方式功能检测出的漏洞）。



图表 126 插桩类漏洞概述

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

- 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。



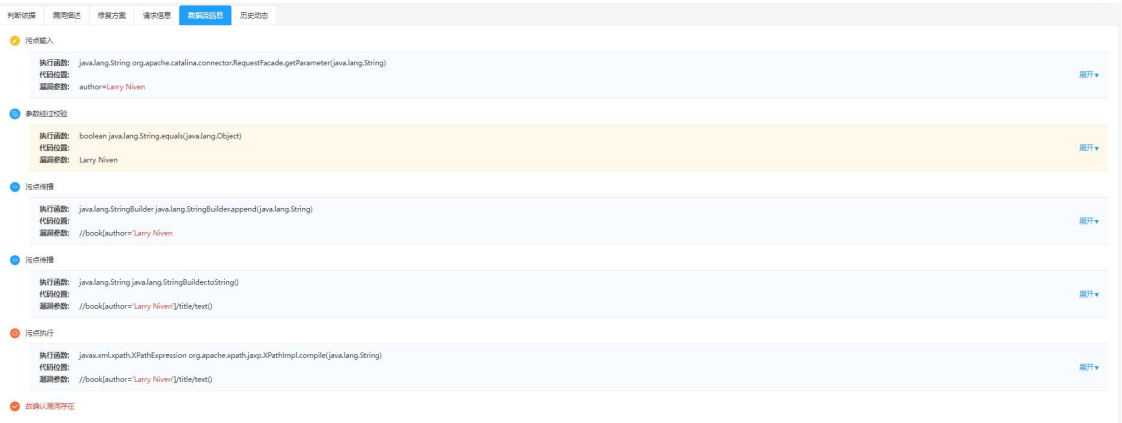
图表 127 漏洞演示及编辑二

- 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

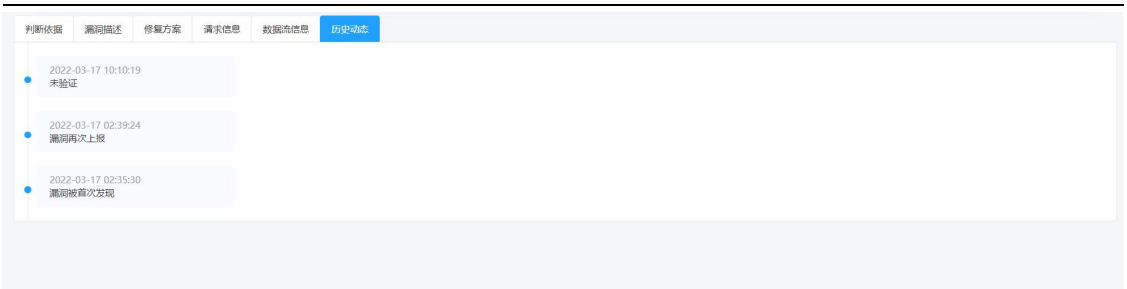
  所有堆栈：展示所有堆栈信息

  用户堆栈：展示用户代码的堆栈信息



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）。



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）。

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。

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。

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。

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。

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

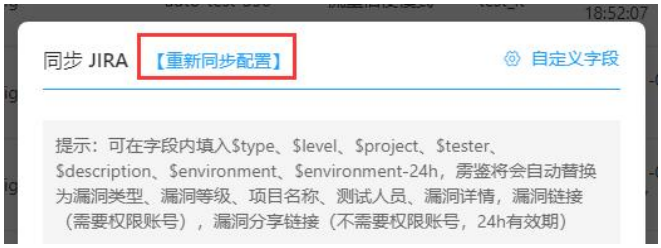
✧ 弹框下方可选择是否记住本次同步的选项及填写信息，若选择记住，则下次点击“同步 JIRA”按钮后弹框内会展示上一次本账号进行同步时的选项及填写信息。

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。

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。



图表 138 同步 JIRA – 重新同步配置

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。

图表 140 漏洞列表 – 查看 JIRA 同步情况

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

- 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。

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。

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。

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

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。

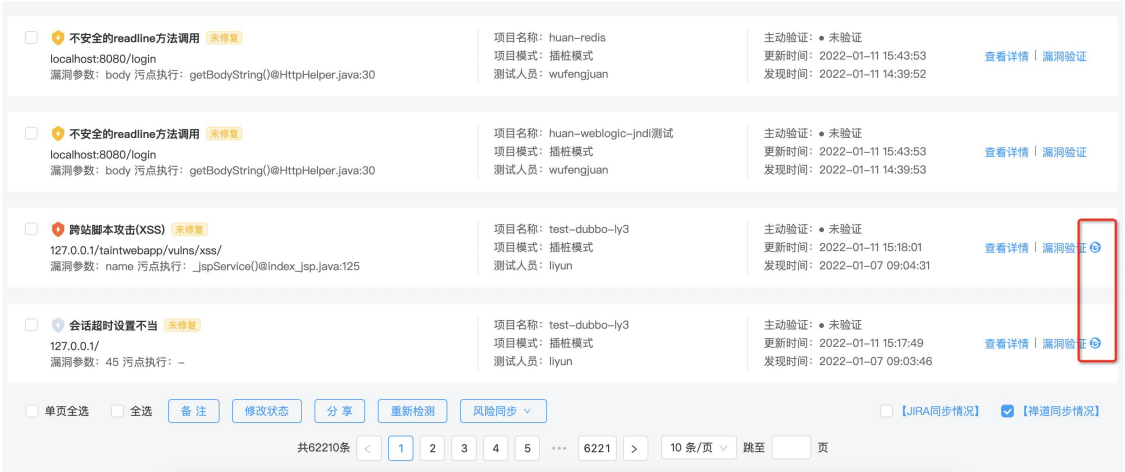
杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

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。



图表 147 同步禅道 - 查看同步情况

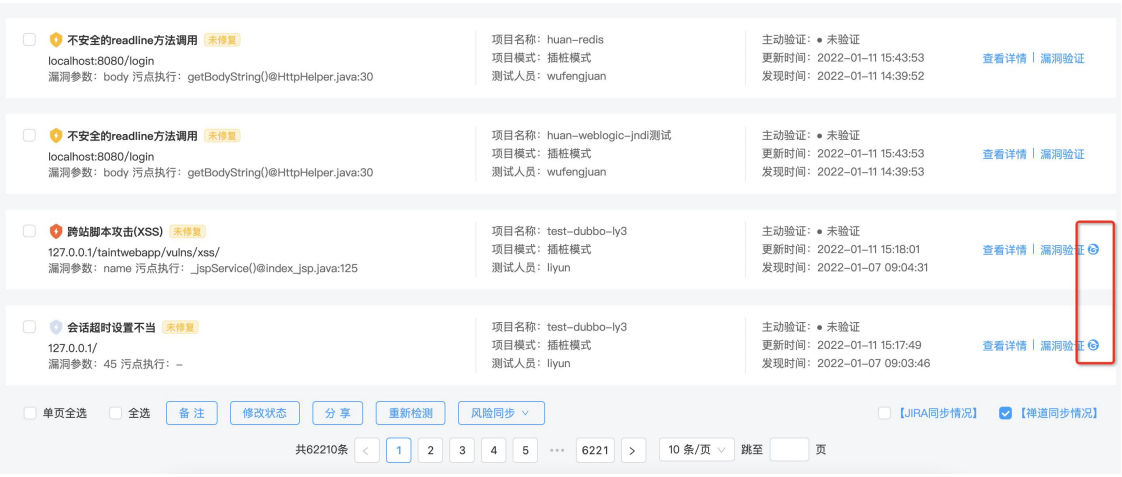
✧ 用户非第一次进行同步禅道操作，点击“同步禅道”按钮会直接展示上次同步配置后的弹框（或上次记住漏洞同步信息的弹框）。

✧ 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。

图表 148 同步禅道 - 重新同步配置

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。



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。

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

图表 151 漏洞列表 - 查看 JIRA 和禅道同步情况

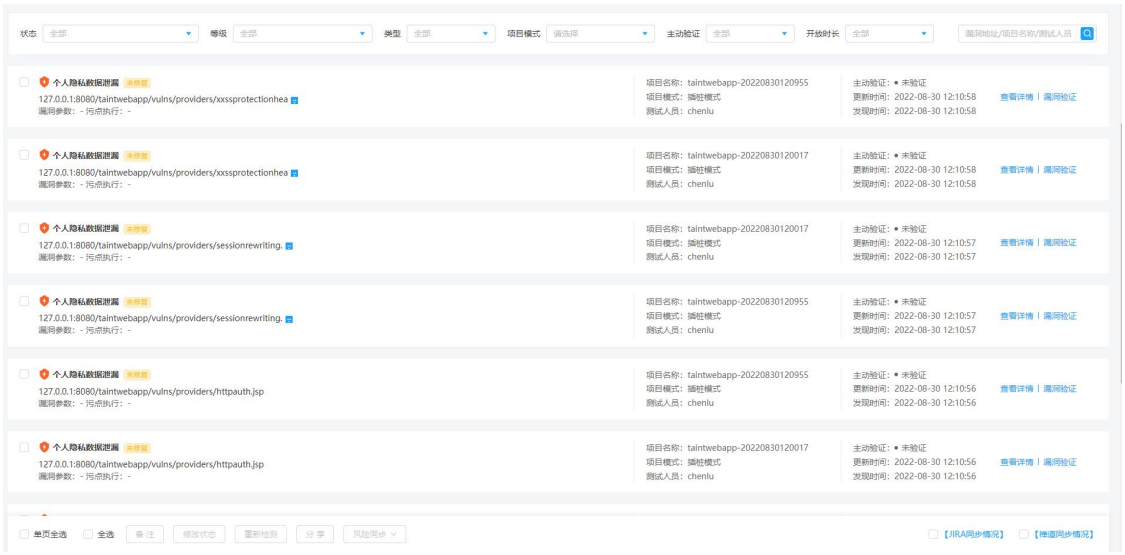
1.7.2数据安全漏洞

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。



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。

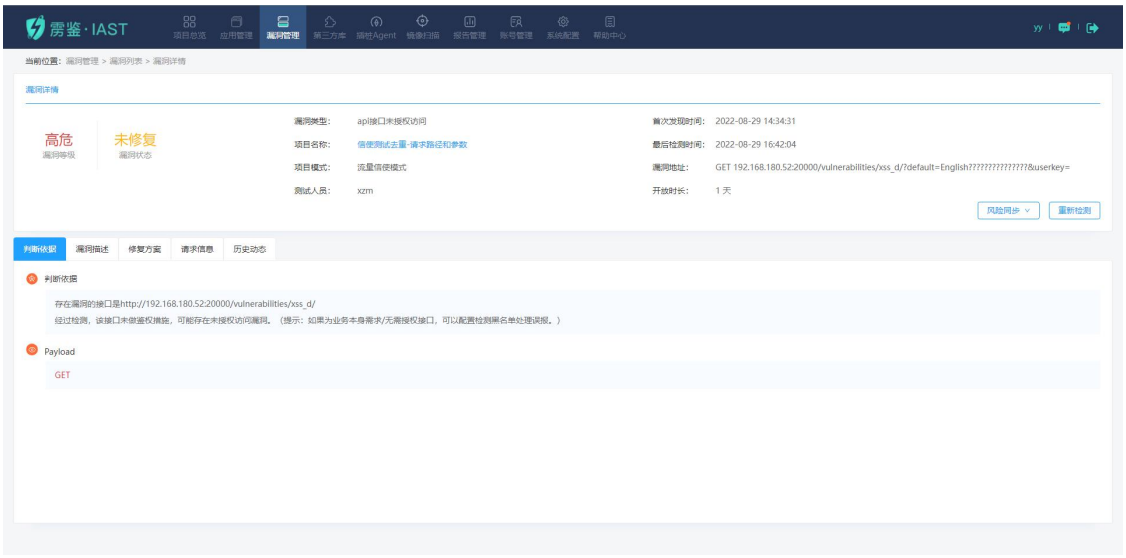
图表 154 漏洞分享

- 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

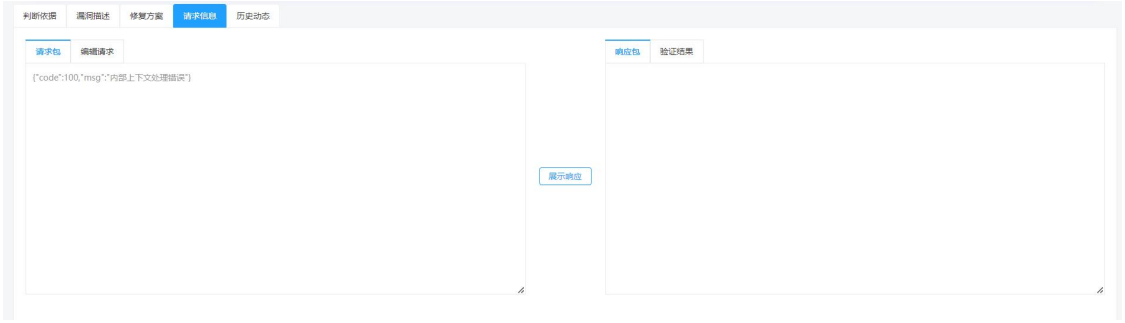
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

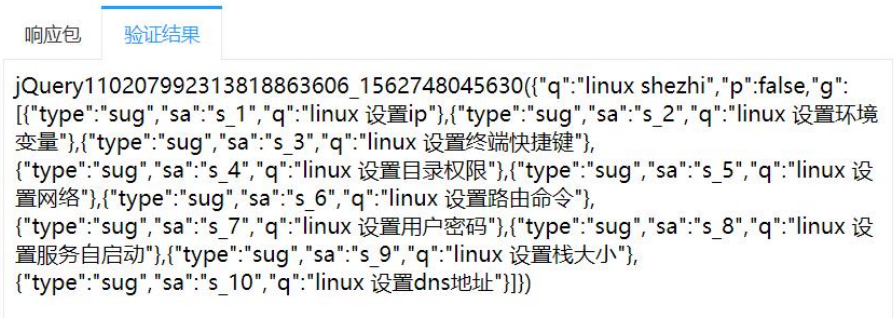


图表 155 数据安全漏洞详情（扫描类）

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。

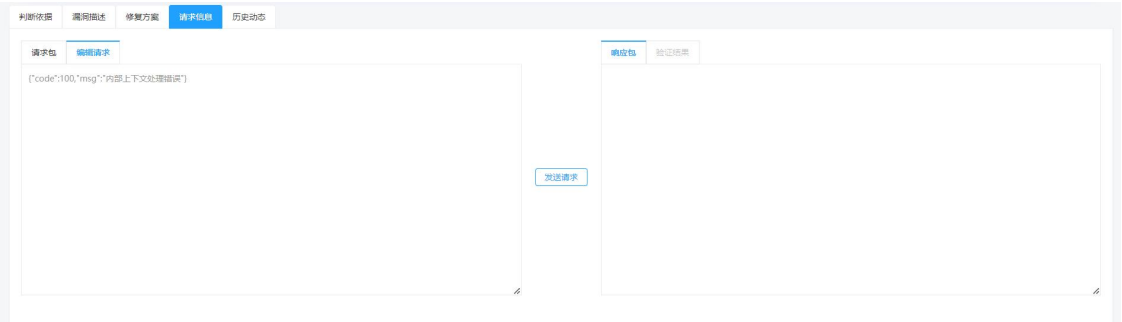


图表 156 漏洞演示及编辑



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。

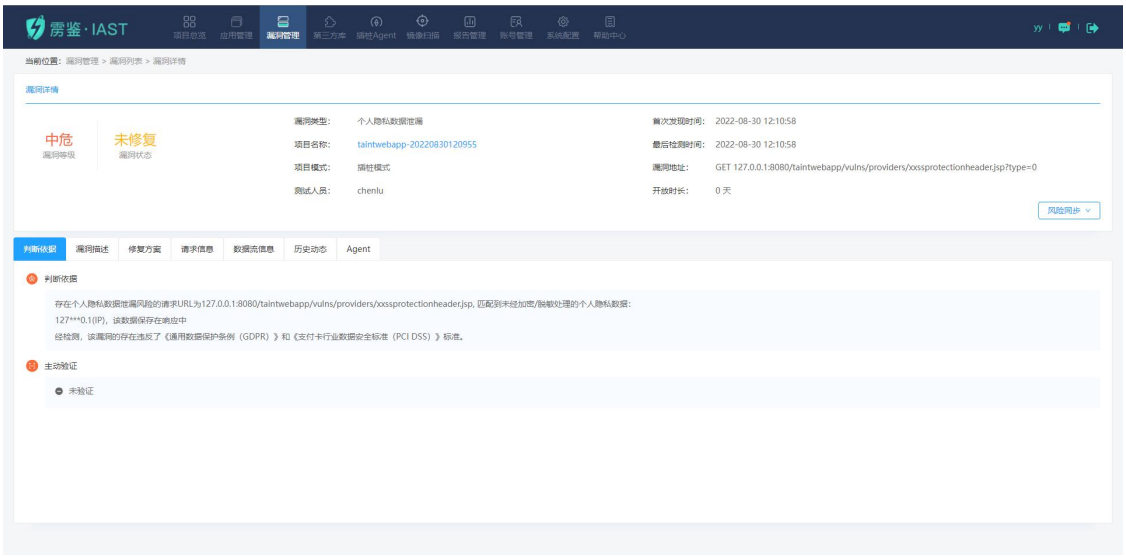


图表 158 漏洞演示及编辑二

- 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）。

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。

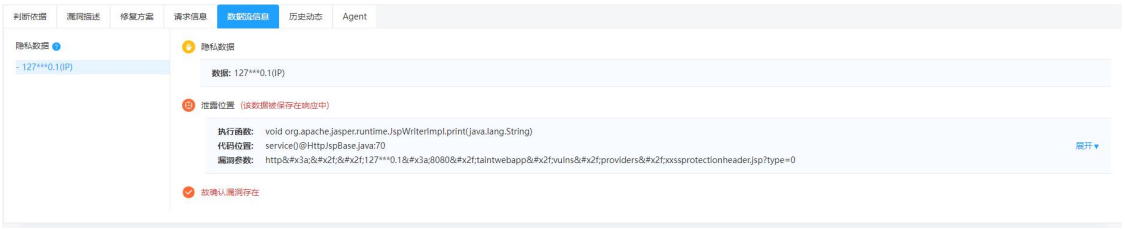


杭州默安科技有限公司

Tel：（+86）400-0571-211　　Email：market_moresec.cn　　Web：www.moresec.cn

图表 160 数据安全漏洞详情

- 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。



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）。

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。

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。

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。

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。

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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

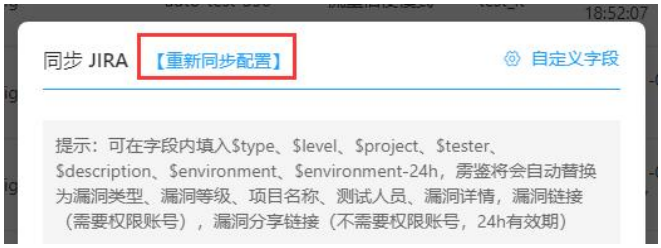
✧ 弹框下方可选择是否记住本次同步的选项及填写信息，若选择记住，则下次点击“同步 JIRA”按钮后弹框内会展示上一次本账号进行同步时的选项及填写信息。

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。

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。



图表 170 同步 JIRA - 重新同步配置

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。

图表 172 漏洞列表 - 查看 JIRA 同步情况

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

- 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。

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。

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。

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

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。

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.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。

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。

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。

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

- 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。

图表 182 漏洞列表 - 查看禅道同步情况

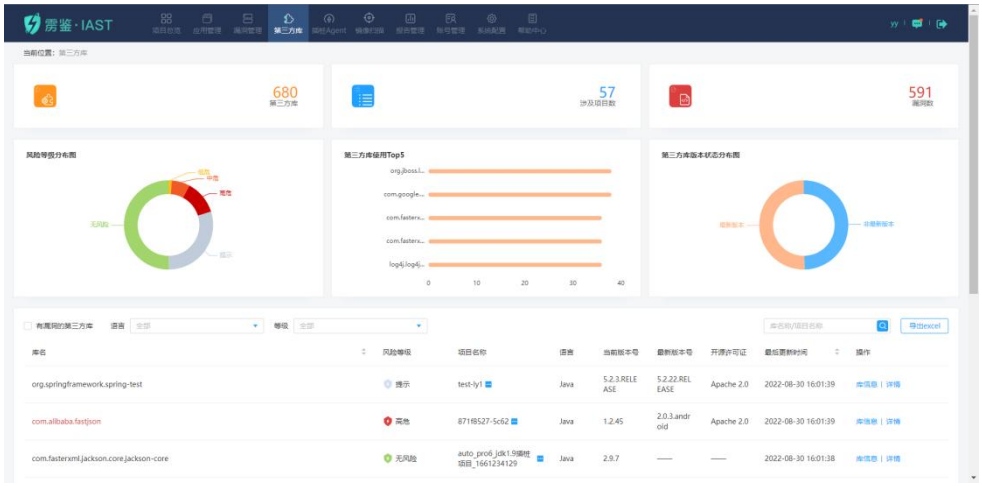
- 同时选择“JIRA 同步情况”和“禅道同步情况”复选框，可同时查看数据安全漏洞同步 JIRA 和禅道的情况，列表右侧展示 JIRA 图标和禅道图标表示均已同步。

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。



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。

图表 185 第三方库概述

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

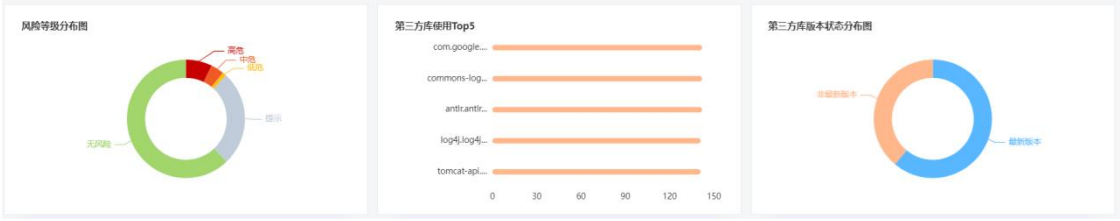
1.8.2图表分析

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。

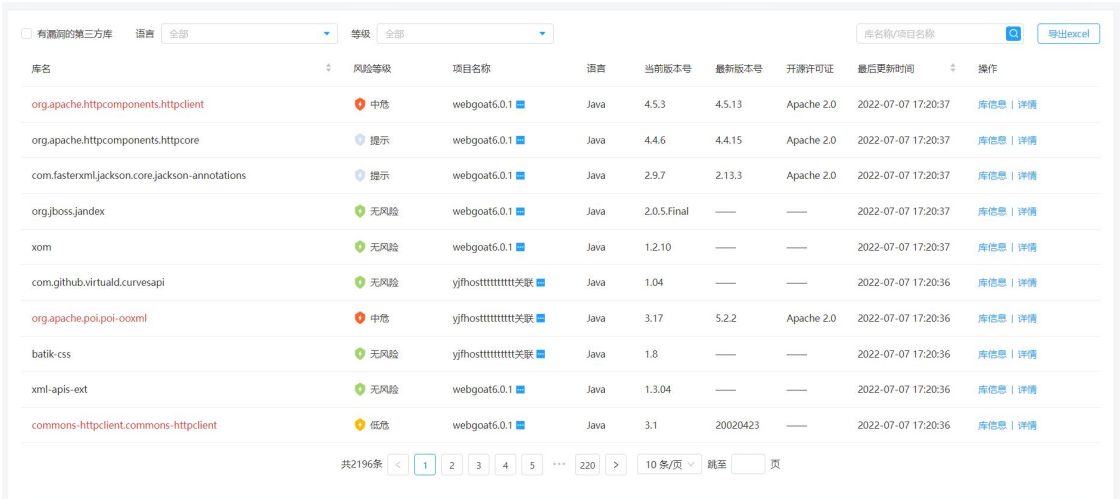


图表 186 第三方库列表图表分析

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。



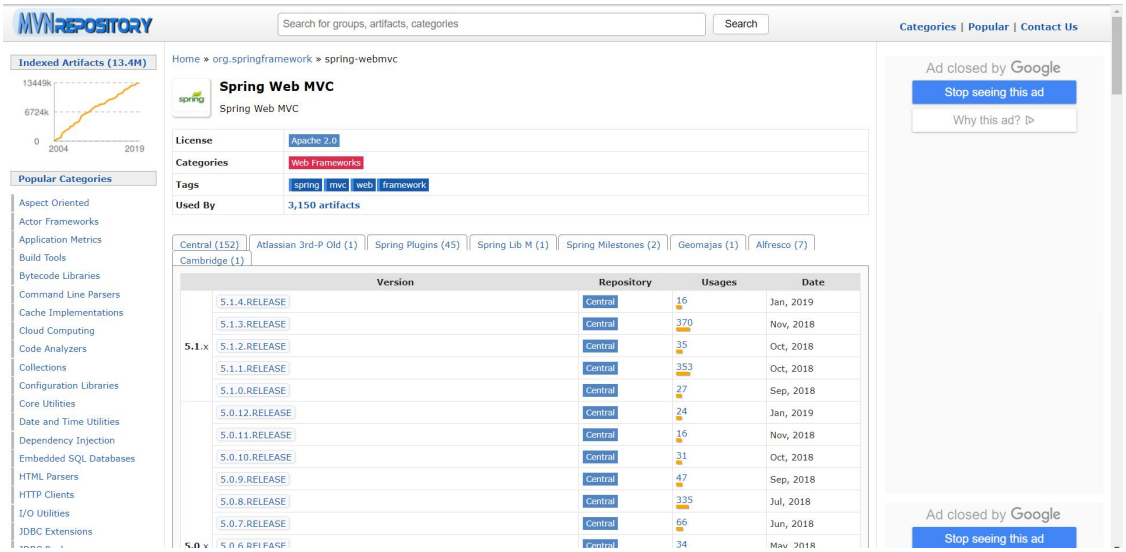
图表 187 第三方库列表

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

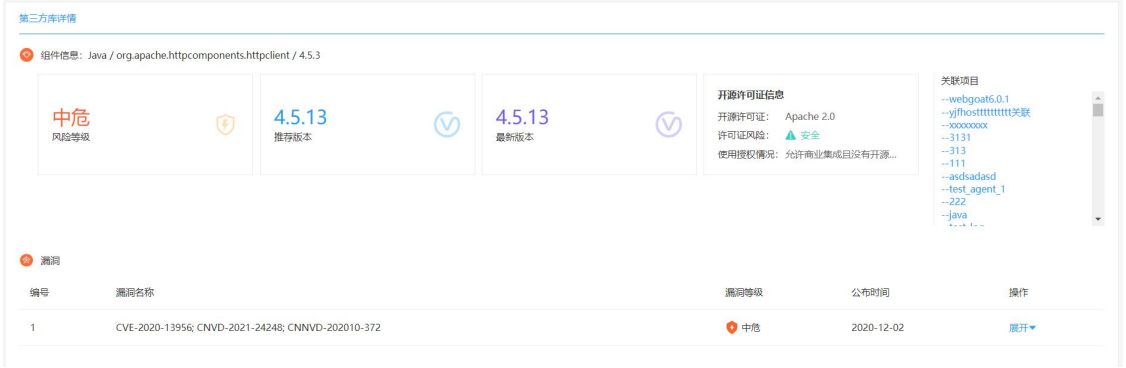
可根据第三方库风险等级、语言、第三方库是否有漏洞进行查看，可查看第三方库信息和第三方库详情，可导出第三方库报告。

- 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。



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。



图表 189 第三方库详情

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

图表 190 第三方库漏洞详情

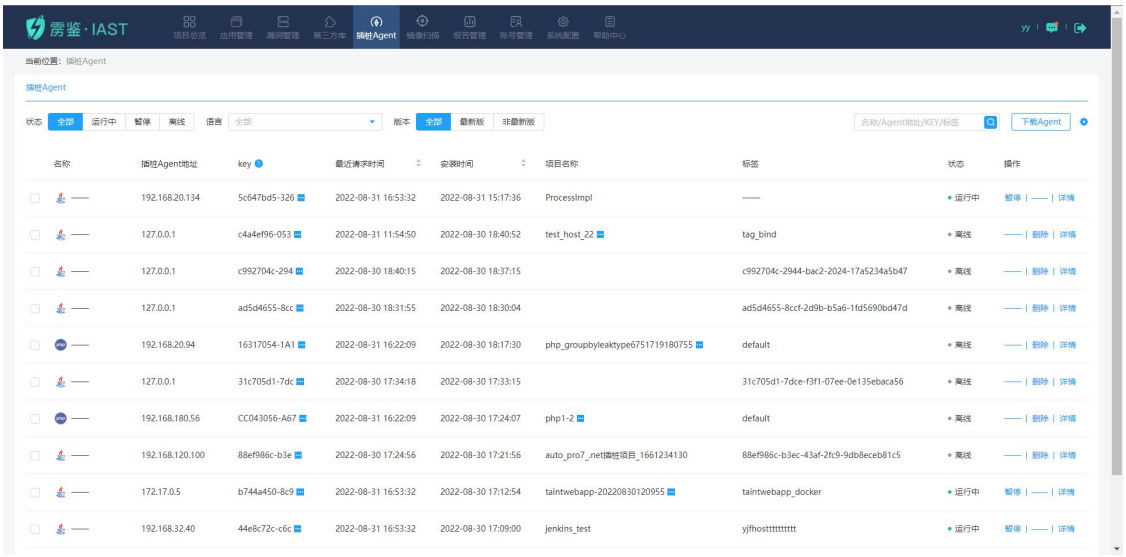
- 导出第三方库报告：点击“导出 EXCEL”，出现弹框后输入报告名称，选择导出内容后点击“确定”，生成的报告可以在报告管理页面下载。

  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。

图表 191 生成项目第三方库报告

1.9 插桩 AGENT（插桩类）



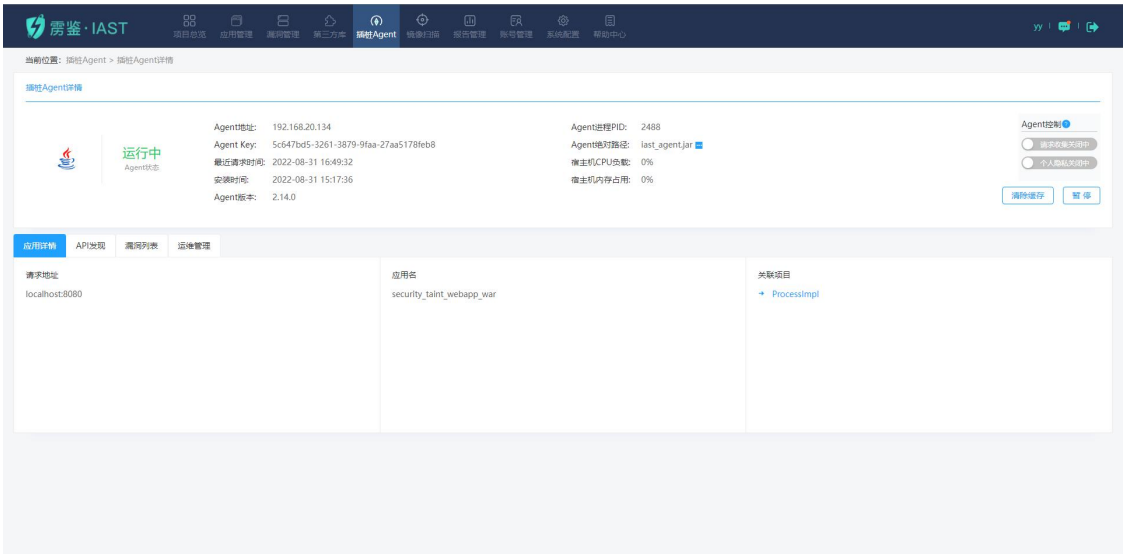
图表 192 插桩 Agent 列表

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。

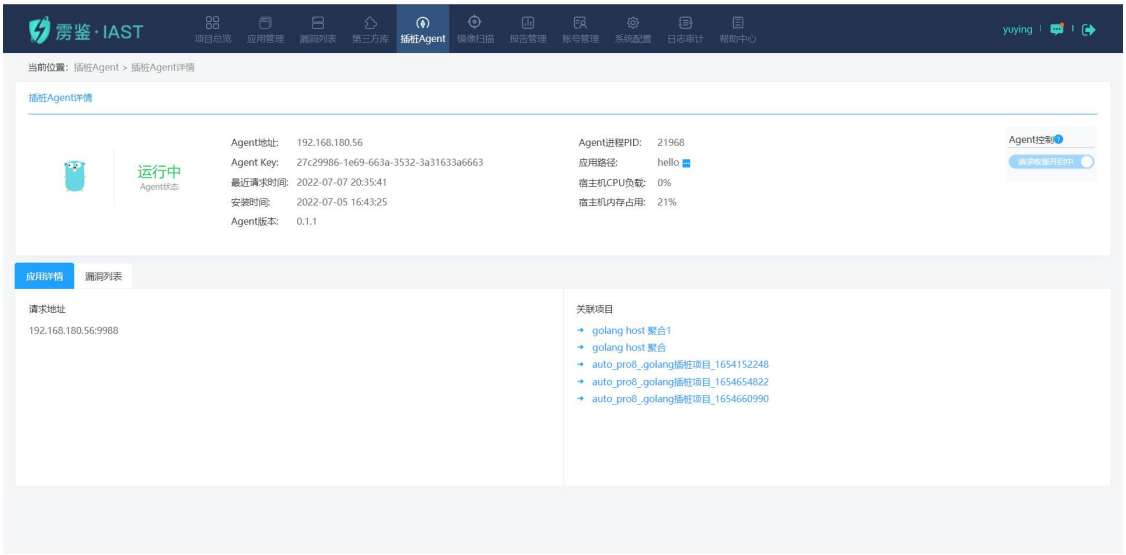
- 名称：Agent 复用时用来区分不同 Agent 之间的名称，自定义名称时需要在启动前加上指定的-Dmoresec 参数。具体参数请参考帮助中心。
- 插桩 Agrnt 语言：每一条 Agent 记录都会在最前端展示语言所属图标
- 插桩 Agent 地址：展示出 Agent 所安装的服务器地址；
- key：用于区分同一台机器上的 Agent，在 iast_agent.jar 中的 config.ini 中可以查看该 Agent 的 key 值；
- 最近请求时间：Agent 最近一条请求上报的时间；
- 安装时间：展示 Agent 安装的时间；
- 项目名称：展示该 Agent 捕获的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；

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

- 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。



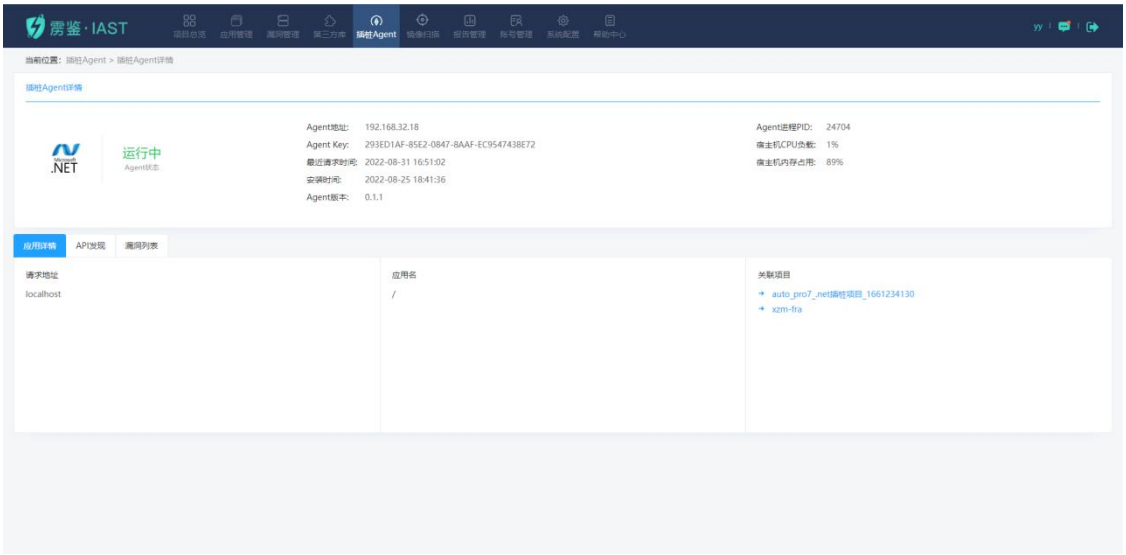
图表 193 Java 语言插桩 AGENT 详情



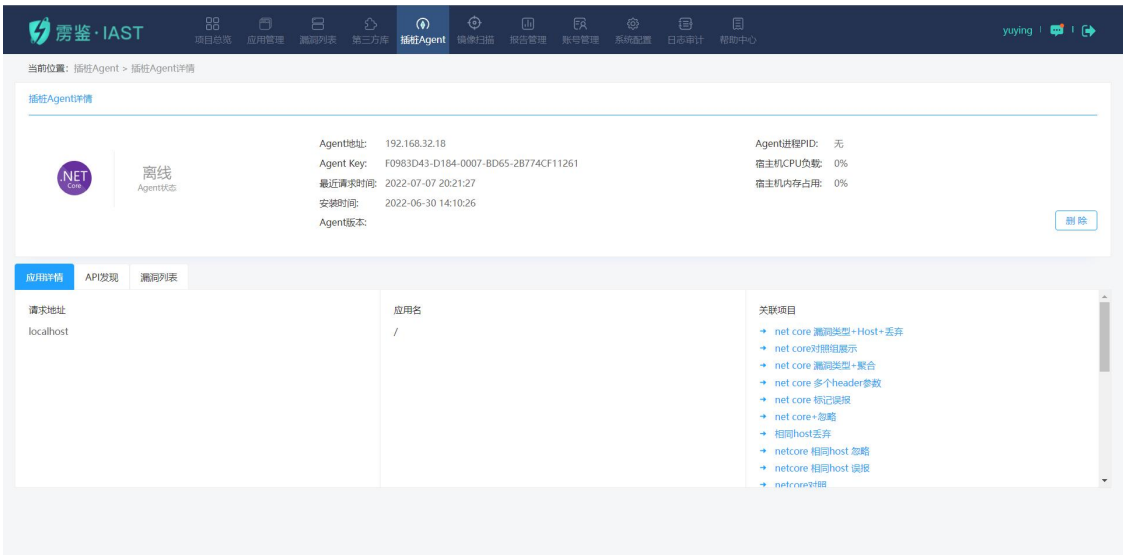
图表 194 Golang 语言插桩 AGENT 详情

杭州默安科技有限公司

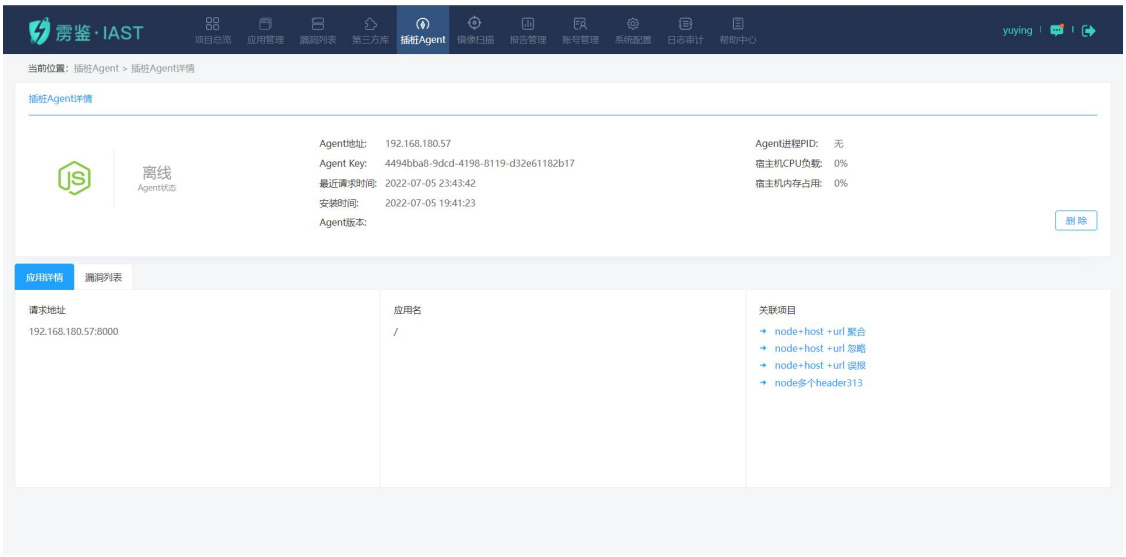
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



图表 195 .NET Framework 语言插桩 AGENT 详情



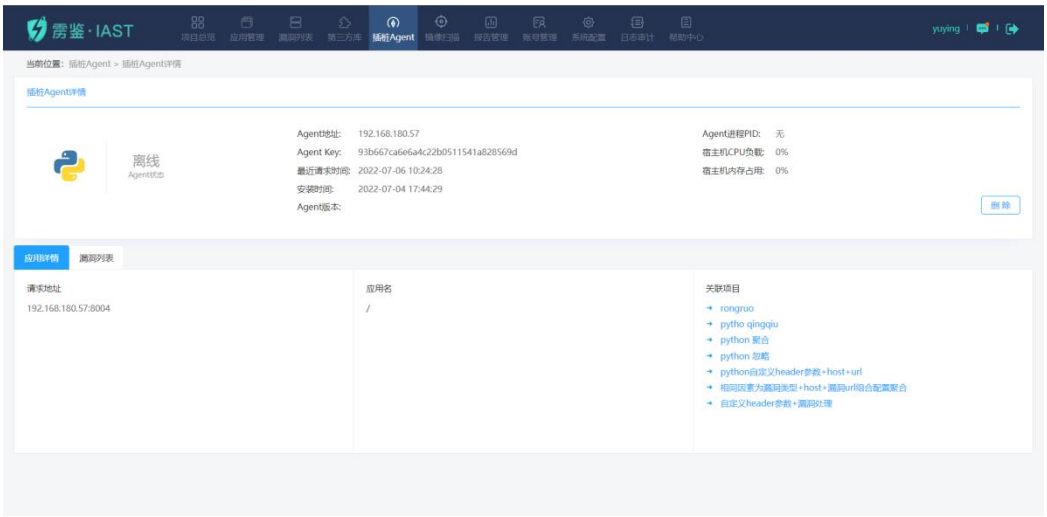
图表 196 .NET Core 语言插桩 AGENT 详情



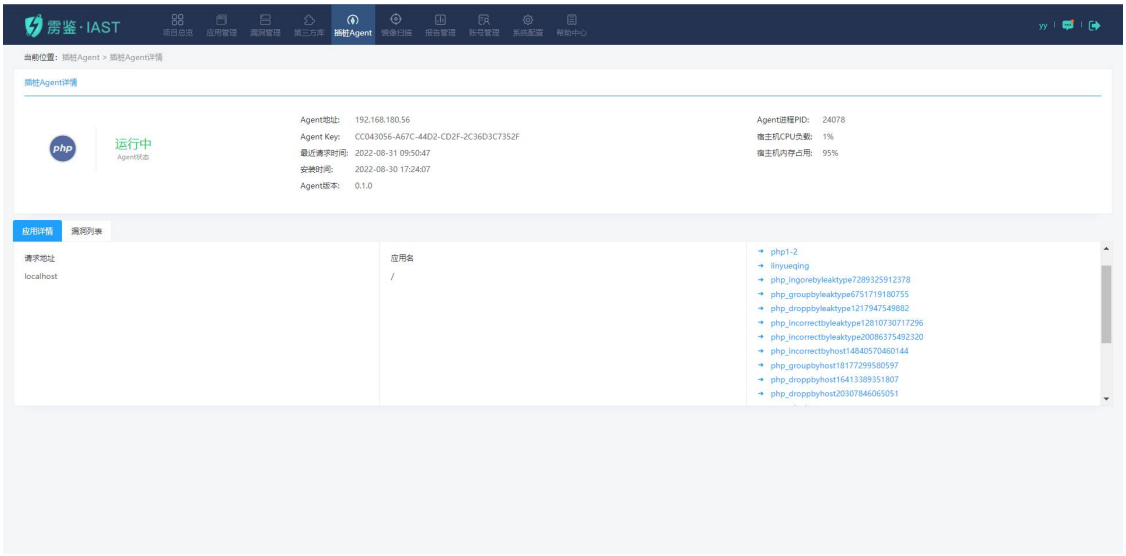
杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

图表 197 Node.js 语言插桩 AGENT 详情



图表 198 Python 语言插桩 Agent 详情



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。

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。

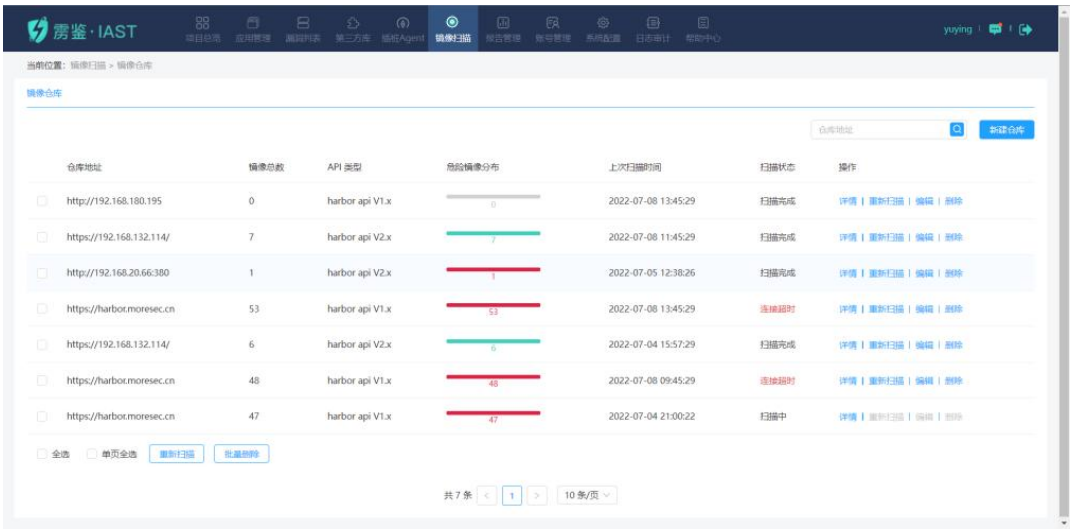
Java 语言的插桩 Agent 详情页面中，还会有 JVM 参数的 tab 页，用来展示 Agent 回传的所在服务器的 JVM 参数。

插桩 AGENT 的安装方式见雳鉴 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。

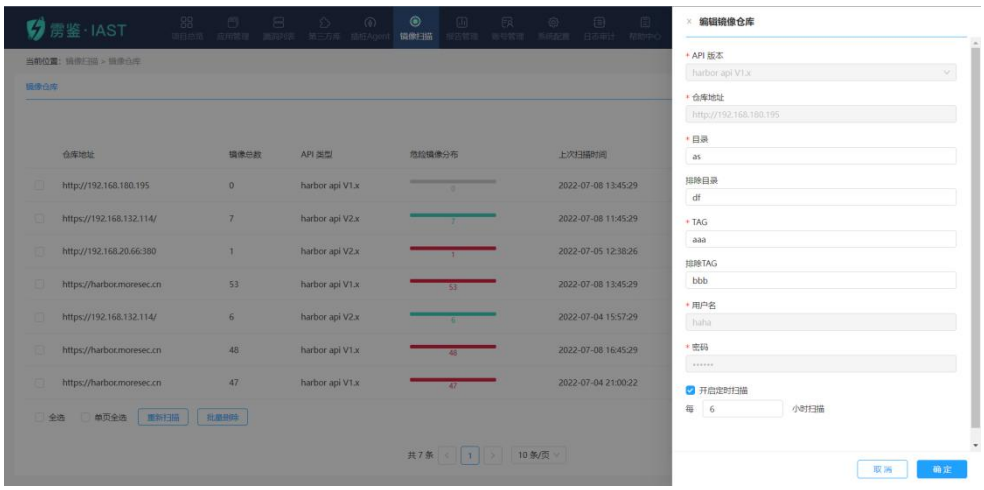


图表 200 镜像仓库

- 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。

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。



图表 202 编辑镜像仓库

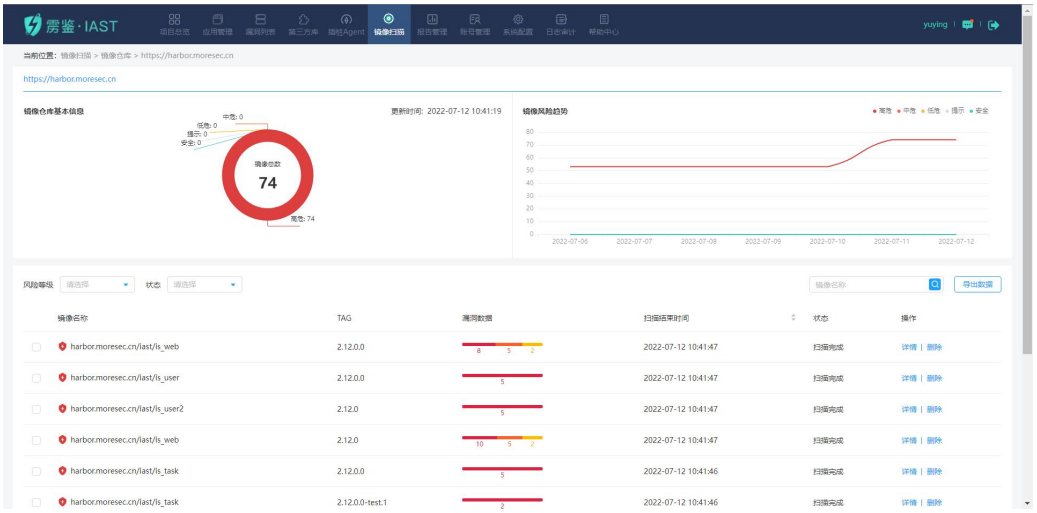
- 点击“删除”，弹出二次确认提示框，点击“确定”后该镜像仓库即被删除，对应漏洞关联删除。

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。

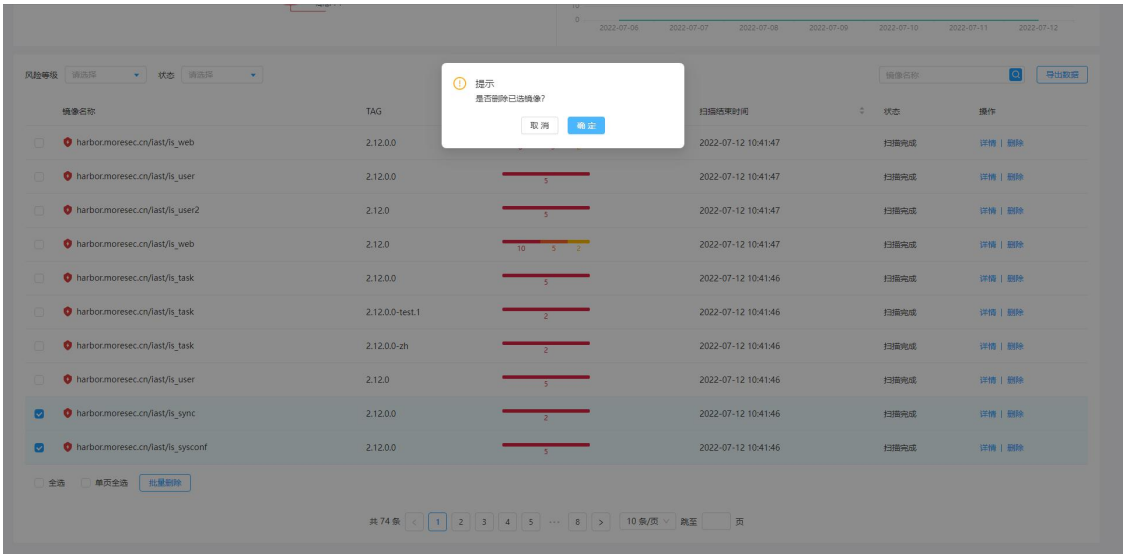
图表 204 新建镜像仓库

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。



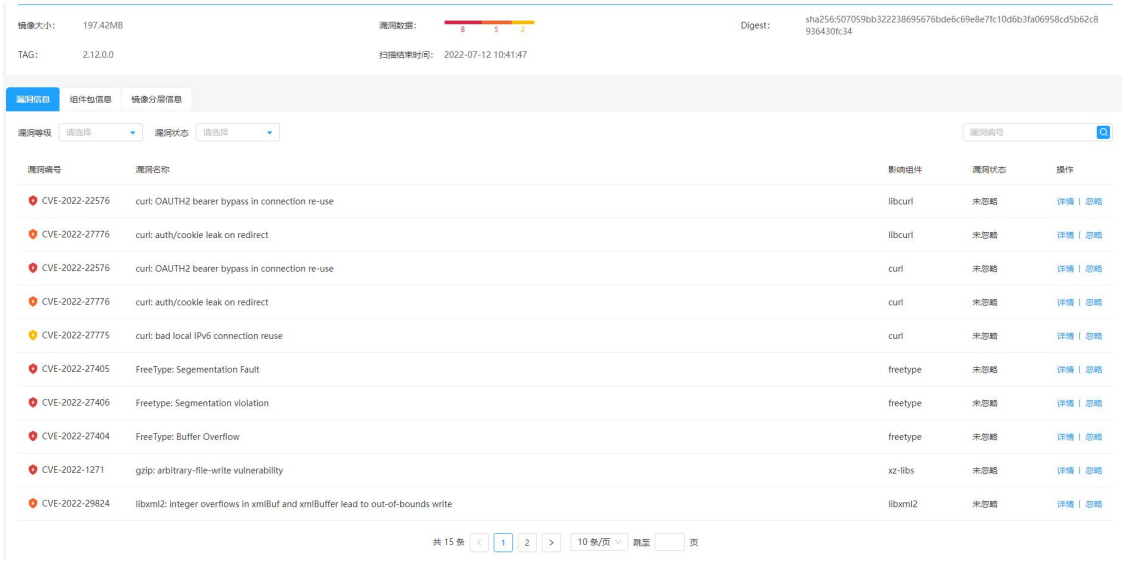
图表 205 镜像仓库详情

- 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；



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。

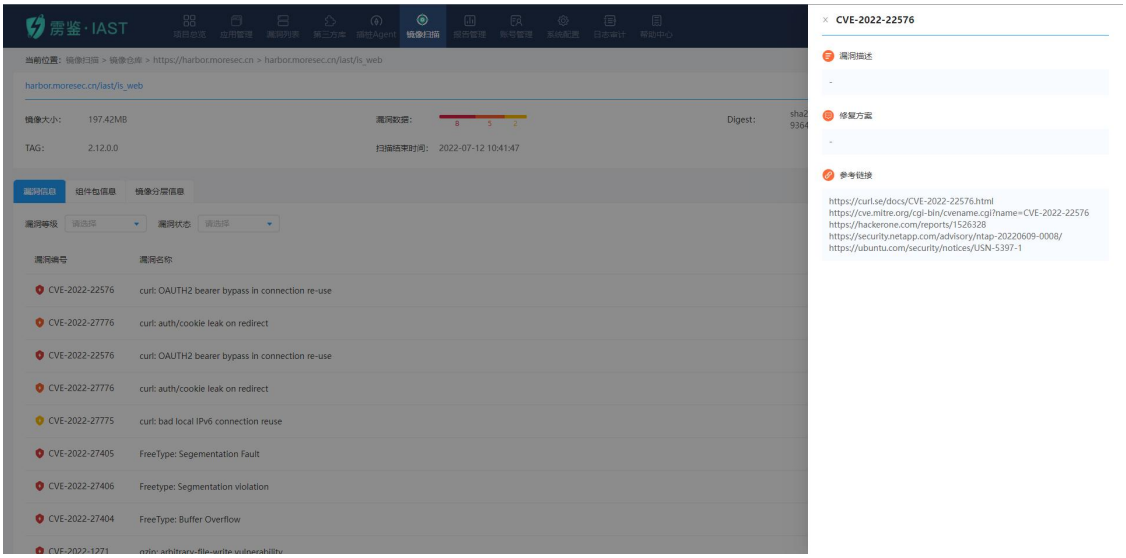


图表 207 镜像详情

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。

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



图表 208 镜像详情-漏洞详情

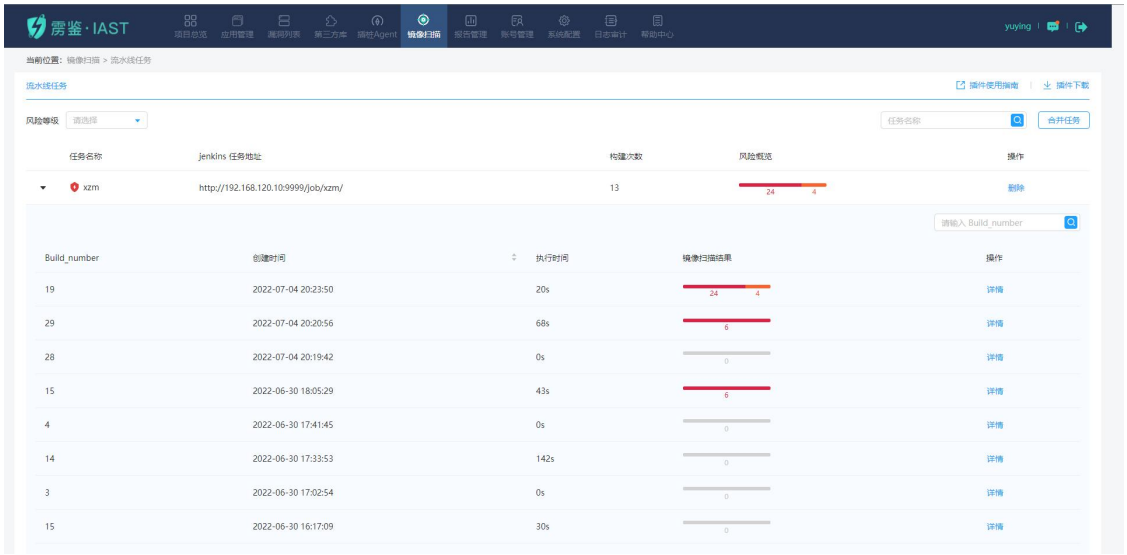
点击“忽略”，出现二次确认的弹框，点击“确定”后，出现“忽略成功”的提示，漏洞置底显示，忽略后的漏洞可点击“恢复”取消忽略。

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。

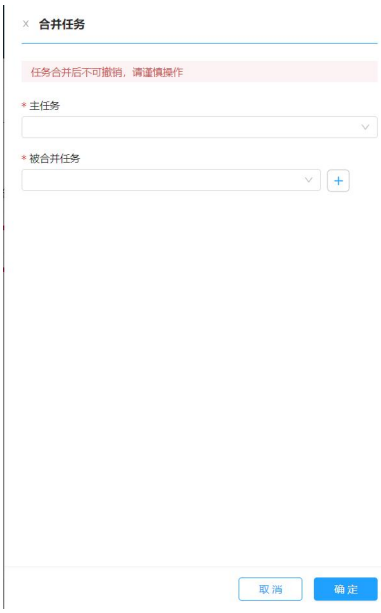
1.10.2 流水线任务

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。



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。

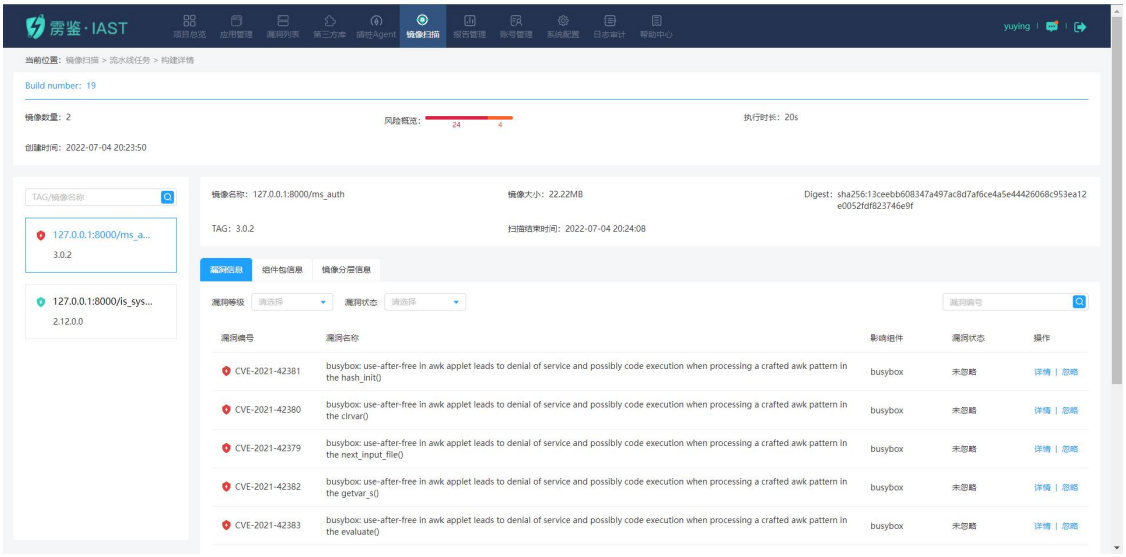


图表 211 流水线任务-合并任务

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。

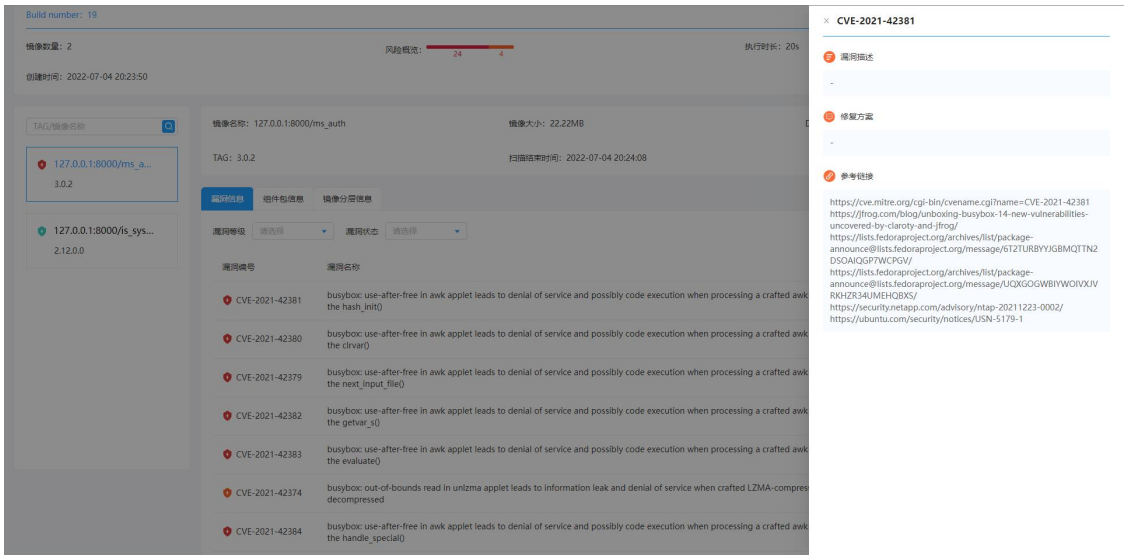
图表 212 流水线任务-删除任务

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。



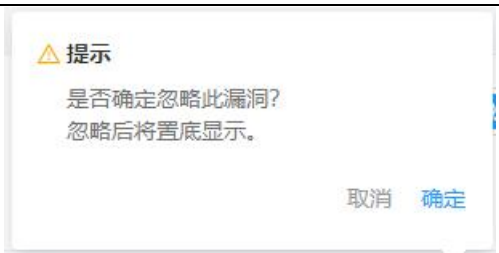
图表 213 流水线任务-构建详情

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。



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

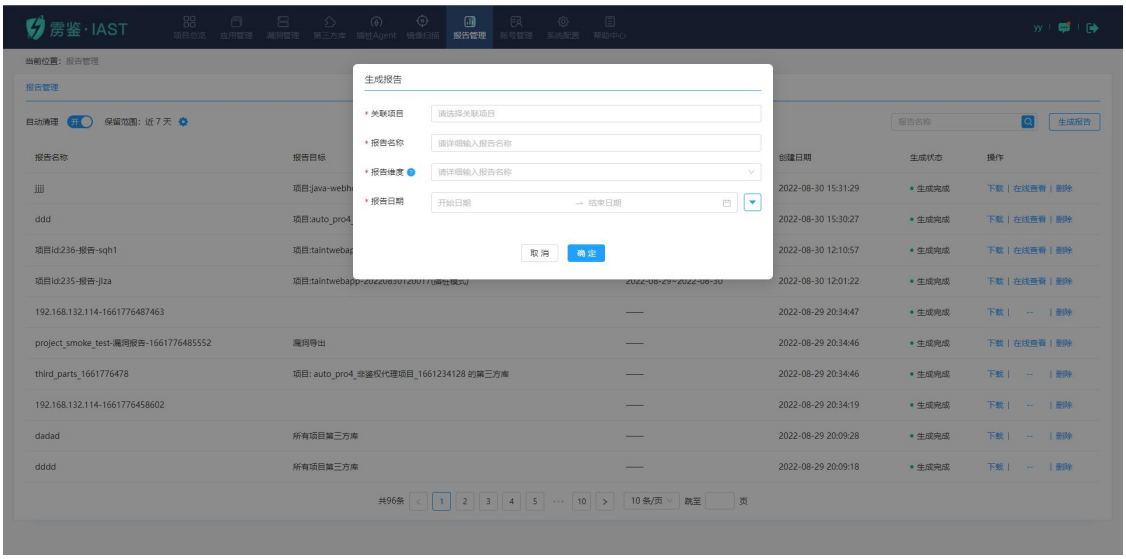
点击可切换 tab 页查看镜像的组件包信息详情和镜像分层信息。

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。

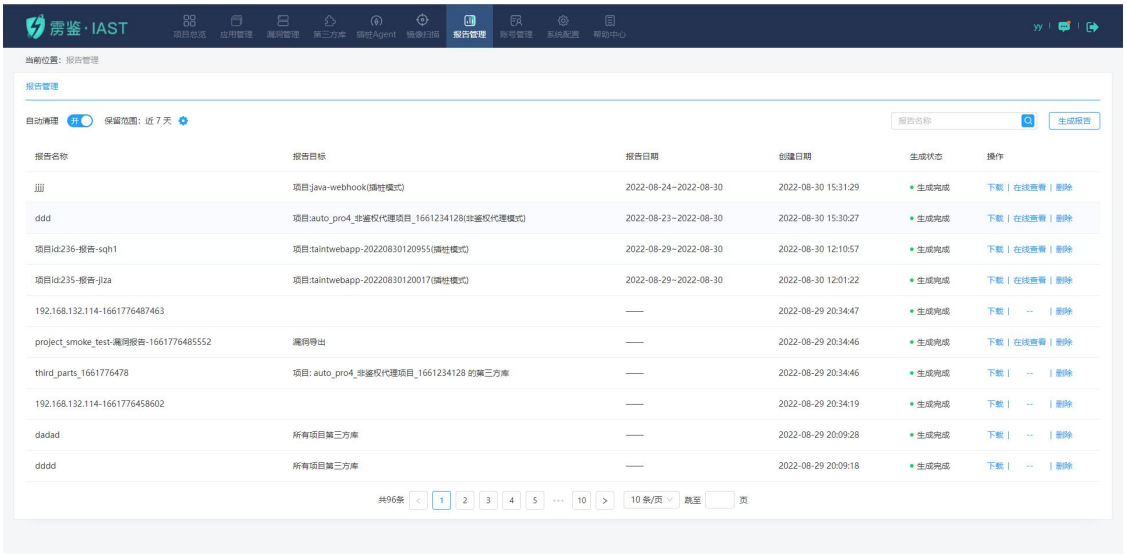


图表 216 选择报告目标

- 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）



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）。

图表 218 报告下载

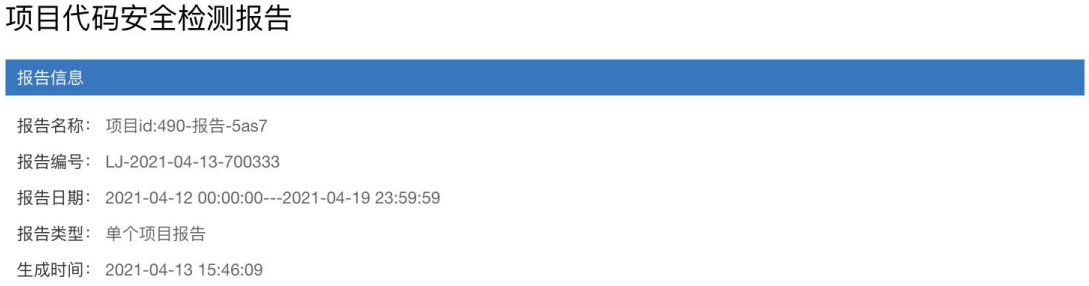
1.11.2 检测报告

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

生成时间： 2021-04-13 15:46:09

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

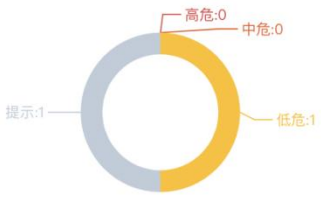
漏洞修复统计

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

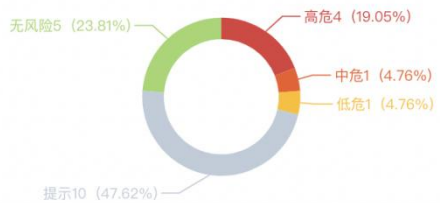
风险类型分布

无漏洞

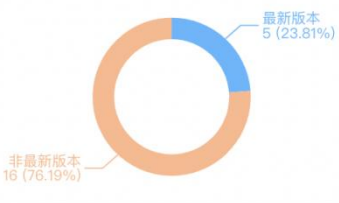
漏洞等级分布



第三方库风险等级分布图



第三方库版本状态分布图



杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

3.漏洞列表

加密秘钥硬编码（漏洞数：1）　　漏洞等级：低危

序号	漏洞地址	发现时间	修复状态
1	192.168.201.100:30002/benchmark/crypto-00/BenchmarkTest00019	2021-04-13 15:46:09	未修复

不安全的加密（漏洞数：1）　　漏洞等级：提示

序号	漏洞地址	发现时间	修复状态
1	192.168.201.100:30002/benchmark/crypto-00/BenchmarkTest00019	2021-04-13 15:46:08	未修复

4.漏洞详情

加密秘钥硬编码（漏洞数：1）　　漏洞等级：低危

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。
同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。

漏洞危害

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。

修复建议

不将密钥硬编码于程序中。

1　风险地址：192.168.201.100:30002/benchmark/crypto-00/BenchmarkTest00019

攻击详情

开发者将密钥硬编码于文件DESKeySpec.java(类:javax.crypto.spec.DESKeySpec)中，
private byte[] key= [hidden];

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: */*
```

不安全的加密（漏洞数：1）　　漏洞等级：提示

漏洞描述

该漏洞产生的原因是使用了不安全的加密算法，导致产生的加密数据可被破解。

漏洞危害

由不安全的加密算法生成的加密数据可被破解，可能会导致严重的漏洞（如对密码等进行破解）。

杭州默安科技有限公司

Tel：（+86）400-0571-211　　Email：market_moresec.cn　　Web：www.moresec.cn

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：192.168.201.100:30002/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.第三方库列表及详情

org.apache.tomcat.tomcat-juli（漏洞数：0） 安全等级：提示

当前版本号： 8.5.34
最新版本号： 10.0.0-M3
开源许可证： Apache 2.0
关联项目： ["dubbo_test1","is_filter","chenlu_test2","benchmark-d","chenlu_test_active1","benchmark_active","benchmark_active2","chenlu_test1","chenlu_test5","chenlu_test3","chenlu_test_2.9_1","chenlu1618300048"]

org.apache.tomcat.tomcat-jasper-el（漏洞数：0） 安全等级：提示

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
关联项目： ["dubbo_test1","is_filter","chenlu_test2","benchmark-d","chenlu_test_active1","benchmark_active","benchmark_active2","chenlu_test1","chenlu_test5","chenlu_test3","chenlu_29_taint","benchmark-1618300048"]

com.sun.jersey.jersey-servlet（漏洞数：0） 安全等级：无风险

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","benchmark-d","Bbenchmark","peload","reload","bench_mark","benchmark_tag","benchmark_tag12","bench_markoff","java_baihe","benchmark-1618300048"]

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。
提示	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

第三方库等级	危害说明
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。
提示	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

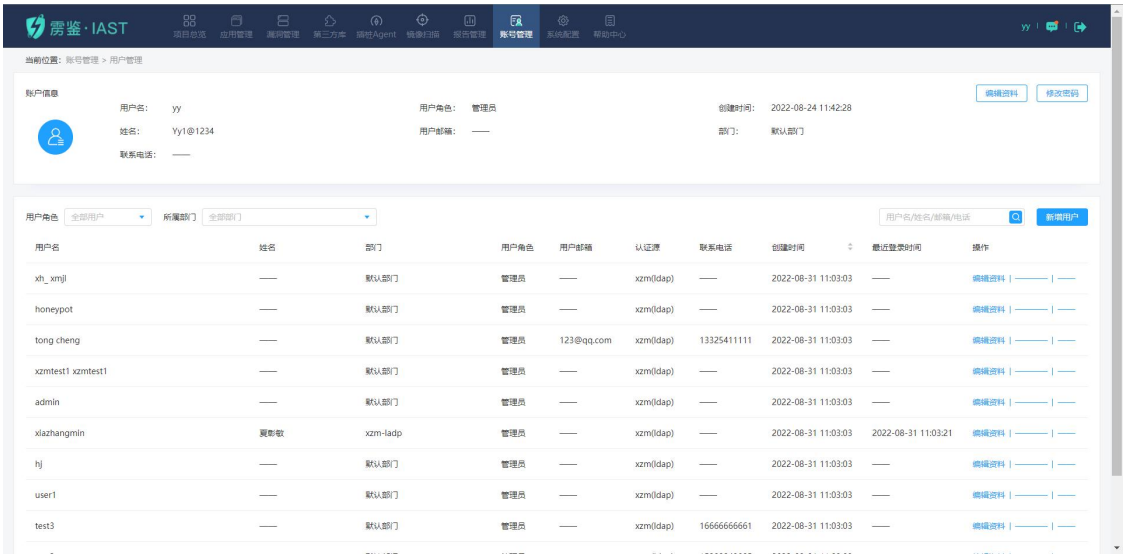
图表 219 检测报告

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。



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。

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

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。

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。

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。

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

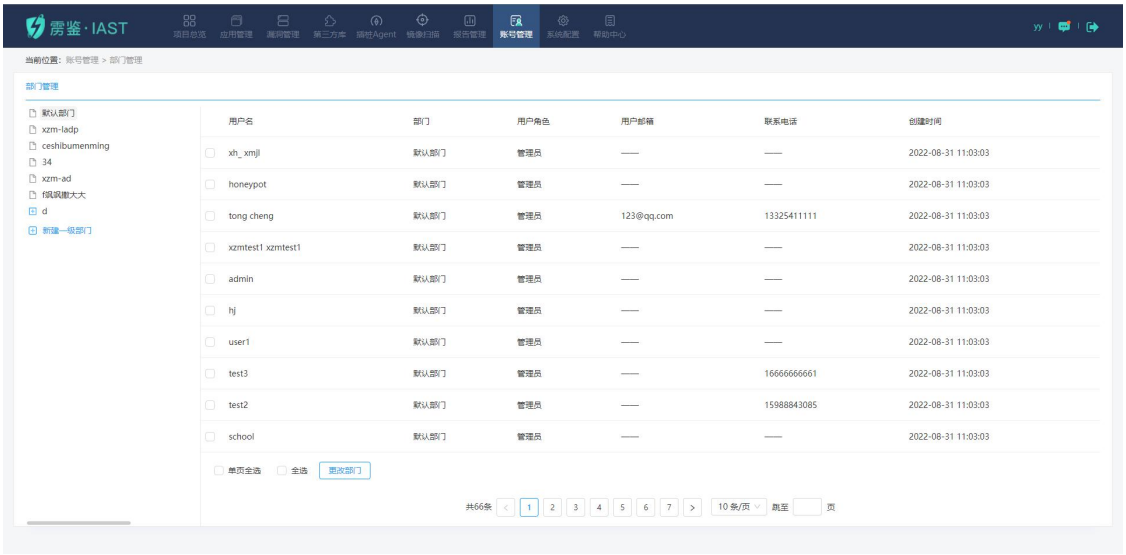
图表 225 修改密码

- 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。

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。



图表 227 部门管理

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。

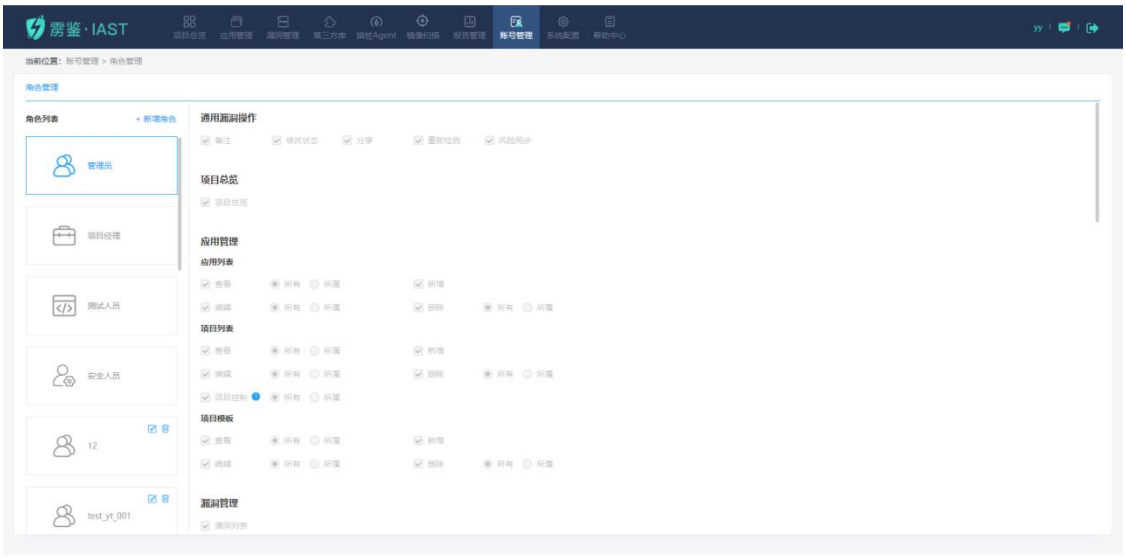
图表 229 部门管理-编辑部门

1.12.3 角色管理

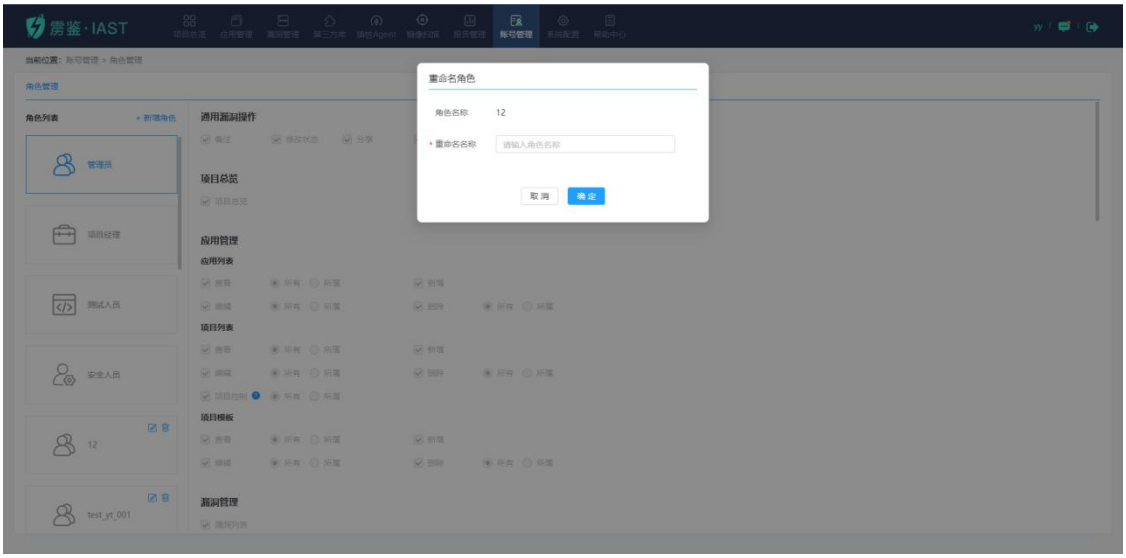
管理员可以在角色管理中查看管理员的权限，可配置测试人员、安全人员及项目经理的

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。



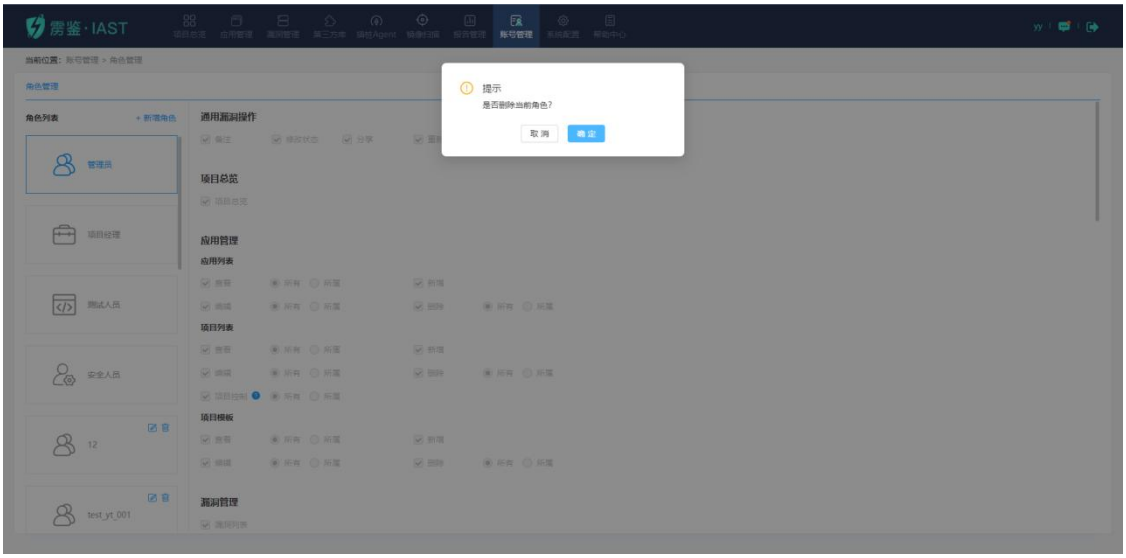
图表 230 角色管理



图表 231 角色管理-重命名

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



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。

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）。

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。

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。

图表 236 认证源

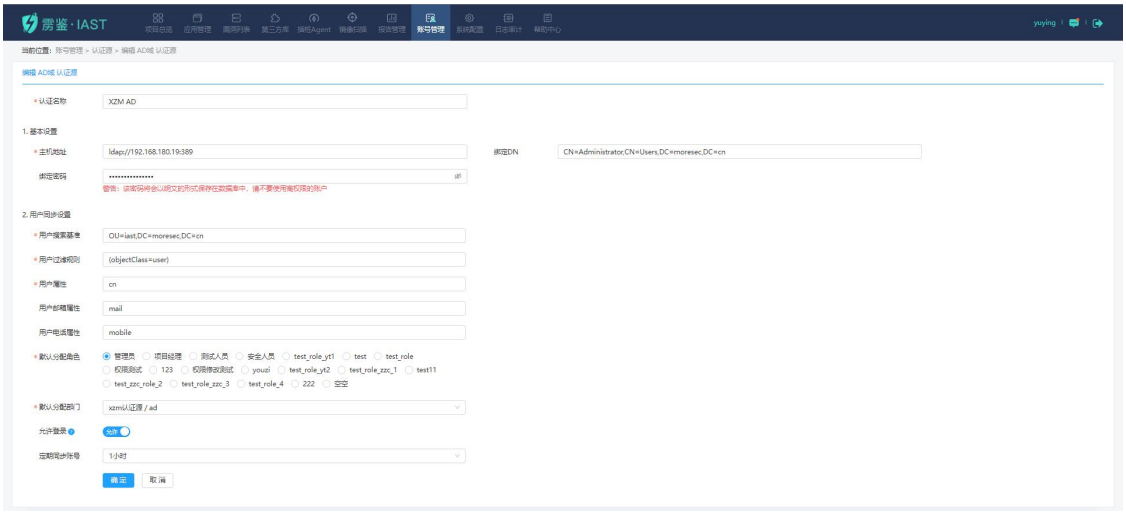
1.12.5.1 认证源管理

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。

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。

➢ 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。



图表 238 编辑认证源

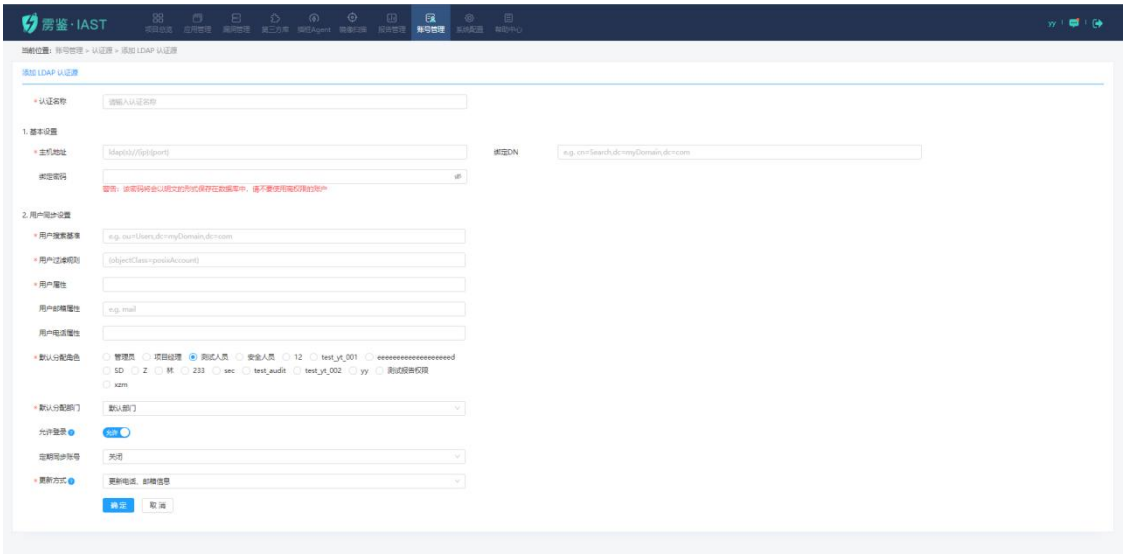
➢ 点击“删除”按钮，需要在弹窗中填写当前账号的密码，校验后才能删除认证源。

图表 239 删除认证源

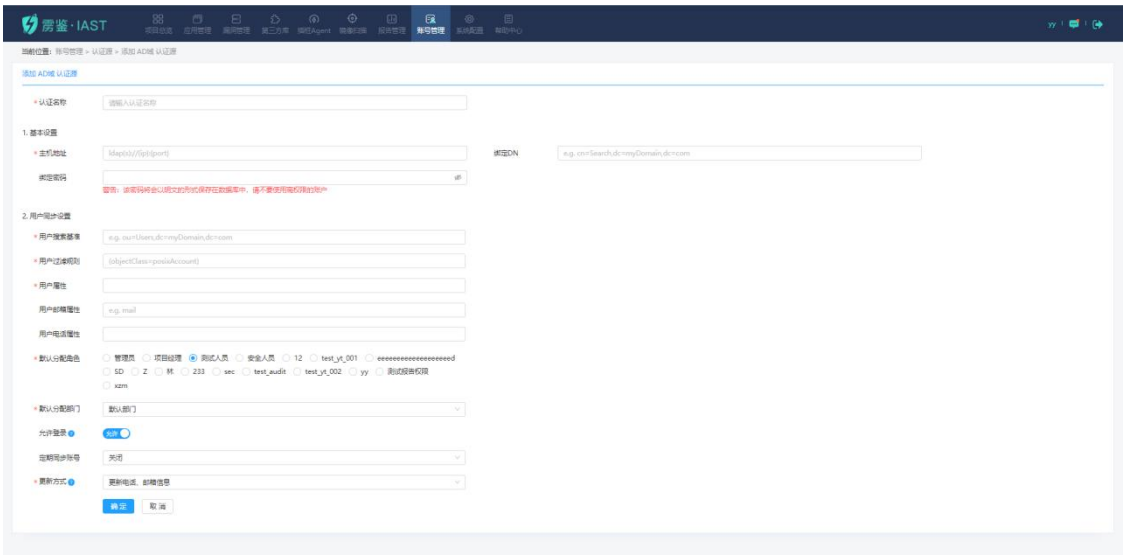
1.12.5.2 添加认证源

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。

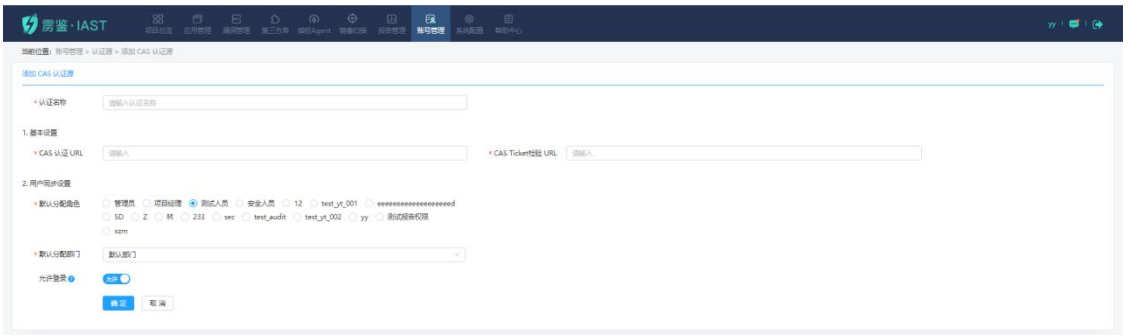
图表 240 添加认证源



图表 241 添加认证源-LDAP



图表 242 添加认证源-AD 域



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

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

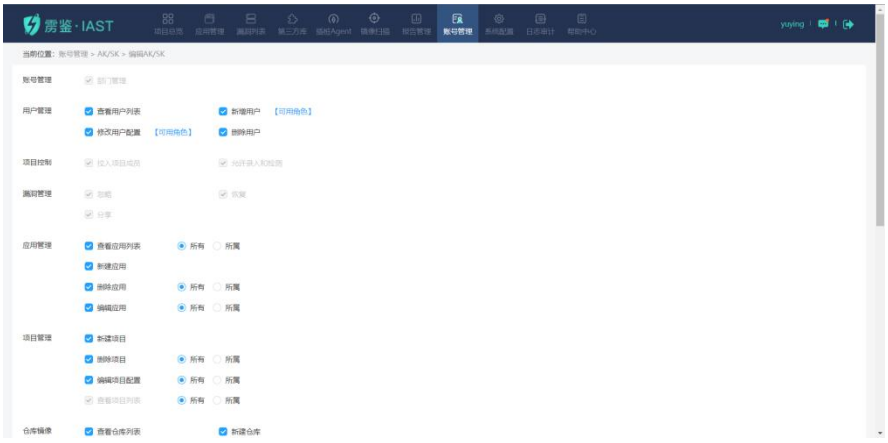
行状态的筛选和批量删除。

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。

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：

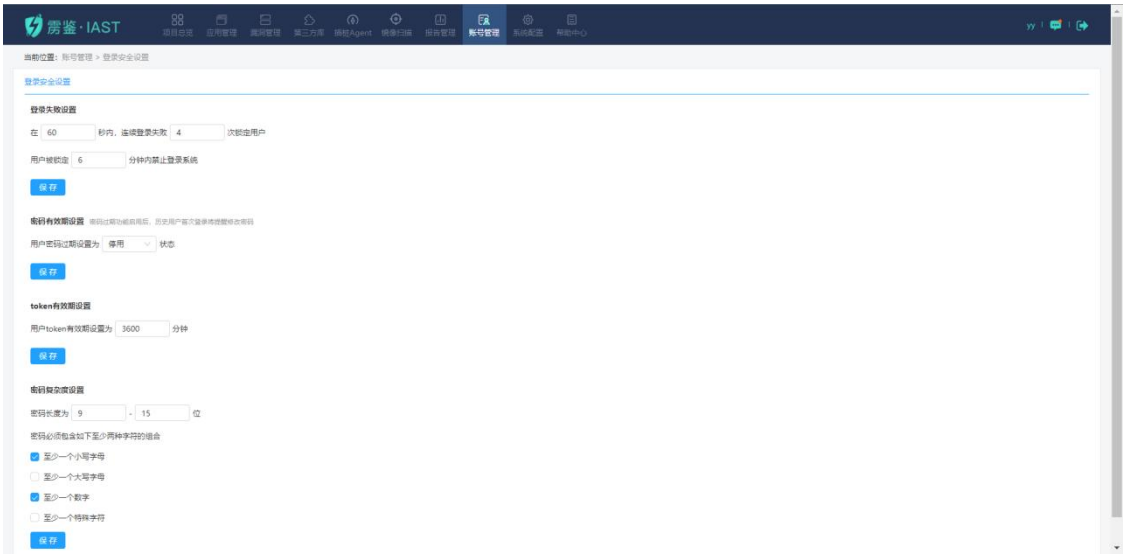


图表 246 AK/SK 编辑页面

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。



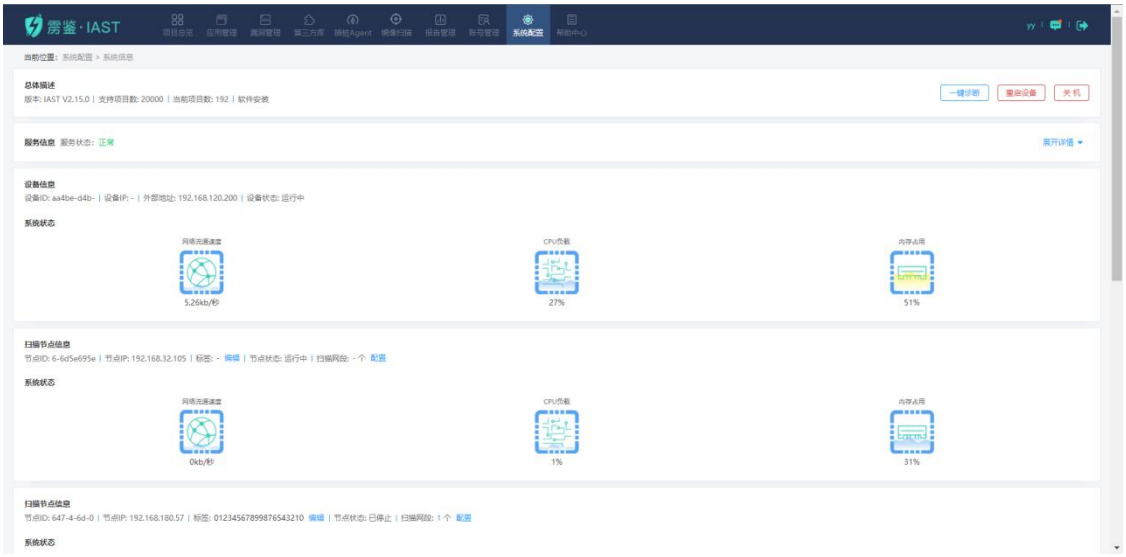
图表 247 登录安全设置

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。

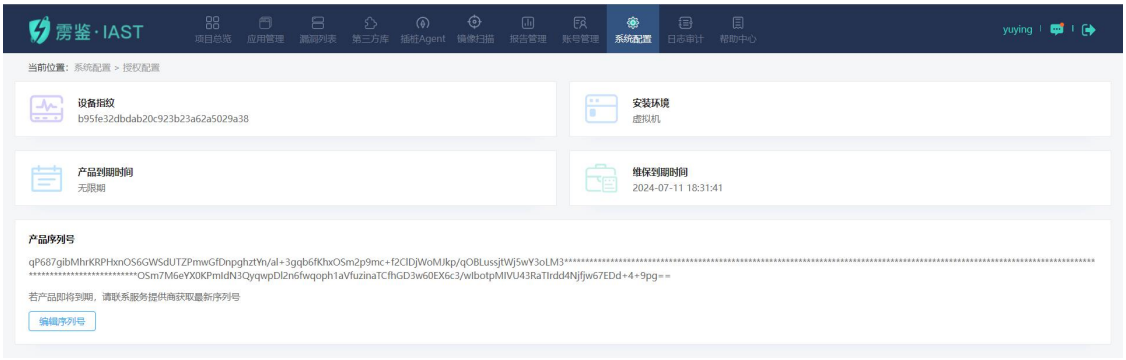
- 总体描述：版本、支持项目数、当前项目数；
- 服务信息：展示设备上服务状态是否正常以及所有服务的名称、状态、运行时间。
- 设备信息：设备 ID、设备 IP、标签、设备状态、扫描网段；
- 系统状态：网络流通速度、CPU 负载、内存占用；
- 系统日志：打包日志，下载系统日志；
- 系统重置：只保留管理员账号并清空所有数据信息；



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。



图表 249 授权配置

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。

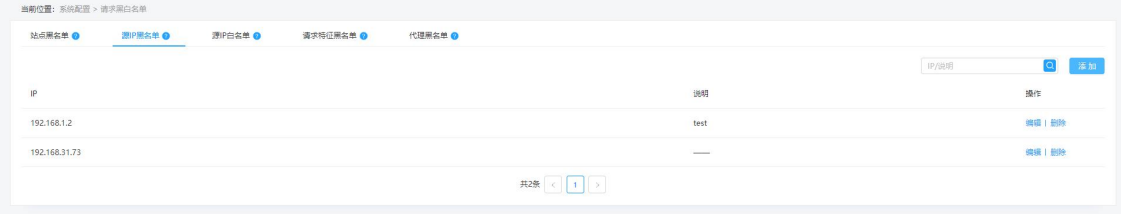
1) 站点黑名单是用户根据实际情况，将不需要扫描的站点加入黑名单，设置后的站点流量不进行录入与扫描。在列表显示包含 host、是否包含子域名、path、匹配方式、说明、操作（编辑和删除），可根据 host 或 path 进行搜索。

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。

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。



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。

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

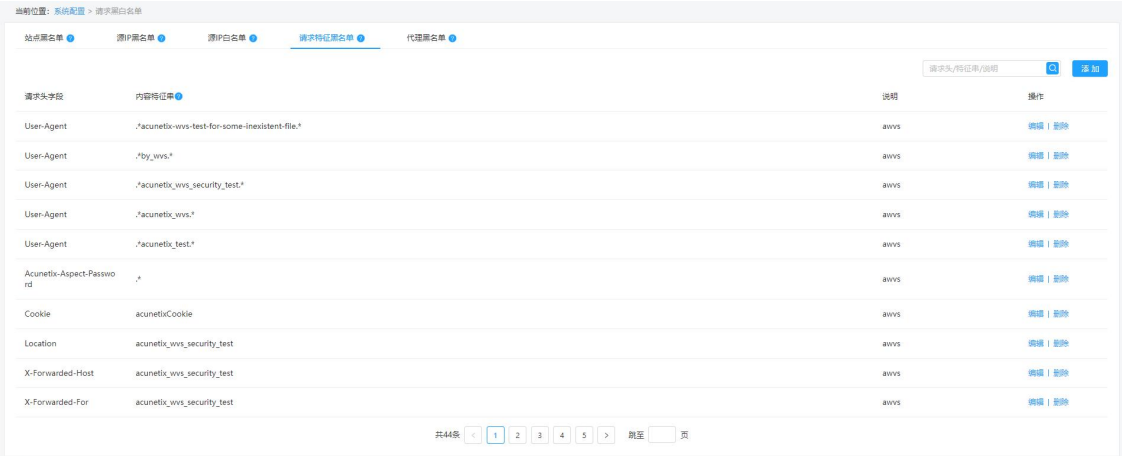
图表 254 源 IP 白名单

- 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

4) 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。



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。

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。

图表 258 代理黑名单

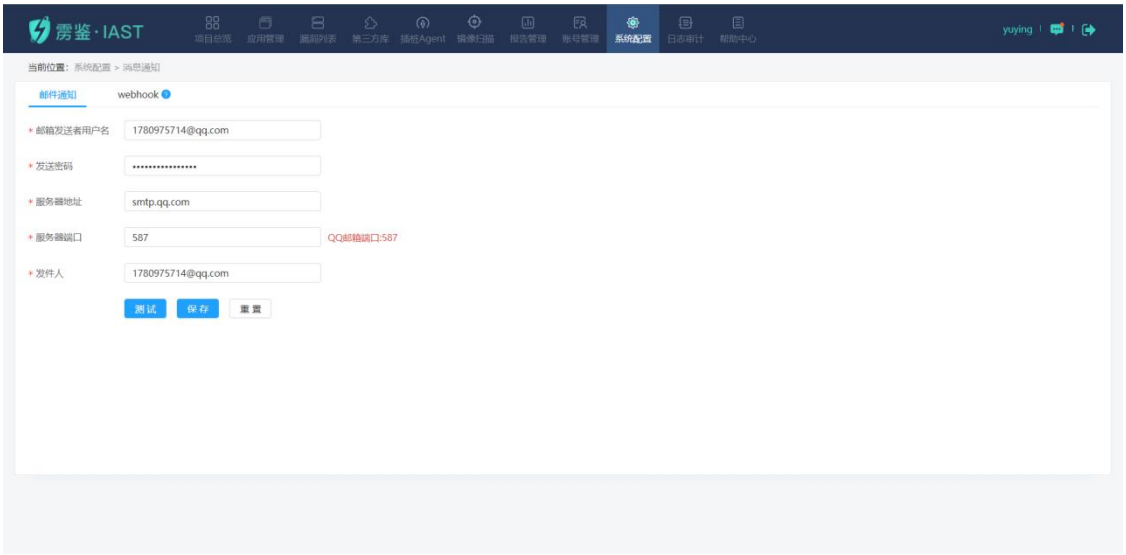
- 点击“添加”，可添加代理黑名单，输入 IP 及对应端口确认填写准确之后点击“确定”

即可完成添加，新增代理黑名单会更新至列表中。

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



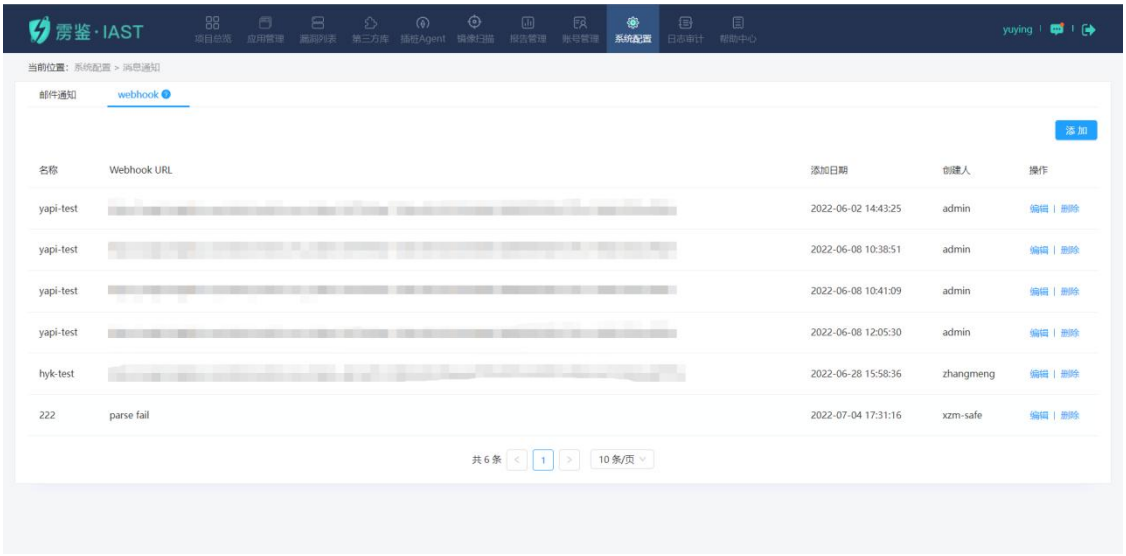
图表 260 邮件通知设置

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

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 url、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。



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。

图表 262 消息通知-添加 webhook

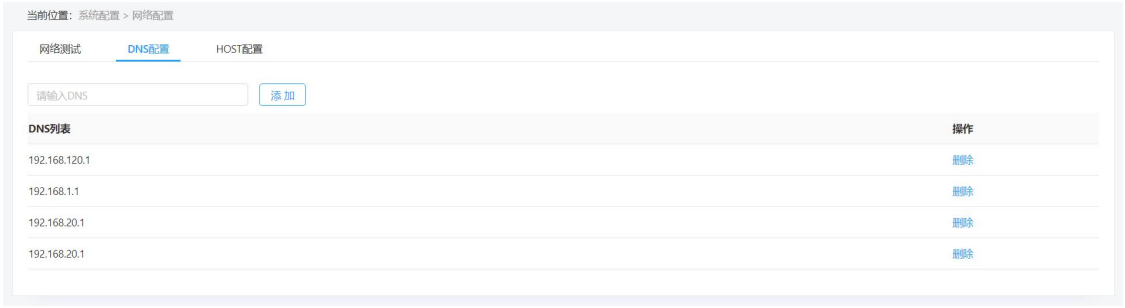
1.13.5 网络配置

➢ 网络测试：输入地址测试，并进行结果输出

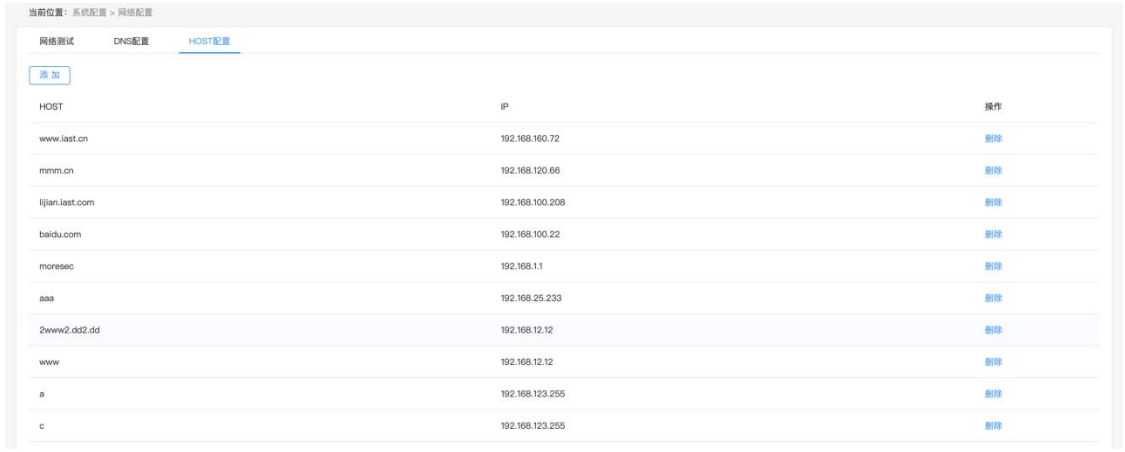
图表 263 网络配置-网络测试

➢ 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

和 Host 同时配置时，优先使用 Host 配置。



图表 264 网络配置-DNS 配置



图表 265 网络配置-HOST 配置

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

图表 267 系统升级

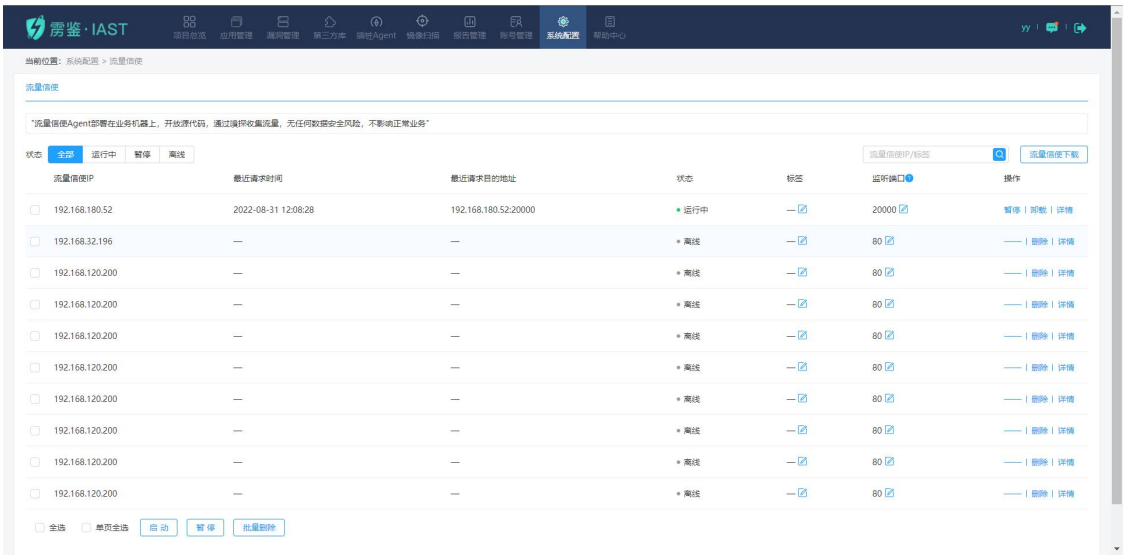
如果当前产品超过了序列号中定义的维保到期时间，升级功能将无法使用。请联系公司售后服务人员。

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。

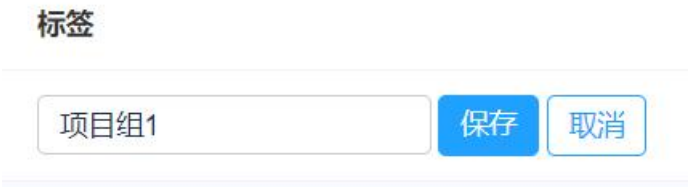
在【系统配置】--【流量信使】中，页面可查看流量信使 agent 的 IP 信息，最近收集到请求的时间，最近请求的 Host 以及流量信使 agent 的状态，设置监听端口，还可对其添加标签及进行操作。



图表 269 流量信使查看页面

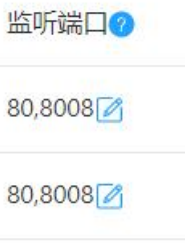
- 可根据流量信使状态进行查看，根据流量信使 IP 或标签进行搜索，列表默认按最近请求时间倒序排列。
- 鼠标点击列表上对应流量信使标签栏的修改按钮，点击修改后保存，标签即修改成功。

图表 270 流量信使-标签



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）。



图表 272 流量信使-监听端口

图表 273 流量信使-修改监听端口

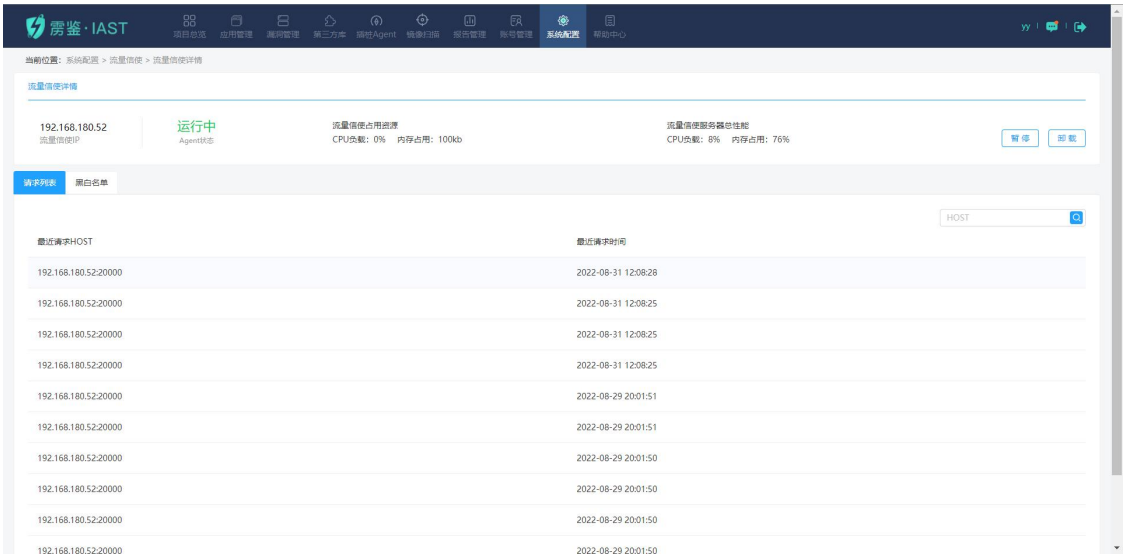
- 点击“暂停”或“批量暂停”，运行中的项目进入已暂停状态。
- 点击“启动”或“批量启动”，暂停状态的 Agent 进入运行模式。

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。

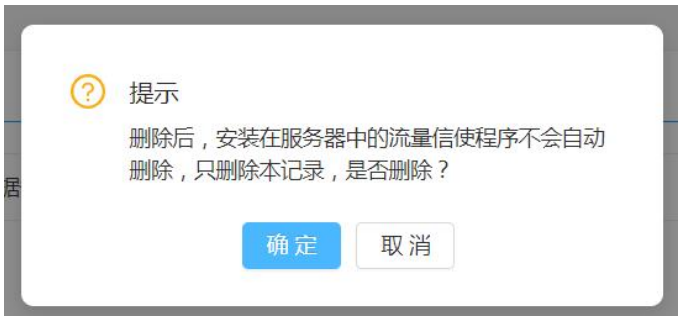
图表 275 流量信使-卸载

- 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）



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。



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）

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

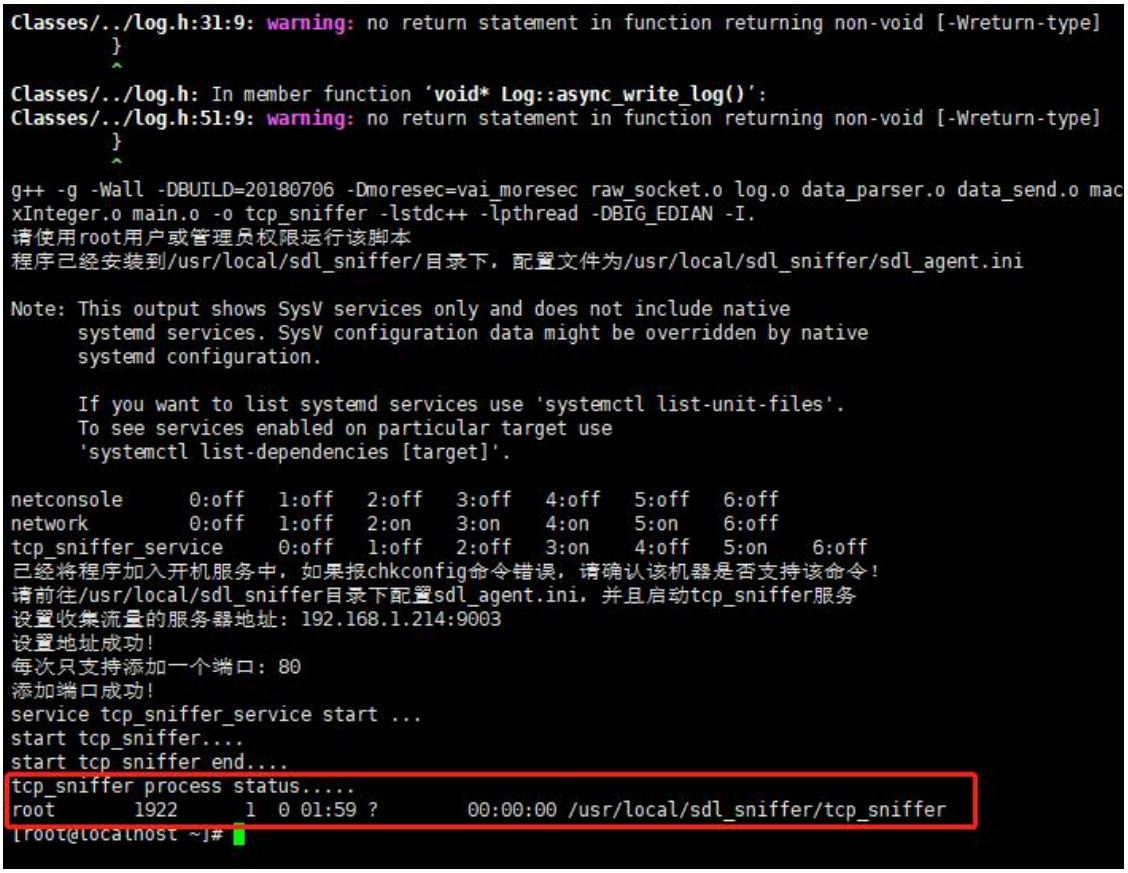
该操作会修改本目录下的 sdl_agent.ini 配置文件，修改后需要 service tcp_sniffer_service restart。

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。

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



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。

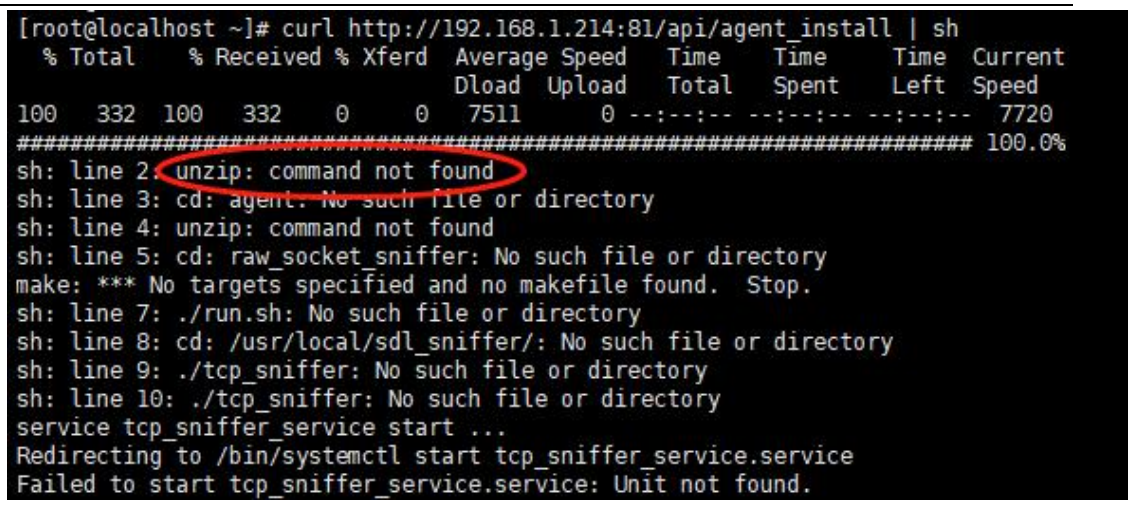
在雳鉴上对被测业务创建一个“简单模式”的项目，在任意 PC 上成功请求被测网站即可录入请求。

1.13.7.3.2 常见错误及解决方法

常见错误 1：

杭州默安科技有限公司

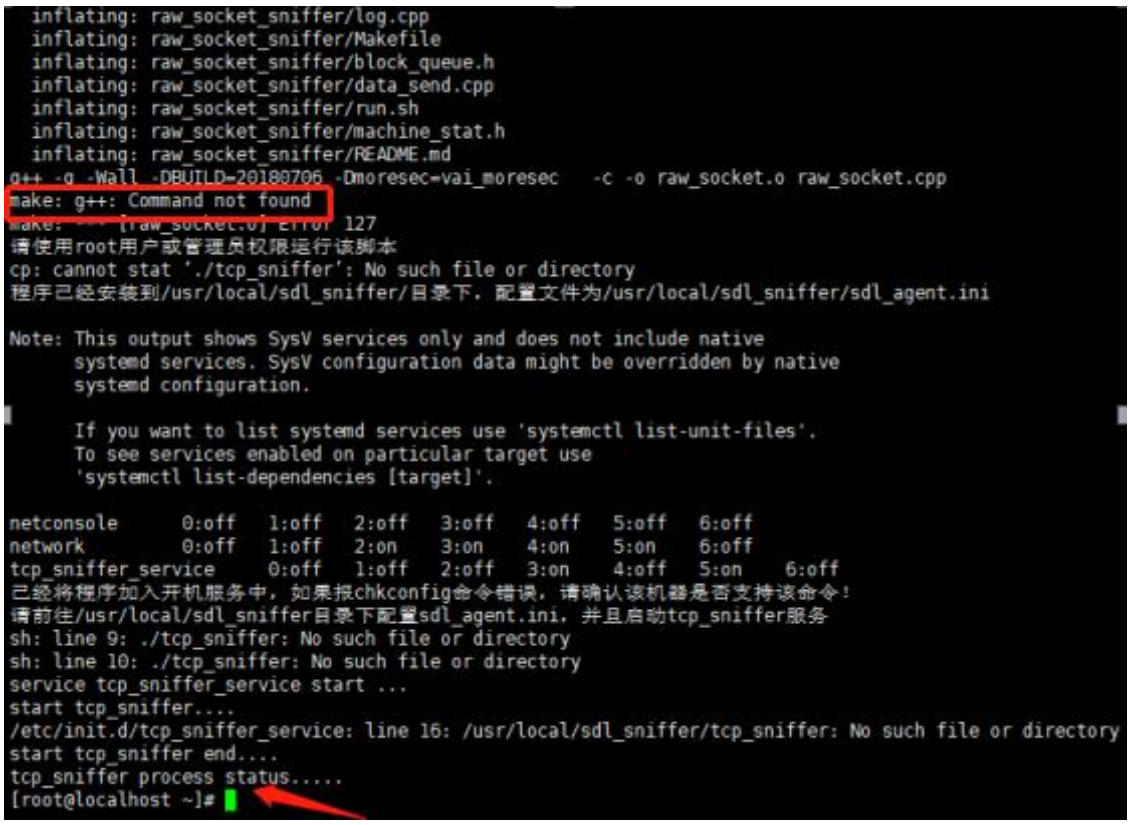
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



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：

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

```
[root@localhost ~]# yum search "gcc-c++"
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.163.com
 * extras: mirrors.cn99.com
 * updates: mirrors.cn99.com
================================================================================ N/S matched: gcc-c++
gcc-c++.x86_64 : C++ support for GCC

  Name and summary matches only, use "search all" for everything.
[root@localhost ~]#
```

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。

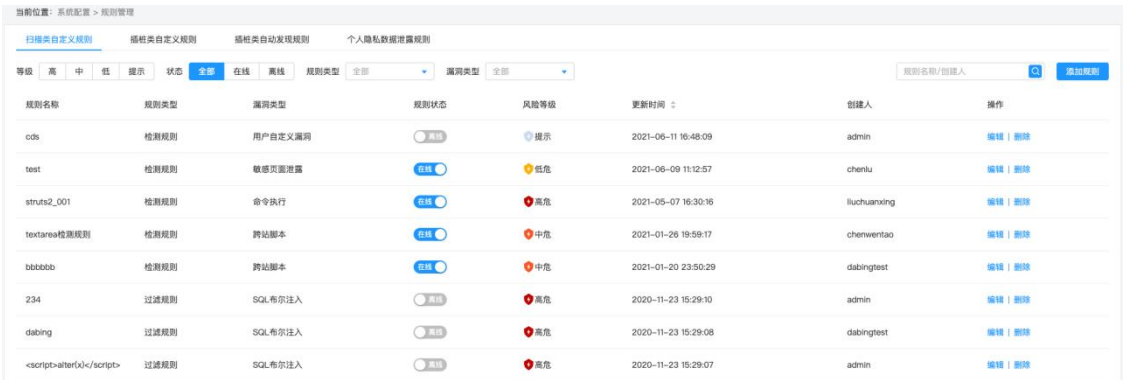
```
[root@localhost ~]# yum install gcc-c++.x86_64
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.163.com
 * extras: mirrors.cn99.com
 * updates: mirrors.cn99.com
Resolving Dependencies
--> Running transaction check
---> Package gcc-c++.x86_64 0:4.8.5-28.el7_5.1 will be installed
--> Processing Dependency: libstdc++-devel = 4.8.5-28.el7_5.1 for package: gcc-c++-4.8.5-28.el7_5.1.x86_64
--> Processing Dependency: libstdc++ = 4.8.5-28.el7_5.1 for package: gcc-c++-4.8.5-28.el7_5.1.x86_64
--> Processing Dependency: gcc = 4.8.5-28.el7_5.1 for package: gcc-c++-4.8.5-28.el7_5.1.x86_64
--> Processing Dependency: libmpfr.so.4()(64bit) for package: gcc-c++-4.8.5-28.el7_5.1.x86_64
--> Processing Dependency: libmpc.so.3()(64bit) for package: gcc-c++-4.8.5-28.el7_5.1.x86_64
--> Running transaction check
---> Package gcc.x86_64 0:4.8.5-28.el7_5.1 will be installed
--> Processing Dependency: libgomp = 4.8.5-28.el7_5.1 for package: gcc-4.8.5-28.el7_5.1.x86_64
--> Processing Dependency: cpp = 4.8.5-28.el7_5.1 for package: gcc-4.8.5-28.el7_5.1.x86_64
--> Processing Dependency: libgcc >= 4.8.5-28.el7_5.1 for package: gcc-4.8.5-28.el7_5.1.x86_64
--> Processing Dependency: glibc-devel >= 2.2.90-12 for package: gcc-4.8.5-28.el7_5.1.x86_64
---> Package libmpc.x86_64 0:1.0.1-3.el7 will be installed
---> Package libstdc++.x86_64 0:4.8.5-28.el7 will be updated
---> Package libstdc++.x86_64 0:4.8.5-28.el7_5.1 will be an update
---> Package libstdc++-devel.x86_64 0:4.8.5-28.el7_5.1 will be installed
---> Package mpfr.x86_64 0:3.1.1-4.el7 will be installed
--> Running transaction check
---> Package cpp.x86_64 0:4.8.5-28.el7_5.1 will be installed
---> Package glibc-devel.x86_64 0:2.17-222.el7 will be installed
```

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。



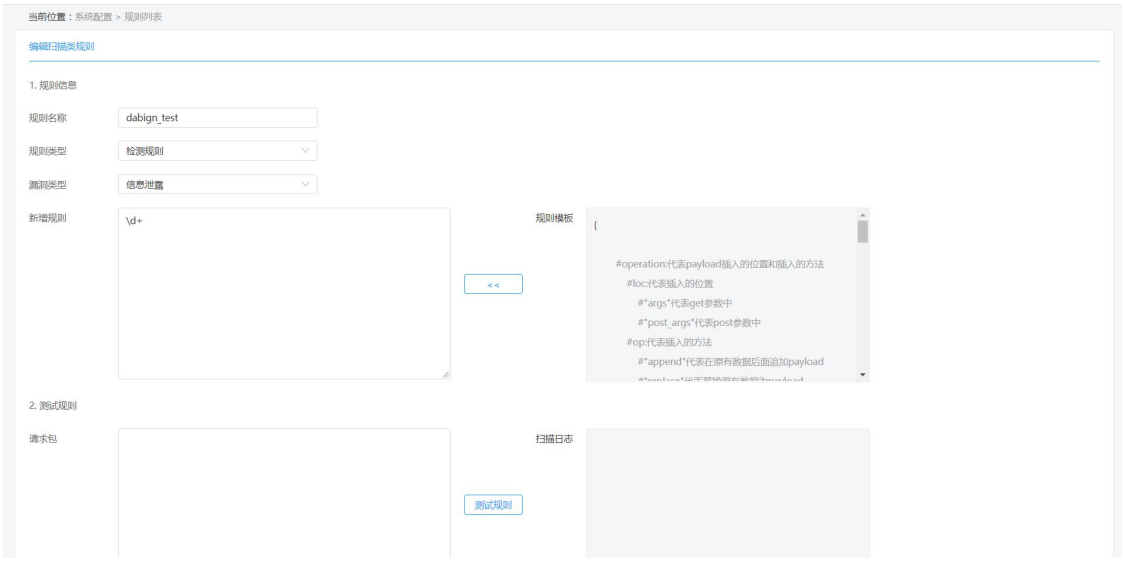
杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

图表 284 规则列表

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）。



图表 285 添加规则

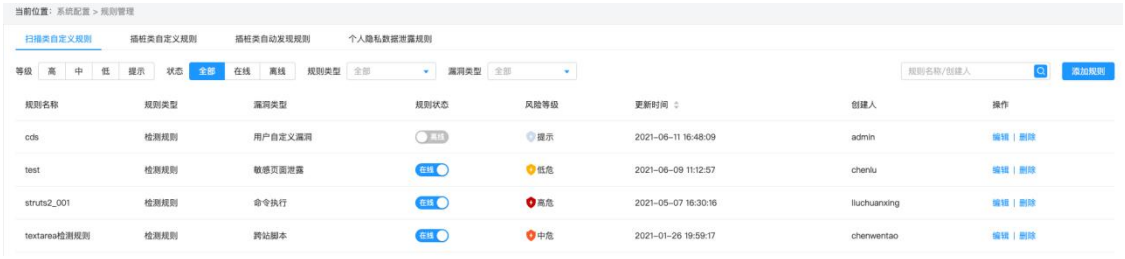
- 规则信息：规则名称、规则类型、漏洞类型、新增规则和规则模板四部分组成。
  1） 规则类型：分为检测规则和过滤规则两种。
  2） 漏洞类型：检测规则分为跨站脚本、SQL 延时注入、文件包含及命令执行等十九种，过滤规则分为信息泄露和 SQL 布尔注入两种。
  3） 新增规则：检测规则对照右侧规则模板向其中填入新增规则，过滤规则按照需求填写规则。
  4） 规则模板：给出左侧相对应新增规则类型的模板及对应注释，点击新增规则和规则模板中间箭头按钮，新增规则模块中会出现相应模板。请对照右侧规则模板中注释进行修改（过滤规则不展示规则模板）。
- 测试规则：请求包和扫描日志两部分组成。
  向请求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

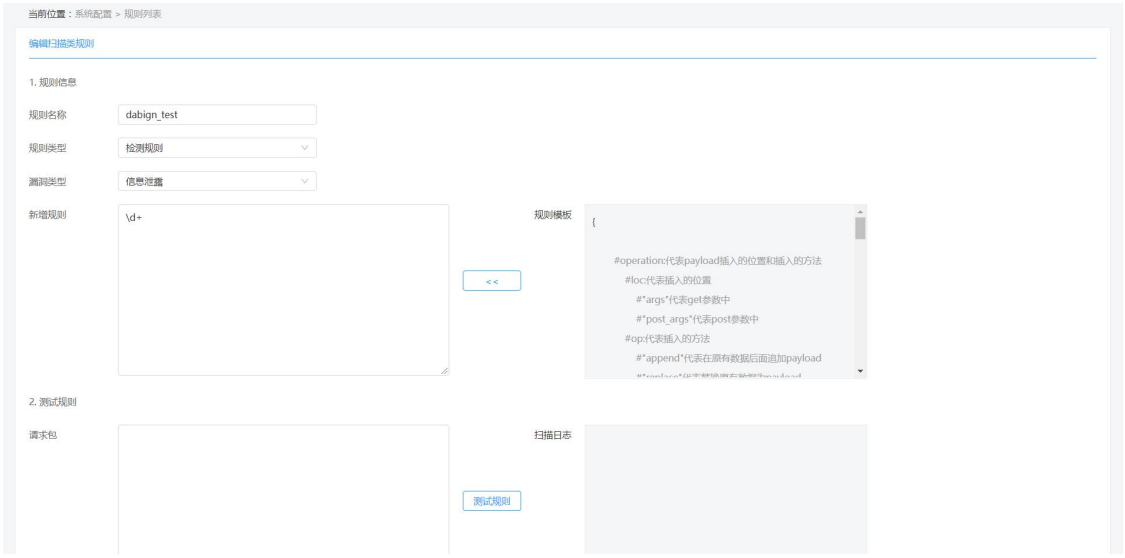
规则列表默认按更新时间倒序排列（最新添加的规则展示在前面），列表内容包括规则名称、规则类型、漏洞类型、规则状态、风险等级、更新时间、创建人及操作。

➢ 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。



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。



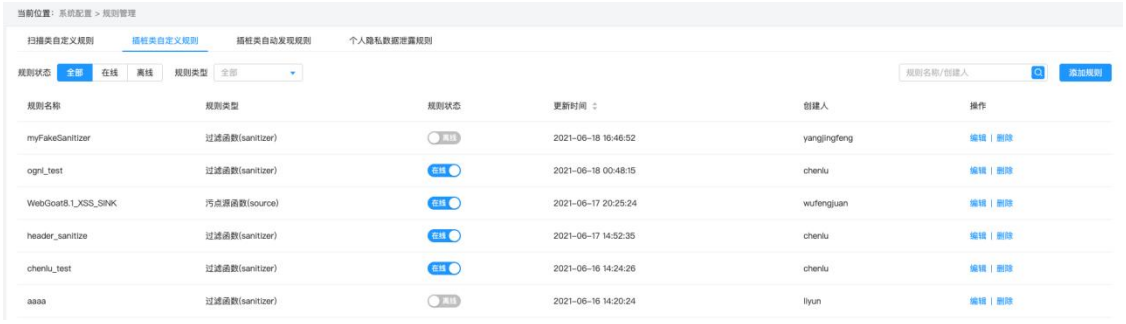
图表 288 编辑规则

● 点击删除，在弹框中进行二次确认后该规则被删除。

图表 289 删除规则

1.13.8.2 规则列表-插桩类

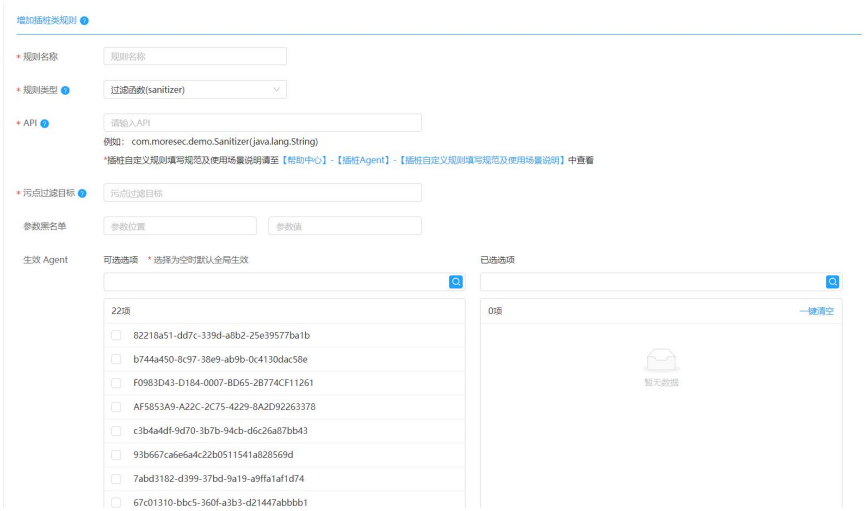
用户可以在规则列表中自定义设置适用的过滤或验证函数至插桩规则中以减少误报。满足在不重启应用和 agent 状态下生效新的过滤函数,且插桩类规则列表中的规则对全局生效。



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。



杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

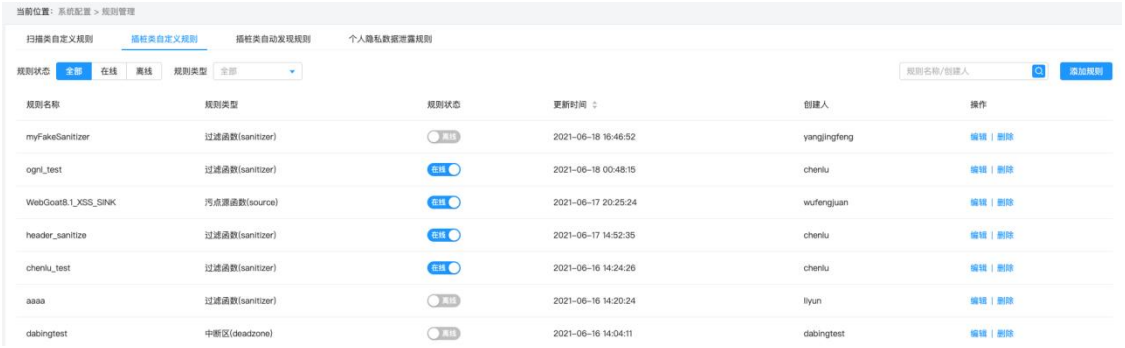
图表 291 添加插桩类规则

- 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

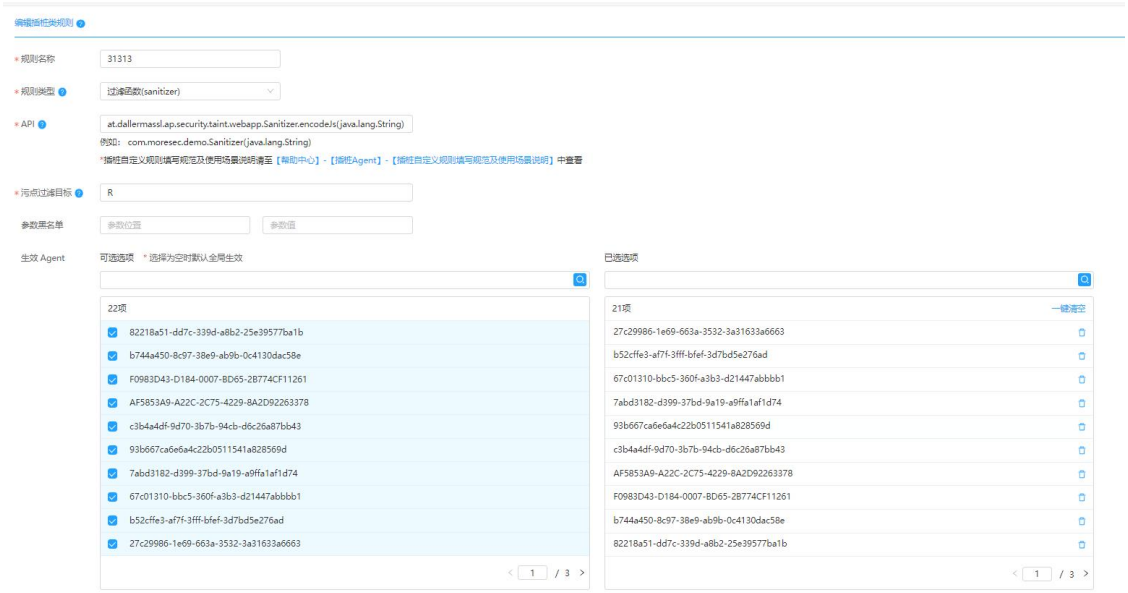
规则列表默认按更新时间倒序排列（最新更新的规则展示在前面），列表内容包括规则名称、规则类型、规则状态、关联项目、更新时间、创建人及操作。

- 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。



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。



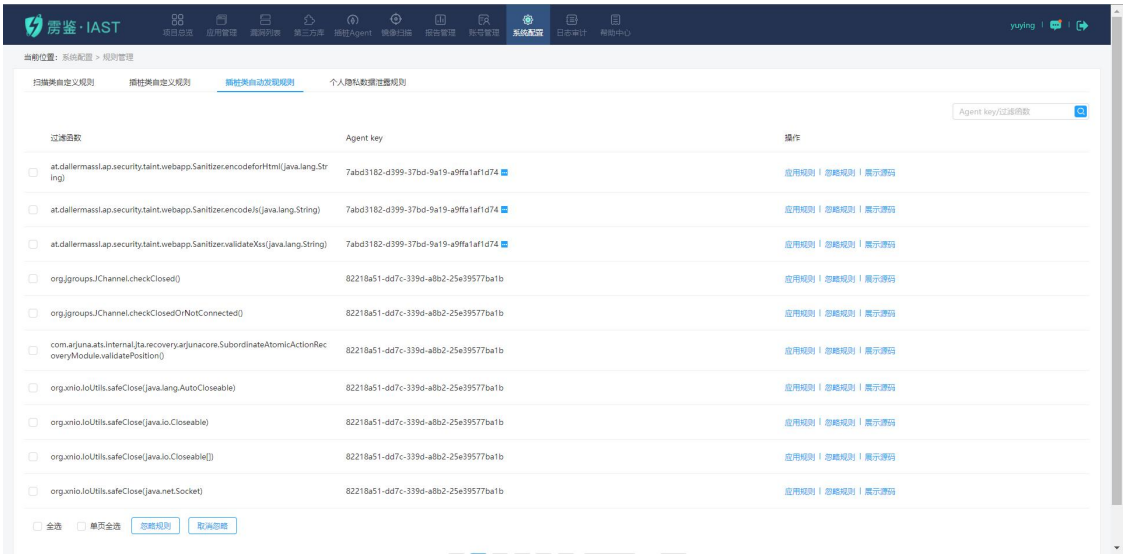
图表 293 编辑插桩类规则

- 点击删除，在弹框中进行二次确认后该规则被删除。

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。



图表 295 插桩类自动发现规则

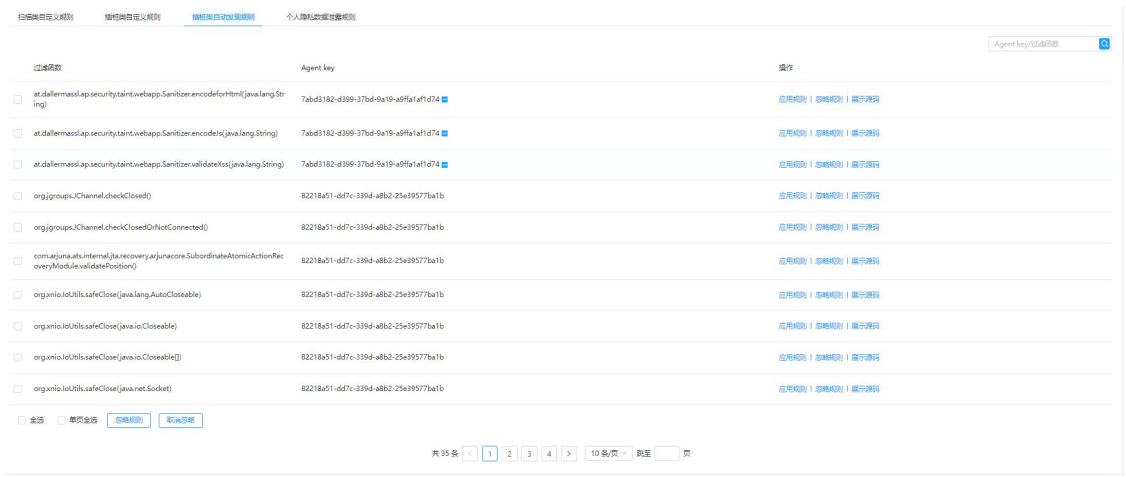
1.13.8.3.1 应用规则

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。

图表 296 应用规则

1.13.8.3.2 忽略规则

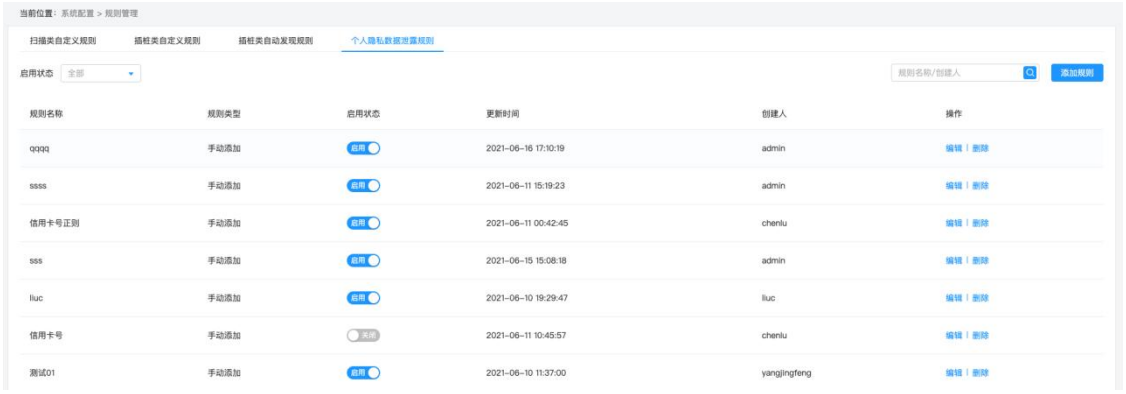
点击“忽略规则”按钮，即可忽略对应的过滤函数。在此点击“取消忽略”即可消除忽略状态。支持批量选择规则进行“忽略规则”和“取消规则”。



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。



图表 298 个人隐私数据泄漏规则

1.13.8.4.1 添加规则

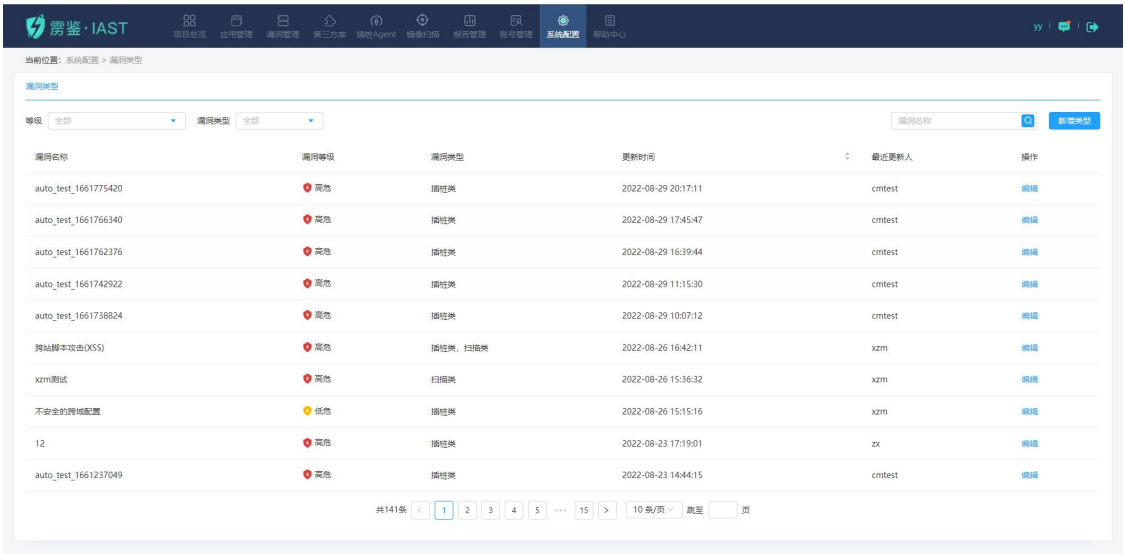
点击“添加规则”按钮，在弹窗中填写规则名称以及规则内容，点击确定即可生效。规则内容为正则表达式。

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。



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）。

杭州默安科技有限公司

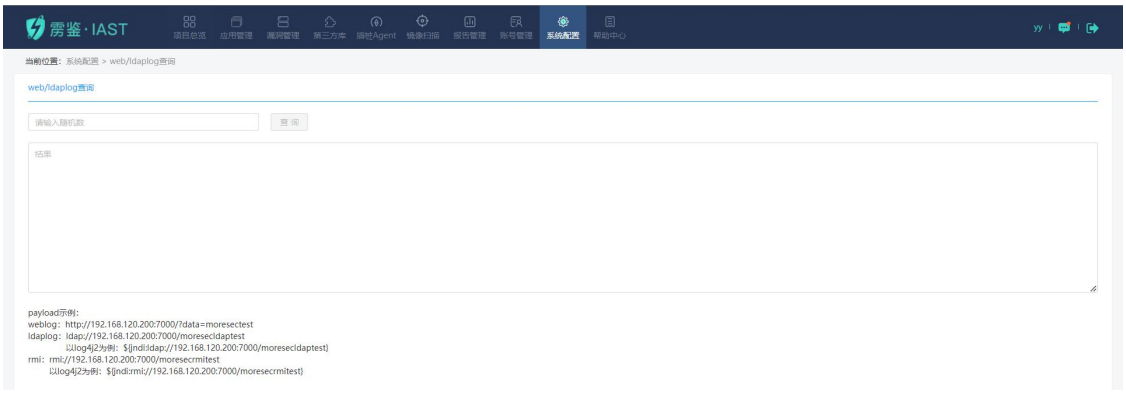
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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/ldaplog 查询



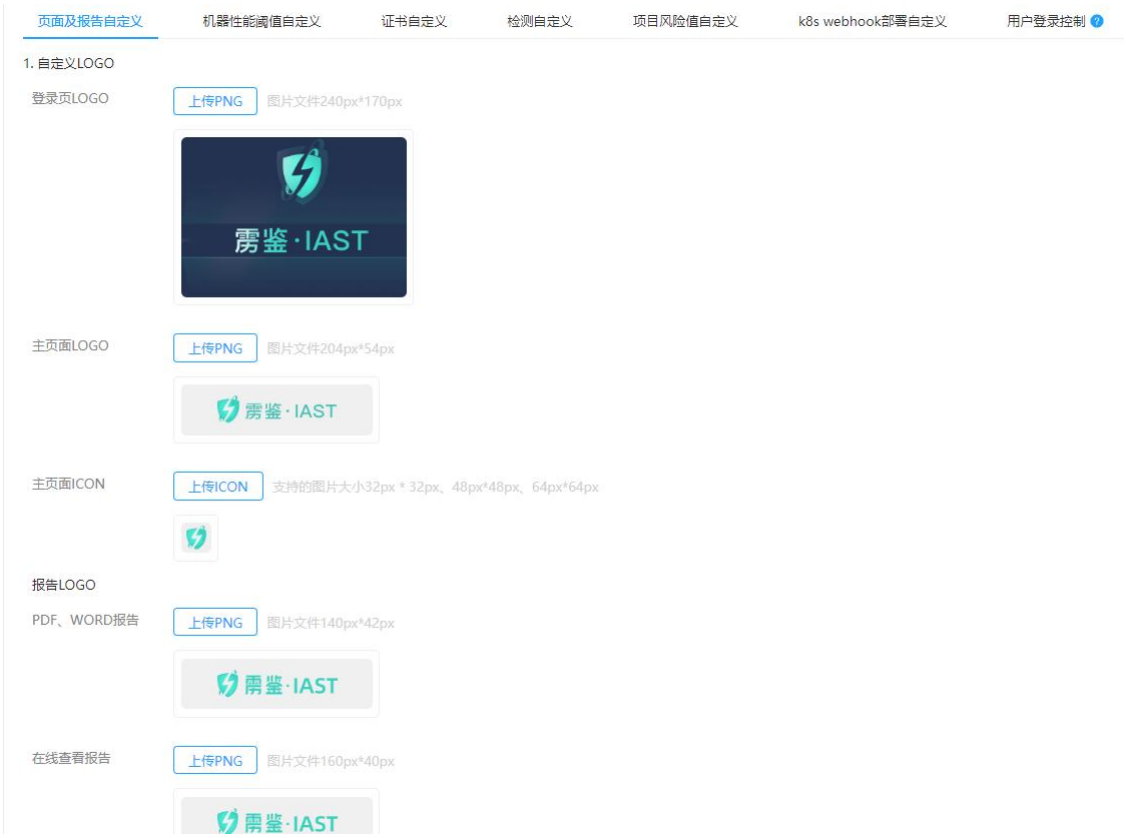
图表 302 web/ldaplog 查询

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。



图表 303 页面自定义

- 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。

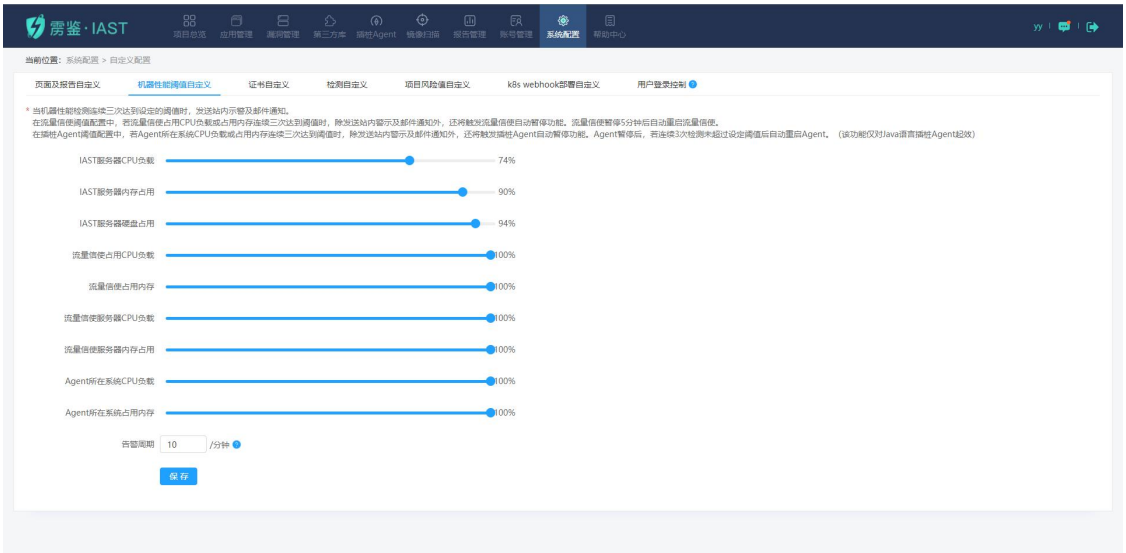
点击保存后提示更新成功。

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）



图表 304 自定义机器性能阈值

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

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。

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。

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。

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，需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。

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

图表 311 k8s webhook 部署自定义

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。编辑可以对已有信息进行修改，点击删除后会弹出对话框，确认是否删除。

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。

图表 313 新增用户白名单

1.13.12 流量镜像管理（扫描类）

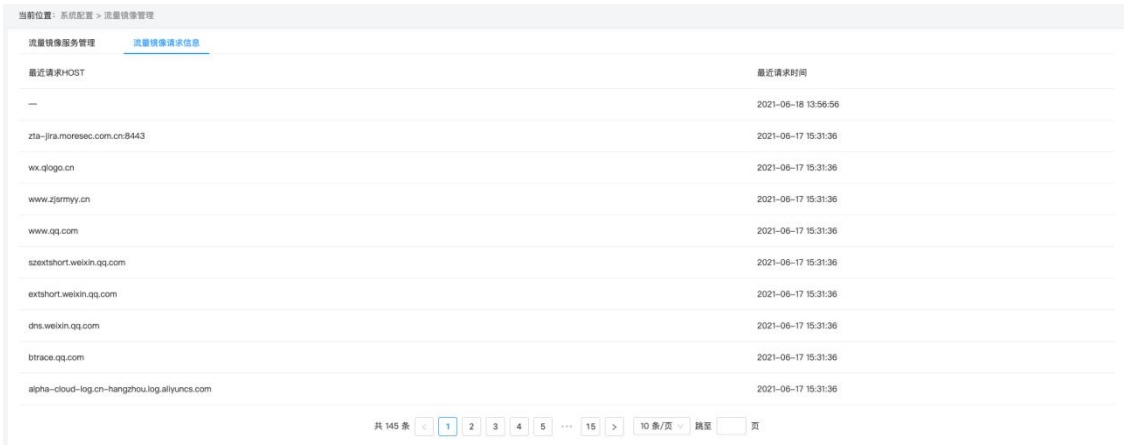
图表 314 流量镜像管理

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

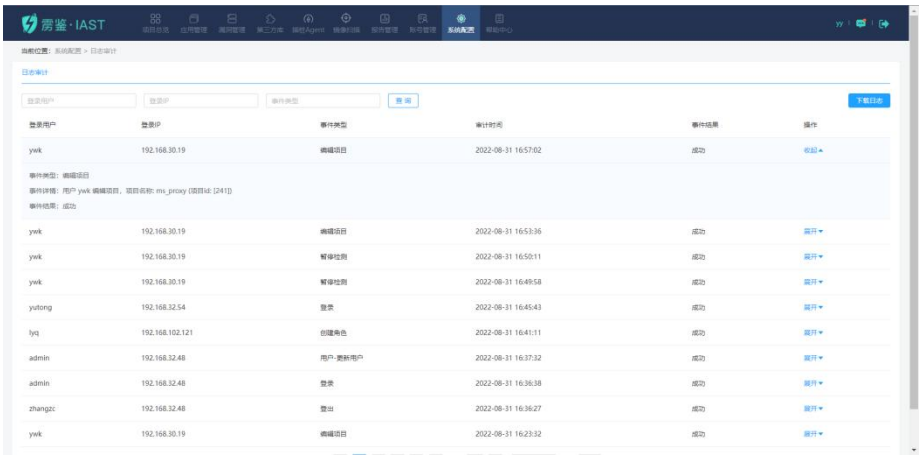
对流量镜像中最近请求 HOST 进行排布与展示



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。



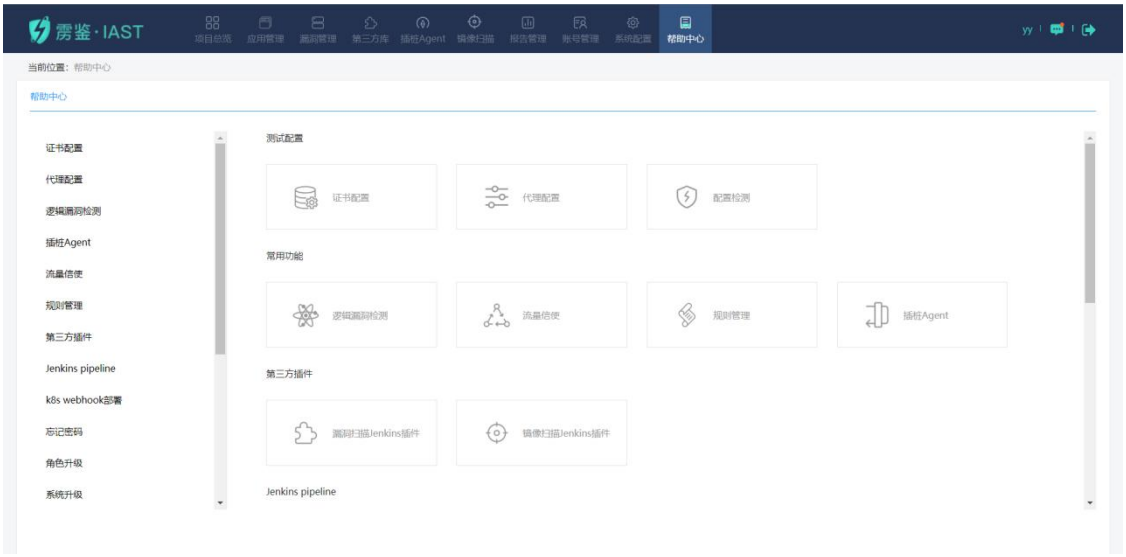
杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

图表 316 日志审计

1.14 帮助中心

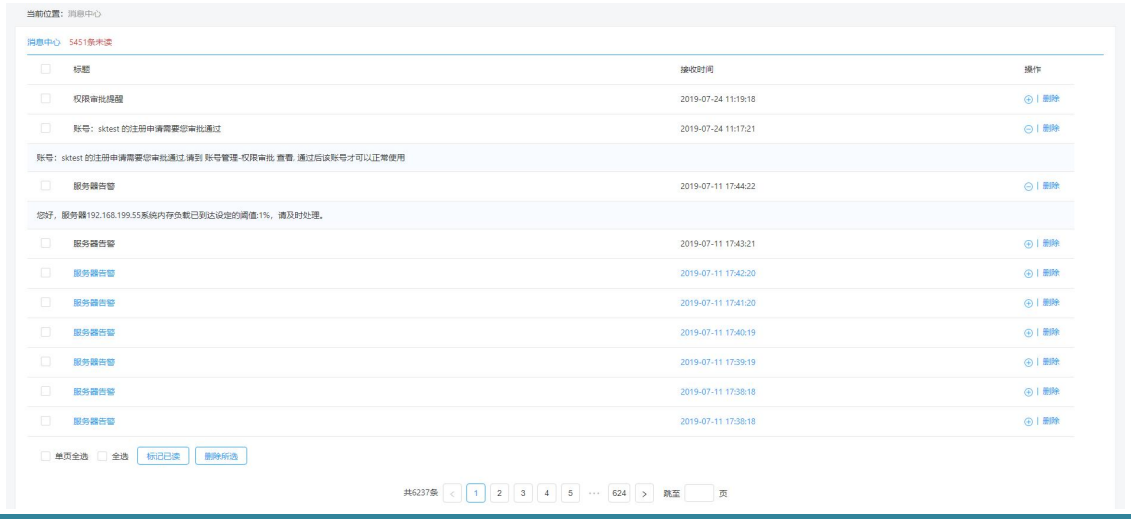
帮助中心主要用于介绍雳鉴的关键使用流程和对用户可能碰到的问题进行答疑，由 15 部分组成：证书配置、代理配置、逻辑漏洞检测、插桩 Agent、流量信使、规则管理、第三方插件、Jenkins pipeline、k8s webhook 部署、忘记密码、角色升级、系统升级、用户手册下载、产品 API 文档查看、安全组件、安全编码规范参考。



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。



杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

图表 318 消息中心

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。 雳鉴生成的 Jenkins 插件是一个将雳鉴与 Jenkins CI 项目集成的工具,可以让您在 Jenkins 中轻松配置雳鉴项目并查看结果。雳鉴 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

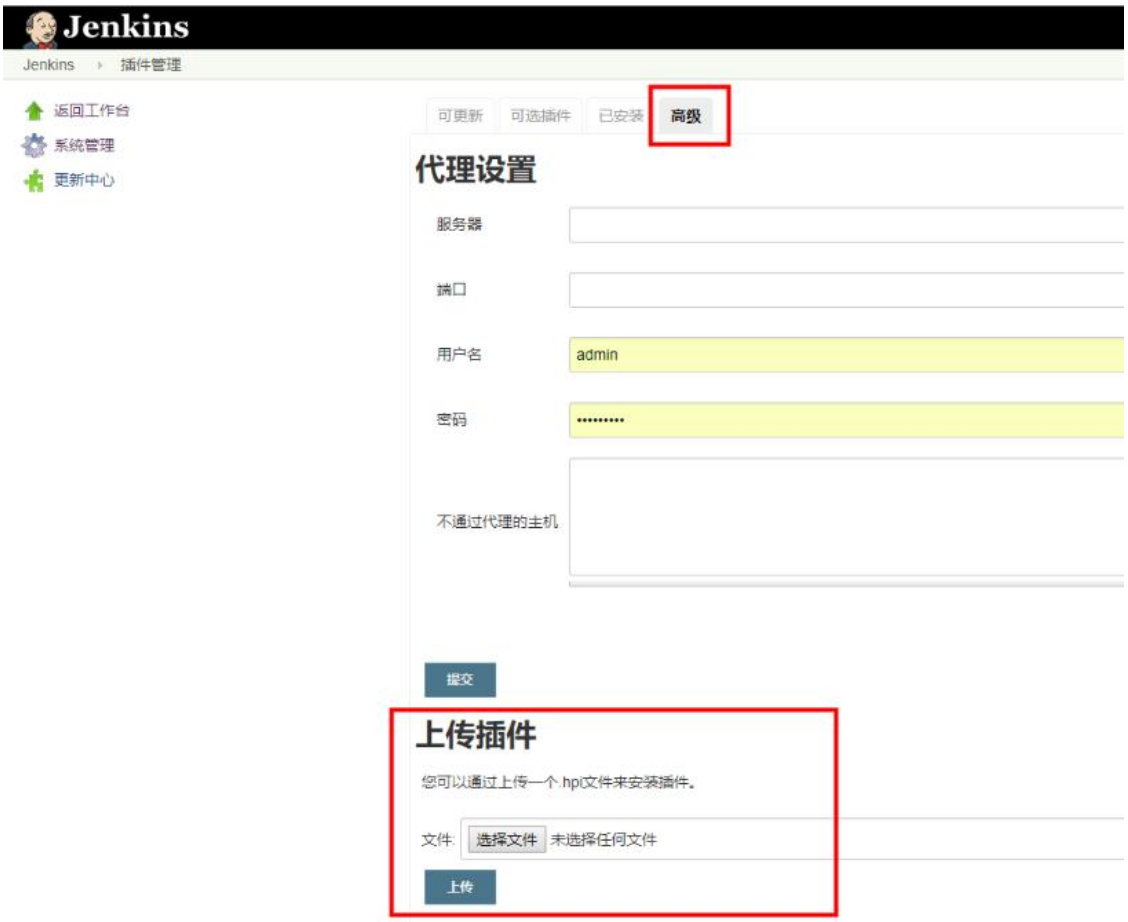
1） 在帮助中心-第三方插件-Jenkins 插件中，下载 Jenkins 插件

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"

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。



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

5) 在“系统设置”内找到“IAST 全局配置”

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。

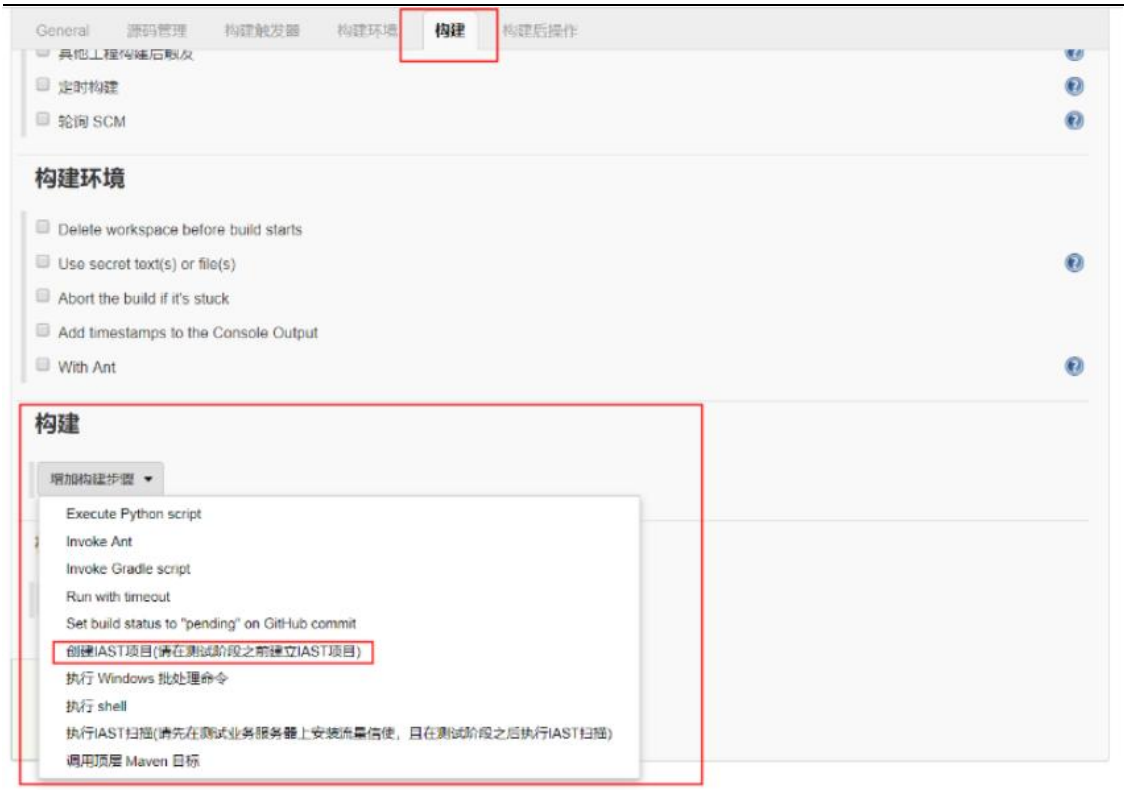
7） 设置“扫描任务超时时间”与“扫描任务超时本次任务状态”，当扫描时间超过设定值后，任务的构建状态将为设定的超时任务状态；设置“漏洞基线”及“漏洞超基线时本次任务状态”，当扫描到的任一等级漏洞数大于或等于设定的基线值时，任务的构建状态将为设定的超基线任务状态。

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”

10）输入名称，选择“构建一个自由风格的软件项目”，点击确定

11）进入项目配置页面后，在“构建”中点击“增加构建步骤”，选择“创建 IAST 项目”



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）

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)

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。

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”

17）在左侧导航栏下方可以查看构建状态

18）构建完成后点击此次构建进入此次构建页面

杭州默安科技有限公司

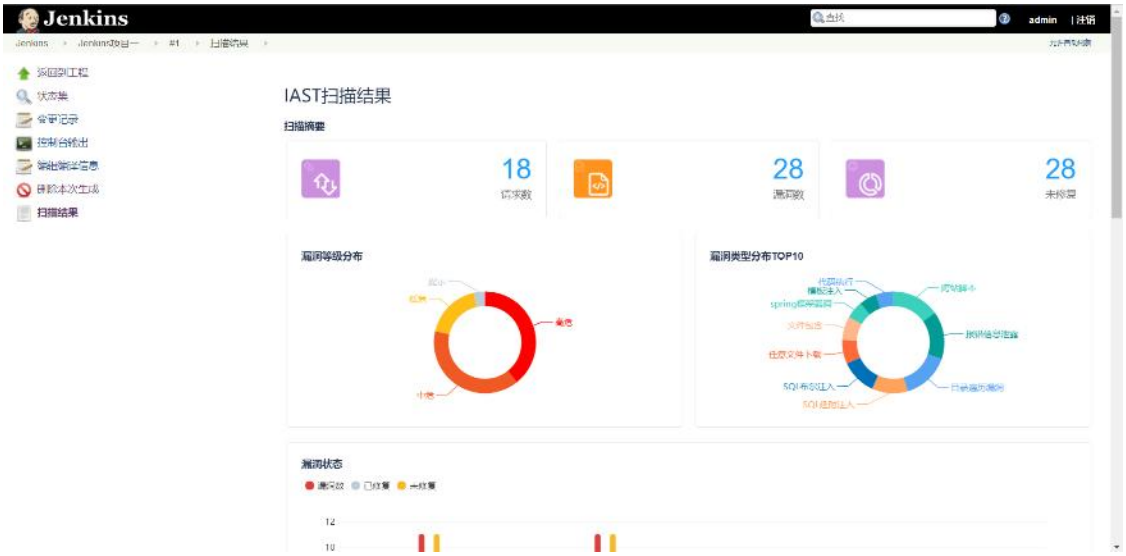
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

19）在左侧导航栏内点击“扫描结果”

20）查看扫描结果

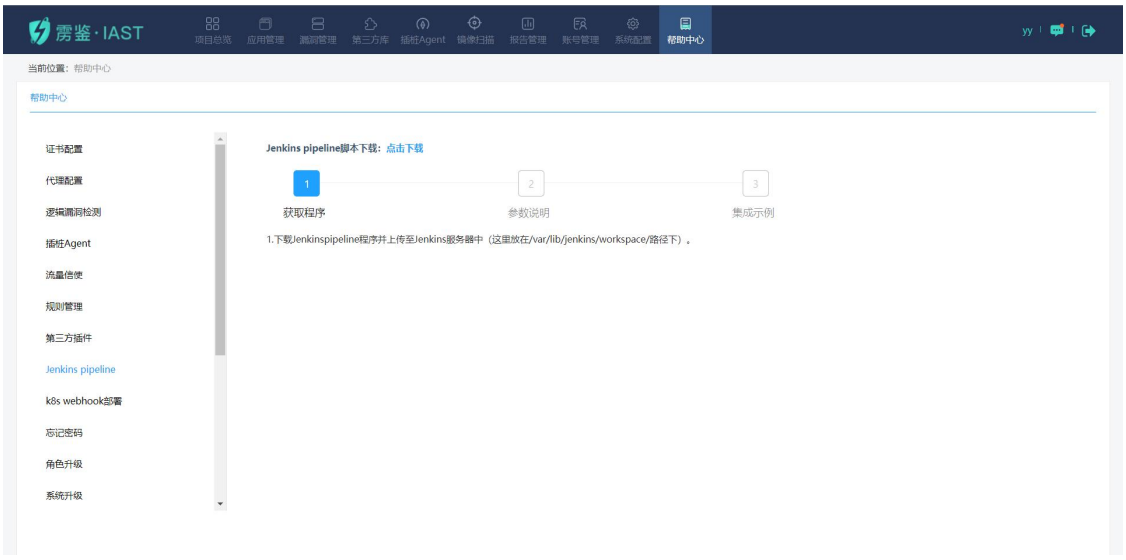
杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



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



2) 使用说明

```
[root@moresec-iast-test ~]# chmod +x go-linux-tool
[root@moresec-iast-test ~]# ./go-linux-tool -h
Usage of ./go-linux-tool:
  -b string
        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 string
        sdl ip addr
  -mode int
        1 unauthorized project mode 2 IAST project mode (default 1)
  -port int
        sdl web port (default 81)
  -t string
        it will force pipeline to stop when localtime is deadline.
```


杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

-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

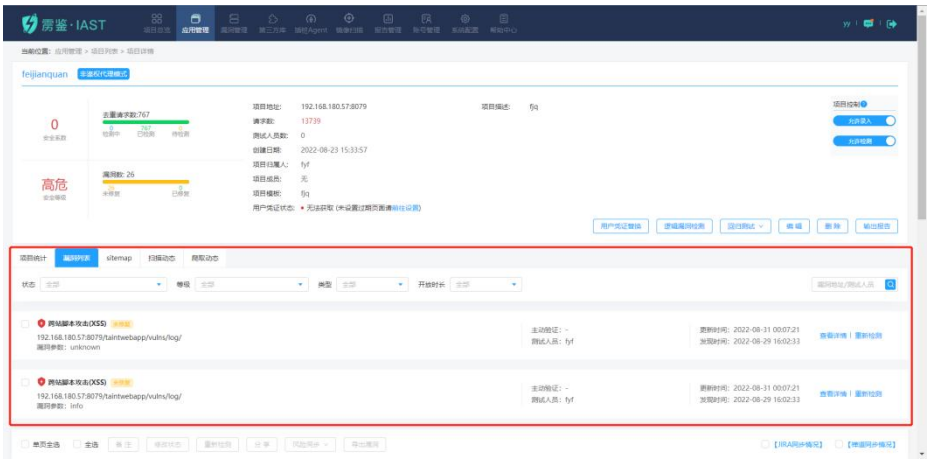
```
[root@moresec-iast-test ~]# ./go-linux-tool -b low -conf www.baidu.com  -ip 192.168.120.62 -mode 1 -t "2020-07-21 11:03:00"
login successfully
creat project successfully, please start sending your request...
tool will wait until end deadline, that -t XXXXXX
```

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

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-iast-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



杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

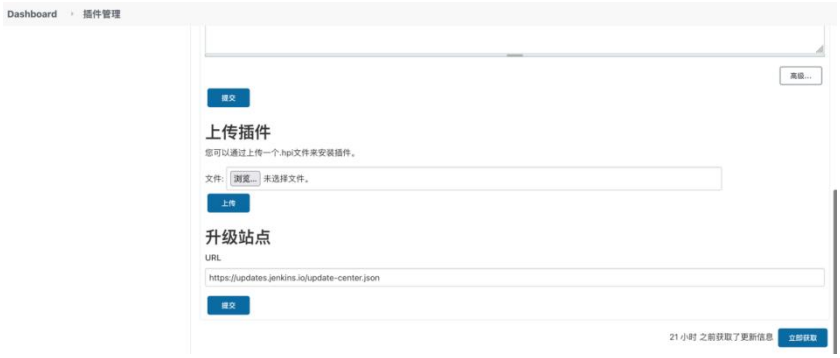
1.16.2 镜像扫描插件

1.16.2.1 镜像扫描插件使用步骤

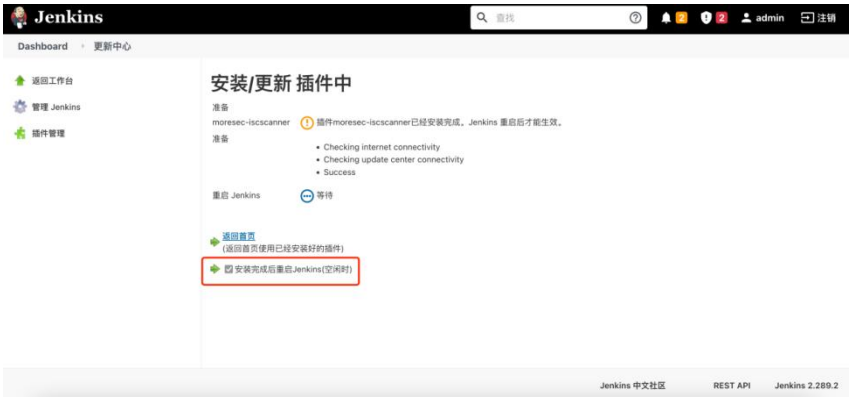
1）下载镜像扫描 Jenkins 插件。

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

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。



4）安装时勾选”重启”Jenkins。



5）安装好插件,等待 Jenkins 重启后在点击系统管理-系统配置。

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）。

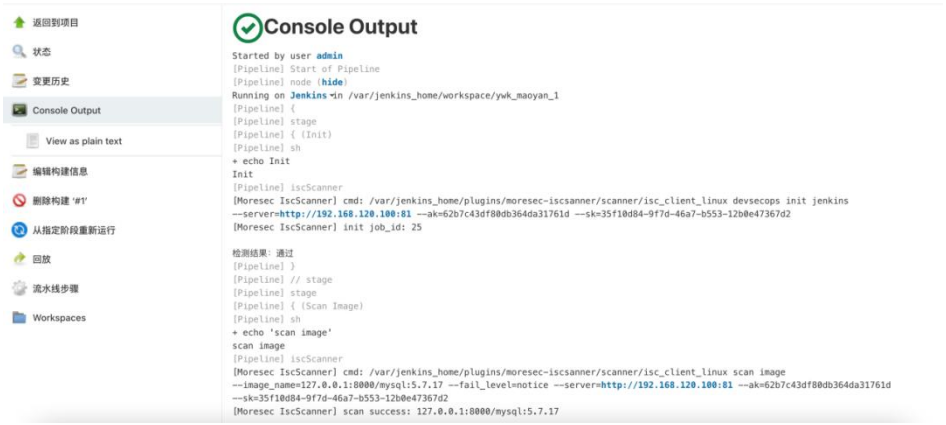
7）AK/SK 认证账户信息可以在 IAST：账号管理-AK/SK 中找到。

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。

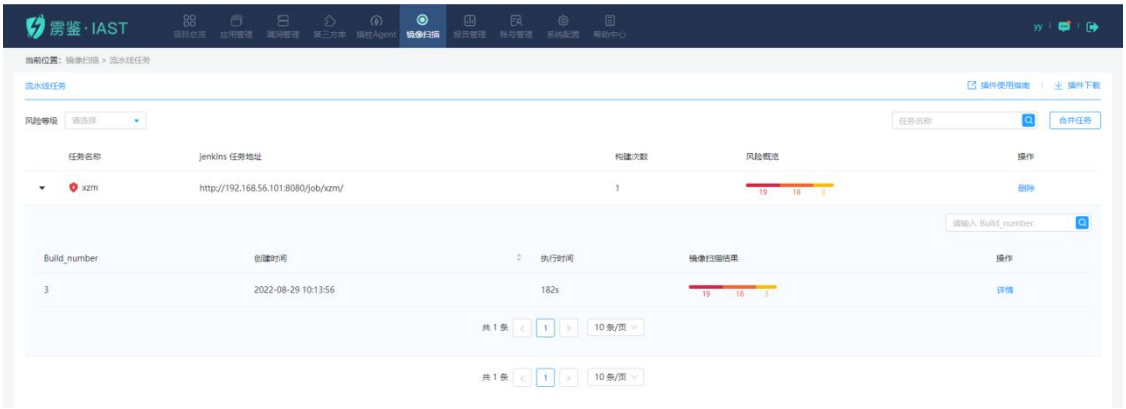
杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

9）项目构建完毕后可在控制台进行查看输出结果。



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。



杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

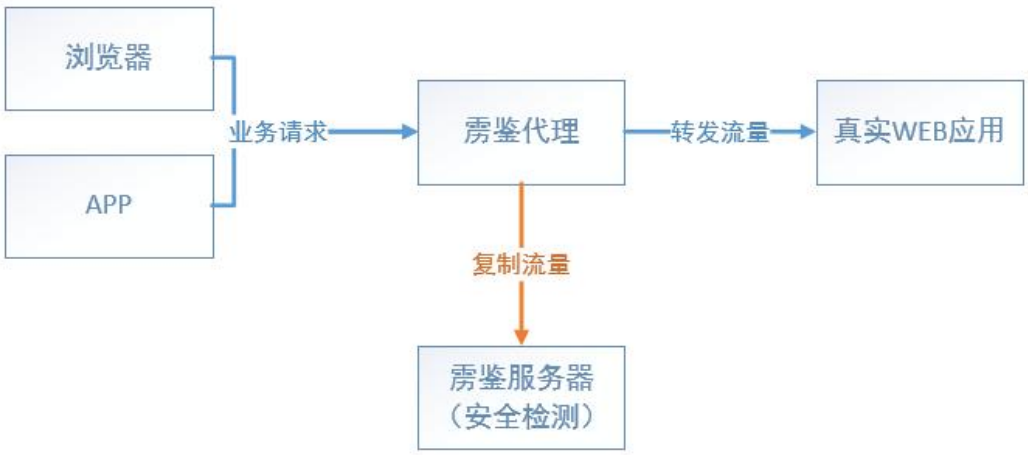
2 附录:配置证书及代理说明（扫描类）

2.1 为什么要设置代理

雳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。而雳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雳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。

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

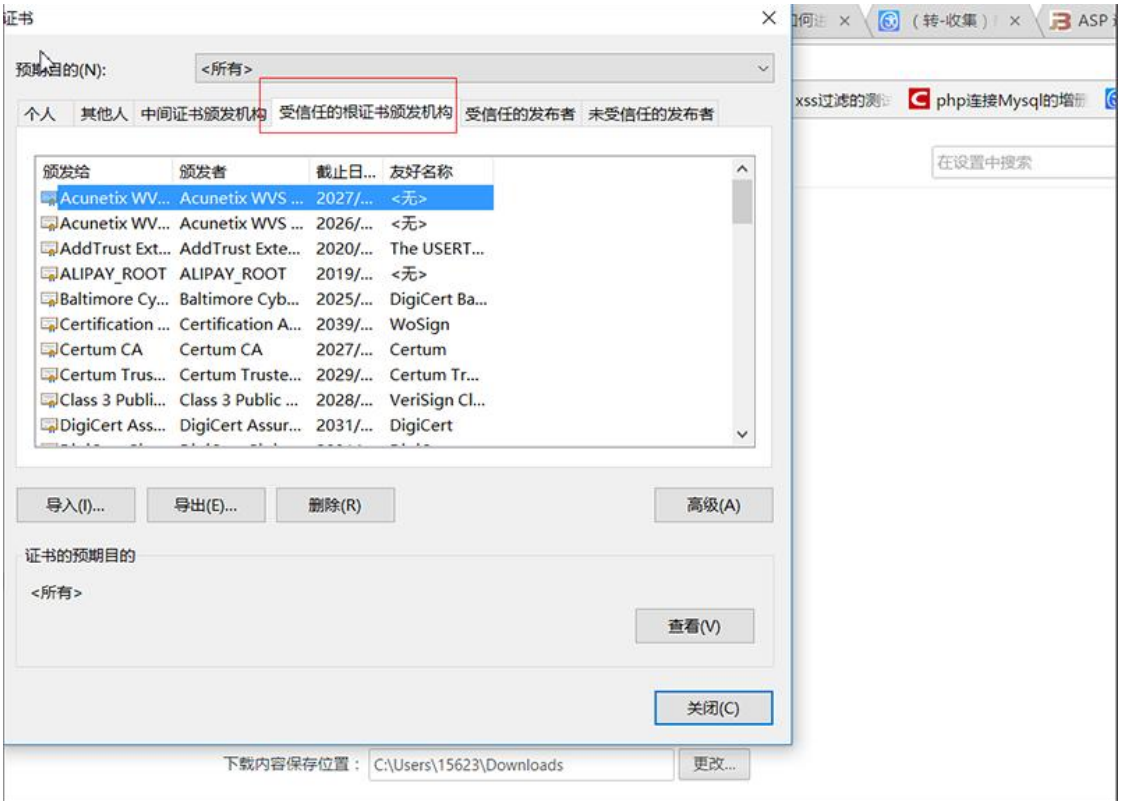
2.3.1PC 端配置

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。）

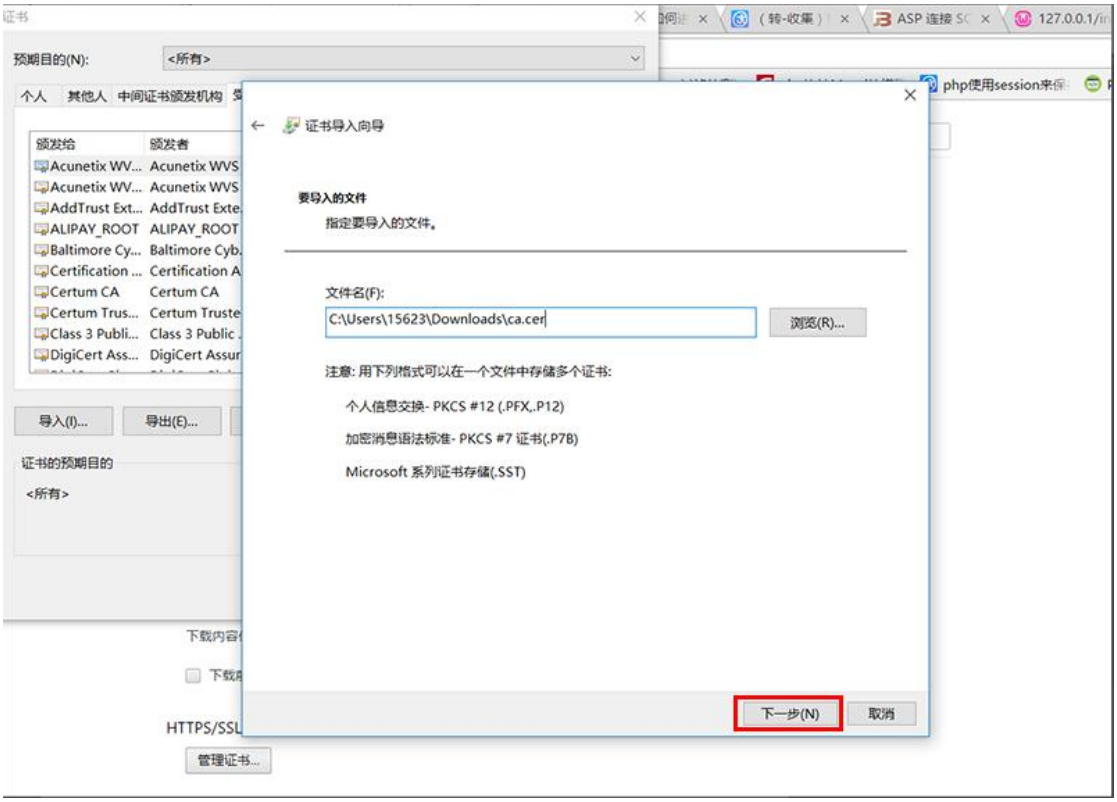
1) 选择设置，拖到最下面，选择高级

2) 然后点击管理证书，选择其中的受信任的颁发机构

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



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



杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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

2) 进入设置-更多设置，进行系统安全调整

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

3) 点击“从存储设备安装”，进行证书安装

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

4) 安装证书时，凭据用途请选择“VPN 和应用”

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

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。）

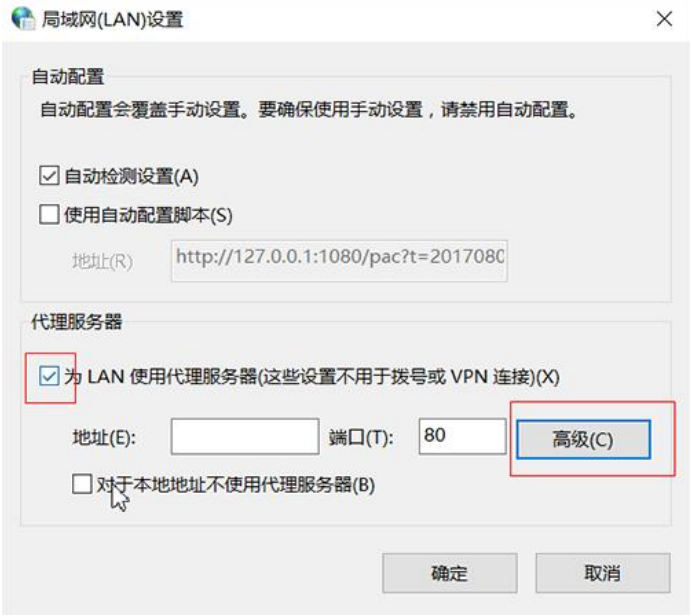
1）选择设置

2）拖到最后，选择高级-->打开代理设置-->局域网设置

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

3）勾选为 LAN 使用代理服务器，选择高级



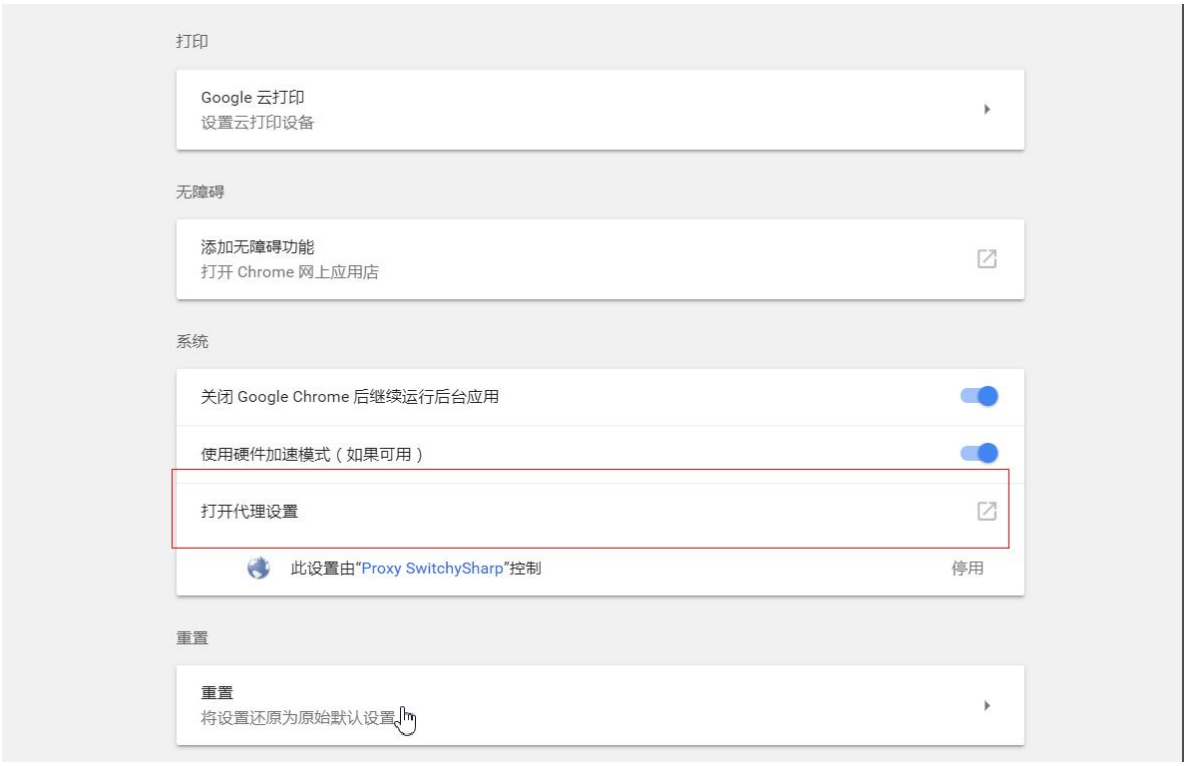
4）将从雳鉴中获取的 http 代理 IP 和端口、https 代理 IP 和端口，分别填入上留下两个框内（任务管理模块中可查看 IP 和端口），然后点击确定即可。

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

2）拖至最下方，并展开高级选项-->打开代理设置

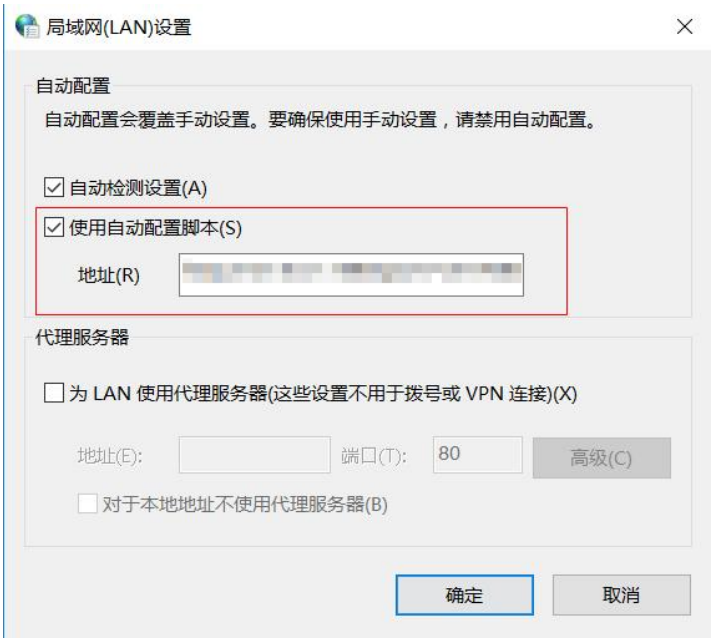


3）选择局域网属性

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

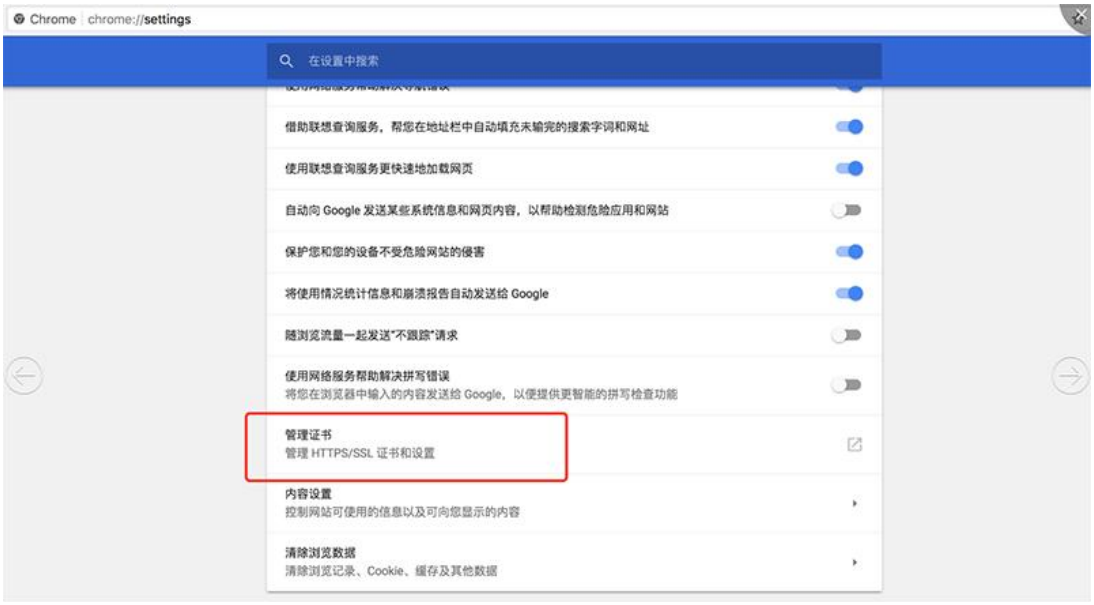
4）勾选使用自动配置脚本，地址填写雳鉴 PAC 文件地址，随后点击确定即可



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

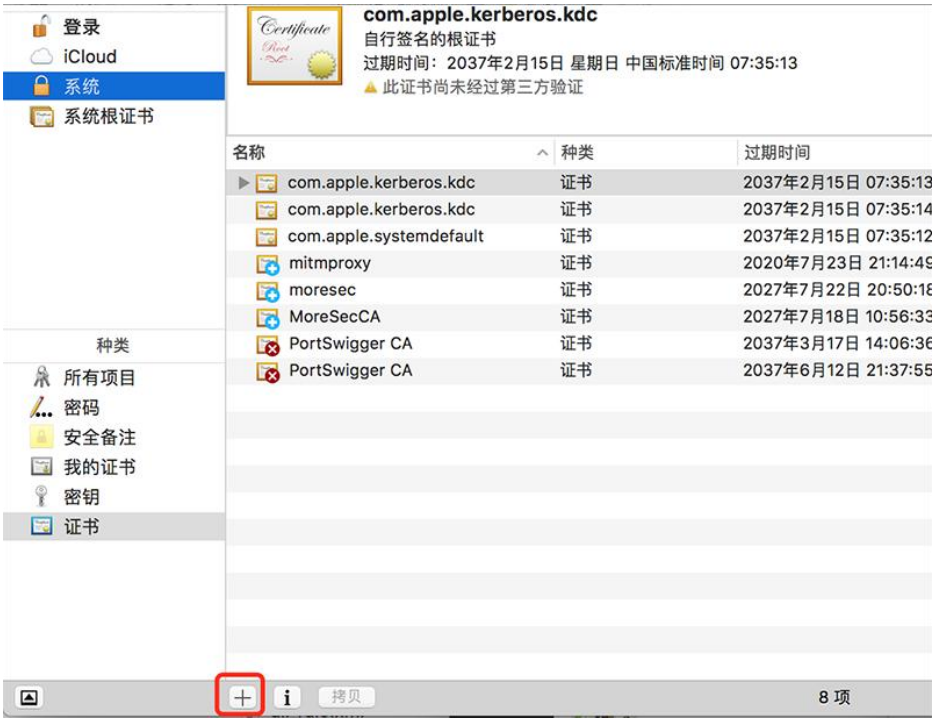
➢ Mac chrome 版安装证书方式如下，其他版安装方式请前往雳鉴帮助中心-测试配置查看。

1）打开设置，拖至最下方，选择高级



2）点击管理证书，选择左下角的加号添加证书

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn



3）选择下载的证书，点击确定

4）然后在证书上，点击右键，选择显示简介

5）展开信任一栏，使用此证书时选择始终信任

杭州默安科技有限公司
Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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

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

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

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，http:sdsd

① 打开 Postern，并添加代理服务器

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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

杭州默安科技有限公司

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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

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

Tel：（+86）400-0571-211 Email：market_moresec.cn Web：www.moresec.cn

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。