技术白皮书

代码审计服务产品

目 录

1 前言

1.1 定义

代码审计是一项白盒检测技术，是指以人工或自动化扫描方式对应用系统软件源代码进行检查，发现软件缺陷或错误，分析其可能引发的安全问题，并提供代码修订措施和建议。

应用软件是应用系统的核心，软件安全亦是应用系统安全的关键组成部分，确保应用软件安全对组织的机密性、完整性和可用性影响至关重要。微软提出的从安全角度指导软件开发过程的软件 SDL（Security Development Lifecycle，安全开发周期），将软件安全的考虑集成在软件开发需求分析、设计、编码、测试、发布、维护的每一个阶段中，其中代码审计常应用于编码和测试阶段：

- **编码阶段：**在软件开发人员实现软件设计的编码过程中，应当在编码过程的每个里程碑阶段，对特定的模块的代码进行检查。
- **测试阶段：**在整个软件开发工作完成，代码将移交生产环境之前，对整体软件代码进行检查。

代码审计的目的：在软件缺陷生效并对运营产生负面影响之前发现安全、性能或可靠性缺陷。

1.2 需求分析

代码审计技术在实际安全工作中已经被广泛应用于各种评估、测评、检查工作中，其主要客户需求基于以下三点：

1）代码审计是一项全面高效的应用系统安全控制与防范措施

代码审计能最早的发现和解决问题，代码审计能对漏洞的利用过程进行描述，清晰明确的呈现应用软件存在的问题，并直接定位到具体的代码文件及对应代码，便于开发人员的整改。而且由于是直接对软件源代码进行检查，相对与其它测试手段对于相同安全问题基本可以做到零疏漏，具有%100 的代码测试覆盖率，是进行安全评估、测试、检查工作的一项极佳的技术手段。

2）代码审计需要具备丰富的安全与编码双重经验的和技能的的人员执行

代码审计是专业性极高的安全检测手段，执行人员既需要精通漏洞原理及安全测试技术，还要对各种软件开发框架、编码语言等有深入理解，是一项对执行人员技术能力要求较高的工作。大部分组织人员往往达不到独立实施代码审计所需的相应技术水平，而出于运营成本考虑相较于独立培养专业性人才，采购使用第三方代码审计服务完成相关工作的效率与成本更低。

3）代码审计应由代码开发者以外的第三方人员执行

当软件开发方（开发人员或开发组织，后同）完成软件系统开发，在软件验收测试阶段进行代码审计工作实际上是在将代码移交生产环境之前对开发方软件开发的工作和成果进行评审，代码审查的结果一定程度上决定应用程序能否被批准进入生产环境，以及在发现问题时关系到软件开发方进行后续返工修复工作的成本。当客户在验收测试阶段不能独立实施代码审计工作时，委托非软件开发方的第三方组织执行代码审查工作是非常必要的。

2 产品综述

2.1 产品简介

启代码审计服务产品是由精通安全漏洞原理、安全测试和软件开发等专业技术能力的资深安全专家，在客户授权范围内，使用专业自动化工具结合人工代码分析的方式对应用程序源代码进行检查，发现安全缺陷，并提供相应的补救建议的专业化服务项目。

2.2 产品内容

审计服务产品由丰富的语言支持库、完善的检查过程及专业的服务成果组成。

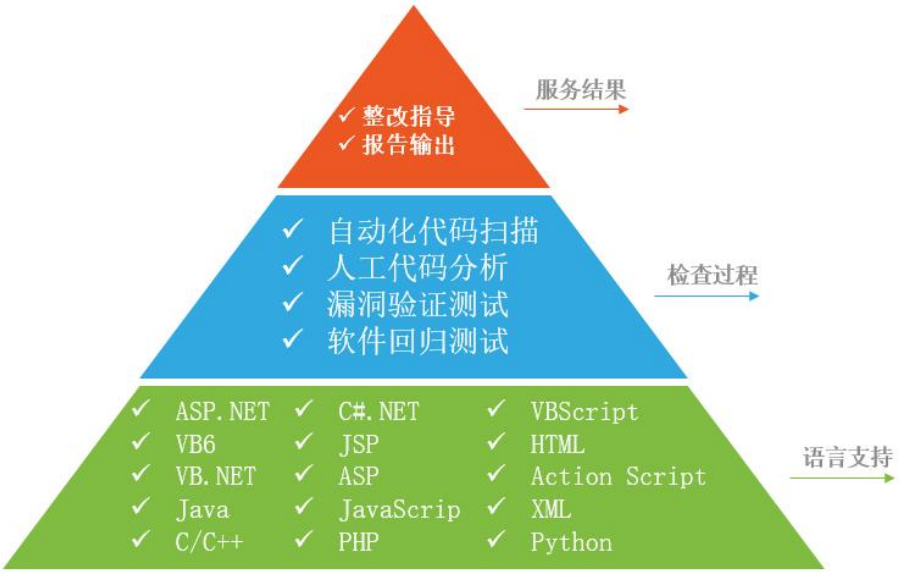

图 1 代码审计服务产品内容

1) 语言支持

专业代码审计服务可支持包括 ASP.NET、VB6、VB.NET、Java、C#.NET、JSP、ASP、JavaScript、VBScript、HTML、Action Script、XML、Objective-C、C/C++、PHP、Python 等主流开发语言，适用于当前大多数的应用系统。

2) 检查过程

使用专业的自动化代码扫描工具对软件代码进行检查，发现常见的编码规范及安全漏洞问题；

人工对扫描结果进行分析和确认，以发现业务逻辑漏洞及工具扫描未发现的漏洞，对重要功能点的代码进地人工通读代码检查；

在检查后整理代码检查结果，定位挖掘到的相应漏洞的利用点，对发现的缺陷进行验证测试，确定审计结果的准确性；

3）服务结果

专业代码审计服务在完成代码检查后，对发现的相应问题提供专业技术解释与整改建议，以帮助客户对相关代码问题进行正确的理解和改进

2.3 产品规格

代码审计服务产品产品规格功能列表如下：

服务模块	服务内容	测试对象	服务方式	服务周期	交付成果
代码审计服务	自动化工具加人工审计方式对软件源代码进行安全检查	软件源代码	现场	单次/系统	代码审计报告

2.4 专业的检测工具

在代码审计服务实施过程中，可根据具体服务内容提供多样化的代码审计工具。使用国际领先的代码扫描器与更贴近国内标准与规范的国产代码审计工具相结合，审计范围基本覆盖了市面上所有的开发语言类型，提供全面、精确的代码审计效率与效果。

3 客户收益

图 3 代码审计服务产品客户收益

3.1 提升安全意识，降低编码陋习

以人员角度来看，无论是代码审计服务人员与客户开发人员的交互过程中，从开发的角度对开发人员安全意识的灌输，提升了开发人员的安全编码意识，还是服务成果中提供的相应代码安全解决措施，对组织安全开发规范的完善，代码审计服务对组织后续软件系统的安全开发工作都具有积极的促进作用。

3.2 提升代码质量，降低安全隐患

从软件系统安全性角度说，由于代码审计是使用工程化、批量化的方法对系统源代码进行审计。可以有效地对所有问题进行检测，对于同一类问题基本可以做到零疏漏，能有效的降低安全隐患。除了安全漏洞、开发规范也是重要的审计目标，因此代码审计对于代码质量的提升具有重要的意义。

3.3 提升验收标准，降低维护成本

从软件系统的组织运营角度看，代码审计服务作用于软件系统移交生产环境之前的编码及验收测试阶段发现安全问题，对发现的问题可以直接由开发人员进行返工修正。直到代码风险处于可接受范围后再进行系统部署。这个阶段除时间成本外，对系统本身运营几乎不产

生任何影响，极大的降低了在软件系统投入运行后因安全缺陷导致负面影响的风险，降低了后期可能因安全问题频繁修补导致系统维护成本。