ICS 35.240.50
CCS L 67

DB33

浙 江 省 地 方 标 准

DB33/T 2419—2021

基于安全检测插件的Web应用系统安全检测技术规范

Technical specification for security detection of web application system based on security detection plug-in

2021－12－24发布　　2022－01－24实施

浙江省市场监督管理局　　发 布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 2
5　安全检测总体要求 2
6　安全检测插件技术要求 4
7　安全检测控制台功能要求 6
8　接口安全要求 7

前　言

本标准按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

本标准由浙江省公安厅提出并归口。

本标准起草单位：浙江警察学院、公安部第一研究所、浙江省互联网信息办公室、浙江省大数据发展管理局、浙江省卫生健康信息中心、浙江省教育技术中心、国家计算机网络应急技术处理协调中心浙江分中心、杭州医学院、浙江省药械采购中心、浙江移动网管中心、杭州孝道科技有限公司、浙江省方大标准信息有限公司。

本标准主要起草人：周国民、陈光宣、辛均益、刘强、杨卫军、吕勇刚、王晓冬、王宏宇、陈坚华、李剑锋、马骏野、蒋熠、赵丹、赵利、诸丽静、李龙、范丙华、徐锋、刘永瑞、朱旭丽、陈群、魏春梅、王宁、黄克鑫、胡博。

本标准为首次发布。

基于安全检测插件的Web应用系统安全检测技术规范

1 范围

本标准规定了安全检测插件、安全检测控制台的术语和定义，规定了基于安全检测插件的Web应用系统安全检测总体要求、安全检测插件技术要求、安全检测控制台功能要求、接口安全要求。

本标准适用于基于安全检测插件的Web应用系统安全检测技术的设计、开发和使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 11457—2006 信息技术 软件工程术语

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 11457—2006和GB/T 25069—2010界定的以及下列术语和定义适用于本标准。

3.1

程序插装 program instrumentation

a) 插入到计算机程序中的探头。如指令或断言，以利于执行监控、正确性证明、资源监控或其他活动。

b) 准备探头并把它插入到计算机程序中去的过程。

[来源：GB/T 11457—2006，2.1235]

3.2

追踪 trace

计算机程序执行的记录，它显示执行的指令的顺序、变量的名和值或两者。类型包括执行踪迹、回顾的踪迹、子例程踪迹、符号踪迹、变量踪迹。

[来源：GB/T 11457—2006，2.1751，有修改]

3.3

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

[来源：GB/T 25069—2010，2.2.2.60]

3.4

安全检测插件 security detection plug-in

通过程序插装和追踪等方法，检测应用程序漏洞，识别应用程序开源组件的动态分析部件。

3.5

安全检测控制台 security detection console

通过网络通信接口接收安全检测插件信息、下发控制指令，集中控制与管理安全检测插件的管理系统。

4 缩略语

下列缩略语适用于本标准。

API：应用编程接口（Application Programming Interface）

HTTP：超文本传输协议(Hypertext Transfer Protocol)

JSON：JavaScript对象表示法(JavaScript Object Notation)

SQL：结构查询语言（Structure Query Language）

URL：统一资源定位符（Universal Resource Locator）

XML：可扩展标记语言（eXtensible Markup Language）

5 安全检测总体要求

5.1 技术架构

基于安全检测插件的Web应用安全检测系统（以下简称“检测系统”）由嵌入了安全检测插件的Web应用系统和安全检测控制台组成，见图1。安全检测插件采用程序插装和追踪技术，对运行时的Web应用安全性进行分析，发现Web应用的漏洞、识别Web应用中开源组件漏洞和许可类型。检测系统用于Web应用软件生存周期的测试和运行阶段，目的是为帮助应用开发者和管理者了解Web应用存在的脆弱性和开源组件的许可类型，改善并提升应用系统抵抗各类Web应用攻击（如：注入攻击、跨站脚本攻击、文件包含和信息泄露等）的能力，以帮助用户建立安全合规的Web应用服务。Web应用系统使用检测系统进行安全性检测时，需在Web应用系统中部署安全检测插件，并对Web应用系统执行功能测试用于驱动安全检测插件的安全性分析。

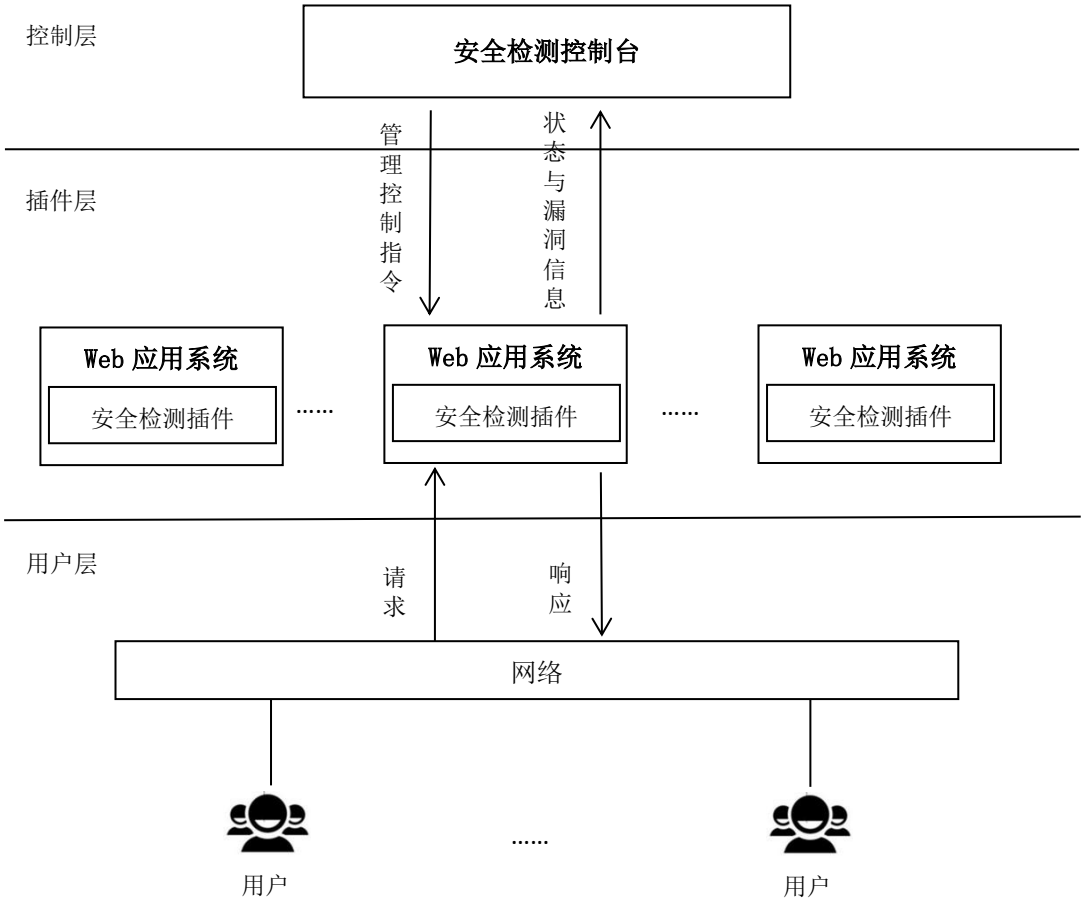

图1　技术架构

5.2　基本要求

5.2.1　检测对象影响

检测系统应避免影响目标Web应用的正常工作，例如应避免产生脏数据和脏操作。

5.2.2　安全验证

5.2.2.1　代码安全审计

检测系统发布前应对安全检测插件执行代码安全审计，减少代码中存在的脆弱性问题。

5.2.2.2　安全功能测试

检测系统发布前应对安全检测控制台的安全功能进行安全性测试。

5.2.2.3　安全性评定

根据检测系统代码安全审计和安全功能测试的结果评定其安全性，检测系统自身不存中危及以上等级的漏洞，方可准许上线运行。

5.3 安全检测

5.3.1 安全检测插件安装

检测对象的所有Web应用服务应安装安全检测插件，安全控制台能正常识别安全检测插件的在线状态。

5.3.2 执行检测

执行检测对象功能测试用例，用于驱动安全检测插件的安全性分析，识别检测对象的漏洞和开源组件风险，功能测试用例应覆盖Web应用的全部功能和接口。

6 安全检测插件技术要求

6.1 适应能力

应能适应具有安全机制的Web应用系统的安全检测，例如在Web应用使用传输报文加密机制、签名验证机制、基于不可重复资源访问控制机制时仍能检测漏洞。

6.2 工作模式

6.2.1 应具备以下工作模式：

a) 失效模式，安全检测功能关闭；
b) 检测模式，安全检测功能开启。

6.2.2 应具备根据以下条件自动切换工作模式的能力：

a) 检测对象所在服务器的 CPU 使用率、内存使用率；
b) 检测对象 Web 服务的响应时间、追踪层次数量。

6.3 漏洞检测

安全检测插件应能识别的Web应用漏洞包括但不限于以下内容：

a) 输入验证错误类
——Hibernate 注入漏洞；
——命令注入漏洞；
——SQL 注入漏洞；
——JAVA 反射注入漏洞；
——XML 路径注入漏洞；
——简单邮件传输协议注入漏洞；
——表达式注入漏洞；
——XML 外部实体注入漏洞；
——轻量级目录访问注入漏洞；
——NoSQL 注入漏洞；
——服务器端请求伪造漏洞；
——跨站脚本攻击漏洞；

——HTTP 响应分割漏洞；
——日志注入漏洞；
——目录遍历漏洞；
——文件包含漏洞；
——URL 跳转漏洞；
——JSON 劫持漏洞；
——文件流拒绝服务漏洞；
——跨站请求伪造漏洞；
——正则表达式拒绝服务漏洞。

b) 授权问题类
——弱口令漏洞；
——反序列化漏洞。

c) 配置错误类
——不安全的 HTTP 方法漏洞；
——不安全的 JSP 访问漏洞；
——会话超时时间配置不当漏洞；
——Web 服务器版本泄露漏洞；
——不充分的 SSL 连接漏洞；
——不安全的认证漏洞；
——HTTP 报文安全头缺失漏洞；
——HTTP 报文安全头配置不当漏洞；
——缺少自定义错误页面漏洞。

d) 处理逻辑错误类
——会话重写漏洞；
——服务器请求不安全的资源漏洞；
——不安全登出漏洞。

e) 加密问题类
——使用弱加密算法漏洞；
——使用弱随机数漏洞；
——密码硬编码漏洞；
——Cookie 敏感信息泄露漏洞。

注：以上漏洞分类依据 GB/T 30279-2020 中给定的漏洞分类方法。

6.4 漏洞验证

6.4.1 应能自动验证漏洞的可利用性。

6.4.2 应能根据漏洞的 URL、类型等参数控制自动验证功能的启停。

6.5 开源组件分析

6.5.1 漏洞分析

应能识别Web应用中引入的开源组件，并能结合漏洞数据库分析组件存在的已知漏洞。

6.5.2 许可分析

应能识别开源组件所使用的许可类型。

6.5.3 漏洞数据库

应包括中国国家信息安全漏洞库、国家信息安全漏洞共享平台、美国国家通用漏洞数据库等机构已披露的漏洞信息。

6.5.4 漏洞库更新

应支持离线、在线更新漏洞数据库，在线自动更新间隔时间应小于72小时。

6.6 环境兼容性

6.6.1 语言兼容

应兼容JAVA、PHP、C#、Python等主流Web开发语言。

6.6.2 操作系统兼容

应兼容Windows、CentOS、Ubuntu、RedHat、统信UOS、中标麒麟等主流操作系统。

6.6.3 开发框架兼容

应兼容Spring、Spring Cloud、Spring Cloud Alibaba、ASP.NET、ThinkPHP、Django等主流Web开发框架类型。

6.6.4 应用服务器兼容

应兼容Nginx、Apache、Tomcat、IIS、WebLogic、WebSphere、东方通、宝兰德等主流Web应用服务器。

7 安全检测控制台功能要求

7.1 安全检测插件管理

7.1.1 应具备安全检测插件安装向导的功能。
7.1.2 应具备供安全检测插件工作模式管理的功能。
7.1.3 应具备安全检测插件升级管理的功能。
7.1.4 应具备集中管理安全检测插件的功能，并满足以下要求：
a) 支持管理安全检测插件的运行状态；
b) 支持管理安全检测插件的工作模式；
c) 支持在线诊断安全检测插件的插装状态、追踪状态等内容。
7.1.5 应具备安全检测插件在线日志收集的功能。

7.2 检测策略

7.2.1 应具备选择漏洞检测规则的功能。
7.2.2 应具备根据漏洞的 URL、类型等参数配置漏洞验证规则的功能。

7.2.3 应具备增加安全函数/方法的功能，对已有的漏洞检测规则进行补充。

注：安全函数/方法是指Web应用开发过程中为保证安全用于数据验证(Validating)、净化(Sanitizing)和转义(Escaping)的函数或方法。

7.2.4 应具备增加监控 Web 应用的函数/方法的功能，对已有的监控函数/方法进行扩展。

7.2.5 应具备增加漏洞检测规则的功能，对已有的漏洞检测规则进行扩展。

7.2.6 应具备根据用户请求的源 IP 地址、URL、HTTP 参数，以及 Web 应用程序包名等信息创建排除规则的功能。

注：排除规则是用于定义安全检测插件不执行漏洞检测的条件。当排除规则生效后，满足排除规则所定义的用户请求不执行漏洞检测，满足程序包名条件的Web应用模块不执行漏洞检测。

7.3 检测结果分析处理

7.3.1 漏洞信息

应提供以下漏洞的相关信息：

a) 应提供漏洞的形成原因、检测依据、漏洞风险、修复建议、代码示例等内容；

b) 应提供漏洞检测时的请求信息、响应信息、漏洞代码位置、程序追踪过程、代码调用栈等环境信息。

7.3.2 漏洞管理

应提供以下漏洞管理的功能：

a) 应提供漏洞状态管理的功能；

b) 应提供状态名称自定义的功能。

7.3.3 统计分析

应提供以下统计分析的功能：

a) 应提供漏洞修复率、漏洞平均修复时间的统计分析的功能；

b) 应提供Web应用不同版本之间的漏洞状态对比分析的功能。

7.4 报告管理

应支持生成 Word、Excel 等格式的报告。

7.5 日志管理

应提供检测系统的运行日志、操作审计日志、安全检测插件日志，满足以下要求：

a) 应提供系统关键错误信息；

b) 应提供操作审计日志，记录事件发生的日期、时间、用户标识、事件描述和结果；

c) 应提供安全检测插件关键错误日志。

7.6 事件管理

应支持根据预设事件条件自动触发处置动作，例如在发现新漏洞时自动调用外部系统创建工单。

8 接口安全要求

8.1 通信接口

安全检测插件应提供通信接口，满足以下要求：

a) 实现的通过接口可对调用者进行身份认证，调用该接口的安全检测控制台须通过身份认证后才能对安全检测插件进行管理；

b) 安全检测控制台和安全检测插件之间传输检测策略或回传安全日志时，需确保通信安全和数据安全，防止重放、窃听或篡改攻击。

8.2 通信协议

安全检测控制台与安全检测插件之间的通信接口应满足如下通信协议要求：

a) 管理命令请求和响应消息格式应满足 JSON 格式要求；

b) 管理命令请求和响应消息应分别封装在 HTTP 协议请求消息和响应消息中进行传输；

c) 将 JSON 格式的管理命令请求和响应消息封装到 HTTP 协议前，应进行加密和编码处理。

8.3 安全连接密钥管理

安全检测控制台应能接受来自安全检测插件的安全连接请求，并采用安全连接密钥验证安全连接的有效性，具体应满足如下要求：

a) 应在安全检测插件安装前或安装过程中，由安全检测控制台为受保护的 Web 应用系统生成一个安全连接密钥，并通过安全方式传输到 Web 应用系统，并由双方安全保存；

b) 安全检测控制台在发送 JSON 格式的安全管理命令请求消息时，应在消息中附加上与所管理的 Web 应用系统匹配的安全管理密钥，Web 应用系统应基于本地安全保存的安全连接密钥对安全检测控制台发送的 JSON 格式管理命令请求消息进行验证，应在安全连接密钥匹配成功情况下，才真正执行安全检测控制台下发的安全管理命令。

8.4 安全管理命令消息解封和封装

安全检测插件应支持对安全检测控制台发送的管理命令请求消息进行安全解封，以及对将要发送到安全检测控制台的管理请求响应消息进行安全封装，具体要求如下：

a) 对于接收到的安全管理命令请求消息，安全检测插件应采用 Base64(RFC3548)解码获取本地存储的会话加密密钥，采用双方协商的加密算法对消息进行解密，得到 JSON 格式的管理命令请求消息；

b) 如解密后 JSON 格式的管理命令请求消息中包含了签名数据，安全检测插件应获取本地存储的会话签名密钥，采用双方协商的签名算法对签名进行验证，如验证失败，应直接丢弃该管理命令；

c) 安全检测插件应从消息中抽取安全连接密钥，并和本地的安全连接密钥进行比较，比对成功后执行管理命令；

d) 对于安全检测插件需发送的安全管理命令响应消息，如 Web 应用系统收到安全检测控制台下发的会话签名密钥，应采用存储于本地的会话签名密钥对消息进行签名以及 Base64 编码，并将编码后的数据封装在 HTTP 响应消息中；

e) 对于安全检测插件需要发送的安全管理命令响应消息，应采用存储于本地的会话加密密钥对消息进行加密，并对加密数据进行 Base64 编码后封装在 HTTP 响应消息中。