ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37931—2019

信息安全技术　Web 应用安全检测系统安全技术要求和测试评价方法

Information security technology—Security technology requirements and testing and evaluation approaches for Web application security detection system

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所(公安部计算机信息系统安全产品质量监督检验中心)、国家信息技术安全研究中心、杭州安恒信息技术股份有限公司、网神信息技术(北京)股份有限公司、北京神州绿盟科技有限公司、上海天泰网络技术有限公司、北京天融信网络安全技术有限公司、浙江省电子信息产品检验所、上海嘉韦思信息技术有限公司、国家电网公司。

本标准主要起草人:俞优、贾徽徽、杨元原、陆臻、邹春明、顾健、万仁忠、李冰、方进社、纪崇廉、李蒙、刘楠、张君、沈亮、范渊、吴云坤、叶晓虎、程胜年、雷晓锋、孙小平、王志佳、金海俊、王伟、向智、赵建飞、邓琦、曲晓东、唐迪、孟亚豪、马海燕、杨灼其、蔡立军、李静、舒首衡、吴舜、刘永清、连纪文。

信息安全技术　Web 应用安全检测系统安全技术要求和测试评价方法

1　范围

本标准规定了 Web 应用安全检测系统的安全技术要求、测评方法及等级划分。

本标准适用于 Web 应用安全检测系统的设计、开发与测评。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.3—2015　信息技术　安全技术　信息技术安全评估准则　第 3 部分：安全保障组件

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

Web 应用安全检测系统　Web application security detection system

对 Web 应用的安全性进行检测的产品，能够依据策略对 Web 应用进行 URL 发现，并对 Web 应用漏洞进行检测。

3.2

URL 发现　URL discovery

从一个 URL 开始，发现通过该 URL 能够链接到的其他 URL，包括在网页中出现的完整的 URL、通过各种计算得出的 URL、各种跳转的 URL 等。

3.3

变形检测　deformation detection

一种通过编码、请求包变化等方法，实现绕过防护过滤的检测机制。

4　缩略语

下列缩略语适用于本文件。

CSRF：跨站请求伪造(Cross Site Request Forgery)

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

HTTPS：安全套接字层的超文本传输协议(HyperText Transfer Protocol over Secure Socket Layer)

LDAP：轻量目录访问协议(Lightweight Directory Access Protocol)

OWASP：开放式网页应用程序安全项目(Open Web Application Security Project)

SQL:结构化查询语言(Structured Query Language)

URL:统一资源定位符,也称网页地址(Universal Resource Locator)

XSS:跨站脚本(Cross Site Scripting)

5 产品描述

Web 应用安全检测系统采用 URL 发现、Web 漏洞检测等技术,对 Web 应用的安全性进行分析,安全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,为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、文件包含和信息泄露等)的能力,以帮助用户建立安全的 Web 应用服务。

本标准将 Web 应用安全检测系统安全技术要求分为安全功能要求、自身安全要求和安全保障要求三个大类。其中,安全功能要求针对 Web 应用安全检测系统应具备的安全功能提出具体要求,主要包括检测能力、检测任务管理和检测结果分析处理等;自身安全要求针对 Web 应用安全检测系统的标识与鉴别、安全管理和审计日志提出具体要求;安全保障要求针对 Web 应用安全检测系统的生命周期过程提出具体要求,包括开发、指导性文档、生命周期支持和测试等。

本标准将 Web 应用安全检测系统(以下简称“产品”)的安全等级分为基本级和增强级。安全功能与自身安全的强弱,以及安全保障要求的高低是等级划分的具体依据,安全等级突出安全特性。与基本级内容相比,增强级中要求有所增加或变更的内容在正文中通过“**黑体**”表示。

6 安全技术要求

6.1 基本级安全技术要求

6.1.1 安全功能要求

6.1.1.1 检测能力

6.1.1.1.1 资源发现

产品应能发现 Web 应用中的各种 URL,发现的 URL 比例应高于 90%。URL 发现包括但不限于:

a) 解析和执行 JavaScript 等脚本而获得的 URL;

b) 页面文件包含的 URL;

c) Flash 中内嵌的 URL。

6.1.1.1.2 Web 应用漏洞检测

产品应能检测 Web 应用漏洞,同类型漏洞的漏报率、误报率应低于 20%。漏洞类型包括但不限于:

a) SQL 注入漏洞,含基于 Get、Post 方式提交的应包括字符、数字和搜索等的注入漏洞;

b) Cookie 注入漏洞,含基于 Cookie 方式提交的应包括字符、数字和搜索等的注入漏洞;

c) XSS 漏洞,含基于 Get、Post 方式的跨站攻击漏洞;

d) CSRF 漏洞;

e) 目录遍历漏洞;

f) 信息泄露漏洞,含路径泄露、备份文件、源代码泄露、目录浏览和 phpinfo 等信息泄露漏洞;

g) 认证方式脆弱,如弱口令等;

h） 文件包含漏洞，含远程、本地方式的文件包含漏洞。

6.1.1.1.3 升级

产品应具备漏洞特征库的更新能力。

6.1.1.1.4 支持 HTTPS

产品应能对基于 HTTPS 协议的 Web 应用进行检测。

6.1.1.1.5 不影响目标对象

产品在检测过程中应避免影响目标 Web 应用的正常工作。

6.1.1.2 检测任务管理

6.1.1.2.1 向导功能

产品应提供向导功能，指导用户进行正确配置。

6.1.1.2.2 检测范围

产品应能按照以下条件配置检测的范围：

a） 指定域名和 URL；

b） 检测的深度；

c） 不检测的 URL，如登出、删除等相关页面。

6.1.1.2.3 登录检测

产品应能基于登录信息对 Web 应用进行检测。如基于录制信息、Cookie、Session 和 Token 等一种或多种方式授权登录并进行检测。

6.1.1.2.4 策略选择

产品应能按照以下方式来选择检测策略：

a） 漏洞类型；

b） 漏洞危害级别。

6.1.1.2.5 检测速度调节

产品应能采用配置 HTTP 请求速度、检测线程或进程数目等方式调节检测速度。

6.1.1.2.6 任务定制

产品应能按照计划任务实现批量启动检测，并根据设置自动生成相应的结果。

6.1.1.2.7 进度控制

产品应能对检测进度进行以下控制：

a） 随时停止；

b） 断点续扫。

6.1.1.3 检测结果分析处理

6.1.1.3.1 结果验证

产品应具备 Web 应用漏洞验证的功能，能够提供参数进一步对 XSS 漏洞、SQL 注入点、目录遍历、信息泄露和命令执行等漏洞进行验证。

6.1.1.3.2 结果保存

检测结果应非明文存储于掉电非易失性存储介质中。

6.1.1.3.3 统计分析

产品应能根据检测结果对漏洞数量、漏洞类型和危害级别进行统计分析。

6.1.1.3.4 报告生成

产品应能对检测结果进行分析并形成报告，报告应包括：

a) 漏洞位置、漏洞名称、漏洞描述和危害级别等漏洞信息；

b) 漏洞修复建议。

6.1.1.3.5 报告输出

产品的检测报告应按以下要求输出：

a) 常用文档格式，如 DOC、PDF 和 HTML；

b) 以便于用户理解的方式展现。

6.1.2 自身安全要求

6.1.2.1 标识与鉴别

6.1.2.1.1 用户标识

6.1.2.1.1.1 安全属性定义

产品应为每个用户规定与之相关的安全属性，如用户标识、隶属组、权限等。

6.1.2.1.1.2 属性初始化

产品应具备使用默认值对创建的每个用户的属性进行初始化。

6.1.2.1.1.3 唯一性标识

产品应为用户提供唯一标识，同时将用户的身份标识与该用户的所有可审计事件相关联。

6.1.2.1.2 身份鉴别

6.1.2.1.2.1 用户鉴别

产品应在执行任何安全功能操作前鉴别用户的身份。

6.1.2.1.2.2 鉴别信息保护

产品应采取技术措施保证用户鉴别信息不被未授权查阅或修改。

6.1.2.2 安全管理

6.1.2.2.1 管理能力

产品应允许授权用户进行以下管理：

a) 查看安全属性；

b) 修改安全属性；

c) 启动、关闭全部或部分安全功能；

d) 制定和修改各种安全策略。

6.1.2.2.2 安全角色管理

产品应具有至少两种不同权限的用户角色，如操作员、审计员等。

6.1.2.2.3 远程安全传输

若产品组件间通过网络进行通信，应采取措施保障传输数据的安全性。

6.1.2.3 审计日志

6.1.2.3.1 审计日志生成

产品应生成以下事件的审计日志：

a) 用户的登录成功和失败；

b) 对安全策略进行配置的操作；

c) 对安全角色进行增加、删除和属性修改的操作。

产品应在每一个审计日志记录中记录事件发生的日期、时间、用户标识、事件描述和结果。若采用远程登录方式还应记录管理主机的 IP 地址。

6.1.2.3.2 审计日志保存

审计日志应存储于掉电非易失性存储介质中。

6.1.2.3.3 审计日志管理

产品应提供以下审计日志管理功能：

a) 只允许授权用户访问审计日志；

b) 根据操作用户、日期时间和操作类型等条件的查询和检索功能；

c) 授权用户应能存档和导出审计日志。

6.1.3 安全保障要求

6.1.3.1 开发

6.1.3.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能的描述范围相一致；

b) 充分描述产品采取的自我保护、不可旁路的安全机制。

6.1.3.1.2 功能规范

开发者应提供完备的功能规范，功能规范应满足以下要求：

a) 完整描述 6.1.1、6.1.2 中定义的功能；

b) 标识和描述产品所有安全功能接口的目的、使用方法及相关参数；

c) 描述安全功能接口相关的安全功能实施行为；

d) 描述由安全功能实施行为处理而引起的直接错误消息。

6.1.3.1.3 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a) 通过子系统描述产品结构，标识和描述产品安全功能的所有子系统，并描述子系统间的相互作用；

b) 提供子系统和安全功能接口间的对应关系。

6.1.3.2 指导性文档

6.1.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，对每一种用户角色的描述应满足以下要求：

a) 描述用户能够访问的功能和特权，包含适当的警示信息；

b) 描述产品安全功能及接口的用户操作方法，包括配置参数的安全值等；

c) 标识和描述产品运行的所有可能状态，包括操作导致的失败或者操作性错误；

d) 描述实现产品安全目的必需执行的安全策略。

6.1.3.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；

b) 描述安全安装产品及其运行环境必需的所有步骤。

6.1.3.3 生命周期支持

6.1.3.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；

b) 使用配置管理系统对组成产品的所有配置项进行维护，并进行唯一标识；

c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法。

6.1.3.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表至少包含产品、安全保障要求的评估证据和产品的组成部分。

6.1.3.3.3 交付程序

开发者应使用规定的交付程序交付产品，并将交付过程文档化。在给用户方交付各版本产品时，交付文档应描述为维护安全所必需的所有程序。

6.1.3.4 测试

6.1.3.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应表明测试文档中所标识的测试项目与功能规范中所描述产品安全功能的对应性。

6.1.3.4.2 功能测试

开发者应测试产品安全功能，并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案；

b) 预期的测评结果，表明测试成功后的预期输出；

c) 实际测评结果和预期的测评结果的对比。

6.1.3.4.3 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

6.1.3.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗基本攻击。

6.2 增强级安全技术要求

6.2.1 安全功能要求

6.2.1.1 检测能力

6.2.1.1.1 资源发现

产品应能发现 Web 应用中的各种 URL，发现的 URL 比例应高于 90%。URL 发现包括但不限于：

a) 解析和执行 JavaScript 等脚本而获得的 URL；

b) 页面文件包括的 URL；

c) Flash、**Flex** 中内嵌的 URL。

6.2.1.1.2 Web 应用漏洞检测

产品应能检测 Web 应用漏洞，同类型漏洞的漏报率、误报率应低于 20%。漏洞类型包括但不限于：

a) SQL 注入漏洞，含基于 Get、Post 方式提交的应包括字符、数字和搜索等的注入漏洞；

b) Cookie 注入漏洞，含基于 Cookie 方式提交的应包括字符、数字和搜索等的注入漏洞；

c) XSS 漏洞，含基于 Get、Post、**Referrer** 和 **Cookie** 方式的跨站攻击漏洞；

d) CSRF 漏洞；

e) 目录遍历漏洞；

f) 信息泄露漏洞，含路径泄露、备份文件、源代码泄露、目录浏览和 phpinfo 等信息泄露漏洞；

g) 认证方式脆弱，如**各种登录绕过**、弱口令等；

h) 文件包含漏洞，含远程、本地方式的文件包含漏洞；

i) **命令执行漏洞**；

j) **第三方组件漏洞，如 Struts2、FCKeditor 编辑器等**；

k) LDAP 注入漏洞；

l) XPath 注入漏洞。

6.2.1.1.3 变形检测

产品应支持 Web 应用漏洞的变形检测，如大小写随机转换、多种绕过空格限制、空格替换和 URL 编码等机制。

6.2.1.1.4 内容检测

产品应能对目标 Web 应用的以下内容进行检测：

a) 不属于目标系统的外链；

b) 目标系统内的坏链；

c) 目标系统内的暗链；

d) 敏感关键字。

6.2.1.1.5 升级

产品应具备以下升级：

a) 漏洞特征库的更新；

b) 至少采取一种安全机制，保证升级的时效性，如自动升级、更新通知等手段。

6.2.1.1.6 支持 HTTPS

产品应能对基于 HTTPS 协议的 Web 应用进行检测。

6.2.1.1.7 不影响目标对象

产品在检测过程中应避免影响目标 Web 应用的正常工作。

6.2.1.2 检测任务管理

6.2.1.2.1 向导功能

产品应提供向导功能，指导用户进行正确配置。

6.2.1.2.2 检测范围

产品应能按照以下条件配置检测的范围：

a) 指定域名和 URL；

b) 检测的深度；

c) 不检测的 URL，如登出、删除等相关页面；

d) 路径模式排重；

e) 路径模式大小写区分。

6.2.1.2.3 登录检测

产品应能基于登录信息对 Web 应用进行检测。如基于录制信息、Cookie、Session 和 Token 等一种或多种方式授权登录并进行检测。

6.2.1.2.4 检测策略

6.2.1.2.4.1 策略选择

产品应能按照以下方式来选择检测策略：

a） 漏洞类型；

b） 漏洞危害级别；

c） **Web 系统指纹信息**。

6.2.1.2.4.2 策略扩展

产品应能自定义检测策略，对已有策略进行扩展。

6.2.1.2.5 检测速度调节

产品应能根据以下方式调节检测速度：

a） 配置 HTTP 请求速度、检测线程或进程数目等；

b） **分布式部署检测引擎**；

c） **多引擎负载均衡**。

6.2.1.2.6 任务定制

产品应能按照计划任务实现批量、**定时、指定时间段和周期性**启动检测，并根据设置自动生成相应的结果。

6.2.1.2.7 进度控制

产品应能对检测进度进行以下控制：

a） 随时停止；

b） 断点续扫；

c） **检测未结束的情况下，能够将已经检测的部分展示并导出报告**。

6.2.1.3 检测结果分析处理

6.2.1.3.1 结果验证

产品应具备 Web 应用漏洞验证的功能，包括：

a） 提供参数进一步对 XSS 漏洞、SQL 注入点、目录遍历、信息泄露和命令执行等漏洞进行验证；

b） **提供自动化工具验证漏洞**。

6.2.1.3.2 结果保存

检测结果应非明文存储于掉电非易失性存储介质中。

6.2.1.3.3 统计分析

产品应能根据检测结果对漏洞数量、漏洞类型和危害级别进行统计分析。

6.2.1.3.4 报告生成

产品应能对检测结果进行分析并形成报告，报告应包括：

a) 漏洞位置、漏洞名称、漏洞描述和危害级别等漏洞信息；
b) 漏洞修复建议；
c) 支持导出行业合规报告；
d) 编辑和自定义设计报告，支持添加自定义注释或详细信息；
e) 支持批量导出报告；
f) 支持根据横向、纵向比较的趋势分析报告。

6.2.1.3.5 报告输出

产品的检测报告应按以下要求输出：
a) 常用文档格式，如 DOC、PDF 和 HTML；
b) 以便于用户理解的方式展现。

6.2.1.4 互动性要求

产品应提供或采用一个标准的、开放的接口。遵照该接口规范，可为其他类型安全产品编写相应的程序模块，达到与产品进行互动的目的。

6.2.2 自身安全要求

6.2.2.1 标识与鉴别

6.2.2.1.1 用户标识

6.2.2.1.1.1 安全属性定义

产品应为每个用户规定与之相关的安全属性，如用户标识、隶属组、权限等。

6.2.2.1.1.2 属性初始化

产品应具备使用默认值对创建的每个用户的属性进行初始化。

6.2.2.1.1.3 唯一性标识

产品应为用户提供唯一标识，同时将用户的身份标识与该用户的所有可审计事件相关联。

6.2.2.1.2 身份鉴别

6.2.2.1.2.1 用户鉴别

产品应在执行任何安全功能操作前鉴别用户的身份。

6.2.2.1.2.2 鉴别信息保护

产品应采取技术措施保证用户鉴别信息不被未授权查阅或修改。

6.2.2.1.2.3 鉴别失败处理

当对用户鉴别失败的次数达到指定次数后，产品应能终止用户的访问。

6.2.2.1.2.4 超时锁定或注销

应具有登录超时锁定或注销功能。在设定的时间段内没有任何操作的情况下，终止会话，需要再次

进行身份鉴别才能够重新操作。最大超时时间仅由授权用户设定。

6.2.2.2 安全管理

6.2.2.2.1 管理能力

产品应允许授权用户进行以下管理：

a) 查看安全属性；

b) 修改安全属性；

c) 启动、关闭全部或部分安全功能；

d) 制定和修改各种安全策略。

6.2.2.2.2 安全角色管理

产品应能对用户角色进行以下区分：

a) 具有至少两种不同权限的用户角色，如操作员、审计员等；

b) 应根据不同的功能模块，自定义各种不同权限角色，并能够对用户分配角色。

6.2.2.2.3 远程安全传输

若产品组件间通过网络进行通信，应采取措施保障传输数据的安全性。

6.2.2.2.4 管理主机限制

若控制台提供远程管理功能，应能对可远程管理的主机地址进行限制。

6.2.2.3 审计日志

6.2.2.3.1 审计日志生成

产品应生成以下事件的审计日志：

a) 用户的登录成功和失败；

b) 对安全策略进行配置的操作；

c) 对安全角色进行增加、删除和属性修改的操作；

d) 对检测结果的备份和删除。

产品应在每一个审计日志记录中记录事件发生的日期、时间、用户标识、事件描述和结果。若采用远程登录方式还应记录管理主机的 IP 地址。

6.2.2.3.2 审计日志保存

审计日志应存储于掉电非易失性存储介质中。

6.2.2.3.3 审计日志管理

产品应提供以下审计日志管理功能：

a) 只允许授权用户访问审计日志；

b) 根据操作用户、日期时间和操作类型等条件的查询和检索功能；

c) 授权用户应能存档和导出审计日志。

6.2.3 安全保障要求

6.2.3.1 开发

6.2.3.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能的描述范围相一致；

b) 充分描述产品采取的自我保护、不可旁路的安全机制。

6.2.3.1.2 功能规范

开发者应提供完备的功能规范，功能规范应满足以下要求：

a) 完整描述 6.2.1、6.2.2 中定义的功能；

b) 标识和描述产品所有安全功能接口的目的、使用方法及相关参数；

c) 描述安全功能实施过程中，与安全功能接口相关的所有行为；

d) 描述可能由安全功能接口的调用而引起的所有直接错误消息。

6.2.3.1.3 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a) 通过子系统描述产品结构，标识和描述产品安全功能的所有子系统，并描述子系统间的相互作用；

b) 提供子系统和安全功能接口间的对应关系；

c) 通过模块描述安全功能，标识和描述模块的目的、相关接口及返回值等，并描述模块间的相互作用及调用的接口；

d) 提供模块和子系统间的对应关系。

6.2.3.1.4 实现表示

开发者应提供产品安全功能的实现表示，实现表示应满足以下要求：

a) 详细定义产品安全功能，包括软件代码、设计数据等实例；

b) 提供实现表示与产品设计描述间的对应关系。

6.2.3.2 指导性文档

6.2.3.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，对每一种用户角色的描述应满足以下要求：

a) 描述用户能够访问的功能和特权，包含适当的警示信息；

b) 描述产品安全功能及接口的用户操作方法，包括配置参数的安全值等；

c) 标识和描述产品运行的所有可能状态，包括操作导致的失败或者操作性错误；

d) 描述实现产品安全目的必需执行的安全策略。

6.2.3.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；

b) 描述安全安装产品及其运行环境必需的所有步骤。

6.2.3.3 生命周期支持

6.2.3.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；

b) 使用配置管理系统对组成产品的所有配置项进行维护，并进行唯一标识；

c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；

d) 配置管理系统提供自动方式来支持产品的生成，通过自动化措施确保配置项仅接受授权变更；

e) 配置管理文档包括一个配置管理计划，描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。配置管理计划应描述如何使用配置管理系统开发产品，开发者实施的配置管理应与配置管理计划相一致。

6.2.3.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) 产品、安全保障要求的评估证据和产品的组成部分；

b) 实现表示、安全缺陷报告及其解决状态。

6.2.3.3.3 交付程序

开发者应使用规定的交付程序交付产品，并将交付过程文档化。在给用户方交付各版本产品时，交付文档应描述为维护安全所必需的所有程序。

6.2.3.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.2.3.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

6.2.3.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

6.2.3.4 测试

6.2.3.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a) 表明测试文档中所标识的测试项目与功能规范中所描述的产品安全功能的对应性；

b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

6.2.3.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a) 表明测试文档中的测试项目与产品设计中的安全功能子系统、模块之间的对应性；

b) 证实产品设计中的所有安全功能子系统、模块都已经进行过测试。

6.2.3.4.3 功能测试

开发者应测试产品安全功能，并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测评结果的任何顺序依赖性；

b) 预期的测评结果，表明测试成功后的预期输出；

c) 实际测评结果和预期的测评结果的对比。

6.2.3.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

6.2.3.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗增强攻击。

7 测评方法

7.1 基本级安全技术要求测评

7.1.1 安全功能测评

7.1.1.1 检测能力

7.1.1.1.1 资源发现

资源发现的测评方法如下：

a) 测评方法：

1) 配置产品检测 JavaScript 脚本的页面地址，执行检测任务，查看检测结果；

2) 配置产品检测包括页面文件的 URL 地址，执行检测任务，查看检测结果；

3) 配置产品检测内嵌 URL 的 Flash 地址，执行检测任务，查看检测结果。

b) 预期结果：

1) 产品能够解析和执行 JavaScript 脚本，发现的 URL 比例高于 90%；

2) 产品能够获取页面文件内包括的 URL，发现的 URL 比例高于 90%；

3) 产品能够获取 Flash 中内嵌的 URL，发现的 URL 比例高于 90%。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.1.2 Web 应用漏洞检测

Web 应用漏洞检测的测评方法如下：

a) 测评方法：

1） 配置产品检测策略，执行对 Web 应用漏洞环境（部署 SQL 注入、Cookie 注入、XSS、CSRF、目录遍历、信息泄露、认证方式脆弱和文件包含等漏洞）的检测任务；

2） 查看检测结果。

b） 预期结果：

1） 产品能够发现基于 Get、Post 方式提交的字符、数字、搜索等的 SQL 注入漏洞；

2） 产品能够发现基于 Cookie 方式提交的字符、数字、搜索等的 Cookie 注入漏洞；

3） 产品能够发现基于 Get、Post 方式的 XSS 漏洞；

4） 产品能够发现 CSRF 漏洞；

5） 产品能够发现目录遍历漏洞；

6） 产品能够发现路径泄漏、备份文件、源代码泄露、目录浏览和 phpinfo 等信息泄露漏洞；

7） 产品能够发现弱口令等认证方式脆弱漏洞；

8） 产品能够发现文件包含漏洞；

9） 以上同类型漏洞的漏报率、误报率应低于 20％。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.1.3 升级

升级的测评方法如下：

a） 测评方法：

检查产品是否具备漏洞特征库的更新能力。

b） 预期结果：

产品提供漏洞特征库的更新功能。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.1.4 支持 HTTPS

支持 HTTPS 的测评方法如下：

a） 测评方法：

1） 配置产品检测基于 HTTPS 协议的 Web 应用，执行检测任务；

2） 查看检测结果。

b） 预期结果：

产品支持检测基于 HTTPS 协议的 Web 应用。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.1.5 不影响目标对象

不影响目标对象的测评方法如下：

a） 测评方法：

1） 配置产品对 Web 应用进行检测，执行检测任务；

2） 检查产品在检测过程中，是否对 Web 应用和正常访问造成明显影响。

b） 预期结果：

产品在检测过程中未对 Web 应用的正常访问造成明显影响。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.2 检测任务管理

7.1.1.2.1 向导功能

向导功能的测评方法如下：

a) 测评方法：

检查产品在配置过程中是否提供向导功能。

b) 预期结果：

产品在配置过程中提供向导功能。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.2.2 检测范围

检测范围的测评方法如下：

a) 测评方法：

1) 配置检测策略，分别指定检测的 URL 范围，包括指定域名和 URL，执行检测任务，查看检测结果；

2) 配置检测的深度，执行检测任务，查看检测结果；

3) 配置不检测的 URL(如登出、删除等页面)，执行检测任务，查看检测结果。

b) 预期结果：

1) 产品能够根据指定域名和 URL 进行检测，且检测结果未超出定义的范围；

2) 产品能够配置检测的深度，且检测结果未超出定义的深度范围；

3) 产品能够配置不检测的 URL，且检测结果未包括设定的 URL 地址。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.2.3 登录检测

登录检测的测评方法如下：

a) 测评方法：

配置登录检测的策略，执行检测任务，查看检测结果。

b) 预期结果：

产品支持基于登录信息(如基于 Cookie、Session、Token、录制的登录信息等一种或多种方式)对 Web 应用进行检测，并检测结果包括登录后的页面。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.2.4 策略选择

策略选择的测评方法如下：

a) 测评方法：

1） 根据漏洞类型配置产品的检测策略，执行检测任务，查看检测结果；

2） 根据漏洞危害级别配置产品的检测策略，执行检测任务，查看检测结果。

b） 预期结果：

1） 产品能够根据漏洞类型对 Web 应用进行检测，且检测结果未超出定义的范围；

2） 产品能够根据漏洞危害级别对 Web 应用进行检测，且检测结果未超出定义的范围。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.2.5 检测速度调节

检测速度调节的测评方法如下：

a） 测评方法：

检查产品是否能够根据 HTTP 请求速度、检测线程或进程数目等调节检测速度。

b） 预期结果：

产品能够根据 HTTP 请求速度、检测线程或进程数目等调节检测速度。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.2.6 任务定制

任务定制的测评方法如下：

a） 测评方法：

配置产品的批量检测计划任务，执行检测任务，查看检测结果。

b） 预期结果：

产品能够根据计划进行批量检测，且能够自动生成检测结果。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.2.7 进度控制

进度控制的测评方法如下：

a） 测评方法：

1） 在检测过程中，检查是否能够随时停止正在执行的检测任务；

2） 停止后再次启动检测任务，检查产品是否支持断点续扫功能。

b） 预期结果：

1） 产品在检测过程中能够随时停止检测任务；

2） 产品能够支持断点续扫功能。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.3 检测结果分析处理

7.1.1.3.1 结果验证

结果验证的测评方法如下：

a） 测评方法：

1） 配置产品检测策略，执行对 Web 应用漏洞环境的检测任务；
2） 查看检测结果，产品是否针对 XSS 漏洞、SQL 注入点、目录遍历、信息泄露和命令执行等漏洞提供验证参数；
3） 进一步通过验证漏洞检查参数的合理性。

b） 预期结果：
产品提供漏洞的验证参数，能够支持验证 XSS 漏洞、SQL 注入点、目录遍历、信息泄露和命令执行等漏洞。

c） 结果判定：
实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.3.2 结果保存

结果保存的测评方法如下：

a） 测评方法：
1） 检查产品检测结果是否非明文存储；
2） 通过断电重启产品或存储设备等手段，检查是否会造成产品检测结果的丢失。

b） 预期结果：
检测结果非明文保存于掉电非易失性存储介质中。

c） 结果判定：
实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.3.3 统计分析

统计分析的测评方法如下：

a） 测评方法：
1） 执行对 Web 应用漏洞环境的检测任务；
2） 查看产品的统计分析结果，是否包含了漏洞数量、漏洞类型和危害级别的统计分析数据。

b） 预期结果：
产品能够根据检测获取的原始数据对漏洞数量、漏洞类型和危害级别进行统计分析。

c） 结果判定：
实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.3.4 报告生成

报告生成的测评方法如下：

a） 测评方法：
1） 执行产品检测任务；
2） 生成并查看检测报告，检测报告中的漏洞信息是否包括漏洞位置、漏洞名称、漏洞描述和危害级别等详细信息；
3） 检测报告是否包括了漏洞的修复建议。

b） 预期结果：
1） 产品检测报告中的漏洞信息包括了漏洞位置、漏洞名称、漏洞描述和危害级别等信息；
2） 产品检测报告中包括了漏洞的修复建议。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.1.3.5 报告输出

报告输出的测评方法如下：

a) 测评方法：

1) 查看检测报告的导出格式；

2) 查看检测报告的内容，是否便于用户理解。

b) 预期结果：

1) 产品的检测报告支持常用文档格式，如 DOC、PDF 和 HTML 等；

2) 产品的检测报告内容便于用户理解。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2 自身安全测评

7.1.2.1 标识与鉴别

7.1.2.1.1 用户标识

7.1.2.1.1.1 安全属性定义

安全属性定义的测评方法如下：

a) 测评方法：

检查产品是否能够创建用户，并为其赋予标识、隶属组、权限等安全属性。

b) 预期结果：

产品能够为创建的用户配置标识、隶属组、权限等安全属性。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.1.1.2 属性初始化

属性初始化的测评方法如下：

a) 测评方法：

检查产品是否能够对创建的每个用户的属性进行初始化。

b) 预期结果：

产品为创建的每个用户的属性提供初始化的功能。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.1.1.3 唯一性标识

唯一性标识的测评方法如下：

a) 测评方法：

检查产品是否不允许命名同一标识的用户，且在日志中将关于该用户的事件与标识相关联。

b) 预期结果：

产品不允许创建同名用户，且将关于该用户的事件与标识相关联。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.1.2 身份鉴别

7.1.2.1.2.1 用户鉴别

用户鉴别的测评方法如下：

a) 测评方法：

1) 通过所有管理接口尝试登录产品，是否均需进行身份鉴别；

2) 检查是否只有通过身份鉴别后，才能访问授权的安全功能模块；

3) 当正常或非正常(如强行断电)退出后，重新尝试登录产品，是否需进行身份鉴别。

b) 预期结果：

只有通过身份鉴别后才能访问授权的安全功能模块，且无论正常或非正常退出后，重新登录产品均需进行身份鉴别。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.1.2.2 鉴别信息保护

鉴别信息保护的测评方法如下：

a) 测评方法：

检查非授权用户是否能够查阅、修改用户鉴别信息。

b) 预期结果：

产品的非授权用户不能查阅、修改用户鉴别信息。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.2 安全管理

7.1.2.2.1 管理能力

管理能力的测评方法如下：

a) 测评方法：

以授权用户身份登录产品，分别进行查看和修改各种安全属性、启动和关闭安全功能、制定和修改各种安全策略等操作，并检查设置是否生效。

b) 预期结果：

产品的授权用户能够进行查看和修改各种安全属性、启动和关闭安全功能、制定和修改各种安全策略等操作，且设置生效。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.2.2 安全角色管理

安全角色管理的测评方法如下：

a) 测评方法：

1) 产品至少提供两类用户角色，如操作员、审计员；

2） 分别以不同角色身份登录，检查权限是否不同。

b） 预期结果：

产品具备两种以上用户角色，且权限各不相同。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.2.3 远程安全传输

远程安全传输的测评方法如下：

a） 测评方法：

若产品组件间通过网络进行通信，使用协议分析仪截取数据并检查内容是否为非明文。

b） 预期结果：

1） 若产品组件间不通过网络传输数据，则此项为非检测项；

2） 若产品组件间通过网络进行通信，传输数据为非明文。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.3 审计日志

7.1.2.3.1 审计日志生成

审计日志生成的测评方法如下：

a） 测评方法：

1） 尝试进行 6.1.2.3.1 要求的各项操作，触发审计事件；

2） 查看审计日志是否包括事件发生的日期、时间、用户标识、事件描述和结果；

3） 若产品支持远程管理，查看审计日志是否记录管理主机的 IP 地址。

b） 预期结果：

产品能够针对上述事件生成审计日志，日志内容包括事件发生的日期、时间、用户标识、事件描述和结果；同时产品支持远程管理时，审计日志能够记录管理主机的 IP 地址。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.3.2 审计日志保存

审计日志保存的测评方法如下：

a） 测评方法：

通过断电重启产品或日志存储设备等手段，检查是否会造成审计日志的丢失。

b） 预期结果：

断电重启后，产品的审计日志未丢失，存储于掉电非易失性存储介质中。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2.3.3 审计日志管理

审计日志管理的测评方法如下：

a） 测评方法：

1） 分别以授权用户身份和未授权用户身份查看审计日志，检查产品是否仅允许授权用户访问审计日志；
2） 检查产品是否能够对审计日志按操作用户、日期时间和操作类型等条件进行查询和检索；
3） 检查产品是否能够存档和导出审计日志。

b） 预期结果：
1） 产品仅允许授权用户访问审计记录，未授权用户无法查看审计日志；
2） 产品应能按条件查询和检索审计日志，且查询结果准确完整；
3） 产品能够存档和导出审计日志。

c） 结果判定：
实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3 安全保障要求测评

7.1.3.1 开发

7.1.3.1.1 安全架构

安全架构的测评方法如下：

a） 测评方法：
检查开发者提供的安全架构证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：
1） 与产品设计文档中对安全功能的描述范围是否相一致；
2） 是否充分描述产品采取的自我保护、不可旁路的安全机制。

b） 预期结果：
开发者提供的信息应满足 6.1.3.1.1 中所述的要求。

c） 结果判定：
实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.1.2 功能规范

功能规范的测评方法如下：

a） 测评方法：
检查开发者提供的功能规范证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：
1） 是否完整描述 6.1.1、6.1.2 中定义的产品安全功能；
2） 是否描述产品所有安全功能接口的目的、使用方法及相关参数；
3） 是否描述安全功能接口相关的安全功能实施行为；
4） 是否描述由安全功能实施行为处理而引起的直接错误消息。

b） 预期结果：
开发者提供的信息应满足 6.1.3.1.2 中所述的要求。

c） 结果判定：
实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.1.3 产品设计

产品设计的测评方法如下：

a） 测评方法：

检查开发者提供的产品设计证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 是否根据子系统描述产品结构；

2） 是否标识和描述产品安全功能的所有子系统；

3） 是否描述安全功能所有子系统间的相互作用；

4） 提供的对应关系是否能够证实设计中描述的所有行为映射到调用的安全功能接口。

b） 预期结果：

开发者提供的信息应满足 6.1.3.1.3 中所述的要求。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.2 指导性文档

7.1.3.2.1 操作用户指南

操作用户指南的测评方法如下：

a） 测评方法：

检查开发者提供的操作用户指南证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 是否描述用户能够访问的功能和特权，包含适当的警示信息；

2） 是否描述如何以安全的方式使用产品提供的可用接口；

3） 是否描述产品安全功能及接口的用户操作方法，包括配置参数的安全值；

4） 是否标识和描述产品运行的所有可能状态，包括操作导致的失败或者操作性错误；

5） 是否描述实现产品安全目的必需执行的安全策略。

b） 预期结果：

开发者提供的信息应满足 6.1.3.2.1 中所述的要求。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.2.2 准备程序

准备程序的测评方法如下：

a） 测评方法：

检查开发者提供的准备程序证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 是否描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；

2） 是否描述安全安装产品及其运行环境必需的所有步骤。

b） 预期结果：

开发者提供的信息应满足 6.1.3.2.2 中所述的要求。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.3 生命周期支持

7.1.3.3.1 配置管理能力

配置管理能力的测评方法如下：

a) 测评方法：

检查开发者提供的配置管理能力证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1) 检查开发者是否为不同版本的产品提供唯一的标识；

2) 现场检查配置管理系统是否对所有的配置项作出唯一的标识，且对配置项进行了维护；

3) 检查开发者提供的配置管理文档，是否描述了对配置项进行唯一标识的方法。

b) 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.1.3.3.1 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.3.2 配置管理范围

配置管理范围的测评方法如下：

a) 测评方法：

检查开发者提供的配置管理范围证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1) 检查开发者提供的配置项列表；

2) 配置项列表是否描述了组成产品的全部配置项及相应的开发者。

b) 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.1.3.3.2 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.3.3 交付程序

交付程序的测评方法如下：

a) 测评方法：

检查开发者提供的交付程序证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1) 现场检查开发者是否使用规定的交付程序交付产品；

2) 检查开发者是否将交付过程形成文档，文档中是否包含以下内容：在给用户方交付各版本产品时，为维护安全所必需的所有程序。

b) 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.1.3.3.3 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.4 测试

7.1.3.4.1 测试覆盖

测试覆盖的测评方法如下：

a) 测评方法：

检查开发者提供的测试覆盖文档，在测试覆盖证据中，是否表明测试文档中所标识的测试项目与功能规范中所描述的产品安全功能是对应的，检查开发者提供的信息是否满足内容和形式的所有要求。

b) 预期结果：

开发者提供的信息应满足 6.1.3.4.1 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.4.2 功能测试

功能测试的测评方法如下：

a) 测评方法：

检查开发者提供的功能测试证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1) 检查开发者提供的测试文档，是否包括测试计划、预期的测评结果和实际测评结果；

2) 检查测试计划是否标识了要测试的安全功能，是否描述了每个安全功能的测试方案；

3) 检查期望的测评结果是否表明测试成功后的预期输出；

4) 检查实际测评结果是否表明每个被测试的安全功能能按照规定进行运作。

b) 预期结果：

开发者提供的信息应满足 6.1.3.4.2 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.4.3 独立测试

独立测试的测评方法如下：

a) 测评方法：

检查开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致，以用于安全功能的抽样测试，并检查开发者提供的资源是否满足内容和形式的所有要求。

b) 预期结果：

开发者提供的资源应满足 6.1.3.4.3 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3.5 脆弱性评定

脆弱性评定的测评方法如下：

a) 测评方法：

从用户可能破坏安全策略的明显途径出发，按照安全机制定义的安全强度级别，对产品进行脆弱性分析。

b) 预期结果：

测评结果应表明产品能够抵抗基本攻击，能够满足 6.1.3.5 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2 增强级安全技术要求测评

7.2.1 安全功能测评

7.2.1.1 检测能力

7.2.1.1.1 资源发现

资源发现的测评方法如下：

a) 测评方法：

1) 配置产品检测 JavaScript 脚本的页面地址，执行检测任务，查看检测结果；

2) 配置产品检测包括页面文件的 URL 地址，执行检测任务，查看检测结果；

3) 配置产品检测内嵌 URL 的 Flash、**Flex** 地址，执行检测任务，查看检测结果。

b) 预期结果：

1) 产品能够解析和执行 JavaScript 脚本，发现的 URL 比例高于 90%；

2) 产品能够获取页面文件内包括的 URL，发现的 URL 比例高于 90%；

3) 产品能够获取 Flash、**Flex** 中内嵌的 URL，发现的 URL 比例高于 90%。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.1.2 Web 应用漏洞检测

Web 应用漏洞检测的测评方法如下：

a) 测评方法：

1) 配置产品检测策略，执行对 Web 应用漏洞平台（部署 SQL 注入、Cookie 注入、XSS、CSRF、目录遍历、信息泄露、认证方式脆弱、文件包含、命令执行、**第三方组件**、**LDAP 注入和 XPath** 等漏洞）的检测任务；

2) 查看检测结果。

b) 预期结果：

1) 产品能够发现基于 Get、Post 方式提交的字符、数字、搜索等的 SQL 注入漏洞；

2) 产品能够发现基于 Cookie 方式提交的字符、数字、搜索等的 Cookie 注入漏洞；

3) 产品能够发现基于 Get、Post、**Referrer**、**Cookie** 方式的 XSS 漏洞；

4) 产品能够发现 CSRF 漏洞；

5) 产品能够发现目录遍历漏洞；

6) 产品能够发现路径泄露、备份文件、源代码泄露、目录浏览和 phpinfo 等信息泄露漏洞；

7) 产品能够发现**登录绕过**、弱口令等认证方式脆弱漏洞；

8) 产品能够发现文件包含漏洞；

9) **产品能够发现命令执行漏洞**；

10) **产品能够发现第三方组件漏洞**；

11) **产品能够发现 LDAP 注入漏洞**；

12) **产品能够发现 XPath 注入漏洞**；

13) 以上同类型漏洞的漏报率、误报率应低于 20%。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.1.3 变形检测

变形检测的测评方法如下：

a) 测评方法：

1) 配置产品变形检测的配置选项，如大小写随机转换、多种绕过空格限制、空格替换和 URL 编码等；

2) 执行检测任务，查看产品的检测参数。

b) 预期结果：

产品支持漏洞的变形检测。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.1.4 内容检测

内容检测的测评方法如下：

a) 测评方法：

配置产品的检测策略，查看产品是否能够对 Web 系统的非正常内容（包括外链、坏链、暗链和敏感关键字等）进行检测。

b) 预期结果：

产品能够检测 Web 系统的外链、坏链、暗链和敏感关键字等内容。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.1.5 升级

升级的测评方法如下：

a) 测评方法：

1) 检查产品是否具备漏洞特征库的更新能力；

2) 检查产品保证升级时效性的安全机制，如自动升级、更新通知等。

b) 预期结果：

1) 产品提供漏洞特征库的更新功能；

2) 产品采取安全机制保证漏洞特征库升级的时效性。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.1.6 支持 HTTPS

支持 HTTPS 的测评方法如下：

a) 测评方法：

1) 配置产品检测基于 HTTPS 协议的 Web 应用，执行检测任务；

2) 查看检测结果。

b) 预期结果：

产品支持检测基于 HTTPS 协议的 Web 应用。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.1.7 不影响目标对象

不影响目标对象的测评方法如下：

a) 测评方法：

1) 配置产品对 Web 应用进行检测，执行检测任务；

2) 检查产品在检测过程中，是否对 Web 应用的正常访问造成明显影响。

b) 预期结果：

产品在检测过程中未对 Web 应用的正常访问造成明显影响。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.2 检测任务管理

7.2.1.2.1 向导功能

向导功能的测评方法如下：

a) 测评方法：

检查产品在配置过程中是否提供向导功能。

b) 预期结果：

产品在配置过程中提供向导功能。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.2.2 检测范围

检测范围的测评方法如下：

a) 测评方法：

1) 配置检测策略，分别制定检测的 URL 范围，包括域名和 URL，执行检测任务，查看检测结果；

2) 配置检测的深度，执行检测任务，查看检测结果；

3) 配置不检测的 URL(如登出、删除等页面)，执行检测任务，查看检测结果；

4) **配置路径模式排重和大小写区分，执行检测任务，查看检测结果**。

b) 预期结果：

1) 产品能够根据指定的 URL、当前域、整个域、IP 地址进行检测，且检测结果未超出定义的范围；

2) 产品能够配置检测的深度，且检测结果未超出定义的深度范围；

3) 产品能够配置不检测的 URL，且检测结果未包括设定的 URL 地址；

4) **产品能够配置路径模式排重和大小写区分，且检测结果准确**。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.2.3 登录检测

登录检测的测评方法如下：

a) 测评方法：

配置登录检测的策略，执行检测任务，查看检测结果。

b) 预期结果：

产品支持基于登录信息(基于 Cookie、Session、Token、录制的登录信息等一种或多种方式)对 Web 应用进行检测，并检测结果包括登录后的页面。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.2.4 检测策略

7.2.1.2.4.1 策略选择

策略选择的测评方法如下：

a) 测评方法：

1） 根据漏洞类型配置产品的检测策略，执行检测任务，查看检测结果；

2） 根据漏洞危害级别配置产品的检测策略，执行检测任务，查看检测结果；

3） **根据 Web 系统指纹信息配置产品的检测策略，执行检测任务，查看检测结果。**

b） 预期结果：

1） 产品能够根据漏洞类型对 Web 应用进行检测，且检测结果未超出定义的范围；

2） 产品能够根据漏洞危害级别对 Web 应用进行检测，且检测结果未超出定义的范围；

3） **产品能够根据 Web 系统指纹信息对 Web 应用进行检测，且检测结果未超出定义的范围。**

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.2.4.2 策略扩展

策略扩展的测评方法如下：

a） **测评方法：**

检查产品是否能够自定义检测策略。

b） **预期结果：**

产品能够自定义检测策略。

c） **结果判定：**

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.2.5 检测速度调节

检测速度调节的测评方法如下：

a） 测评方法：

1） 检查产品是否能够根据 HTTP 请求速度、检测线程或进程数目等调节检测速度；

2） **检查产品是否支持分布式部署检测引擎；**

3） **检查产品是否支持多引擎负载均衡。**

b） 预期结果：

1） 产品能够根据 HTTP 请求速度、检测线程或进程数目等调节检测速度；

2） **产品支持分布式部署检测引擎；**

3） **产品支持多引擎负载均衡。**

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.2.6 任务定制

任务定制的测评方法如下：

a） 测评方法：

配置产品的批量、**定时、定时间段和周期性**检测计划任务，执行检测任务，查看检测结果。

b） 预期结果：

产品能够根据计划进行批量、**定时、定时间段和周期性**检测，且能够自动生成检测结果。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.2.7 进度控制

进度控制的测评方法如下：

a) 测评方法：

1) 在检测过程中，检查是否能够随时停止正在执行的检测任务；

2) 停止后再次启动检测任务，检查产品是否支持断点续扫功能；

3) **在检测过程中，检查产品是否能够导出已检测的内容结果报告。**

b) 预期结果：

1) 产品在检测过程中能够随时停止检测任务；

2) 产品能够支持断点续扫功能；

3) **产品在检测过程中能够导出已检测的内容结果报告。**

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.3 检测结果分析处理

7.2.1.3.1 结果验证

结果验证的测评方法如下：

a) 测评方法：

1) 配置产品检测策略，执行对 Web 应用漏洞环境的检测任务；

2) 查看漏洞检测结果，产品是否针对 XSS 漏洞、SQL 注入点、目录遍历、信息泄露和命令执行等漏洞提供验证参数；

3) 进一步通过验证漏洞检查参数的合理性；

4) **检查产品是否提供自动化工具验证漏洞。**

b) 预期结果：

1) 产品提供漏洞的验证参数，能够支持验证 XSS 漏洞、SQL 注入点、目录遍历、信息泄露和命令执行等安全漏洞；

2) **产品提供自动化工具对漏洞进行验证。**

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.3.2 结果保存

结果保存的测评方法如下：

a) 测评方法：

1) 检查产品检测结果是否非明文存储；

2) 通过断电重启产品或存储设备等手段，检查是否会造成产品检测结果的丢失。

b) 预期结果：

检测结果非明文保存于掉电非易失性存储介质中。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.3.3 统计分析

统计分析的测评方法如下：

a) 测评方法：

1) 执行对 Web 应用漏洞环境的检测任务；

2) 查看产品的统计分析结果，是否包含了漏洞数量、漏洞类型和危害级别的统计分析数据。

b） 预期结果：

产品能够根据检测获取的原始数据对漏洞数量、漏洞类型和危害级别进行统计分析。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.3.4 报告生成

报告生成的测评方法如下：

a） 测评方法：

1） 执行产品检测任务；

2） 生成并查看检测报告，检测报告中的漏洞信息是否包括漏洞位置、漏洞名称、漏洞描述和危害级别等详细信息；

3） 检测报告是否包括了漏洞的修复建议；

4） **检测报告是否包括行业合规内容（如 OWASP TOP10）；**

5） **检查产品是否支持编辑和自定义设计报告，添加自定义注释或详细信息；**

6） **检查产品是否支持批量导出报告，是否能够根据横向、纵向比较的趋势分析报告。**

b） 预期结果：

1） 产品检测报告中的漏洞信息包括了漏洞位置、漏洞名称、漏洞描述和危害级别等信息；

2） 产品检测报告中包括了漏洞的修复建议；

3） **产品检测报告包括行业合规内容；**

4） **产品支持编辑和自定义设计报告，添加自定义注释或详细信息，能够为技术人员修复安全缺陷提供帮助；**

5） **产品支持批量导出报告，能够根据横向、纵向比较的趋势分析报告。**

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.3.5 报告输出

报告输出的测评方法如下：

a） 测评方法：

1） 查看检测报告的导出格式；

2） 查看检测报告的内容，是否便于用户理解。

b） 预期结果：

1） 产品的检测报告支持常用文档格式，如 DOC、PDF 和 HTML 等；

2） 产品的检测报告内容便于用户理解。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.1.4 互动性要求

互动性要求的测评方法如下：

a） **测评方法：**

查看厂商提供的接口文档。

b） **预期结果：**

产品厂商提供的文档清晰的说明了接口调用的方法。

c） **结果判定：**

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2 自身安全测评

7.2.2.1 标识与鉴别

7.2.2.1.1 用户标识

7.2.2.1.1.1 安全属性定义

安全属性定义的测评方法如下：

a) 测评方法：

检查产品是否能够创建用户，并为其赋予标识、隶属组、权限等安全属性。

b) 预期结果：

产品能够为创建的用户配置标识、隶属组、权限等安全属性。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.1.1.2 属性初始化

属性初始化的测评方法如下：

a) 测评方法：

检查产品是否能够对创建的每个用户的属性进行初始化。

b) 预期结果：

产品为创建的每个用户的属性提供初始化的功能。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.1.1.3 唯一性标识

唯一性标识的测评方法如下：

a) 测评方法：

检查产品是否不允许命名同一标识的用户，且在日志中将关于该用户的事件与标识相关联。

b) 预期结果：

产品不准许创建同名用户，且将关于该用户的事件与标识相关联。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.1.2 身份鉴别

7.2.2.1.2.1 用户鉴别

用户鉴别的测评方法如下：

a) 测评方法：

1) 通过所有管理接口尝试登录产品，是否均需进行身份鉴别；

2) 检查是否只有通过身份鉴别后，才能访问授权的安全功能模块；

3) 当正常或非正常(如强行断电)退出后，重新尝试登录产品，是否需进行身份鉴别。

b) 预期结果：

只有通过身份鉴别后才能访问授权的安全功能模块，且无论正常或非正常退出后，重新登录产

品均需进行身份鉴别。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.1.2.2 鉴别信息保护

鉴别信息保护的测评方法如下：

a) 测评方法：

检查非授权用户是否能够查阅、修改用户鉴别信息。

b) 预期结果：

产品的非授权用户不能查阅、修改用户鉴别信息。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.1.2.3 鉴别失败处理

鉴别失败处理的测评方法如下：

a) 测评方法：

1) 尝试连续失败登录产品，次数到达产品设定值；

2) 检查产品是否能够终止用户的访问。

b) 预期结果：

若登录失败次数到达设定值，产品能够终止用户的访问。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.1.2.4 超时锁定或注销

超时锁定或注销的测评方法如下：

a) 测评方法：

1) 以授权用户身份登录产品设置最大超时时间，并在设定的时间段内不进行任何操作；

2) 检查产品是否能够终止会话，再次登录是否需重新进行身份鉴别。

b) 预期结果：

产品具备登录超时锁定或注销功能，且最大超时时间仅由授权用户设定。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.2 安全管理

7.2.2.2.1 管理能力

管理能力的测评方法如下：

a) 测评方法：

以授权用户身份登录产品，分别进行查看和修改各种安全属性、启动和关闭安全功能、制定和修改各种安全策略等操作，并检查设置是否生效。

b) 预期结果：

产品的授权用户能够进行查看和修改各种安全属性、启动和关闭安全功能、制定和修改各种安全策略等操作，且设置生效。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.2.2 安全角色管理

安全角色管理的测评方法如下：

a) 测评方法：

1) 产品至少提供两类用户角色，如操作员、审计员；

2) 分别以不同角色身份登录，检查权限是否不同；

3) **检查产品是否能够根据功能模块定义用户角色，并分别以不同角色身份登录，检查权限是否不同。**

b) 预期结果：

1) 产品具备两种以上用户角色，且权限各不相同；

2) **产品能够根据功能模块定义不同的用户角色。**

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.2.3 远程安全传输

远程安全传输的测评方法如下：

a) 测评方法：

若检测结果通过网络传输时，使用协议分析仪截取数据并检查内容是否为非明文。

b) 预期结果：

1) 若产品组件间不通过网络传输数据，则此项为非检测项；

2) 若当产品组件间通过网络进行通信，传输数据为非明文。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.2.4 管理主机限制

管理主机限制的测评方法如下：

a) **测评方法：**

若产品具备远程管理功能，登录产品限制远程管理主机的 IP 地址，并分别使用受限和未受限的主机进行尝试登录。

b) **预期结果：**

1) **若产品未提供远程管理功能，则此项为非检测项；**

2) **若产品提供远程管理功能，且受限主机无法登录产品，而未受限主机能够正常访问。**

c) **结果判定：**

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.3 审计日志

7.2.2.3.1 审计日志生成

审计日志生成的测评方法如下：

a) 测评方法：

1) 尝试进行 6.2.2.3.1 要求的操作，触发审计事件；

2） 查看审计日志是否包括事件发生的日期、时间、用户标识、事件描述和结果；

3） 若产品支持远程管理，查看审计日志是否记录管理主机的 IP 地址。

b） 预期结果：

产品能够针对上述事件生成审计日志，日志内容包括事件发生的日期、时间、用户标识、事件描述和结果；同时产品支持远程管理时，审计日志能够记录管理主机的 IP 地址。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.3.2 审计日志保存

审计日志保存的测评方法如下：

a） 测评方法：

通过断电重启产品或日志存储设备等手段，检查是否会造成审计日志的丢失。

b） 预期结果：

断电重启后，产品的审计日志未丢失，存储于掉电非易失性存储介质中。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2.3.3 审计日志管理

审计日志管理的测评方法如下：

a） 测评方法：

1） 分别以授权用户身份和未授权用户身份查看审计日志，检查产品是否仅允许授权用户访问审计日志；

2） 检查产品是否能够对审计日志按条件进行查询；

3） 检查产品是否能够存档和导出审计日志。

b） 预期结果：

1） 产品仅允许授权用户访问审计记录，未授权用户无法查看审计日志；

2） 产品应能按条件查询审计日志，且查询结果准确完整；

3） 产品能够存档和导出审计日志。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3 安全保障要求测评

7.2.3.1 开发

7.2.3.1.1 安全架构

安全架构的测评方法如下：

a） 测评方法：

检查开发者提供的安全架构证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1） 与产品设计文档中对安全功能的描述范围是否相一致；

2） 是否充分描述产品采取的自我保护、不可旁路的安全机制。

b） 预期结果：

开发者提供的信息应满足 6.2.3.1.1 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.1.2 功能规范

功能规范的测评方法如下：

a) 测评方法：

检查开发者提供的功能规范证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1) 是否完整描述 6.2.1、6.2.2 中定义的功能；

2) 是否描述产品所有安全功能接口的目的、使用方法及相关参数；

3) **描述安全功能实施过程中，是否描述与安全功能接口相关的所有行为；**

4) **是否描述可能由安全功能接口的调用而引起的所有直接错误消息。**

b) 预期结果：

开发者提供的信息应满足 6.2.3.1.2 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.1.3 产品设计

产品设计的测评方法如下：

a) 测评方法：

检查开发者提供的产品设计证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1) 是否根据子系统描述产品结构；

2) 是否标识和描述产品安全功能的所有子系统；

3) 是否描述安全功能所有子系统间的相互作用；

4) 提供的对应关系是否能够证实设计中描述的所有行为映射到调用的安全功能接口；

5) **是否根据模块描述安全功能；**

6) **是否描述所有模块的安全功能要求相关接口、接口的返回值、与其他模块间的相互作用及调用的接口；**

7) **是否提供模块和子系统间的对应关系。**

b) 预期结果：

开发者提供的信息应满足 6.2.3.1.3 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.1.4 实现表示

实现表示的测评方法如下：

a) 测评方法：

检查开发者提供的实现表示证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1) 是否通过软件代码、设计数据等实例详细定义产品安全功能；

2) 是否提供实现表示与产品设计描述间的对应关系。

b) 预期结果：

开发者提供的信息应满足 6.2.3.1.4 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.2 指导性文档

7.2.3.2.1 操作用户指南

操作用户指南的测评方法如下：

a) 测评方法：

检查开发者提供的操作用户指南证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1) 是否描述用户能够访问的功能和特权，包含适当的警示信息；
2) 是否描述如何以安全的方式使用产品提供的可用接口；
3) 是否描述产品安全功能及接口的用户操作方法，包括配置参数的安全值；
4) 是否标识和描述产品运行的所有可能状态，包括操作导致的失败或者操作性错误；
5) 是否描述实现产品安全目的必需执行的安全策略。

b) 预期结果：

开发者提供的信息应满足 6.2.3.2.1 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.2.2 准备程序

准备程序的测评方法如下：

a) 测评方法：

检查开发者提供的准备程序证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1) 是否描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
2) 是否描述安全安装产品及其运行环境必需的所有步骤。

b) 预期结果：

开发者提供的信息应满足 6.2.3.2.2 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.3 生命周期支持

7.2.3.3.1 配置管理能力

配置管理能力的测评方法如下：

a) 测评方法：

检查开发者提供的配置管理能力证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1) 检查开发者是否为不同版本的产品提供唯一的标识；
2) 现场检查配置管理系统是否对所有的配置项作出唯一的标识，且对配置项进行了维护；
3) 检查开发者提供的配置管理文档，是否描述了对配置项进行唯一标识的方法；
4) 现场检查是否能够通过自动化配置管理系统支持产品的生成，是否仅通过自动化措施对

配置项进行授权变更；

5） 检查配置管理计划是否描述了用来接受修改过的或新建的作为产品组成部分的配置项的程序；

6） 检查配置管理计划是否描述如何使用配置管理系统开发产品，现场核查活动是否与计划一致。

b） 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.2.3.3.1 中所述的要求。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.3.2 配置管理范围

配置管理范围的测评方法如下：

a） 测评方法：

检查开发者提供的配置管理范围证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1） 检查开发者提供的配置项列表；

2） 配置项列表是否描述了组成产品的全部配置项及相应的开发者；

3） 检查开发者是否将实现表示、安全缺陷报告及其解决状态纳入配置管理范围，是否对安全缺陷进行跟踪。

b） 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.2.3.3.2 中所述的要求。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.3.3 交付程序

交付程序的测评方法如下：

a） 测评方法：

检查开发者提供的交付程序证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1） 现场检查开发者是否使用规定的交付程序交付产品；

2） 检查开发者是否将交付过程形成文档，文档中是否包含以下内容：在给用户方交付各版本产品时，为维护安全所必需的所有程序。

b） 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.2.3.3.3 中所述的要求。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.3.4 开发安全

开发安全的测评方法如下：

a） 测评方法：

检查开发者提供的开发安全证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1） 检查开发者提供的开发安全文档，该文档是否描述在系统的开发环境中，为保护系统设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施；

2） 现场检查产品的开发环境，开发者是否使用了物理的、程序的、人员的和其他方面的安全

措施保证产品设计和实现的保密性和完整性，这些安全措施是否得到了有效的执行。

b) 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.2.3.3.4 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.3.5 生命周期定义

生命周期定义的测评方法如下：

a) 测评方法：

检查开发者提供的生命周期定义证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1) 现场检查开发者是否使用生命周期模型对产品的开发和维护进行的必要控制；

2) 检查开发者提供生命周期定义文档是否描述了用于开发和维护产品的模型。

b) 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.2.3.3.5 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.3.6 工具和技术

工具和技术的测评方法如下：

a) 测评方法：

检查开发者提供的工具和技术证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1) 现场检查开发者所是否明确定义用于开发产品的工具；

2) 是否提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

b) 预期结果：

开发者提供的信息和现场活动证据内容应满足 6.2.3.3.6 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.4 测试

7.2.3.4.1 测试覆盖

测试覆盖的测评方法如下：

a) 测评方法：

检查开发提供的测试覆盖证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1) 检查开发者提供的测试覆盖文档，在测试覆盖证据中，是否表明测试文档中所标识的测试项目与功能规范中所描述的产品安全功能是对应的；

2) 检查开发者提供的测试覆盖分析结果，是否表明功能规范中的所有安全功能接口都进行了测试。

b) 预期结果：

开发者提供的信息应满足 6.2.3.4.1 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.4.2 测试深度

测试深度的测评方法如下：

a) 测评方法：

检查开发者提供的测试深度证据，并检查开发者提供的信息是否满足证据的内容和形式的所有要求：

1) 检查开发者提供的测试深度分析，是否说明了测试文档中所标识的对安全功能的测试，并足以表明与产品设计中的安全功能子系统和模块之间的对应性；

2) 是否能够证实所有安全功能子系统、模块都已经进行过测试。

b) 预期结果：

开发者提供的信息应满足 6.2.3.4.2 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.4.3 功能测试

功能测试的测评方法如下：

a) 测评方法：

检查开发者提供的功能测试证据，并检查开发者提供的信息是否满足内容和形式的所有要求：

1) 检查开发者提供的测试文档，是否包括测试计划、预期的测评结果和实际测评结果；

2) 检查测试计划是否标识了要测试的安全功能，是否描述了每个安全功能的测试方案；

3) 检查期望的测评结果是否表明测试成功后的预期输出；

4) 检查实际测评结果是否表明每个被测试的安全功能能按照规定进行运作。

b) 预期结果：

开发者提供的信息应满足 6.2.3.4.3 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.4.4 独立测试

独立测试的测评方法如下：

a) 测评方法：

检查开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致，以用于安全功能的抽样测试，并检查开发者提供的资源是否满足内容和形式的所有要求。

b) 预期结果：

开发者提供的信息应满足 6.2.3.4.4 中所述的要求。

c) 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.2.3.5 脆弱性评定

脆弱性评定的测评方法如下：

a) 测评方法：

从用户可能破坏安全策略的明显途径出发，按照安全机制定义的安全强度级别，对产品进行脆弱性分析。

b） 预期结果：

渗透性测评结果应表明产品能够抵抗增强攻击，能够满足 6.2.3.5 中所述的要求。

c） 结果判定：

实际测评结果与预期结果一致则判定为符合，其他情况判定为不符合。

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 Web 应用安全检测
系统安全技术要求和测试评价方法
GB/T 37931—2019
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019 年 7 月第一版
*
书号:155066·1-63263

GB/T 37931-2019