



中华人民共和国国家标准

GB/T 32917—2016

信息安全技术 WEB 应用防火墙 安全技术要求与测试评价方法

Information security technology—
Security technique requirements and testing and evaluation approaches
for WEB application firewall

2016-08-29 发布

2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

| | |
|----------------------------|-----|
| 前言 | III |
| 引言 | IV |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语、定义和缩略语 | 1 |
| 3.1 术语和定义 | 1 |
| 3.2 缩略语 | 1 |
| 4 安全技术要求 | 2 |
| 4.1 基本级 | 2 |
| 4.1.1 安全功能要求 | 2 |
| 4.1.2 自身安全保护 | 3 |
| 4.1.3 安全保障要求 | 4 |
| 4.2 增强级 | 7 |
| 4.2.1 安全功能要求 | 7 |
| 4.2.2 自身安全保护 | 9 |
| 4.2.3 安全保障要求 | 10 |
| 4.3 性能要求 | 13 |
| 4.3.1 HTTP 吞吐量 | 13 |
| 4.3.2 HTTP 最大请求速率 | 13 |
| 4.3.3 HTTP 最大并发连接数 | 13 |
| 5 测试评价方法 | 13 |
| 5.1 测试环境 | 13 |
| 5.2 基本级 | 15 |
| 5.2.1 安全功能要求测试评价方法 | 15 |
| 5.2.2 自身安全保护测试评价方法 | 18 |
| 5.2.3 安全保障要求测试评价方法 | 20 |
| 5.3 增强级 | 25 |
| 5.3.1 安全功能要求测试评价方法 | 25 |
| 5.3.2 自身安全保护测试评价方法 | 28 |
| 5.3.3 安全保障要求测试评价方法 | 32 |
| 5.4 性能测试评价方法 | 37 |
| 5.4.1 HTTP 吞吐量 | 37 |
| 5.4.2 HTTP 最大请求速率 | 37 |
| 5.4.3 HTTP 最大并发连接数 | 37 |
| 6 WEB 应用防火墙安全技术要求分级表 | 38 |
| 参考文献 | 40 |

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、上海天泰网络技术有限公司、北京神州绿盟科技有限公司、北京中软华泰信息技术有限责任公司。

本标准主要起草人:邱梓华、张艳、顾健、胡亚兰、叶志强、李从宇、宋万龙、俞优、程胜年、罗宇、任浩、张笑笑、宋好好、吴其聪。

引 言

本标准包含两部分内容,一部分是 WEB 应用防火墙的安全技术要求,用以指导设计者如何设计和实现 WEB 应用防火墙;另一部分是依据技术要求,提出了具体的测试评价方法,用以指导评估者对 WEB 应用防火墙评估,同时也为 WEB 应用防火墙的开发者提供测试参考。

本标准将 WEB 应用防火墙划分为 2 个等级:基本级和增强级。为清晰表示增强级相较于基本级的安全技术要求的增加和增强,在第 4 章、第 5 章的描述中,增强级的新增部分用“**宋体加粗**”表示。在第 6 章 WEB 应用防火墙安全技术要求分级表中,以表格形式列举了基本级和增强级的差异。

信息安全技术 WEB 应用防火墙

安全技术要求与测试评价方法

1 范围

本标准规定了 WEB 应用防火墙的安全功能要求、自身安全保护要求、性能要求和安全保障要求，并提供了相应的测试评价方法。

本标准适用于 WEB 应用防火墙的设计、生产、检测及采购。

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 25069—2010 信息安全技术 术语

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1.1

WEB 应用防火墙 WEB application firewall

是根据预先定义的过滤规则和安全防护规则，对所有 WEB 服务器的访问请求和 WEB 服务器的响应进行协议和内容过滤，对 WEB 服务器及 WEB 应用实现安全防护功能的信息安全产品。

3.1.2

WEB 服务器 WEB server

Web 服务器是向发出请求的客户端(如浏览器)提供服务的程序。当 Web 浏览器(客户端)连到服务器上并请求资源时，服务器将处理该请求并将资源发送到该浏览器上。Web 服务器使用 HTTP 与 Web 浏览器进行信息交流。常用的 Web 服务器有 Apache 和 Internet 信息服务器。

3.1.3

WEB 应用 WEB application

基于 WEB 服务器软件，为用户提供具体业务应用的程序或文件。

3.2 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 | 安全超文本传输协议 | (Hypertext Transfer Protocol over Secure Socket Layer) |
| SSL | 安全套接层协议 | (Secure Socket Layer) |
| SQL | 结构化查询语言 | (Structured Query Language) |