ICS 35.040
L 80

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

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)