ICS 35.240
A 90

GA

# 中华人民共和国公共安全行业标准

GA/T 1140—2014

# 信息安全技术
# web 应用防火墙安全技术要求

**Information security technology—**
**Security technical requirements for web application firewall**

2014-03-12 发布　　2014-03-12 实施

中华人民共和国公安部　　发 布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、杭州安恒信息技术有限公司、神州数码网络(北京)有限公司、北京安氏领信科技发展有限公司、北京神州绿盟信息安全科技股份有限公司、蓝盾信息安全技术股份有限公司、上海天泰网络技术有限公司、公安部第三研究所。

本标准主要起草人：俞优、陆臻、李毅、顾健、张笑笑、张艳、杨元原、范渊、孙小平、黄坚、高继明、秦波、杨育斌、叶志强。

# 引　言

本标准详细描述了与web应用防火墙安全环境相关的假设、威胁和组织安全策略，定义了web应用防火墙及其支撑环境的安全目的，论证了安全功能要求能够追溯并覆盖产品安全目的，安全目的能够追溯并覆盖安全环境相关的假设、威胁和组织安全策略。

本标准基本级参照了GB/T 18336.3—2008中规定的EAL2级安全保证要求，增强级在EAL4级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

本标准仅给出了web应用防火墙应满足的安全技术要求，但对web应用防火墙的具体技术实现方式、方法等不做要求。

# 信息安全技术
# web 应用防火墙安全技术要求

## 1 范围

本标准规定了 web 应用防火墙的安全功能要求、安全保证要求及等级划分要求。

本标准适用于 web 应用防火墙的设计、开发及检测。

## 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 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336—2008(所有部分) 信息技术 安全技术 信息技术安全性评估准则

GB/T 25069—2010 信息安全技术 术语

## 3 术语和定义

GB 17859—1999、GB/T 18336—2008(所有部分)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 应用防火墙 web application firewall**

部署于 web 客户端和 web 服务器之间，通过分析 web 应用层的通信，根据预先定义的过滤规则和防护策略，实现对 web 应用保护的产品。

3.2

**SQL 注入 SQL injection**

把 SQL 命令插入到 web 表单递交或者页面请求的参数中，以达到欺骗服务器执行恶意 SQL 命令目的的行为。

3.3

**跨站脚本 cross site scripting**

恶意攻击者往 web 页面里插入恶意 HTML 代码，当用户浏览该页面时，嵌入 web 页面里面的 HTML 代码会被执行，从而达到恶意攻击用户目的的行为。

3.4

**旁路功能 bypass function**

当 web 应用防火墙出现异常情况时(断电、故障等)，能够让连接在 web 应用防火墙上的网络相互导通。

## 4 缩略语

下列缩略语适用于本文件。