WEB 应用防火墙测评基准

VER 1.0

作者：OWASP 中国 WAF 项目组

目录

WEB 应用防火墙测评基准介绍

Web 应用防火墙是通过执行一系列针对 HTTP/https 的安全策略来专门为 web 应用提供保护的产品，本文档描述了 Web 应用防火墙产品（以下简称 WAF）的测试参考基准。

WAF 测评基准项目起源于 OWASP 2010 WAF 测评项目，结合国内外安全测评的基准、Web 安全测试方法、渗透测试等一系列资料，于 2012 年正式推出 WAF 测评基准。

除本文件的特别要求外，除非另有说明，在安装和配置的过程中，所测试的 web 应用防火墙产品必须符合该文档的要求，同时产品在安装前后及整个过程都必须符合要求。

参照词汇表了解该文档中的专业术语。

参考资料：

《Nsslab WAF 测评标准》

《OWASP Web Application Firewall Certification Criteria》

说明

概述：请确认厂商提供了足够的文件说明，确保管理人员能正确、安全的安装和管理、测试 WAF 产品。

安装文档：

测试设备 WAF 必须包含下列信息（书面或电子版）：

A. WAF 安装指引

B. WAF 所有组件的最低系统要求

C. 默认设置（例如：用户名、密码、IP 地址等等）

D. WAF 产品的所有软件和防火墙组件的基本版本

E. 提供厂商技术支持

管理文档

WAF 必需包含书面或电子版的管理和维护文档

1 基础功能测试

概述：验证被测 Web 应用防火墙产品提供的服务运行良好，以达到用户的预期希望。任何有疑义的地方都将被测试，验证其真实性和准确性！

1.1 测试策略

被测 Web 应用防火墙产品必需进行不可避免的各类测试

1.2 防护策略

被测 Web 应用防火墙产品执行任一项安全策略时，必需保障被防护系统的正常运行

1.3 数据完整性

所有通过 Web 应用防火墙的数据，必须保证其完整性

1.4 数据保密性

被测 Web 应用防火墙产品必须通过测试，证明它能够被配置为保留原始所有机密数据的性能。

1.5 用户认证：

被测 Web 应用防火墙产品支持补充用户身份验证，必须通过测试以证明它能够正确使用认证机制来验证任何试图访问受保护网络资源的用户

1.6 用户授权

被测 Web 应用防火墙产品支持补充的用户身份验证，必须通过测试，只允许用户访问经过授权的资源。

2 WAF 防御功能

2.1 网络攻击的保护和预防

被测 Web 应用防火墙产品必需包含基本的配置，用来防护 OWASP TOP 10 Web 漏洞，并且不会对所保护的网站有负面影响，包含但不限于以下分类/漏洞：

- 缓冲区溢出
- SQL 注入/代码注入
- 跨站脚本
- 跨站伪造请求
- 身份认证
- 不当输入验证
- 拒绝服务
- 会话管理不善
- 无效的应用资源保护/信息泄露
- 错误存取控制/认证编码

2.2 防护策略

被测 Web 应用防火墙可以通过配置的安全防护策略，来阻断 Web 攻击。

- 网址重写/标准化：被测 Web 应用防火墙产品必需可以利用网址的标准化和重写来防止恶意攻击
- 主动学习：被测 Web 应用防火墙产品必需有主动的学习机制以扩大网站应用保护，并且不会对被保护的网站应用产生负面的功能影响。

2.3 隐藏内部网络结构

被测 Web 应用防火墙必须能够隐藏内部网络应用架构、结构和命名。

2.4 SSL 支持

被测 Web 应用防火墙产品必需支持网站交易数据的加密。

2.5 透明服务

被测 Web 应用防火墙产品必需能透传执行安全政策以外的网络应用程序。

2.6 协议配置

被测 Web 应用防火墙产品必须可以配置在协议层提供网络流量控制，包括支持断点续传，编码方法/类型，协议验证以及配置协议等参数如要求，响应和 header 长度。

3 WAF 自身安全测试

3.1 管理端安全

被测 Web 应用防火墙产品必需通过测试，证明不能获得未经授权的管理功能

3.2 攻击测试

被测 Web 应用防火墙产品必需通过测试，证明它是不易受攻击

被测 Web 应用防火墙产品集成了第三方操作系统（如 Microsoft © Windows ™, *NIX），被测 Web 应用防火墙产品必须提供合理和适当的措施保护主机操作系统免受任何攻击。

3.3 拒绝服务

被测 Web 应用防火墙产品必需通过测试，证明该设备不会因任何拒绝服务攻击而宕机

被测 Web 应用防火墙产品必须保证在标称的性能范围内正常工作。

4 WAF 性能测试

验证 WAF 实际性能与标称性能之间的差距，性能测试重要指标参数包括：

A. WAF 实际 HTTP/HTTPS 流量承载能力

B. WAF 支持最大 HTTP 并发连接数

C. WAF 支持最大 HTTP 新建连接数

D. WAF 在不同性能下的检测率

注意：所有的测试项目在不影响业务正常访问情况下进行，需考虑网站的延迟率;

所有的测试项目，均采用真实的网站（google、facebook 等）访问流量进行测试

4.1 流量测试

验证被测 WAF 实际 HTTP 流量与标称 HTTP 流量的比值不小于 60%，其延迟率小于 250ms

4.2 最大并发连接数

测试 WAF 实际的最大 HTTP 并发连接数

4.3 最大新建连接数

测试 WAF 实际的最大 HTTP 新建连接数

4.4 负载下 WAF 检测率

测试 HTTP 流量分别为 10%、50%、100%情况下，WAF 对攻击的检测以及防御能力

5 日志功能

验证被测 Web 应用防火墙产品有能力给管理员提供用于审核安全相关事件的必要方法。捕捉到的日志数据能够给管理员提供足够的信息，以此来检测可能影响被测 Web 应用防火墙产品自身安全和数据完整性的事件，以及它用来保护的网站情况。

5.1 日志事件

被测 Web 应用防火墙产品必需默认记录以下所有事件类型

A. 所有试图访问被保护对象的成功或失败行为

B. 所有成功和失败的尝试身份验证都将被重定向到指定页面

C. 每一次系统启动

D. 所有对 WAF 的修改行为

5.2 日志数据

对于每一个被测 Web 应用防火墙，下面的日志数据，必需可以在日志上找到：

A. 日期和时间

1. 被测 Web 应用防火墙产品记录的每条日志数据必需由四位数的年份、月份和日期组成

2. 被测 Web 应用防火墙产品记录的每条日志时间必需小时、分、秒组成

B. IP 源地址或主机名称

C. 目的 IP 地址和主机名称

D. 源端口

E. 目的端口

F. 服务名称或协议（HTTP,HTTPS）

G. 通用网址（路径、参数）

H. HTTP 方法（获取，post）

I. 会话识别（依据被测 Web 应用防火墙产品）

J. 配置事项（例如：允许、拒绝）

K. 失败原因，如果拒绝访问

L. 用户识别，适用范围

M. 安全策略的描述

N. 在管理接口成功验证和失败验证的说明（失败的验证需包含失败原因）

O. 所有日志数据必须准确无误

5.3 准确的日志数据

所有被被测 Web 应用防火墙产品捕捉到的数据必需准确无误。

被测 Web 应用防火墙产品记录的时间和日期必需确切反应该事件发生的时间（精确到秒）

5.4 标准日志格式

被测 Web 应用防火墙产品必须至少产生一个行业标准日志格式（例如：W3C, syslog 等等）输出到外部应用程序（应用水平取证工具，应用漏洞扫描器，等等）

5.5 连接多个日志文件为单一事件

被测 Web 应用防火墙产品使用多项日志信息记录一项日志事件时，每一条日志信息必须清晰、准确地表达相应日志信息之间的联系。

5.6 遵守用户隐私

被测 Web 应用防火墙产品必须能够识别和屏蔽敏感的、机密的或是私人领域的日志，这些领域都会被管理员界定

5.7 取证功能

被测 Web 应用防火墙产品必须能够提供应用程序级取证功能，包括调查、分析与之相关的事件

6 WAF 管理

6.1 管理界面

被测 Web 应用防火墙产品必需有一个安全管理界面，通过这个界面管理员可以操控所有的管理功能。此界面不能被证明是不安全的，它必需能够控制界面并且可以行使所有的管理功能，包括：

A. 设置和更改安全策略

B. 配置和更改管理用户认证信息

C. 配置和更改远程管理设置，如果适用的话

D. 配置、更改或获取时间和日期

E. 启用所需的日志事件

F. 审查所需的日志数据

6.2 管理功能测试

被测 Web 应用防火墙产品必需通过测试以证明所有的管理功能运行正常

6.3 管理界面认证

被测 Web 应用防火墙产品必需要用户提供有效的用户名和密码组合或是更强有力的认证才允许访问管理功能。

6.4 安全保密政策

被测 Web 应用防火墙产品必需通过测试，证明其可以采取合理的措施来保护数据的保密性和完整性

6.5 远程管理

被测 Web 应用防火墙产品必需通过测试，证明其可以行使远程管理界面的配置，至少可以支持下列要求：

A. 使用工业标准加密，接受密码和密钥长度

B. 活动超时

C. 具备注销当前管理会话的能力

7 WAF 持久性

7.1 管理配置持久性

被测 Web 应用防火墙产品当遇到重启、断电或删除时，所有的管理配置信息必须存在，并且信息内容没有发生变化

7.2 安全策略持久性

当重新接上电源，被测 Web 应用防火墙产品所有的安全策略必须存在，并且策略配置没有任何变化

7.3 日志数据持久性

当被测 Web 应用防火墙产品遇到系统重启、电力丢失或删除的时，所有的日志数据仍然存在且不会发生任何更改
注意：被测 Web 应用防火墙产品可以使用一个单独的日志服务器来实现这一功能

当日志等待或是批量发送到日志查看器（不论是本地的被测 Web 应用防火墙产品还是远程登录机制）这些信息都不会因为电力丢失或删除而受到影响。

7.4 时间和日期持久性

当被测 Web 应用防火墙产品遇到系统重启、电力丢失或删除的时候，日期和时间仍然存在且不会发生任何更改注意。

7.5 远程管理配置持久性

当被测 Web 应用防火墙产品遇到系统重启、电力丢失或删除的时候，远程管理设置必需和断电之前一致

8 WAF 整合能力

8.1 WAF 部署

WAF 支持多种部署模式：

A. 单机部署模式，支持 Bypass；

B. HA 双机部署模式；

C. 集群部署模式（可选）；

D. 私有云部署模式（可选）；

8.2 与 WEB 扫描器整合

支持主流 Web 扫描器结果导入，并自动对扫描结果漏洞进行防御；