WAF 测评方案

版本 2.0 BETA

作者：OWASP 中国 WAF 测评组

目录

1 WAF 测评介绍

1.1 WAF 测评的意义

随着各行业应用技术的不断发展，各类基于 B/S 架构的业务系统面临越来越多的安全威胁，如何解决应用安全问题？成为摆在业务运营公司、业务开发商、用户面前的一大难题！

Web 应用防火墙（以下简称“WAF”）正是在此背景下，为了解决基于 B/S 架构应用安全问题，而逐渐被大家所接受和认同。近几年来，全球越来越多的安全厂商都推出自主品牌的 WAF，由于缺乏统一标准，用户无从进行选择。

OWASP 作为全球应用安全技术的引领者，为了解决技术、产品、市场的矛盾，启动了 WAF 产品认证项目。此项目的意义在于:

1. 帮助用户选择合适的 WAF 产品;
2. 帮助厂商完善 WAF 产品;
3. 制定 WAF 行业统一标准。

本文主要从这三个角度，介绍如何对 WAF 进行测评。

1.2 WAF 测评内容

WAF 产品测评主要从产品的功能、性能、用户体验等多个角度来全面衡量 WAF 的能力，具体测试内容包括：

1、 WAF 功能测试

1) WAF 检测引擎，主要测试 WAF 对漏洞的识别能力。
2) WAF 防护能力，主要验证 WAF 是否能够将检测引擎识别到的不同漏洞进行有效的策略匹配（比如记录、阻断）。
3) WAF 安全策略，主要测试 WAF 是否具备足够全面、灵活的安全策略，方便用户调整。
4) WAF 扩展性，主要测试 WAF 是否可以灵活使用于不同用户的环境，例如对各类应用环境的支持、分布式部署等。
5) WAF 自身安全，主要用于测试 WAF 设备自身的安全性，是否可以被攻击或者突破。

2、 WAF 性能测试

1) 超负荷下性能，主要用于测试 WAF 最高处理能力。
2) 负载下性能，主要用于测试 WAF 在不同环境下负载处理能力。
3) 稳定性测试，主要用于测试设备在各种极限环境下的稳定性。

3、 用户体验：从用户需求的角度，来检测 WAF 在各种配置管理的全面性以及可操作性。

1.3 测评结果说明

1、 本次测评过程中，测评结果采取星级标识的方式，各不同结果代表的意思如下：

1) ★★★★★：100%符合测评基准相关要求

2) ★★★★☆：90%及以上符合测评基准相关要求

3) ★★★★：80%及以上符合测评基准相关要求

4) ★★★☆：70%及以上符合测评基准要求

5) ★★★：60%及以上符合测评基准要求

2、 测评特别说明

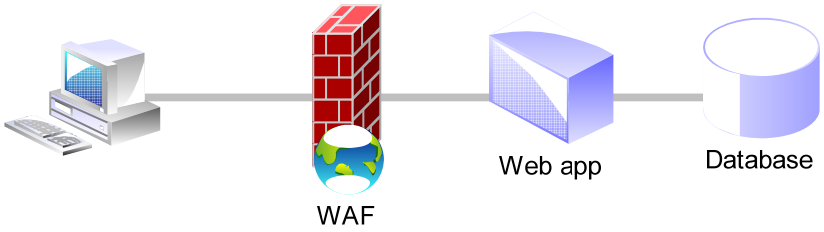
本次测评部分测评项目由于时间原因，没有进行测试，未进行测试的项，在测评结果中将以“/”显示。

2 WAF 测试方案

2.1 WAF 功能测试

2.1.1 测试环境

1、 基本拓扑图



2、 准备软硬件清单

按照上图所示准备环境，包括：

1) Web 服务器、数据库服务器，并同 WAF 连接

2) 客户端电脑，可预装 Web 扫描测试工具（如 Web Scanner）

2.1.2 检测引擎测试

1、 测试内容

1) 检测引擎对 OWAPS TOP 10 漏洞识别率

2) 检测引擎对各类 Web 扫描器扫描漏洞种类识别率

2、 测试方法

1) 开启 WAF 检测模式，并确保在目标网站可以正常访问情况下，尽量启用最全的检测模块。

2) 针对 OWASP TOP 10 的漏洞对 WAF 进行探测，确认 WAF 对攻击结果的检测率。

3) 使用 Appscan、Cenzic 扫描器全策略对目标站点进行扫描。将扫描器策略包项目与 WAF 检测到的项目进行对比，确认是否完全包含。

3、 测试结果

厂家名称（首字母拼音排序）	OWASP TOP 10 检测	Web 扫描器检测
安恒	★★★★	/
Imperva	★★★★☆	/
绿盟	★★★★	/
启明	★★★☆	/
Trustwave	★★★★★	/
网神	★★★☆	/

2.1.3 防护能力测试

1、 测试内容

1) 检测引擎对 OWAPS TOP 10 漏洞攻击防护

2) 检测引擎对其他漏洞的攻击防护

2、 测试方法

1) 将目标网站配置为 Webgoat 平台，或其他有漏洞的平台。

2) 将 Web 应用防火墙开启阻断模式，并确保在目标网站可以正常访问情况下，开启最全的防护模式。

3) 确认 WebGoat 平台（或其他漏洞平台）的各漏洞无法被访问；重复 2.1.2 节测试方法第 2）、3）条，均无法检测到漏洞。

3、 测试结果

厂家名称（首字母拼音排序）	OWASP TOP 10 防护能力	穿透性测试
安恒	★★★★	★★★☆
Imperva	★★★★	★★★★
绿盟	★★★☆	★★★☆
启明	★★★	★★★
Trustwave	★★★★☆	★★★★☆
网神	★★★	★★★

2.1.4 WAF 安全策略

1、 测试内容

1) 检测安全策略种类是否齐全，是否包含合规性

2) 检测安全策略是否灵活，是否可以自行定义

2、 测试方法

1) 可查看策略配置，确认内容是否足够细致，是否包含合规性策略包

2) 用户可自行定义各种不同类型漏洞检测方法和策略，确认策略是否可以生效。

3、 测试结果

厂家名称（首字母拼音排序）	合规性报表	策略灵活度
安恒	★★★☆	★★★☆
Imperva	★★★★★	★★★★☆
绿盟	★★★☆	★★★☆
启明	★★★☆	★★★★
Trustwave	★★★★★	★★★★☆
网神	★★★☆	★★★☆

2.1.4WAF 扩展性

1、 测试内容（待完善）

1) 部署方式测试：分布式部署、透明直连部署、旁路部署

2) HA 功能测试

3) 集成 Web 扫描功能，以及支持其他扫描结果的导入

4) 与其他网络安全平台的联动

2、 测试方法

1) 参考产品说明书及部署方式（本项仅从产品现有的功能层面来看）

3、 测试结果

厂家名称（首字母拼音排序）	部署方式	其他扩展性
安恒	★★★☆	★★★☆
Imperva	★★★★★	★★★★★
绿盟	★★★★	★★★★
启明	★★★☆	★★★☆
Trustwave	★★★★★	★★★★★
网神	★★★☆	★★★☆

2.1.5 WAF 自身安全性

1、 测试内容

1) WAF 自身安全性检测

2) WAF 防护端口检测（待完善）

2、 测试方法

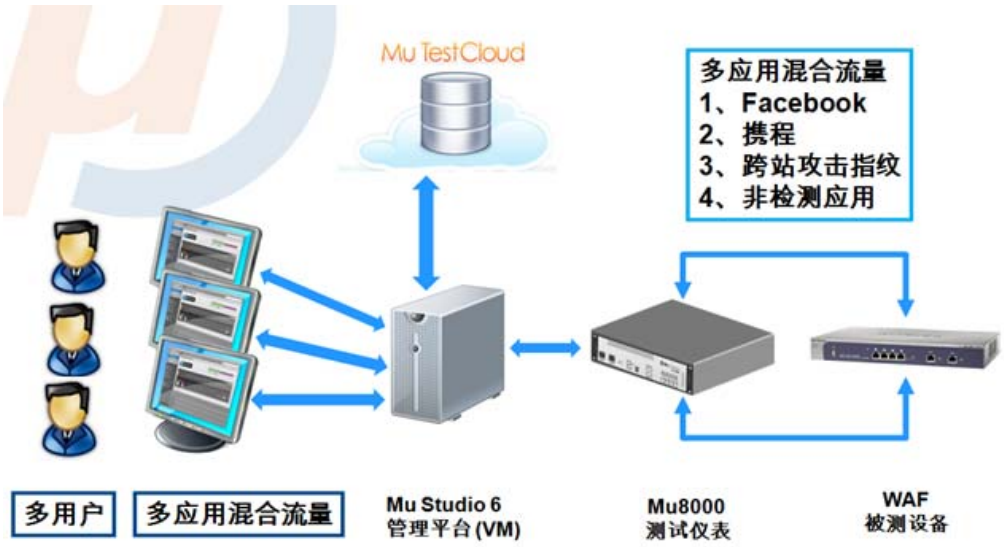
1) 针对 WAF 管理端口，可采取系统扫描、应用扫描以及渗透测试工具，对其自身安全及稳定性进行测试。

3、 测试结果

厂家名称（首字母拼音排序）	WAF 自身安全性
安恒	★★★☆
Imperva	★★★★★
绿盟	★★★☆
启明	★★★☆
Trustwave	★★★★★
网神	★★★★

2.2 WAF 性能测试

1、 测试环境



2、 测试内容和测试方法

1) 最大连接数：被测试设备能够支持最大并发 HTTP 连接数量

测试方法：测试采用单一 HTTP 连接的测试用例，通过连续增加的并发连接，验证 WAF 支持的最大并发 HTTP 连接数量。

2) 每秒新建连接数：每秒钟设备能够新建的连接数

测试方法：测试采用单一 HTTP 连接的测试用例，快速循环建立新连接的方法，验证每秒钟 WAF 能够支持的新建 HTTP 连接数量

3) 最大并发数：设备能够支持的最大并发事务数

测试方法：测试中采用多 HTTP 连接的测试用例，一个用例全部完成为一次事务，通过快速循环执行新事务的方法，验证 WAF 能够支持的最大并发用户（事务）数

4) 攻击特征检测率：指被测设备能够成功阻断带有攻击特征的流量的比率。

测试方法：测试中，采用了上小节列举的三种不同类型应用的混合流量，通过一段时间的连续运行，检查被测设备能够成功截断的带攻击特征的事务的流量比率。

3、 测试结果

厂家名称（首字母拼音排序）	整体性能（仅做参考）
安恒	★★★
Imperva	★★★★★
绿盟	★★★★
启明	★★★☆
Trustwave	★★★★
网神	★★★☆

备注：由于各家所送产品的型号不一致，Imperva、Trustwave 均为低端产品，其他厂家均为中、高端产品，所以从整体的性能上做了宏观判断，不计入实际总得分。

2.3 用户体验

体验结果：（测评项参考如下章节说明）

厂家名称（首字母拼音排序）	用户体验
安恒	★★★☆
Imperva	★★★★
绿盟	★★★☆
启明	★★★★
Trustwave	★★★★
网神	★★★★

2.3.1 管理和配置

管理和配置主要检查项：

测试类别	测试类别说明
管理界面	包含安全管理界面，管理员能访问所有管理功能。如果发现不安全的访问界面，能禁止该界面，同时其他管理功能不受影响，能正常访问
管理功能	管理功能作为 WAF 产品的一部分，有以下功能 A. 配置和改变安全策略 B. 配置和改变管理用户认证信息 C. 配置和改变远程管理设置（如果适用） D. 配置和改变或获取日期和时间 E. 启动所需日志事件的日志记录 F. 审查所需的日志数据 G. 激活之前系统配置和所需安全策略

管理功能测试	测试所有的管理功能正常工作
管理界面认证	在运行访问任意管理功能前，能使用有效地用户名和密码通过验证，或更强形式的验证
安全策略保密性	包含合理的措施，保护安全策略的数据的保密性和完整性
远程管理	能远程访问管理界面，至少符合以下要求： A. 使用行业标准加密，并接受加密和密匙长度 B. 闲置超时 C. 根据需要对当前管理会话注销能力

2.3.2 并行会话管理

并行管理主要测试项

测试类别	测试类型说明
并行管理会话（条件限制）	**如果 WAF 允许并行管理会话，那么它必须采取足够措施保护改变中的配置安全策略的完整性**
所需日志事件	能记录下列所有事件类型。 注意：当日志不启用或默认情况下不启用时，不要求进行该测试。 A. 对受配置安全策略所保护的资源的所有成功或失败访问 B. 对管理界面的所有成功或失败的认证 C. 安全策略保护的资源的所有成功和失败的访问操作 D. 配置安全策略的所有编号 E. 每次系统启动 F. 所有手动输入改变系统时间
要求日志数据	对于 WAF 记录的每一个事件，日志数据中至少包含如下因素： A. 日期和时间： 1. 日志中每个事件记录的日期必须包含 3 位年，月，日的数据 2. 日志中每个事件记录的时间都必须包含时间，分，秒 B. 源 IP 地址或主机名 C. 目标 IP 地址和主机名 D. 源端口 E. 目标端口 F. 服务名称或协议（HTTP,HTTPS） G. URL（路径，参数） H. HTTP 方法（GET,POST） I. 会话标识（根据 WAF 产品不同） J. 事件处理结果（如，允许，拒绝） K. 如果拒绝，说明失败原因 L. 用户识别（如果适用的话） M. 说明安全策略的改变，增加或删除 N. 管理界面认证的成败说明

日志数据的准确性	所有的日志时间必须准确
日期和时间精确	所有日志记录的日期和时间必须精确到秒
日志数据介绍	所有要求的日志事件中的日志数据必须按照可读形式便于审查，同时保留了事件的相对顺序
标准日志格式	至少按照一种行业标准的日志格式产生日志（如 W3C,syslog），便于导出到外部应用程序（如应用取证工具，应用漏洞扫描器）
单一事件链接到多个日志文件	（条件）使用多个日志信息记录某个日志事件时，每个日志信息必须包含其他相应日志信息的清楚准确的链接
用户隐私合规性	根据管理员定义，识别并屏蔽日志中的敏感、机密或私人信息
应用级取证功能	能够提供应用级取证功能，包括事件调查，导航及其相关功能。

2.3.3 持久性

持久性主要检查项

测试类别	测试类型说明
持久性	
管理配置持久性	当 WAF 重启或电源丢失或删除的情况下，所有管理配置信息必须坚持和保持不变。
安全策略持久性	如果 WAF 电源在丢失或删除后重新启动，WAF 必须： A. 实施电源丢失前相同的安全策略 B. 强制执行一切拒绝的安全策略， 包括管理功能中恢复到电源丢失前的安全策略
日志数据持久性	WAF 电源重启或丢失时，所有的未经传输的日志数据应该保留并无修改。注意：WAF 可通过单独的日志服务器实现这一要求。 PE3 注意：如果日志事件在排队，并且是大批量发送给日志查看器（不论是本地访问 WAF 还是远程登录机制），这些信息必须保留，在断电时不丢失。
日期和时间持久性	当 WAF 产品重启或断电时，日期和时间数据必须保持不变。 注意： 可以在 RFC1305 定义的对称主动模式中使用 NTP 满足这一要求。

远程管理配置持久性	当 WAF 产品断电时，远程管理设置在重启时必须保持和之前一样配置。 注意 1 持久性要求-持久性要求并没有包含所有使用管理功能时断电的情况 注意 2 持久性要求—除了 PE1 的情况外，持久性要求并没有包含 WAF 产品的硬件由于断掉而导致故障的所有情况。

3.测评结果

厂家名称（首字母拼音排序）	安恒	Imperva	绿盟	启明	Trustwave	网神
OWASP TOP 10 检测	★★★★	★★★★☆	★★★★	★★★☆	★★★★★	★★★☆
Web 扫描器检测	/	/	/	/	/	/
OWASP TOP 10 防护能力	★★★★	★★★★	★★★☆	★★★	★★★★☆	★★★
穿透性测试	★★★☆	★★★★	★★★☆	★★★	★★★★☆	★★★
合规性报表	★★★☆	★★★★★	★★★☆	★★★☆	★★★★★	★★★☆
策略灵活度	★★★☆	★★★★☆	★★★☆	★★★★	★★★★☆	★★★☆
部署方式	★★★☆	★★★★★	★★★★	★★★☆	★★★★★	★★★☆
其他扩展性	★★★☆	★★★★★	★★★★	★★★☆	★★★★★	★★★☆
WAF 自身安全性	★★★☆	★★★★★	★★★☆	★★★☆	★★★★★	★★★★
整体性能（仅做参考）	★★★	★★★★★	★★★★	★★★☆	★★★★	★★★☆
用户体验	★★★☆	★★★★	★★★☆	★★★★	★★★★	★★★★
综合	★★★☆	★★★★☆	★★★☆	★★★☆	★★★★☆	★★★☆