

WEB 应用防火墙测评认证 2.0

实施规则

一、 WEB 应用防火墙测评认证意义

随着各行业应用技术的不断发展，Web 应用防火墙(以下简称“WAF” 逐渐被大家所接受和认同。全球越来越多的安全厂商都推出自主品牌的 WAF，以期帮助客户解决基于 B/S 架构应用安全问题。但是由于缺乏统一标准，通常用户无从进行选择。

为了解决技术、产品、市场的矛盾，SecZone 在 OWASP 中国的技术支撑下，启动了中立、第三方的 WAF 产品测评和认证，帮助用户衡量 WAF 的合规性、可靠性以及性能。从市场的层面，还可以做到：

- 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。

二、 认证标准-《WEB 应用防火墙测评认证 2.0》

《Web 应用防火墙测评认证 2.0》在 1.0 的基础上对整体测试框架重新定义，在新型攻击、产品性能（增值服务）、产品安全性能做了全面的拓展，增加了以 OWASP TOP 2017 为主延伸出业务逻辑层防护、绕过防御多维度评级等。

三、 认证范围

- WEB 应用防火墙
- 具备 WEB 应用安全防护的产品（仅测试 WEB 应用防护功能）

四、 认证模式

产品标准化测评

五、 认证测评范围

安全有效性评估 (SE)	本项测试主要基于 OWASP TOP 10 风险延伸出全面的安全漏洞防护测试，被测系统需要对从传统漏洞到业务逻辑层多维度的各类安全漏洞给予有效防护。	40%
安全性能评估 (PE)	在识别安全漏洞保护 Web 应用时，被测系统应能够全面保障自身安全性，并需同时满足准确率和误报率。	25%
可靠性评估 (SR)	通过特定环境、在特定时间内，检测被测系统执行指定功能的稳定性。	20%
可管理性评估 (M)	对被测设备进行架构设计、联动性、容错性、拓展性等测试。	15%

六、 WAF 测评申请流程

1. 认证申请及受理	<ul style="list-style-type: none">➤ 填写 WAF 测评认证申请表;➤ 审核通过, 签订测评合同。
2. 提供 WAF 测试机及市场调研	<ul style="list-style-type: none">➤ 提供产品详细技术文档资料➤ 确保样机与市场销售机型一致性
3. 产品测试	测试初期过程, 需厂方人员配合。
4. 测评结果沟通	确认未通过测试项细节。
5. 测评结果交付	<ul style="list-style-type: none">➤ 测评通过, 颁发 WAF 认证证书;➤ 测评不通过, 提供测评报告及改进建议, 预备下次测评。
6. 测评证书发布及监督	确保认证信息可被查询 (www.seczone.org), 并确保证书用于被测试产品。

七、 联系方式

电话: 0755-32880880

邮箱: xufei@seczone.org

网址: www.seczone.org