

**广西民族大学**

**中云zyWAF防护报告**

|  |
| --- |
| 发布单位：中云网安科技（北京）有限公司 |
| 公司网址：http://www.zyprotect.com/ |
| 发布日期： |

目录

[1. 概述 1](#_Toc516818623)

[2. 部署方案 2](#_Toc516818624)

[2.1 部署环境 2](#_Toc516818625)

[2.2 部署配置 2](#_Toc516818626)

[3. 防护摘要 3](#_Toc516818627)

[3.1 防护周期 3](#_Toc516818628)

[3.2 参与人员 3](#_Toc516818629)

[3.3 工作记录 3](#_Toc516818630)

[3.4 防护总结与建议 4](#_Toc516818631)

[4. 详细防护报告 5](#_Toc516818632)

[4.1 保护站点配置 5](#_Toc516818633)

[4.2 报告分析 5](#_Toc516818634)

[4.3 高危攻击行为 7](#_Toc516818635)

[5. zyWAF优势 9](#_Toc516818636)

[6. 附录 10](#_Toc516818637)

[6.1 攻击类型索引 10](#_Toc516818638)

1. 概述

随着互联网、物联网行业整体的快速发展，目前国内外的网络安全问题越来越突出，许多大型企业网站与服务器经常遭受到黑客攻击，攻击手段也越来越多样化，从传统的通过人工手动发动攻击的方式，逐步发展为自动化攻击，以及采用人工智能手段通过机器发动攻击，攻击后对于公司以及相关业务产生的影响也是越来越广，当前传统的WAF通过预定义规则的方式进行防护的方法已经无法抵御日益先进的攻击方式，一些国外的安全厂商也会经常爆出一些自身产品的安全问题。

有别于传统WAF的技术架构，中云网安研发的下一代zyWAF采用行业领先的AI机器学习技术，建立智能的安全模型，除了能够抵御传统的常见的攻击方法以外，最大的优势在于对于新型的未知的攻击也能够进行全面的抵御，采用比传统WAF更积极主动的方式保护目标网站。

本报告的防护对象为广西民族大学相思湖网站，广西民族大学本次在测试中部署了先进的AI机器学习为核心架构的zyWAF系统，保护广西民族大学相思湖的安全，同时为部署zyWAF 之后的web系统的安全风险与防护效果提供详细的数据依据。 用户可以重点关注本文档攻击报告分析部分，通过报告中的信息了解到“不可信访问”的次数，分类统计，以及相应安全建议。

1. 部署方案

本部署方案为在广西民族大学相思湖网络环境中的Linux服务器上部署安装软件形式的zyWAF，在初始阶段打开zyWAF被动模式，让zyWAF能够在实际用户访问流量的条件下进行机器学习，建立被保护网站的安全模型。

通过一段时间的机器学习过程，中云网安项目组成员在现场提取告警日志，对告警日志进行分析，处理误报。上述过程结束后，项目组成员在zyWAF上启动主动防御模式，对不符合安全模型的所有访问行为进行拦截。

2.1 部署环境

Xxxx

拓扑说明：

xxxxxxxxxxxxxxxxx

2.2 部署配置

1. xxx服务器

|  |  |
| --- | --- |
| 硬件配置 | CPU：xxx  内存：xxx |
| 软件环境 | xxx |

1. zyWAF配置

|  |  |
| --- | --- |
| zyWAF数量 | xxx |
| 服务器IP地址 | xx |
| 被保护网站的IP:端口 | xxxx |
| 被保护域名 | xxx |

1. 防护摘要

3.1 防护采样周期

4月9日-6月6日

3.2 参与人员

|  |  |  |
| --- | --- | --- |
|  |  | 中云网安 |
| 角色 |  |  |
| 姓名 |  |  |
| 联系方式 |  |  |
| 职责说明 |  |  |

3.3 工作记录

|  |  |
| --- | --- |
| 日期 | 工作内容 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

3.4 防护总结与建议

1. 防护采样周期内网站不可信访问总数为238381次，日均6870次。
2. 报告中“强制浏览”，“链接参数篡改”，“非正常HTTP请求”，“服务器域名无效”数量居多，说明网站长期遭受扫描器扫描，疑似有黑客进行无具体目标的扫描收集网站信息
3. 网站日均不可信访问在？？？次以下属于比较正常范围的。超过6000以上疑似遭到漏洞扫描。1月中旬，3月21日前后遭受多轮扫描，不可信流量分别是正常水平的16倍和9倍。
4. 从攻击IP地址分析上看，绝大部分的异常流量来自于国内，分布于广西南宁地区，其中有1204次来自于一个美国云主机提供商。建议将频繁对网站进行不符合安全模型的行为的IP地址配置在IP黑名单中
5. 建议在重要时期重点关注14：00， 18：00和20：00时间段的恶意扫描和黑客攻击行为

4. 详细防护报告

4.1 保护站点配置

1. 快速设置

页面名称：快速设置

页面功能： zyWAF提供了一个简洁的配置页面，可以最大的简化管理员的配置工作，该页面展示了WAF防护对象基本配置信息，也可以在该页面上进行配置的修改和保存。

页面位置：【控制台】->【快速设置】

4.2 报告分析

1. 不可信访问分类统计

注：不可信访问类型详细描述见附录

1. 不可信访问的时间分布

从上图中可以获知网站遭遇扫描或者黑客攻击的高发日期为2018年4月12日(19998次)，2018年4月13日(22464次)，2018年4月25日(21674次)。

1. 不可信访问IP分布

前十大攻击源IP分析：

|  |  |  |
| --- | --- | --- |
| 序号 | 前十攻击源IP地址 | IP归属地 |
| 1 | 210.36.64.59 | 中国 广西 南宁 广西民族大学 |
| 2 | 10.240.1.203 | 局域网内部IP |
| 3 | 210.36.64.18 | 中国 广西 南宁 广西民族大学 |
| 4 | 10.240.1.202 | 局域网内部IP |
|  |  |  |

安全建议：

1. 前十大攻击源IP列表中有两个IP地址内网IP，建议开启边界代理设备或者负载均衡设备的X-Forward-For功能，在应用层插入客户端IP信息。这样有利于攻击溯源，获取真实的攻击IP地址。如果有VPN接入流量，建议开始VPN的虚拟地址池功能，便于记录VPN接入流量的攻击溯源。若果怀疑该内部IP频繁发动攻击，请检查该IP所属机器的责任人。
2. 210.36.64.59和210.36.64.18 构成了攻击流量的95%以上，疑似安全扫描主机。
3. 不可信访问24小时时间分布

从24小时的分布图上来看，攻击行为在14点进入高发期。

安全建议：

在重要的时期，建议在上述时段安排人员值守。

4.3 高危攻击行为

针对前一章节报告中的不可信攻击统计信息，我们也通过传统分类的方式对其中高危类型攻击部分进行解析，详细内容如下：

1. 扫描器

|  |  |
| --- | --- |
| 类型 | Scanner Detection |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. http协议漏洞

|  |  |
| --- | --- |
| 类型 | Protocol Enforcement |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. http协议攻击

|  |  |
| --- | --- |
| 类型 | Protocol Attack |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. 本地文件包含

|  |  |
| --- | --- |
| 类型 | Local File Inclusion |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. 远程文件包含

|  |  |
| --- | --- |
| 类型 | Remote File Inclusion |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. 远程代码执行

|  |  |
| --- | --- |
| 类型 | Remote Code Execution |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. PHP攻击

|  |  |
| --- | --- |
| 类型 | PHP Attack |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. 跨站脚本攻击

|  |  |
| --- | --- |
| 类型 | XSS |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. SQL注入

|  |  |
| --- | --- |
| 类型 | SQL Injection |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. 固定会话

|  |  |
| --- | --- |
| 类型 | Session Fixation |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

1. 数据泄露

|  |  |
| --- | --- |
| 类型 | Data Leakages |
| 样例 |  |
| 次数 | 0 |
| 危害 |  |

注：攻击行为分类基于OWASP核心规则库。

5. zyWAF优势

中云网安拥有一支国内资深的安全研发团队，专注于AI Security领域。从技术角度讲，zyWAF最大的优势是能够基于对用户访问交互行为的机器学习建立安全模型，不仅能够识别传统的常见的高危攻击行为，而且能够识别潜在的未知的攻击行为，这些未知攻击行为包括了新型攻击，无效访问，0-Day攻击以及其他一些不符合访问规范的行为。传统WAF无法做到有效识别这些未知攻击行为，而且需要大量安全人员定期对特征库进行维护。而zyWAF这一通过AI自动演进为核心技术的防护原理，能够做到“贴身防护”，“一对一防护”，为目标保护网站打造独一无二的防护网。

6. 附录

6.1 攻击类型索引

|  |  |
| --- | --- |
| 攻击类型 | 攻击解释 |
| 强制浏览 | 检测到的未知URL请求。 |
| Cookie篡改 | HTTP的cookie值被篡改。 |
| 隐藏字段篡改 | HTML表单中隐藏字段值被篡改 |
| 链接参数篡改 | 链接中包含的查询参数被篡改 |
| HTTP请求方法无效 | 检测到的请求方法无效如非GET或POST |
| 服务器域名无效 | 检测到请求的服务器域名不是zyWAF所保护的域名 |
| 非正常HTTP请求 | 检测到的请求信息违反了HTTP标准请求信息不符合HTTP标准 |
| 特殊字符 | HTML表单中存在特殊字符或危险字符 |