

Apache 安装开源 WAF

——无涯

说明：

本文以 Windows 环境下的 Apache 安装 mod_security 为例，介绍开源 WAF 产品的安装使用。

<http://www.modsecurity.cn/>

<https://github.com/SpiderLabs/ModSecurity>

一、WAF 基本介绍

WAF 全称 Web Application Firewall，即 Web 应用防火墙。

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 应用提供保护的一款产品，跟网络防火墙的作用不同。

WAF 的使用场景：例如服务器中有些安全性比较差的应用程序，比如旧版的 wordpress、discuz、phpwind 等，审计和修改全部代码比较麻烦，这时候最好的办法就是通过部署 WAF 来实现安全防护。

WAF 可以防护的常见风险包括：SQL 注入、XSS、利用本地/远程文件包含漏洞进行攻击、PHP 代码注入、黑客扫描网站、源代码/错误信息泄露等等。

目前市面上的 WAF 非常多，总体上可以分成 3 类：硬件型 WAF（厂商安装）、云 WAF（比如阿里云腾讯云华为云的 WAF，购买服务）、软件型 WAF（可以部署在 Apache、Nginx 等 HTTP Server 中，有很多开源的产品）。

二、下载 mod_security

下载和安装 Apache 的步骤参考：《02-Windows 安装 phpstudy》。

如果使用 phpstudy 内置的 Apache，Apache 文件在 Extensions 目录下，如：

E:\phpstudy_pro\Extensions\Apache2.4.39



1、下载 mod_security

下载 mod_security，根据操作系统位数选择，win64 是 64 位，win32 是 32 位。

<https://www.apachelounge.com/download/>

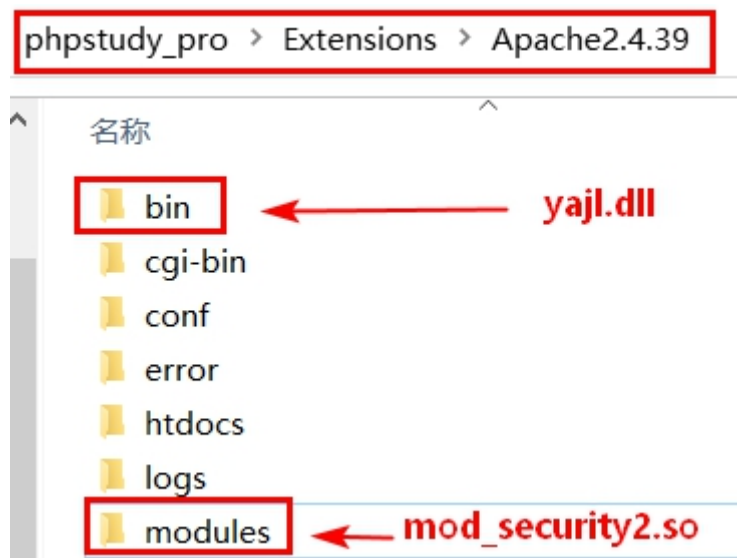
mod_security

Application firewall, intrusion detection and prevention engine

 mod_security-2.9.3-win64-VS16.zip	info	16 Jun '19	626K
 mod_security-2.9.3-win32-VS16.zip			542K

解压 mod_security-2.9.3-win64-VS16.zip，复制两个文件：

- 1) 复制 mod_security2.so 到 apache/modules 文件夹
- 2) 复制 yajl.dll 到 apache/bin 文件夹



2、修改 Aapche 配置文件

修改 Apache2.4.39\conf\httpd.conf

主要修改内容（没有就加上，有就取消注释，放在相同的模块附近）：

取消注释：

```
LoadModule security2_module modules/mod_security2.so
```

下面添加一行：

```
LoadModule unique_id_module modules/mod_unique_id.so
```

```
177 LoadModule unique_id_module modules/mod_unique_id.so
178 LoadModule security2_module modules/mod_security2.so
```

添加

```
Include conf/modsecurity/*.conf
```

```
467 #Include conf/extra/httpd-mpm.conf
468 Include conf/modsecurity/*.conf
```

3、修改 modsecutiry 配置文件

打开 mod_security-2.9.3-win64-VS16\mod_security-2.9.3\mod_security

复制一个 modsecurity.conf-recommended，改名为
modsecurity.conf

在 Apache2.4.39\conf 下创建一个文件夹，命名为 modsecurity
把 modsecurity.conf 放在 modsecurity 文件夹下

\\pp > phpstudy_pro > Extensions > Apache2.4.39 > conf > modsecurity

名称	修改日期
rules	2021/4/7 15:49
crs-setup.conf	2019/9/24 16:54
modsecurity.conf	2021/4/14 14:13

modsecurity.conf 修改/添加两行配置：

```
SecRuleEngine On
```

```
SecDefaultAction "deny,phase:2,status:403"
```

```
9  SecRuleEngine On
10 SecDefaultAction "deny,phase:2,status:403"
```

此处含义是开启安全规则引擎，如果触发规则，默认防护措施是返回 HTTP 403 错误。

修改日志路径，否则 Apache 启动会报路径不存在的错误：

```
SecAuditLog E:\phpstudy_pro\Extensions\Apache2.4.39\logs\modsec_audit.log
```

```
195 SecAuditLog E:\phpstudy_pro\Extensions\Apache2.4.39\logs\modsec_audit.log
```

因为没有 unicode.mapping 文件，这一行要注释

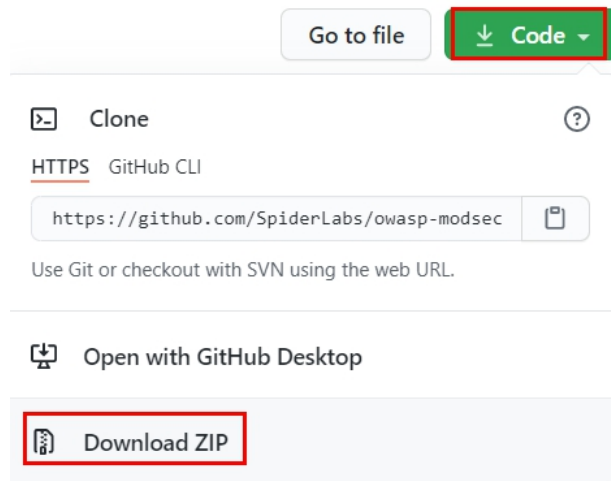
```
#SecUnicodeMapFile unicode.mapping 20127
```

```
220 #SecUnicodeMapFile unicode.mapping 20127
```

三、添加 owasp 规则

1、下载规则文件

<https://github.com/SpiderLabs/owasp-modsecurity-crs>

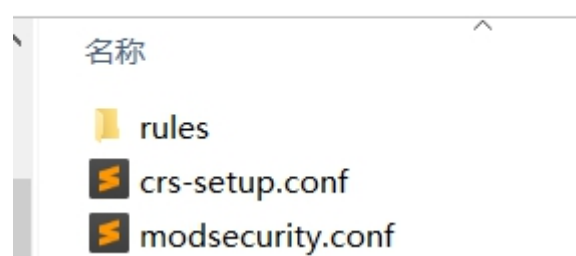


2、配置规则

解压 owasp-modsecurity-crs-3.2.0, 把 rules 文件夹复制到
Apache2.4.39\conf\modsecurity 目录下

复制 crs 根目录下的 crs-setup.conf.example, 重命名为
crs-setup.conf, 放在 Apache2.4.39\conf\modsecurity 目录下

Apache2.4.39 > conf > modsecurity



3、修改 httpd.conf

Apache2.4.39\conf\httpd.conf 再添加下面这一行(第一行前面添加过了)：

```
Include conf/modsecurity/rules/*.conf
```

```
468 Include conf/modsecurity/*.conf
469 Include conf/modsecurity/rules/*.conf
```

4、重启 Apache

所有配置修改完以后重启 Apache。

5、测试注入

这时候尝试注入，返回 phpstudy 的 403 页面：

403 - Forbidden 禁止访问: 访问被拒绝

错误说明：禁止访问，服务器拒绝访问

sqlmap 也无法注入：

```
sqlmap --purge      (先清空缓存)
```

```
sqlmap.py -u http://localhost/school/url.php?id=1
```

```
[11:43:47] [WARNING] GET parameter 'id' does not seem to be injectable
[11:43:47] [CRITICAL] all tested parameters do not appear to be injectable.
wish to perform more tests. Please retry with the switch '--text-only' (al
ndidate (low textual content along with inability of comparison engine to d
ere is some kind of protection mechanism involved (e.g. WAF) maybe you coul
) and/or switch '--random-agent'
[11:43:47] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 75 times
```

结果显示有 75 次 403 禁止访问的错误。

马士兵教育 运维安全学院 无涯老师

QQ: 3499590161

微信: wuyaaq

最后修改时间: 2021 年 5 月 17 日 17:07:35