网络对抗原理
大作业

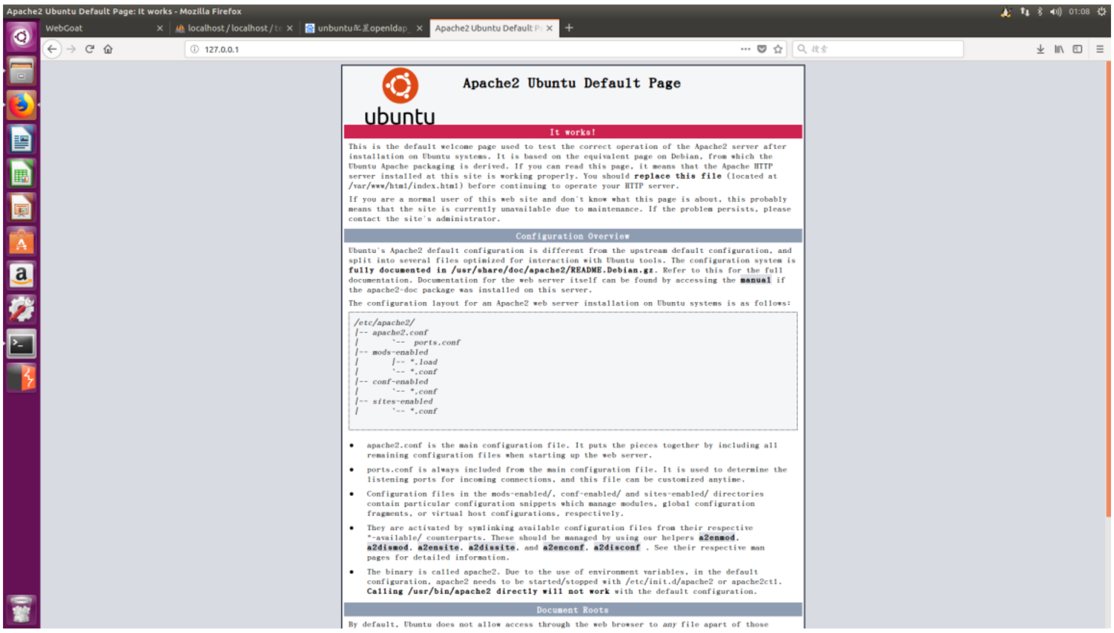
实验三

学　　院　　网络与信息安全学院

专　　业　　信息安全

姓　　名　　任旭杰 15180110034

1. 配置 apache2



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

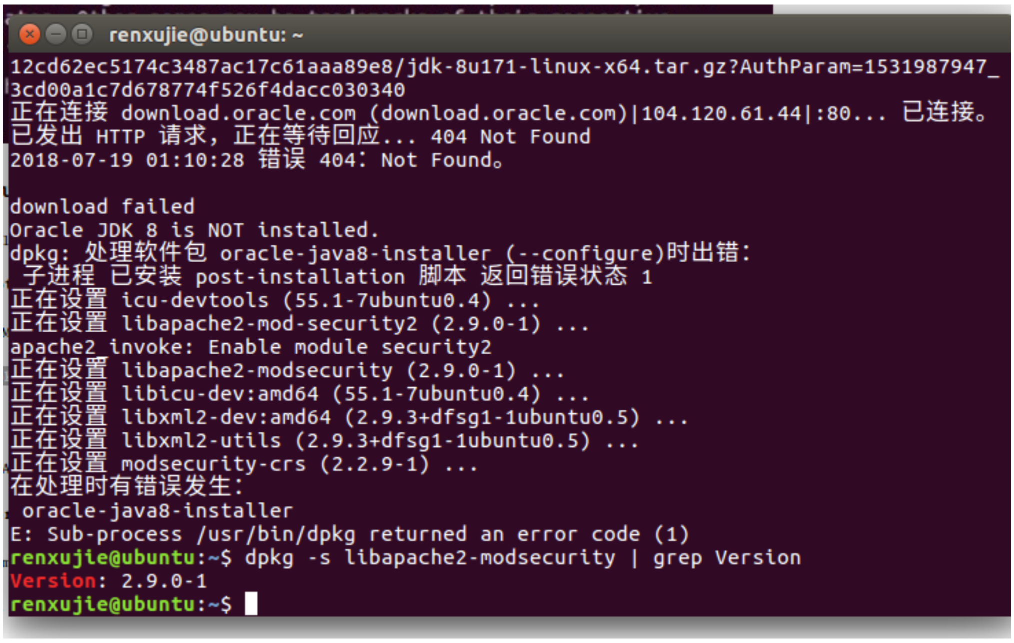
- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **a2enmod**, **a2dismod**, **a2ensite**, **a2dissite**, and **a2enconf**, **a2disconf** . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those

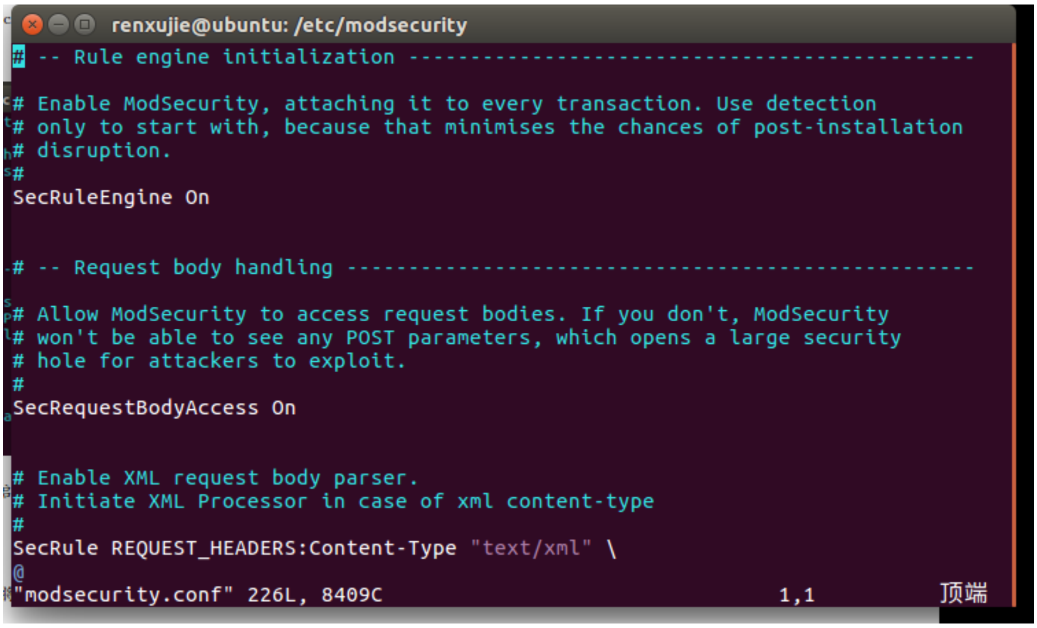
2. 安装并配置 ModSecurity 模块，搭建 WAF

安装 libapache2-modsecurity 模块



```
12cd62ec5174c3487ac17c61aaa89e8/jdk-8u171-linux-x64.tar.gz?AuthParam=1531987947_
3cd00a1c7d678774f526f4dacc030340
正在连接 download.oracle.com (download.oracle.com)|104.120.61.44|:80... 已连接。
已发出 HTTP 请求，正在等待回应... 404 Not Found
2018-07-19 01:10:28 错误 404: Not Found。

download failed
Oracle JDK 8 is NOT installed.
dpkg: 处理软件包 oracle-java8-installer (--configure)时出错:
 子进程 已安装 post-installation 脚本 返回错误状态 1
正在设置 icu-devtools (55.1-7ubuntu0.4) ...
正在设置 libapache2-mod-security2 (2.9.0-1) ...
apache2_invoke: Enable module security2
正在设置 libapache2-modsecurity (2.9.0-1) ...
正在设置 libicu-dev:amd64 (55.1-7ubuntu0.4) ...
正在设置 libxml2-dev:amd64 (2.9.3+dfsg1-1ubuntu0.5) ...
正在设置 libxml2-utils (2.9.3+dfsg1-1ubuntu0.5) ...
正在设置 modsecurity-crs (2.2.9-1) ...
在处理时有错误发生:
 oracle-java8-installer
E: Sub-process /usr/bin/dpkg returned an error code (1)
renxujie@ubuntu:~$ dpkg -s libapache2-modsecurity | grep Version
Version: 2.9.0-1
renxujie@ubuntu:~$
```

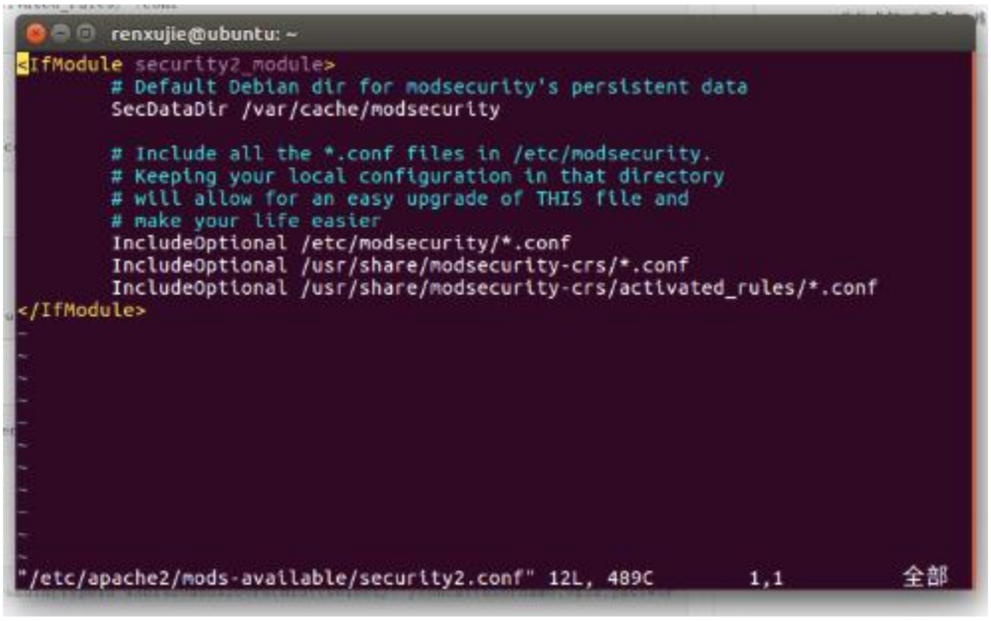
修改/etc/modsecurity/ modsecurity.config 开启拦截模式



```
# -- Rule engine initialization ----------------------------------------------

# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On


# -- Request body handling ---------------------------------------------------

# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On


# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "text/xml" \
@
"modsecurity.conf" 226L, 8409C                              1,1           顶端
```

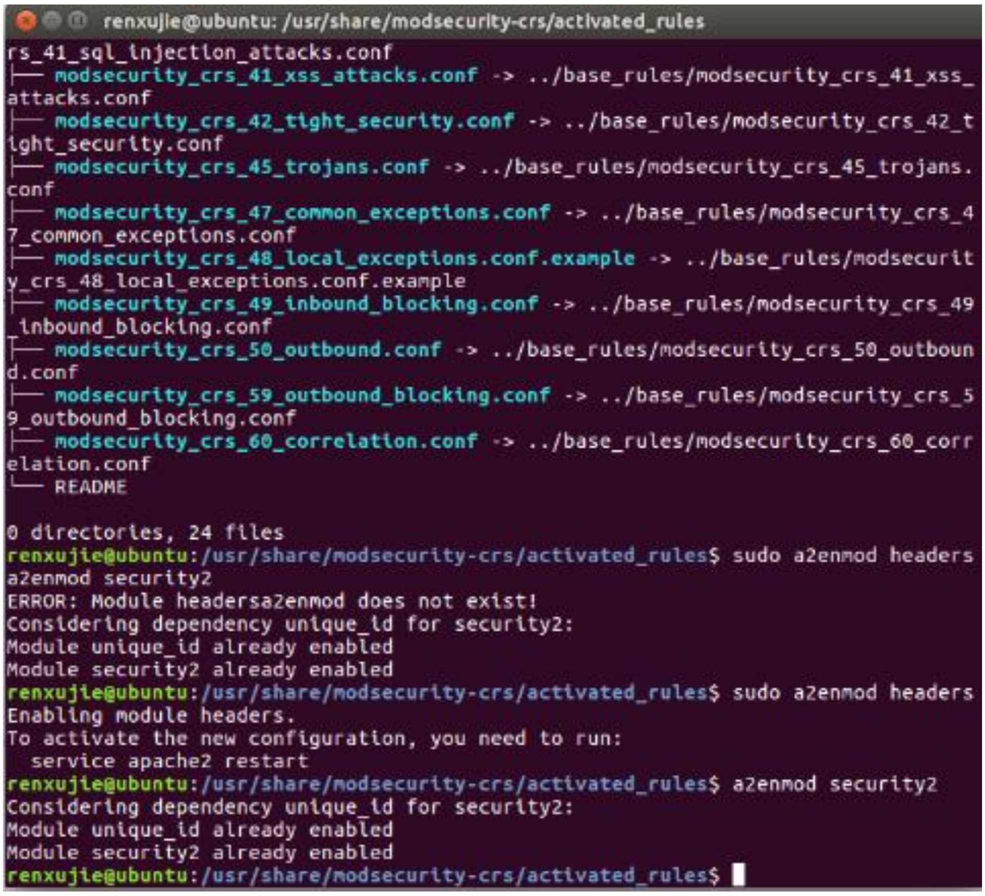
进入到/usr/share/modsecurity-crs/activated_rules/目录下，使用命令 for f in $(ls ../base_rules/); do ln -s ../base_rules/$f; done，建立默认规则集。

修改/etc/apache2/mods-available/security2.conf，添加 IncludeOptional /usr/share/modsecurity-crs/activated_rules/*.conf



```
<IfModule security2_module>
        # Default Debian dir for modsecurity's persistent data
        SecDataDir /var/cache/modsecurity

        # Include all the *.conf files in /etc/modsecurity.
        # Keeping your local configuration in that directory
        # will allow for an easy upgrade of THIS file and
        # make your life easier
        IncludeOptional /etc/modsecurity/*.conf
        IncludeOptional /usr/share/modsecurity-crs/*.conf
        IncludeOptional /usr/share/modsecurity-crs/activated_rules/*.conf
</IfModule>
~
~
~
~
~
~
~
~
~
~
~
"/etc/apache2/mods-available/security2.conf" 12L, 489C        1,1           全部
```

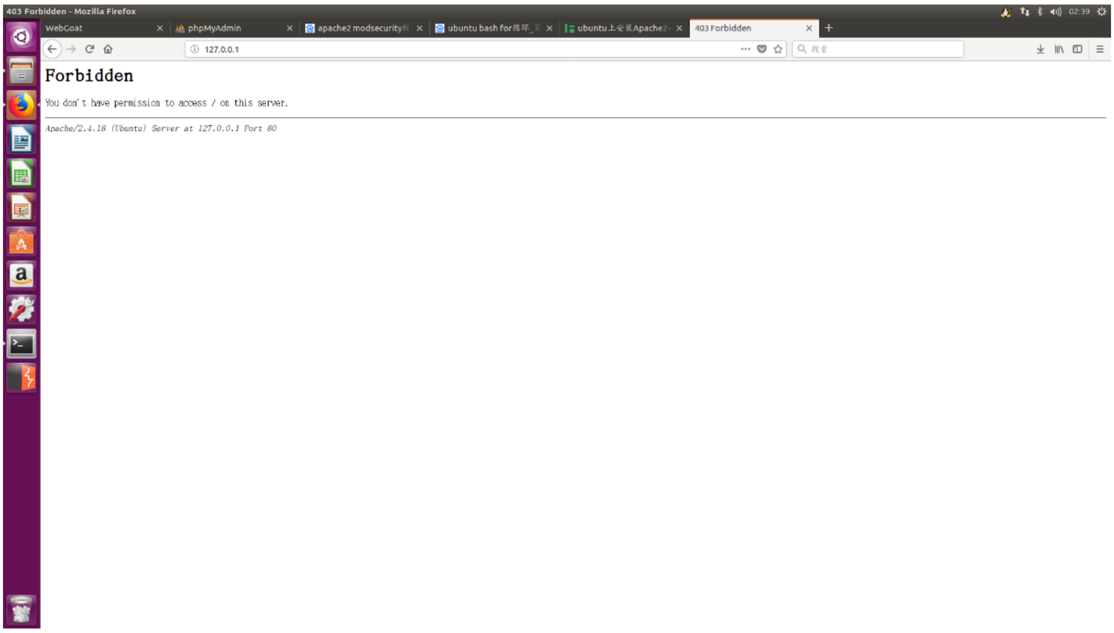
启用 modsecurity 模块



renxujie@ubuntu: /usr/share/modsecurity-crs/activated_rules

```
rs_41_sql_injection_attacks.conf
├── modsecurity_crs_41_xss_attacks.conf -> ../base_rules/modsecurity_crs_41_xss_
attacks.conf
├── modsecurity_crs_42_tight_security.conf -> ../base_rules/modsecurity_crs_42_t
ight_security.conf
├── modsecurity_crs_45_trojans.conf -> ../base_rules/modsecurity_crs_45_trojans.
conf
├── modsecurity_crs_47_common_exceptions.conf -> ../base_rules/modsecurity_crs_4
7_common_exceptions.conf
├── modsecurity_crs_48_local_exceptions.conf.example -> ../base_rules/modsecurit
y_crs_48_local_exceptions.conf.example
├── modsecurity_crs_49_inbound_blocking.conf -> ../base_rules/modsecurity_crs_49
_inbound_blocking.conf
├── modsecurity_crs_50_outbound.conf -> ../base_rules/modsecurity_crs_50_outboun
d.conf
├── modsecurity_crs_59_outbound_blocking.conf -> ../base_rules/modsecurity_crs_5
9_outbound_blocking.conf
├── modsecurity_crs_60_correlation.conf -> ../base_rules/modsecurity_crs_60_corr
elation.conf
└── README

0 directories, 24 files
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ sudo a2enmod headers
a2enmod security2
ERROR: Module headersa2enmod does not exist!
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  service apache2 restart
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ 
```

尝试访问 127.0.0.1，Apache 拒绝访问



403 Forbidden - Mozilla Firefox

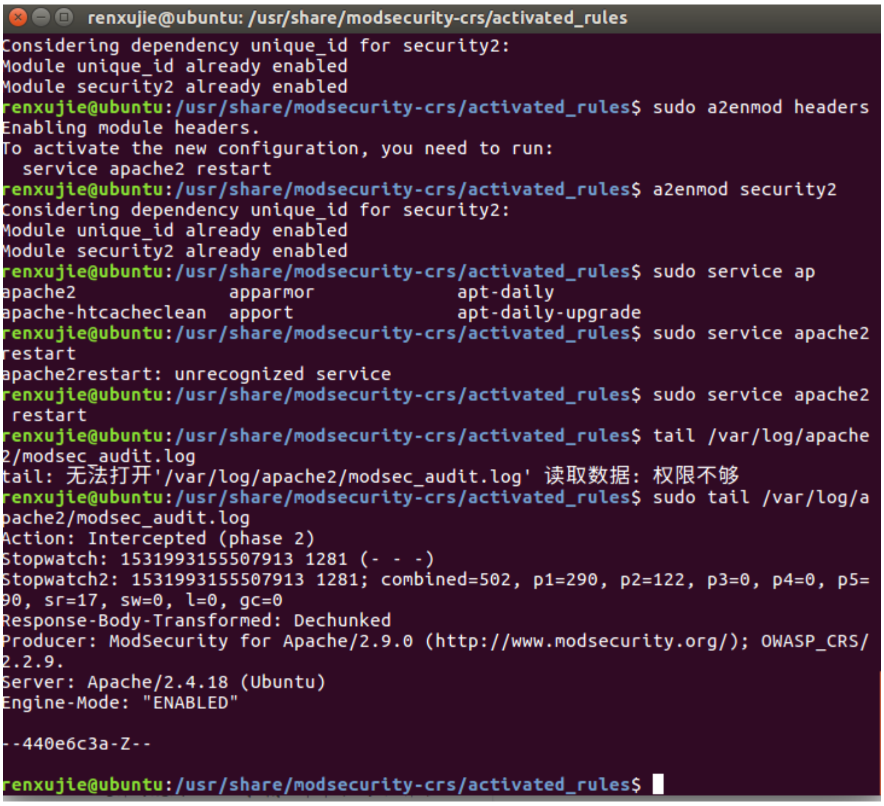
127.0.0.1

Forbidden

You don't have permission to access / on this server.

Apache/2.4.18 (Ubuntu) Server at 127.0.0.1 Port 80

查看/var/log/apache2/modsec_audit.log 日志文件

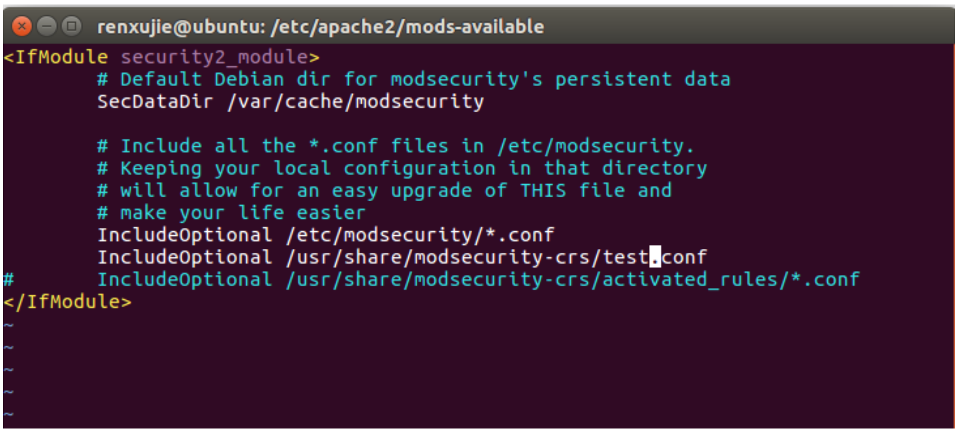


renxujie@ubuntu: /usr/share/modsecurity-crs/activated_rules

```
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  service apache2 restart
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ sudo service ap
apache2              apparmor             apt-daily
apache-htcacheclean  apport               apt-daily-upgrade
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ sudo service apache2
restart
apache2restart: unrecognized service
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ sudo service apache2
 restart
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ tail /var/log/apache
2/modsec_audit.log
tail: 无法打开'/var/log/apache2/modsec_audit.log' 读取数据: 权限不够
renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ sudo tail /var/log/a
pache2/modsec_audit.log
Action: Intercepted (phase 2)
Stopwatch: 1531993155507913 1281 (- - -)
Stopwatch2: 1531993155507913 1281; combined=502, p1=290, p2=122, p3=0, p4=0, p5=
90, sr=17, sw=0, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.0 (http://www.modsecurity.org/); OWASP_CRS/
2.2.9.
Server: Apache/2.4.18 (Ubuntu)
Engine-Mode: "ENABLED"

--440e6c3a-Z--

renxujie@ubuntu:/usr/share/modsecurity-crs/activated_rules$ 
```

3. 根据文档自行编写规则对 SQL 注入攻击进行阻断并报警

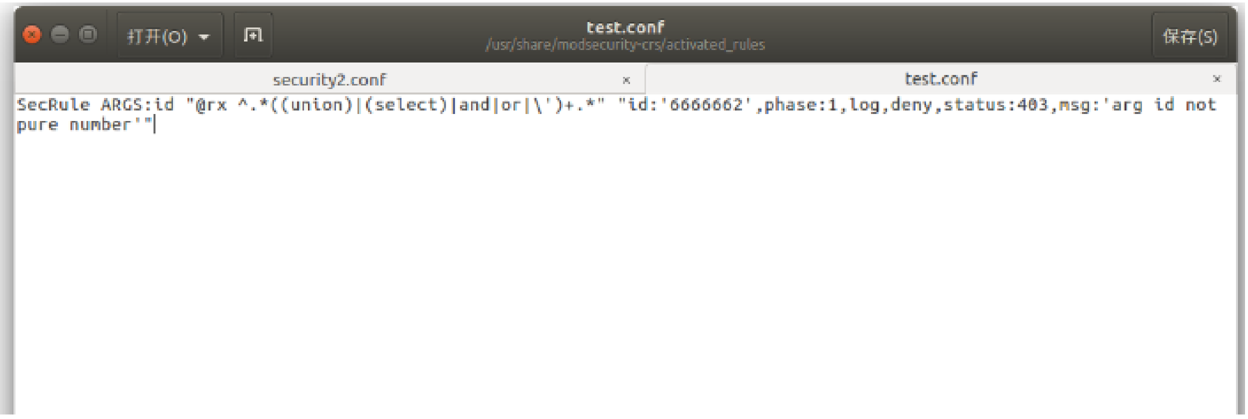
自行编写配置文件 test.conf，将路径添加到 security2.conf 中



renxujie@ubuntu: /etc/apache2/mods-available

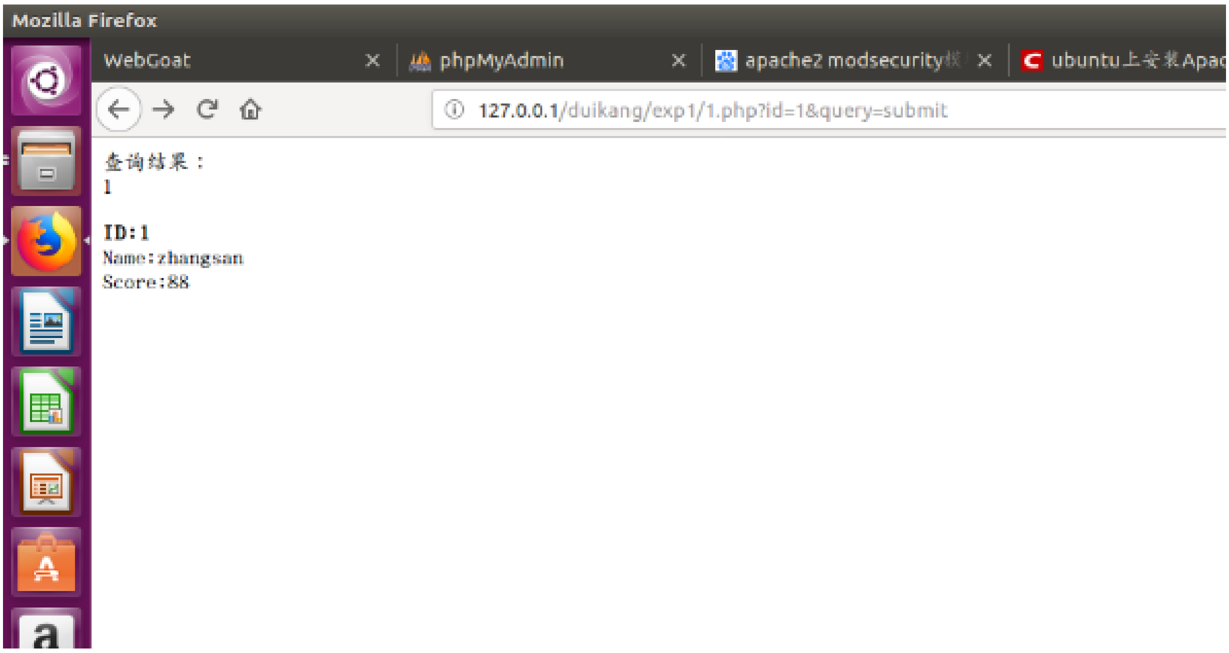
```
<IfModule security2_module>
        # Default Debian dir for modsecurity's persistent data
        SecDataDir /var/cache/modsecurity

        # Include all the *.conf files in /etc/modsecurity.
        # Keeping your local configuration in that directory
        # will allow for an easy upgrade of THIS file and
        # make your life easier
        IncludeOptional /etc/modsecurity/*.conf
        IncludeOptional /usr/share/modsecurity-crs/test.conf
#       IncludeOptional /usr/share/modsecurity-crs/activated_rules/*.conf
</IfModule>
~
~
~
~
~
```

Test.conf 的过滤规则设置为过滤 union、select、引号等关键字



```
SecRule ARGS:id "@rx ^.*((union)|(select)|and|or|\')+.*" "id:'6666662',phase:1,log,deny,status:403,msg:'arg id not
pure number'"
```

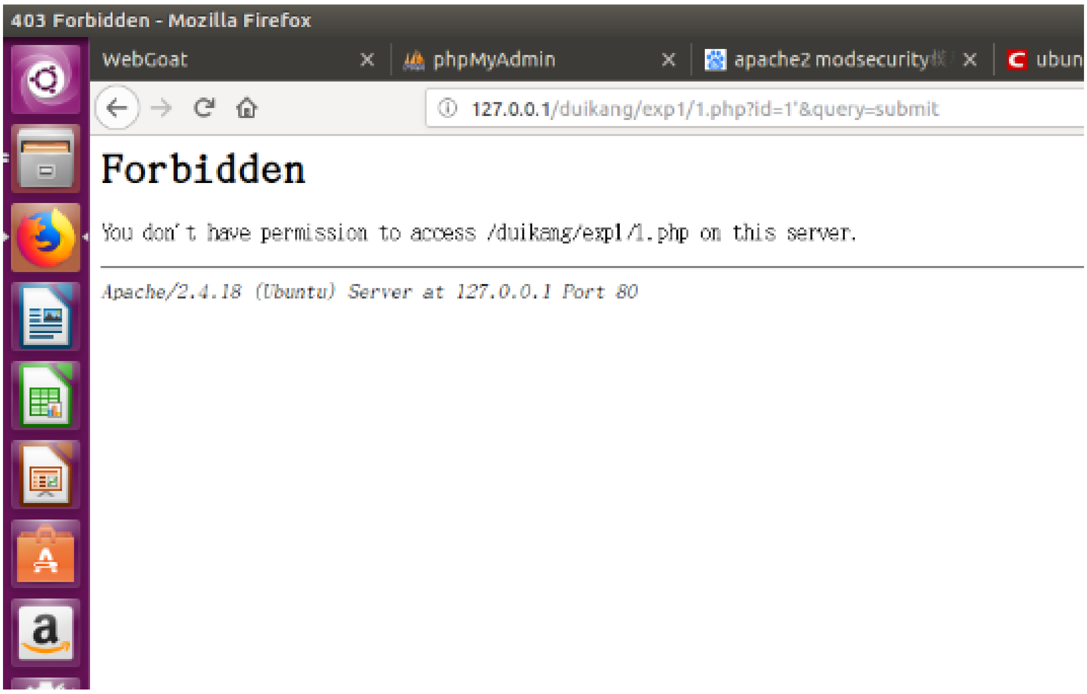
正常输入 id=1 时，页面正常显示



查询结果：
1

ID:1
Name:zhangsan
Score:88

尝试注入，页面拒绝访问



403 Forbidden - Mozilla Firefox

127.0.0.1/duikang/exp1/1.php?id=1'&query=submit

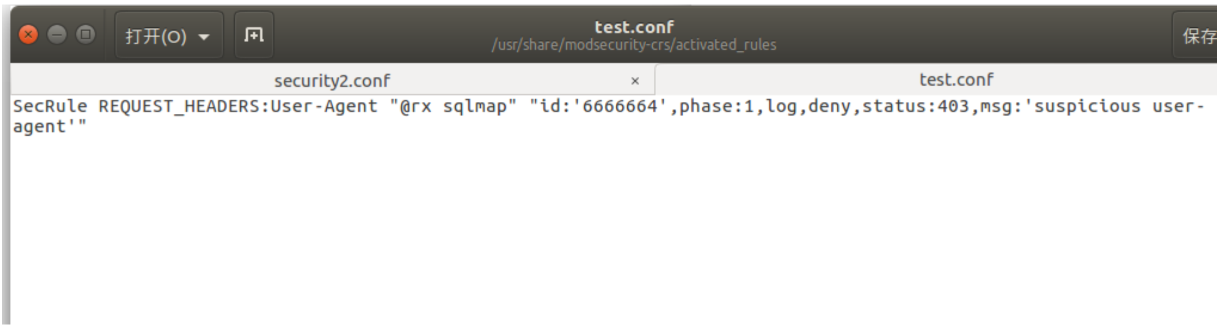
Forbidden

You don't have permission to access /duikang/exp1/1.php on this server.

Apache/2.4.18 (Ubuntu) Server at 127.0.0.1 Port 80

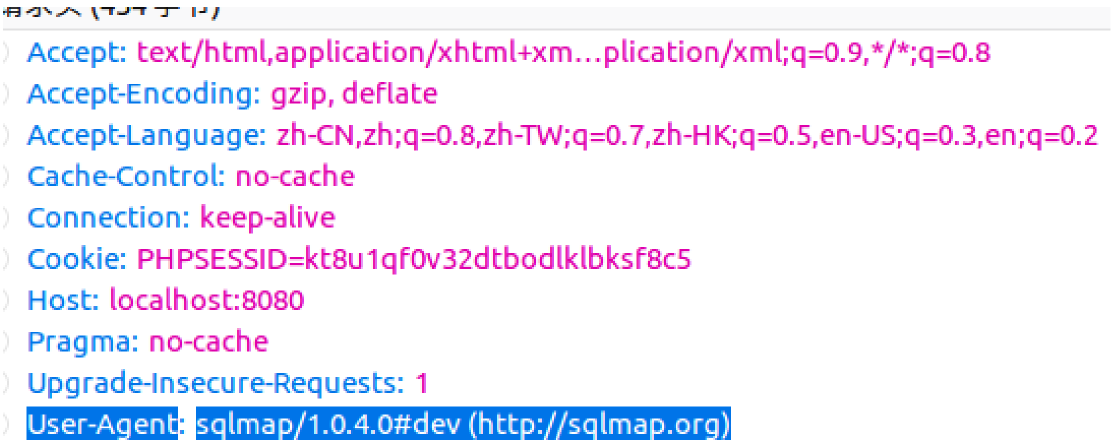
4. **尝试对特定扫描器或发包工具（paros、w3af 等）的 User-Agent 进行检测和报警，并在单个 IP 访问数量超过一定门限后对来源 IP 进行封禁**

使用 sqlmap 注入并抓包，可以知道 sqlmap 的 user-agent 头为 sqlmap/1.0.4.0#dev (http://sqlmap.org)，所以，在 test.conf 中添加如下一行：



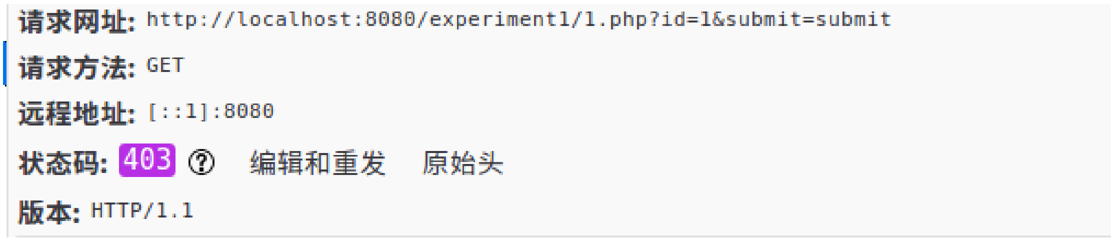
```
SecRule REQUEST_HEADERS:User-Agent "@rx sqlmap" "id:'6666664',phase:1,log,deny,status:403,msg:'suspicious user-agent'"
```

当我们用 sqlmap 进行测试时：



```
Accept: text/html,application/xhtml+xm…plication/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cache-Control: no-cache
Connection: keep-alive
Cookie: PHPSESSID=kt8u1qf0v32dtbodlklbksf8c5
Host: localhost:8080
Pragma: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: sqlmap/1.0.4.0#dev (http://sqlmap.org)
```

可以看到请求被拦截：



请求网址: http://localhost:8080/experiment1/1.php?id=1&submit=submit

请求方法: GET

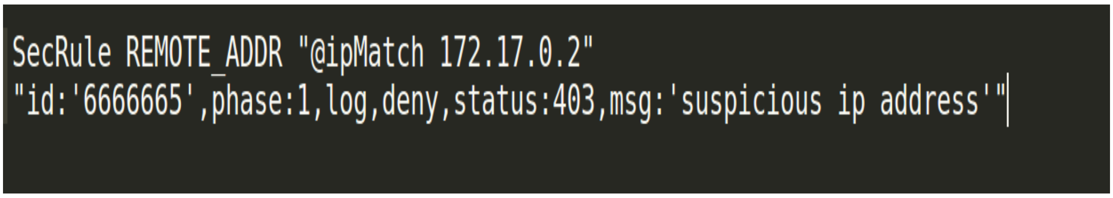
远程地址: [::1]:8080

状态码: 403

版本: HTTP/1.1

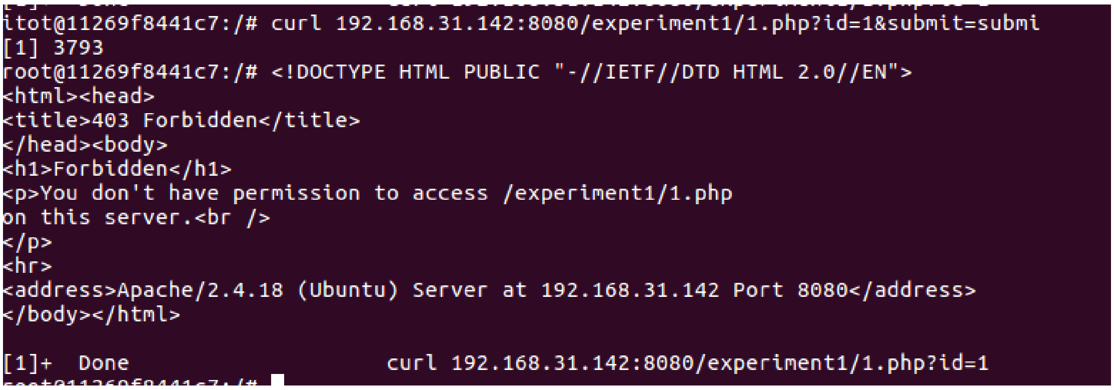
当我们探测到有一个 ip 以非常规的速率访问我们的服务器，使用 modsecurity 封禁 ip。

添加的配置语句如下：

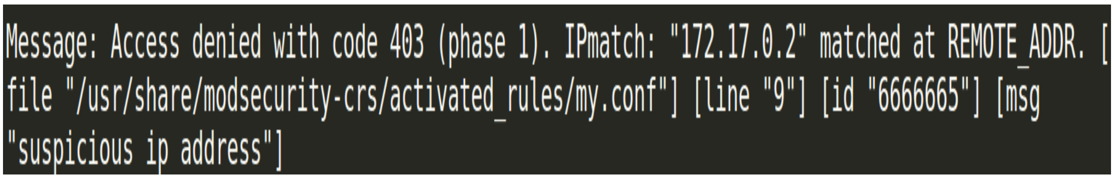


```
SecRule REMOTE_ADDR "@ipMatch 172.17.0.2"
"id:'6666665',phase:1,log,deny,status:403,msg:'suspicious ip address'"
```

当我们使用我们 docker 出来的 kali 通过 curl 访问我们主机时，就会被拦截。如下：



```
itot@11269f8441c7:/# curl 192.168.31.142:8080/experiment1/1.php?id=1&submit=submi
[1] 3793
root@11269f8441c7:/# <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /experiment1/1.php
on this server.<br />
</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 192.168.31.142 Port 8080</address>
</body></html>

[1]+  Done                    curl 192.168.31.142:8080/experiment1/1.php?id=1
root@11269f8441c7:/# 
```



```
Message: Access denied with code 403 (phase 1). IPmatch: "172.17.0.2" matched at REMOTE_ADDR. [
file "/usr/share/modsecurity-crs/activated_rules/my.conf"] [line "9"] [id "6666665"] [msg
"suspicious ip address"]
```