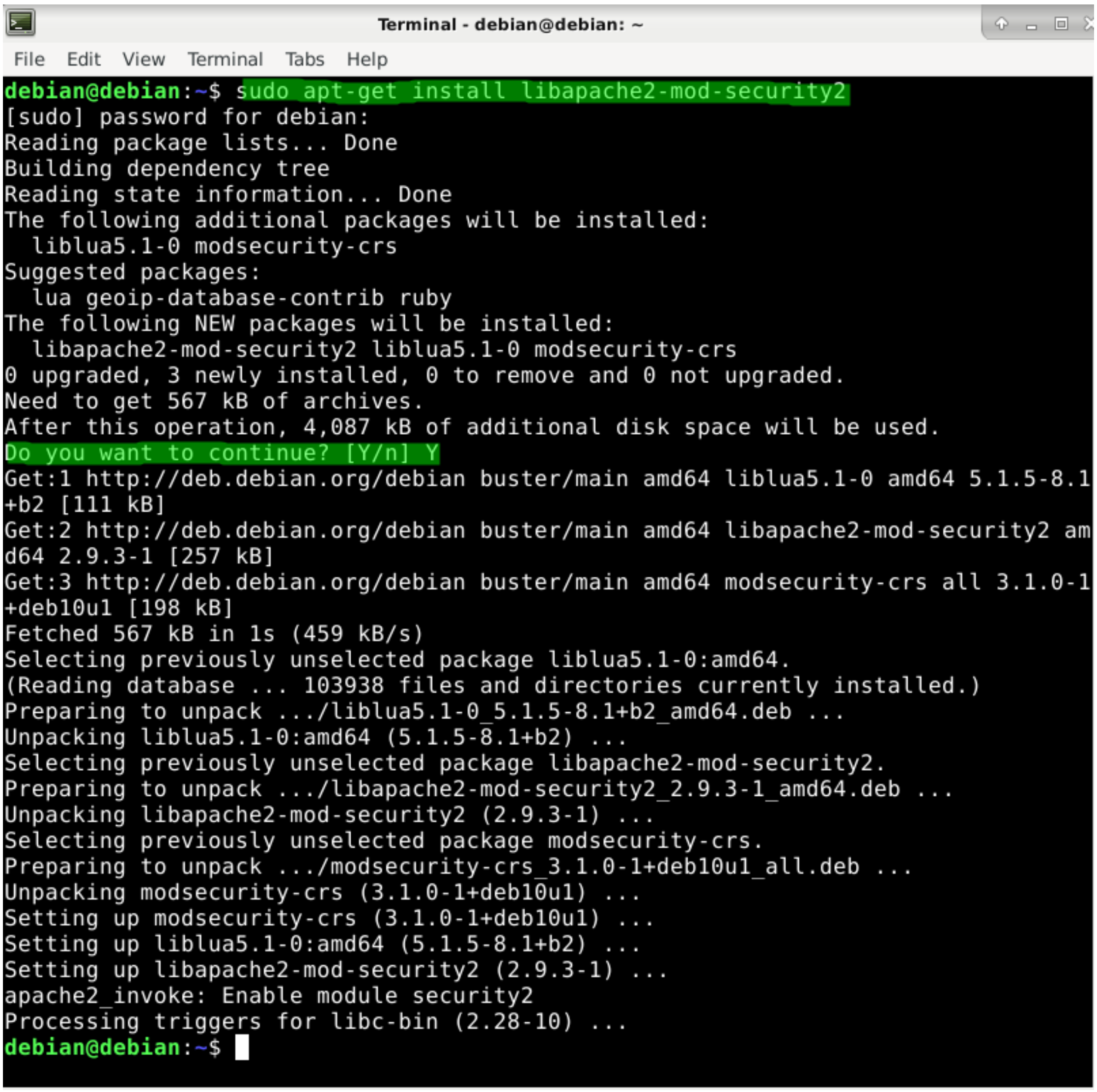
SQLi to Shell - Instalación y configuración de Modsecurity

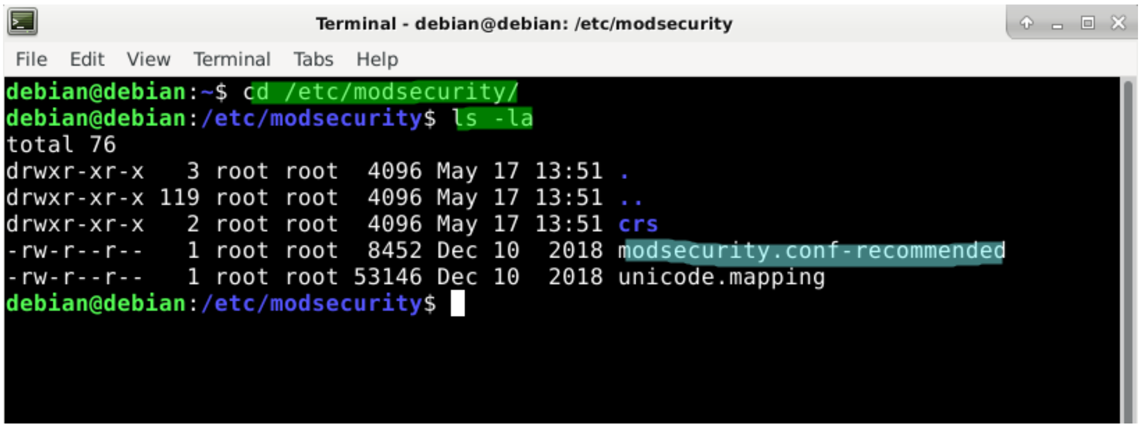
1) Ejecutar *“sudo apt-get install libapache2-mod-security2”* e *“Y”* para instalar Modsecurity.



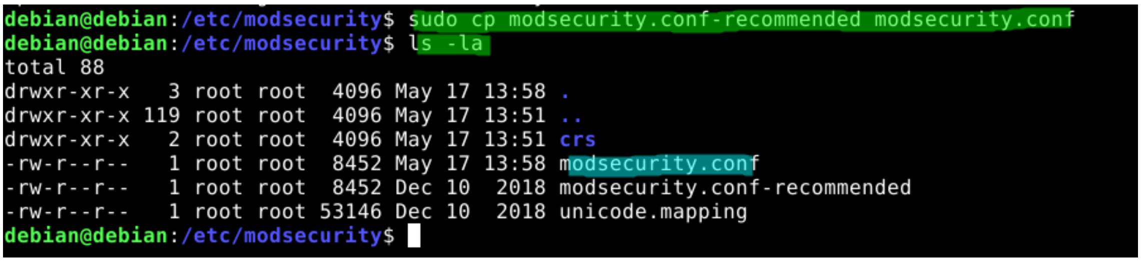
Terminal - debian@debian: ~
File Edit View Terminal Tabs Help

```
debian@debian:~$ sudo apt-get install libapache2-mod-security2
[sudo] password for debian:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  liblua5.1-0 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby
The following NEW packages will be installed:
  libapache2-mod-security2 liblua5.1-0 modsecurity-crs
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 567 kB of archives.
After this operation, 4,087 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian buster/main amd64 liblua5.1-0 amd64 5.1.5-8.1
+b2 [111 kB]
Get:2 http://deb.debian.org/debian buster/main amd64 libapache2-mod-security2 am
d64 2.9.3-1 [257 kB]
Get:3 http://deb.debian.org/debian buster/main amd64 modsecurity-crs all 3.1.0-1
+deb10u1 [198 kB]
Fetched 567 kB in 1s (459 kB/s)
Selecting previously unselected package liblua5.1-0:amd64.
(Reading database ... 103938 files and directories currently installed.)
Preparing to unpack .../liblua5.1-0_5.1.5-8.1+b2_amd64.deb ...
Unpacking liblua5.1-0:amd64 (5.1.5-8.1+b2) ...
Selecting previously unselected package libapache2-mod-security2.
Preparing to unpack .../libapache2-mod-security2_2.9.3-1_amd64.deb ...
Unpacking libapache2-mod-security2 (2.9.3-1) ...
Selecting previously unselected package modsecurity-crs.
Preparing to unpack .../modsecurity-crs_3.1.0-1+deb10u1_all.deb ...
Unpacking modsecurity-crs (3.1.0-1+deb10u1) ...
Setting up modsecurity-crs (3.1.0-1+deb10u1) ...
Setting up liblua5.1-0:amd64 (5.1.5-8.1+b2) ...
Setting up libapache2-mod-security2 (2.9.3-1) ...
apache2_invoke: Enable module security2
Processing triggers for libc-bin (2.28-10) ...
debian@debian:~$
```

2) Ingresar a la carpeta de Modsecurity *“cd /etc/modsecurity”* y copiar el archivo de configuración *“sudo cp modsecurity.conf-recommended modsecurity.conf”*

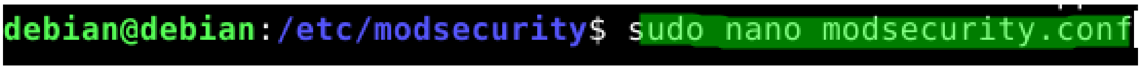

Terminal - debian@debian: /etc/modsecurity
File Edit View Terminal Tabs Help

```
debian@debian:~$ cd /etc/modsecurity/
debian@debian:/etc/modsecurity$ ls -la
total 76
drwxr-xr-x   3 root root  4096 May 17 13:51 .
drwxr-xr-x 119 root root  4096 May 17 13:51 ..
drwxr-xr-x   2 root root  4096 May 17 13:51 crs
-rw-r--r--   1 root root  8452 Dec 10  2018 modsecurity.conf-recommended
-rw-r--r--   1 root root 53146 Dec 10  2018 unicode.mapping
debian@debian:/etc/modsecurity$
```



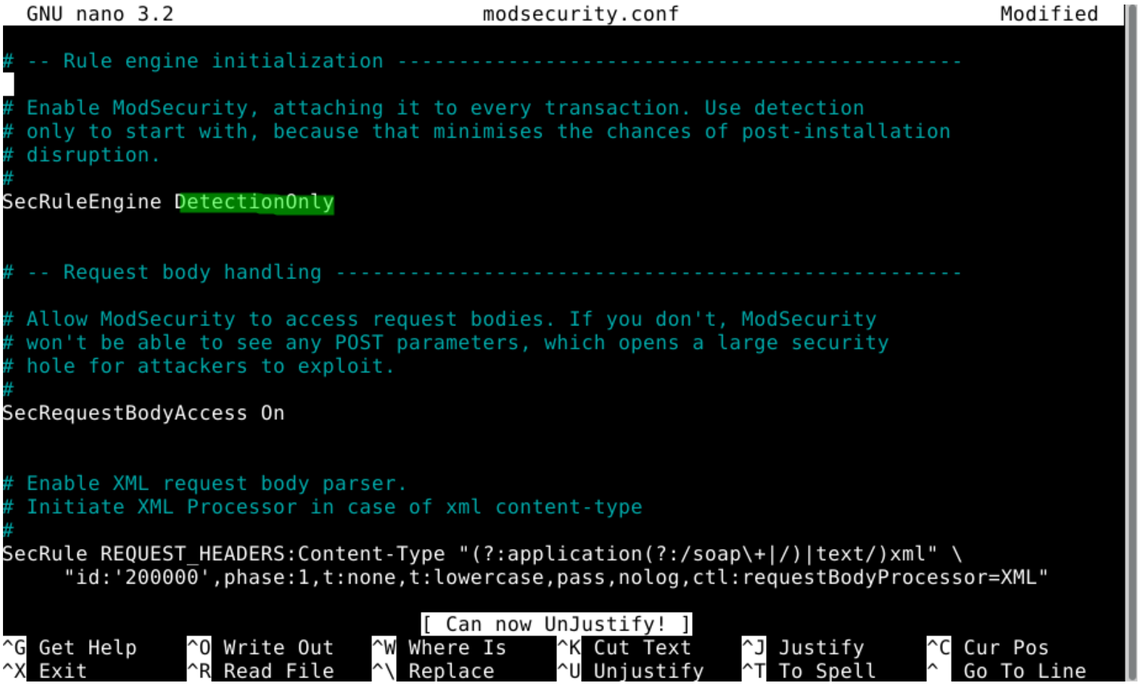
```
debian@debian:/etc/modsecurity$ sudo cp modsecurity.conf-recommended modsecurity.conf
debian@debian:/etc/modsecurity$ ls -la
total 88
drwxr-xr-x   3 root root  4096 May 17 13:58 .
drwxr-xr-x 119 root root  4096 May 17 13:51 ..
drwxr-xr-x   2 root root  4096 May 17 13:51 crs
-rw-r--r--   1 root root  8452 May 17 13:58 modsecurity.conf
-rw-r--r--   1 root root  8452 Dec 10  2018 modsecurity.conf-recommended
-rw-r--r--   1 root root 53146 Dec 10  2018 unicode.mapping
debian@debian:/etc/modsecurity$
```

3) Abrir el archivo copiado con un editor de texto *“sudo nano modsecurity.conf”*

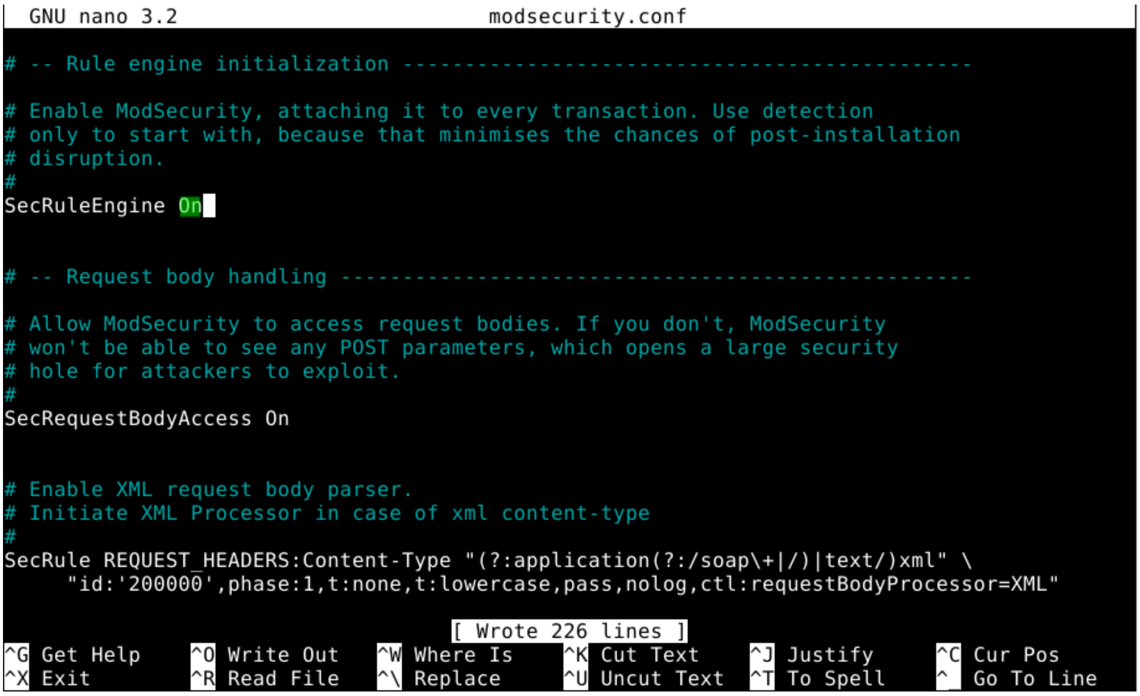


```
debian@debian:/etc/modsecurity$ sudo nano modsecurity.conf
```

4) En el apartado *“Rule engine initialization”* cambiar la propiedad *“DetectionOnly”* por *“On”*.

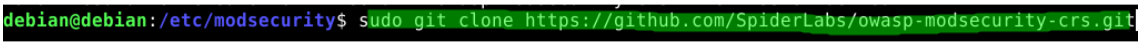


```
  GNU nano 3.2                      modsecurity.conf                     Modified

# -- 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 DetectionOnly


# -- 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 "(?:application(?:/soap\+|/)|text/)xml" \
     "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"

                           [ Can now UnJustify! ]
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
^X Exit         ^R Read File    ^\ Replace      ^U Unjustify    ^T To Spell     ^_ Go To Line
```



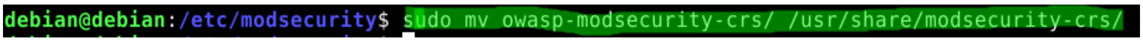
```
  GNU nano 3.2                          modsecurity.conf

# -- 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 "(?:application(?:/soap\+|/)|text/)xml" \
     "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"

                                    [ Wrote 226 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

5) Dentro de */etc/modsecurity/* clonar el repositorio de Git: *"sudo git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git"*



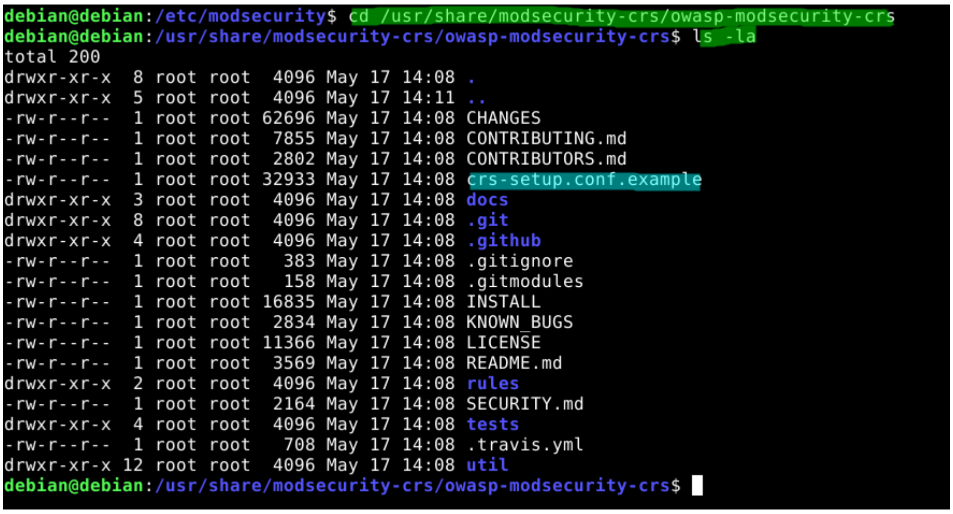
```
debian@debian:/etc/modsecurity$ sudo git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git
```

6) Mover la carpeta *owasp-modsecurity-crs/* al directorio */usr/share/modsecurity-crs/* : *"sudo mv owasp-modsecurity-crs/ /usr/share/modsecurity-crs/"*



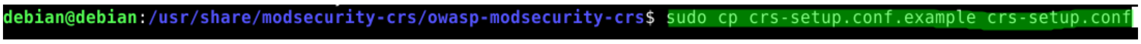
```
debian@debian:/etc/modsecurity$ sudo mv owasp-modsecurity-crs/ /usr/share/modsecurity-crs/
```

7) Ingresar a la carpeta */usr/share/modsecurity-crs/owasp-modsecurity-crs/*: *"cd /usr/share/modsecurity-crs/owasp-modsecurity-crs/"*



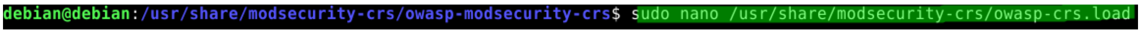
```
debian@debian:/etc/modsecurity$ cd /usr/share/modsecurity-crs/owasp-modsecurity-crs
debian@debian:/usr/share/modsecurity-crs/owasp-modsecurity-crs$ ls -la
total 200
drwxr-xr-x  8 root root  4096 May 17 14:08 .
drwxr-xr-x  5 root root  4096 May 17 14:11 ..
-rw-r--r--  1 root root 62696 May 17 14:08 CHANGES
-rw-r--r--  1 root root  7855 May 17 14:08 CONTRIBUTING.md
-rw-r--r--  1 root root  2802 May 17 14:08 CONTRIBUTORS.md
-rw-r--r--  1 root root 32933 May 17 14:08 crs-setup.conf.example
drwxr-xr-x  3 root root  4096 May 17 14:08 docs
drwxr-xr-x  8 root root  4096 May 17 14:08 .git
drwxr-xr-x  4 root root  4096 May 17 14:08 .github
-rw-r--r--  1 root root   383 May 17 14:08 .gitignore
-rw-r--r--  1 root root   158 May 17 14:08 .gitmodules
-rw-r--r--  1 root root 16835 May 17 14:08 INSTALL
-rw-r--r--  1 root root  2834 May 17 14:08 KNOWN_BUGS
-rw-r--r--  1 root root 11366 May 17 14:08 LICENSE
-rw-r--r--  1 root root  3569 May 17 14:08 README.md
drwxr-xr-x  2 root root  4096 May 17 14:08 rules
-rw-r--r--  1 root root  2164 May 17 14:08 SECURITY.md
drwxr-xr-x  4 root root  4096 May 17 14:08 tests
-rw-r--r--  1 root root   708 May 17 14:08 .travis.yml
drwxr-xr-x 12 root root  4096 May 17 14:08 util
debian@debian:/usr/share/modsecurity-crs/owasp-modsecurity-crs$ 
```

8) Copiar el archivo *crs-setup.conf.example:*
"sudo cp crs-setup.conf.example crs-setup.conf"



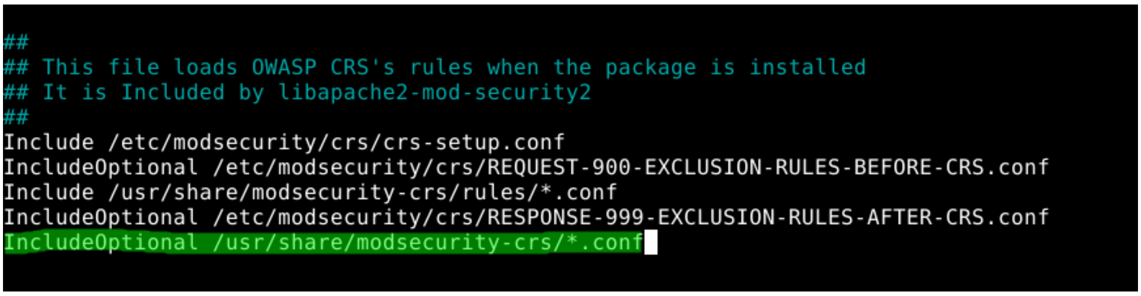
```
debian@debian:/usr/share/modsecurity-crs/owasp-modsecurity-crs$ sudo cp crs-setup.conf.example crs-setup.conf
```

9) Editar el archivo *owasp-crs.load:*
"sudo nano /usr/share/modsecurity-crs/owasp-crs.load"



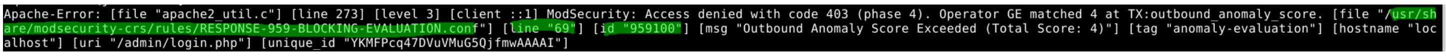
```
debian@debian:/usr/share/modsecurity-crs/owasp-modsecurity-crs$ sudo nano /usr/share/modsecurity-crs/owasp-crs.load
```

10) Agregar la siguiente línea al final del archivo:
"IncludeOptional /usr/share/modsecurity-crs/.conf"*



```
##
## This file loads OWASP CRS's rules when the package is installed
## It is Included by libapache2-mod-security2
##
Include /etc/modsecurity/crs/crs-setup.conf
IncludeOptional /etc/modsecurity/crs/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf
Include /usr/share/modsecurity-crs/rules/*.conf
IncludeOptional /etc/modsecurity/crs/RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf
IncludeOptional /usr/share/modsecurity-crs/*.conf
```

11) Comentar las reglas que bloqueen funcionalidades necesarias de la aplicación (chequear el log en: */var/log/apache2/modsec_audit.log*). Por ejemplo:



```
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client ::1] ModSecurity: Access denied with code 403 (phase 4). Operator GE matched 4 at TX:outbound_anomaly_score. [file "/usr/sh
are/modsecurity-crs/rules/RESPONSE-959-BLOCKING-EVALUATION.conf"] [line "69"] [id "959100"] [msg "Outbound Anomaly Score Exceeded (Total Score: 4)"] [tag "anomaly-evaluation"] [hostname "loc
alhost"] [uri "/admin/login.php"] [unique_id "YKMFPcq47DVuVMuG5QjfmwAAAAI"]
```

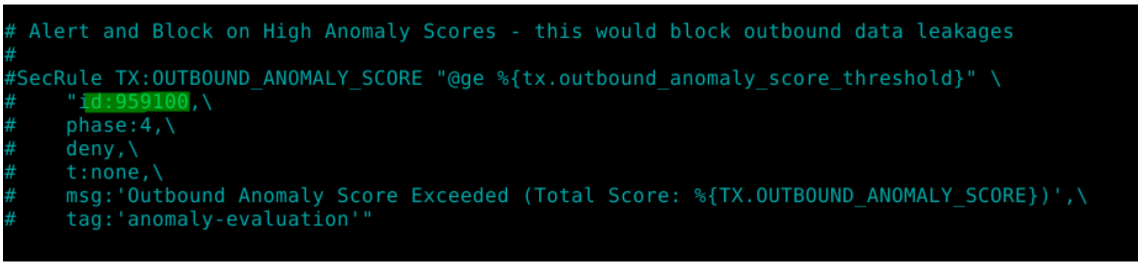
Abrir el archivo señalado con un editor de texto:
"sudo nano
/usr/share/modsecurity-crs/rules/RESPONSE-959-BLOCKING-EVALUATION.conf"

Buscar:
"CTRL+W"

Introducir el ID

“959100”

Comentar la regla:

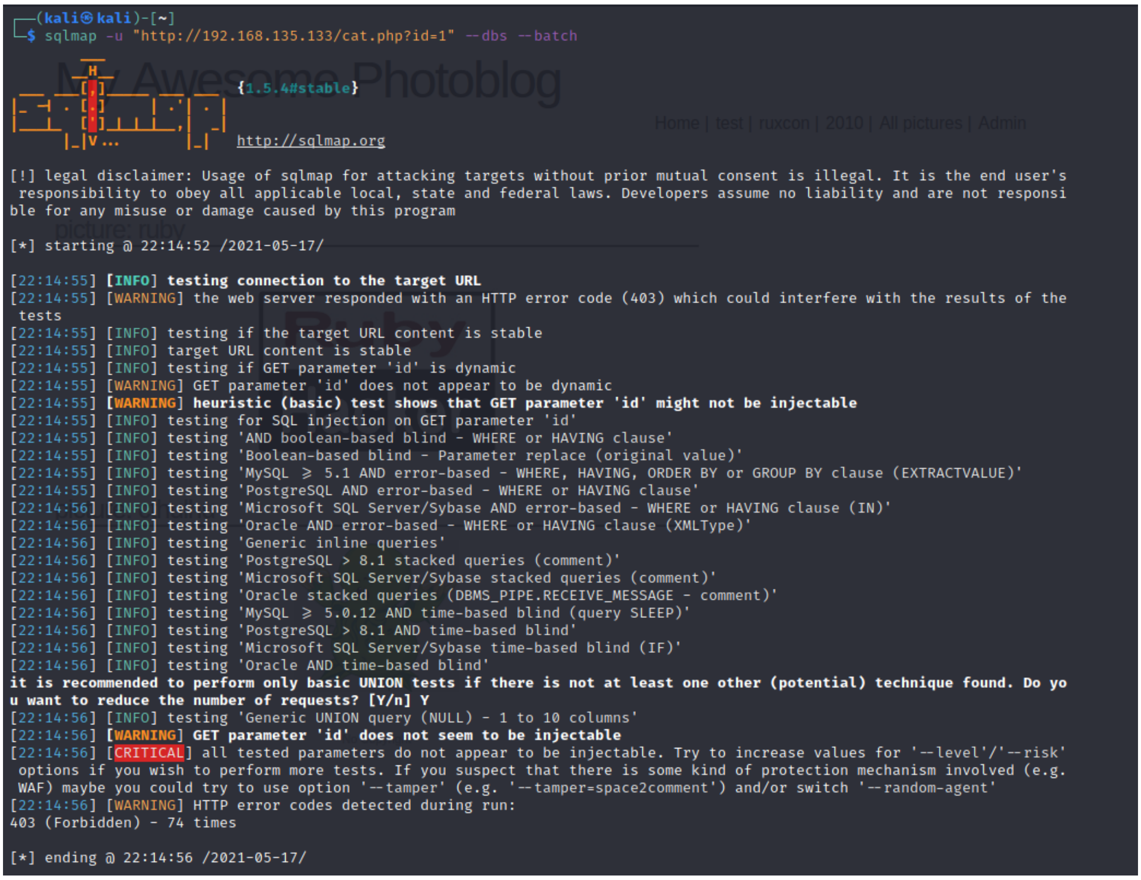


```
# Alert and Block on High Anomaly Scores - this would block outbound data leakages
#
#SecRule TX:OUTBOUND_ANOMALY_SCORE "@ge %{tx.outbound_anomaly_score_threshold}" \
#     "id:959100,\
#     phase:4,\
#     deny,\
#     t:none,\
#     msg:'Outbound Anomaly Score Exceeded (Total Score: %{TX.OUTBOUND_ANOMALY_SCORE})',\
#     tag:'anomaly-evaluation'"
```

12) Reiniciar el servicio de apache:
“systemctl restart apache2”

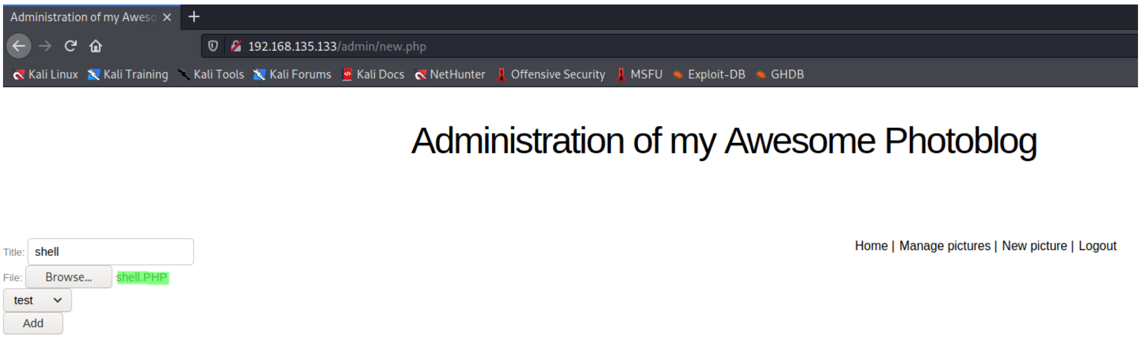
Intentos de ataque luego de instalar Modsecurity

1) Inyección de SQL



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.135.133/cat.php?id=1" --dbs --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
 responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsi
ble for any misuse or damage caused by this program

[*] starting @ 22:14:52 /2021-05-17/

[22:14:55] [INFO] testing connection to the target URL
[22:14:55] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the
 tests
[22:14:55] [INFO] testing if the target URL content is stable
[22:14:55] [INFO] target URL content is stable
[22:14:55] [INFO] testing if GET parameter 'id' is dynamic
[22:14:55] [WARNING] GET parameter 'id' does not appear to be dynamic
[22:14:55] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[22:14:55] [INFO] testing for SQL injection on GET parameter 'id'
[22:14:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:14:55] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:14:55] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:14:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:14:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:14:56] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:14:56] [INFO] testing 'Generic inline queries'
[22:14:56] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:14:56] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:14:56] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[22:14:56] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[22:14:56] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:14:56] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:14:56] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do yo
u want to reduce the number of requests? [Y/n] Y
[22:14:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:14:56] [WARNING] GET parameter 'id' does not seem to be injectable
[22:14:56] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk'
 options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g.
 WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[22:14:56] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 74 times

[*] ending @ 22:14:56 /2021-05-17/
```

2) Carga de archivos sin restricciones



Administration of my Awesome Photoblog

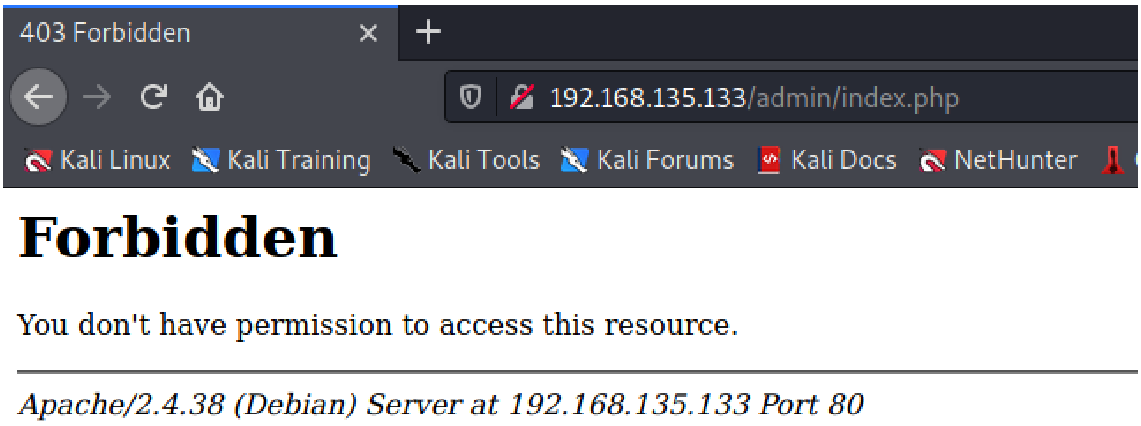
Home | Manage pictures | New picture | Logout

Title: shell

File: Browse... shell.PHP

test

Add

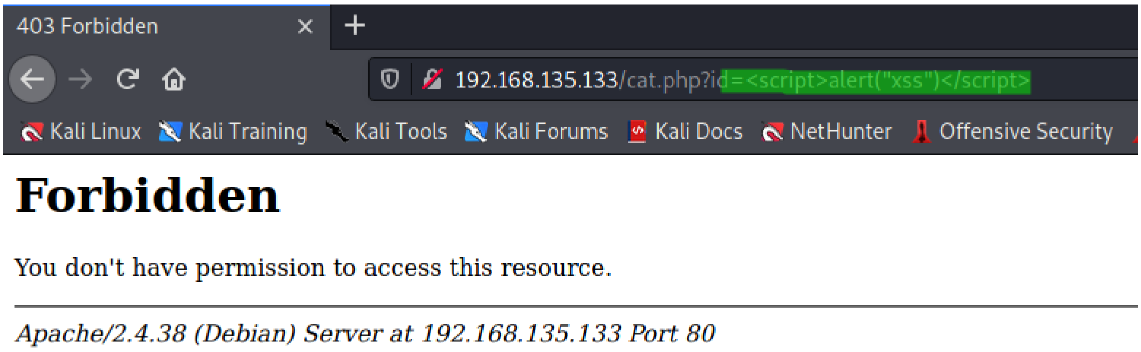


Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 192.168.135.133 Port 80

3) XSS Reflejado



Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 192.168.135.133 Port 80

- Reporte Clockify: https://clockify.me/shared/60a3178c9c65a6590cdc1be8