EJERCICIOS MODSECURITY

Prerrequisitos

- Debian 11
- Windows Server 2012 Protección de Activos

Ejercicio 1 - ModSecurity

- Instalar y configurar ModSecurity en Debian 11.

  Para esto realizaremos lo siguiente, instalaremos el paquete a continuacion

```
root@Debian11:/var/log# apt install libmodsecurity-dev libmodsecurity3 modsecurity-crs
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libmodsecurity-dev is already the newest version (3.0.4-2).
libmodsecurity3 is already the newest version (3.0.4-2).
modsecurity-crs is already the newest version (3.3.0-1+deb11u1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

  Luego instalamos apache2

```
root@Debian11:/home/vboxuser# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.56-1~deb11u2).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

  Tras esto el apt-file

```
root@Debian11:/home/vboxuser# apt install apt-file
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apt-file is already the newest version (3.2.2).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

  Realizamos el siguiente comando

```
root@Debian11:/home/vboxuser# apt-file search apachectl
apache2: /usr/sbin/apachectl
apache2: /usr/share/man/man8/apachectl.8.gz
apache2-doc: /usr/share/doc/apache2-doc/manual/da/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/de/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/en/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/es/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/fr/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/ja/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/ko/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/pt-br/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/ru/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/tr/programs/apachectl.html
apache2-doc: /usr/share/doc/apache2-doc/manual/zh-cn/programs/apachectl.html
zsh-common: /usr/share/zsh/functions/Completion/Unix/_apachectl
```

  Aplicamos este

```
root@Debian11:/home/vboxuser# /usr/sbin/apachectl -M
Loaded Modules:
 core_module (static)
 so_module (static)
 watchdog_module (static)
 http_module (static)
 log_config_module (static)
 logio_module (static)
 version_module (static)
 unixd_module (static)
 access_compat_module (shared)
 alias_module (shared)
 auth_basic_module (shared)
 authn_core_module (shared)
 authn_file_module (shared)
 authz_core_module (shared)
 authz_host_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 deflate_module (shared)
 dir_module (shared)
 env_module (shared)
 filter_module (shared)
 mime_module (shared)
 mpm_prefork_module (shared)
 negotiation_module (shared)
 php7_module (shared)
 reqtimeout_module (shared)
 security2_module (shared)
 setenvif_module (shared)
 status_module (shared)
 unique_id_module (shared)
```

Reinstalamos el paquete modsecurity2

```
root@Debian11:/home/vboxuser# sudo apt install libapache2-mod-security2 --reinstall
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 1 reinstalled, 0 to remove and 1 not upgraded.
Need to get 259 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 libapache2-mod-security2 amd64 2.9.3-3+deb1
1u1 [259 kB]
Fetched 259 kB in 0s (2,871 kB/s)
(Reading database ... 186154 files and directories currently installed.)
Preparing to unpack .../libapache2-mod-security2_2.9.3-3+deb11u1_amd64.deb ...
Unpacking libapache2-mod-security2 (2.9.3-3+deb11u1) over (2.9.3-3+deb11u1) ...
Setting up libapache2-mod-security2 (2.9.3-3+deb11u1) ...
apache2_invoke security2: already enabled
```

No movemos a la carpeta de este mismo y realizamos el siguiente comando

```
root@Debian11:/etc/modsecurity# sudo a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
```

A continuación modificamos el archivo modsecurity.conf

```
  GNU nano 5.4                    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 DetectionOnly
#SecRuleEngine On
```

Reiniciamos el sistema para que se apliquen los cambios

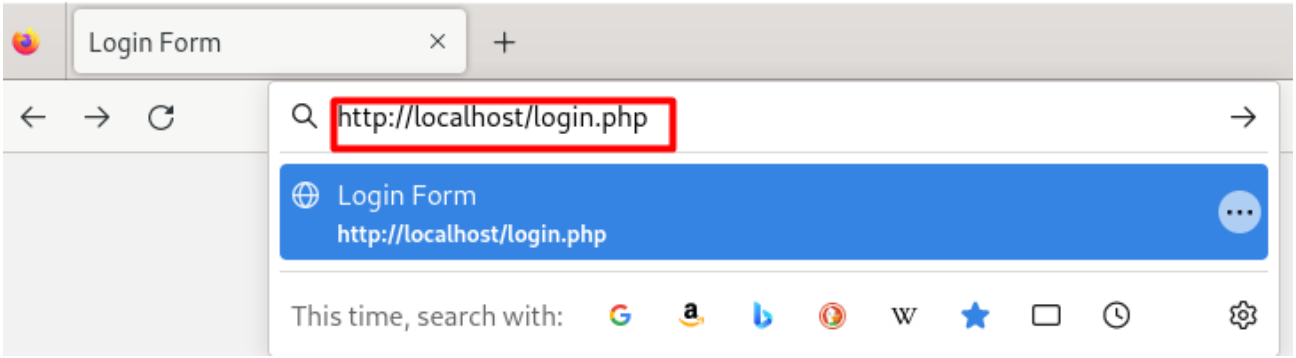
```
root@Debian11:/etc/modsecurity# sudo systemctl restart apache2
```

Ahora modificamos el nombre del archivo

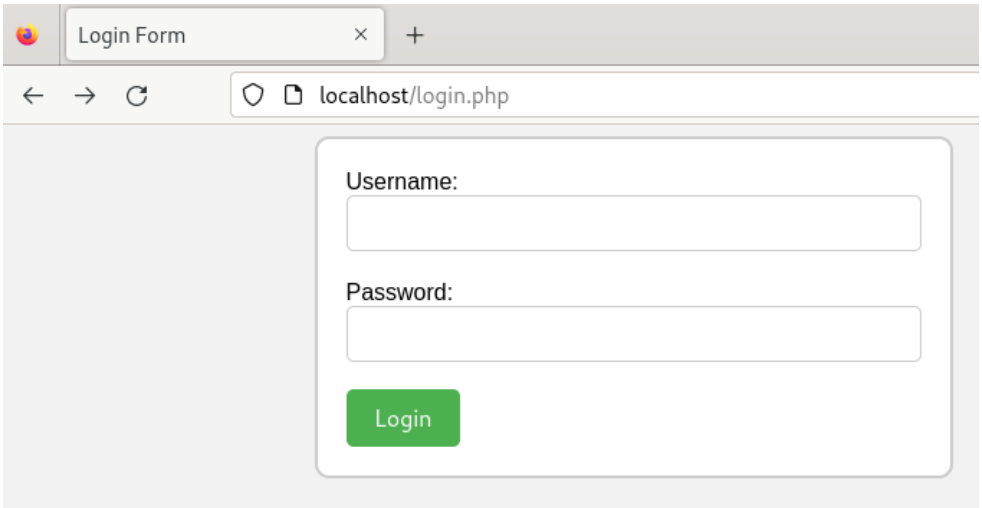
```
root@Debian11:/etc/modsecurity# sudo mv /etc/modsecurity/modsecurity.conf-recomm
ended /etc/modsecurity/modsecurity.conf
root@Debian11:/etc/modsecurity# ls
crs  modsecurity.conf  unicode.mapping
```

- Ralizar ataques SQLi.

  Una vez hecho lo anterior nos dirigimos al buscador y copiamos lo siguiente



Como resultado obtenemos la siguiente interfaz

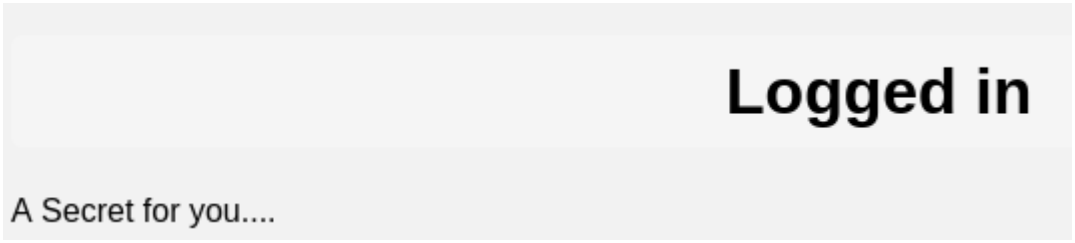


Mientras tanto en nuestra terminal nos dirigimos a la siguiente carpeta y copiamos el siguiente comando

```
root@Debian11:/var/log/apache2# tail -f modsec_audit.log
Apache-Handler: application/x-httpd-php
Stopwatch: 1701359192341376 82567 (- - -)
Stopwatch2: 1701359192341376 82567; combined=17094, p1=1275, p2=14685, p3=0, p4=0, p5=1134, sr=95, sw=0,
 l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.3 (http://www.modsecurity.org/); OWASP_CRS/3.3.0.
Server: Apache/2.4.56 (Debian)
Engine-Mode: "ENABLED"
```

Realizamos un ataque SQL

Obtenemos lo siguiente si nos logueamos



Y cuando volvemos a la terminal vemos esto

```
--4b94c65e-H--
Message: Warning. detected SQLi using libinjection with fingerprint 's&sos' [file "/usr/share/modsecurit
y-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "65"] [id "942100"] [msg "SQL Injection Att
ack Detected via libinjection"] [data "Matched Data: s&sos found within ARGS:username: ' OR '1' = '1' --
"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "
platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248
/66"] [tag "PCI/6.5.2"]
Message: Warning. Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQ
UEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Tota
l Score: 5)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-mul
ti"] [tag "platform-multi"] [tag "attack-generic"]
Message: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/r
ules/RESPONSE-980-CORRELATION.conf"] [line "91"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Tot
al Inbound Score: 5 - SQLI=5,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level sc
ores: 5, 0, 0, 0"] [ver "OWASP_CRS/3.3.0"] [tag "event-correlation"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 127.0.0.1] ModSecurity: Warning. dete
cted SQLi using libinjection with fingerprint 's&sos' [file "/usr/share/modsecurity-crs/rules/REQUEST-94
2-APPLICATION-ATTACK-SQLI.conf"] [line "65"] [id "942100"] [msg "SQL Injection Attack Detected via libin
jection"] [data "Matched Data: s&sos found within ARGS:username: ' OR '1' = '1' --"] [severity "CRITICAL
"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/66"] [tag "PCI/6.5.2"
] [hostname "localhost"] [uri "/login.php"] [unique_id "ZW4-2klyxoqv8r6u_NZjPgAAAAA"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 127.0.0.1] ModSecurity: Warning. Oper
ator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVAL
UATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 5)"] [severit
y "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-mu
lti"] [tag "attack-generic"] [hostname "localhost"] [uri "/login.php"] [unique_id "ZW4-2klyxoqv8r6u_NZjP
gAAAAA"]
```

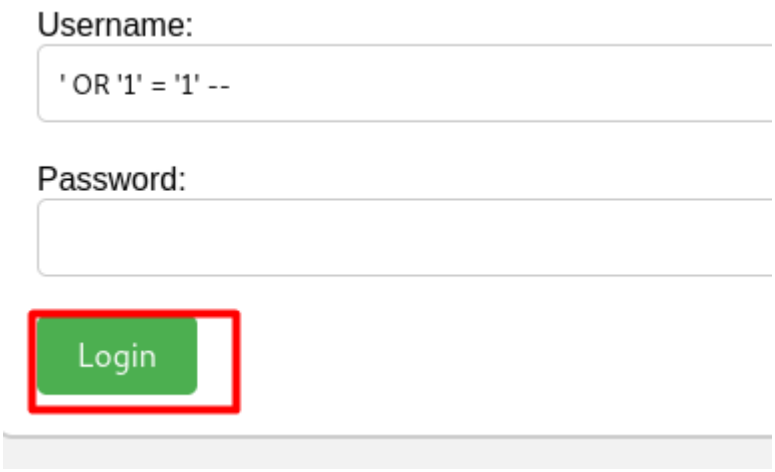
- Demostrar que ModSecurity funciona en modo detección y en modo bloqueo.

  Para esto volvemos a la carpeta etc y modificamos el archivo .conf

```
  GNU nano 5.4                                  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 DetectionOnly
SecRuleEngine On
```

Volvemos a la pagina de nuestro buscador y volvemos a inyectar un SQL



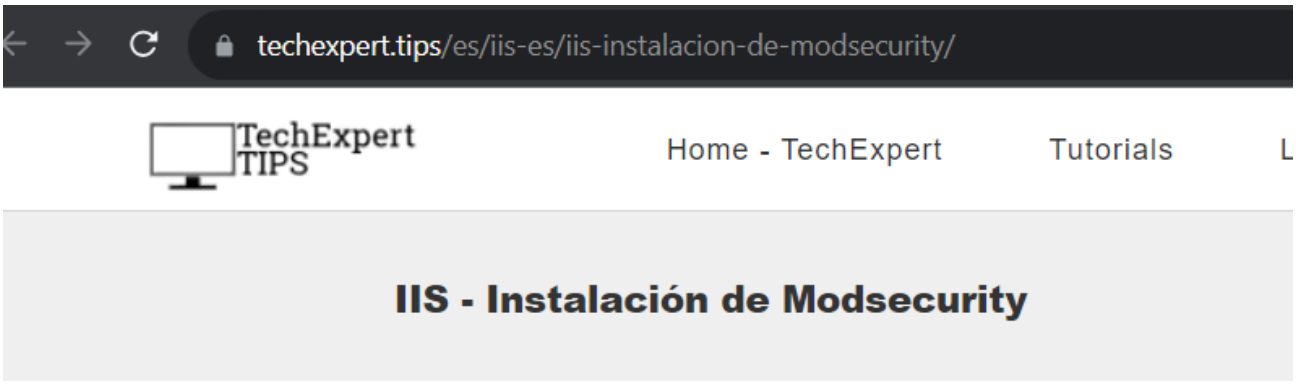
Como resultado en nuestra terminal tenemos lo siguiente

```
--4b94c65e-H--
Message: Warning. detected SQLi using libinjection with fingerprint 's&sos' [file "/usr/share/modsecurit
y-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "65"] [id "942100"] [msg "SQL Injection Att
ack Detected via libinjection"] [data "Matched Data: s&sos found within ARGS:username: ' OR '1' = '1' --
"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "
platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248
/66"] [tag "PCI/6.5.2"]
Message: Warning. Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQ
UEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Tota
l Score: 5)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-mul
ti"] [tag "platform-multi"] [tag "attack-generic"]
Message: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/r
ules/RESPONSE-980-CORRELATION.conf"] [line "91"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Tot
al Inbound Score: 5 - SQLI=5,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level sc
ores: 5, 0, 0, 0"] [ver "OWASP_CRS/3.3.0"] [tag "event-correlation"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 127.0.0.1] ModSecurity: Warning. dete
cted SQLi using libinjection with fingerprint 's&sos' [file "/usr/share/modsecurity-crs/rules/REQUEST-94
2-APPLICATION-ATTACK-SQLI.conf"] [line "65"] [id "942100"] [msg "SQL Injection Attack Detected via libin
jection"] [data "Matched Data: s&sos found within ARGS:username: ' OR '1' = '1' --"] [severity "CRITICAL
"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/66"] [tag "PCI/6.5.2"
] [hostname "localhost"] [uri "/login.php"] [unique_id "ZW5BVQ-LGiXuRv2xwS600QAAAAE"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 127.0.0.1] ModSecurity: Warning. Oper
ator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVAL
UATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 5)"] [severit
y "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-mu
lti"] [tag "attack-generic"] [hostname "localhost"] [uri "/login.php"] [unique_id "ZW5BVQ-LGiXuRv2xwS600
QAAAAE"]
```

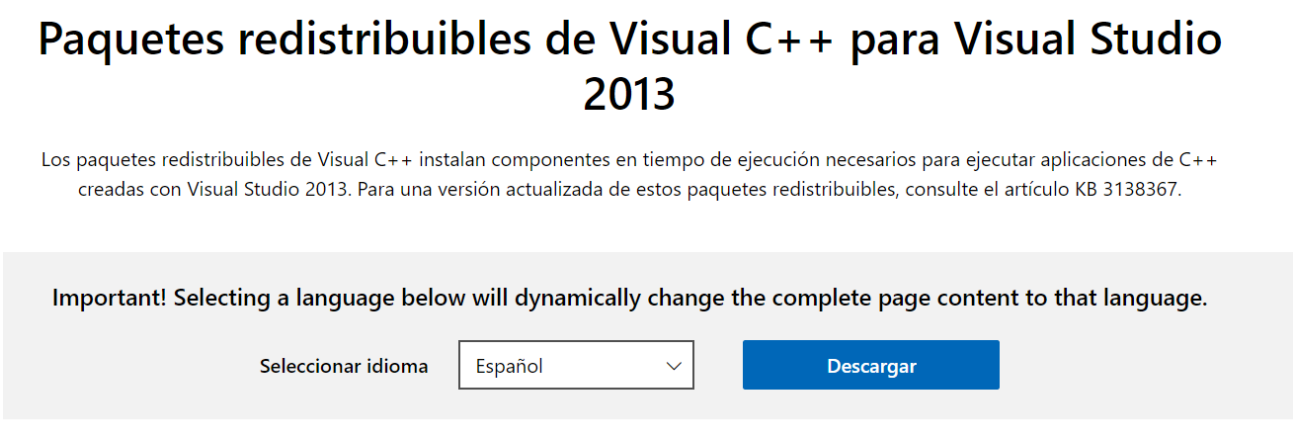
Ejercicio 2 - ModSecurity

- Instalar ModSecurity en Windows Server 2012 Protección de Activos siguiendo la guía:
- https://techexpert.tips/es/iis-es/iis-instalacion-de-modsecurity/

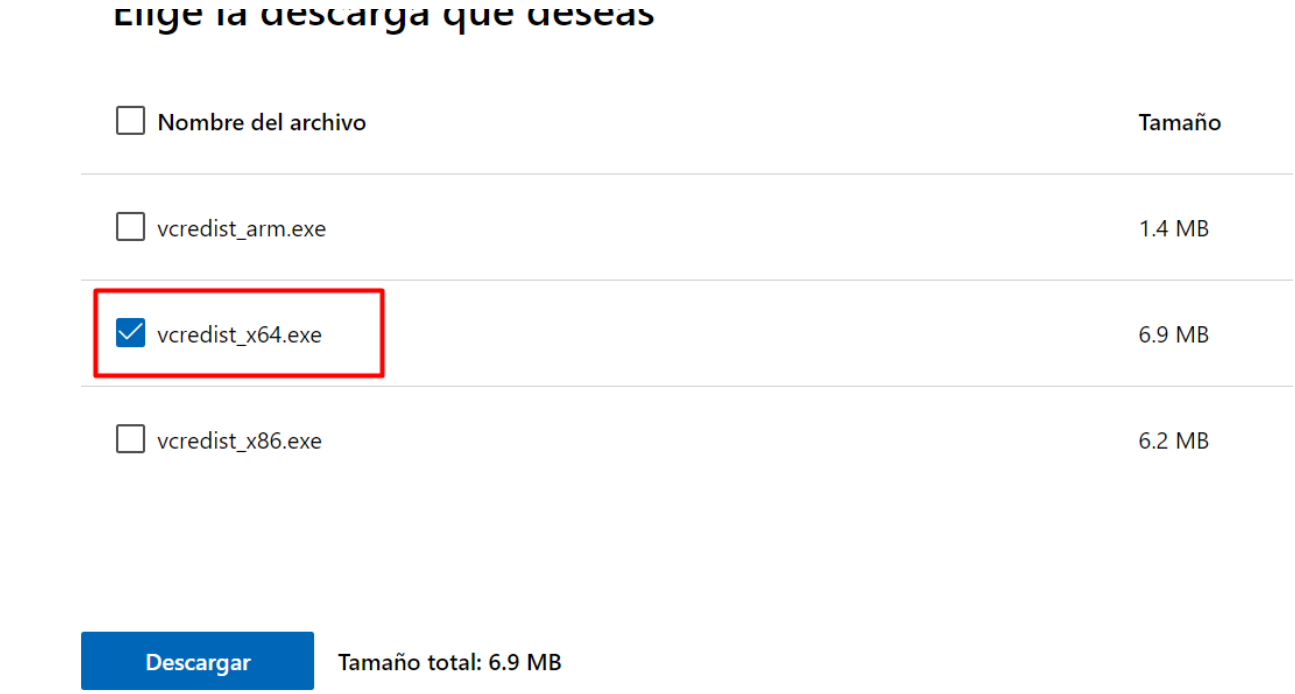
Accedemos a la página



Le damos al enlace de microsfot

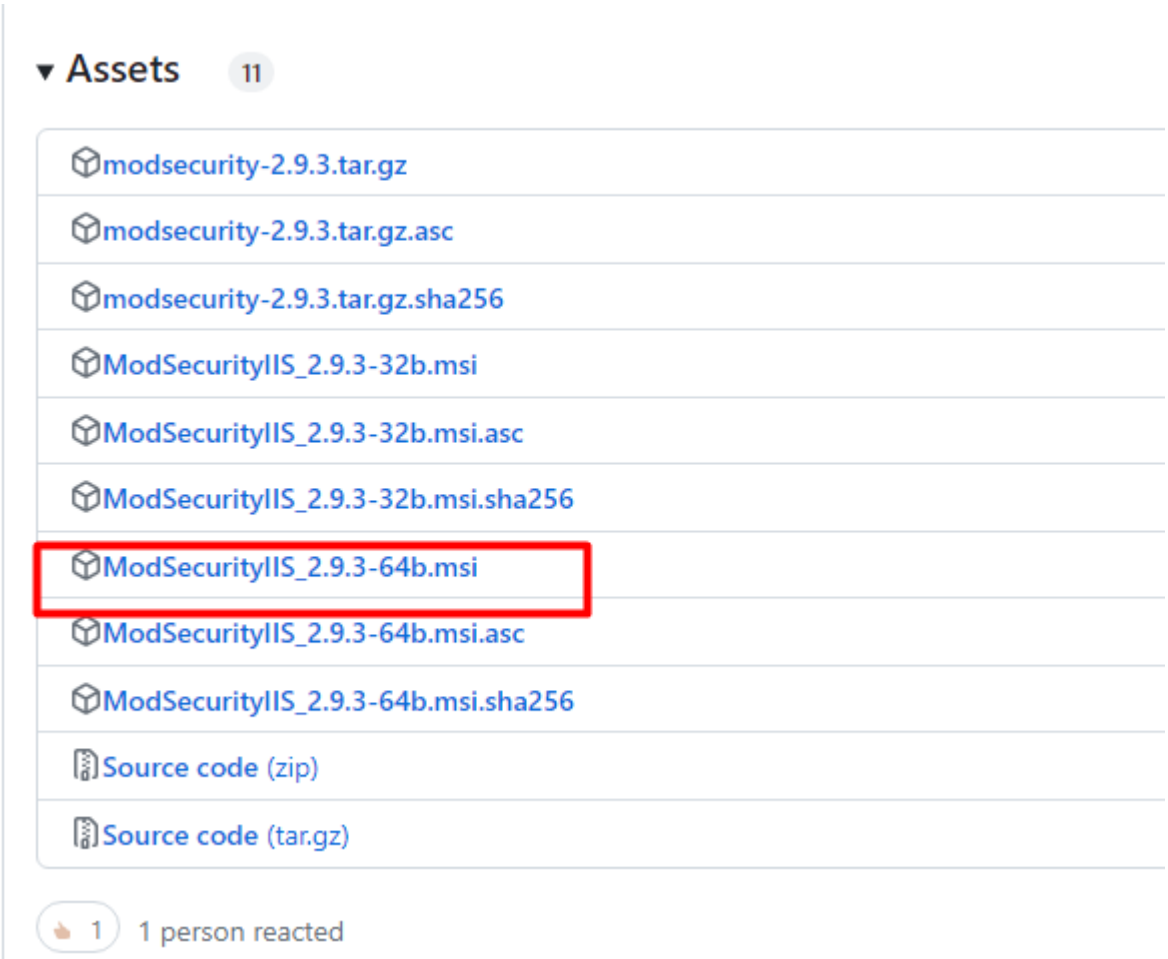


Damos a descargar y escogemos la opción x64



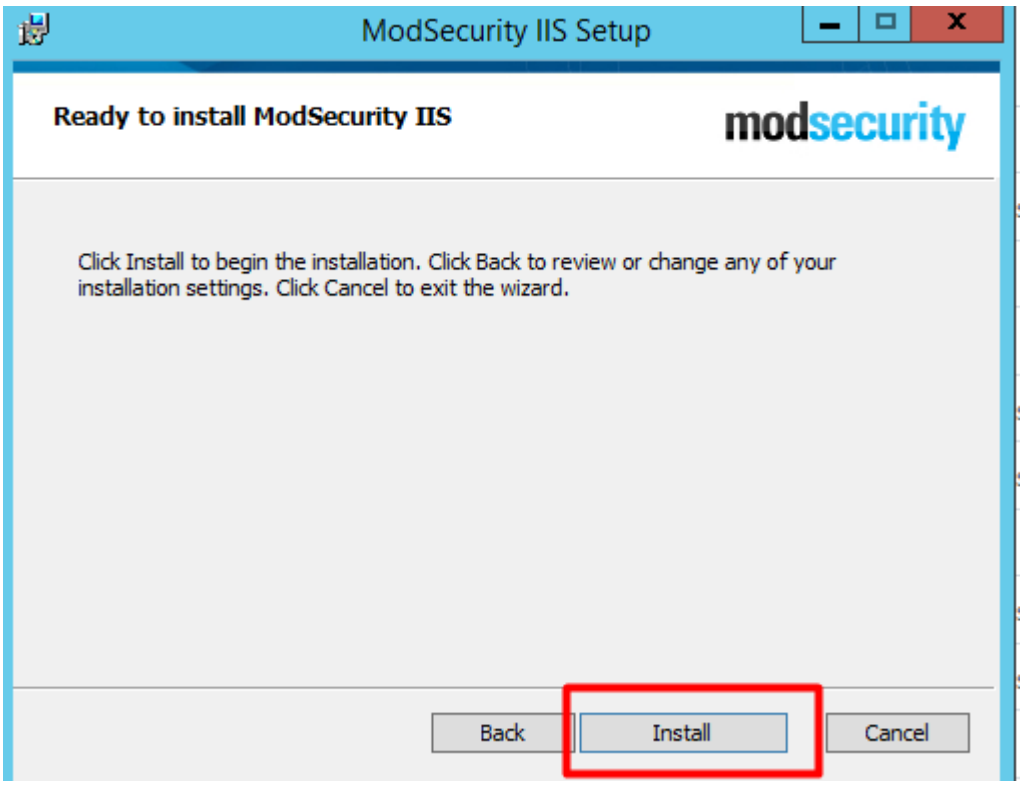
Abrimos el archivo descargado e iniciamos el instalador

Una vez hemos terminado la instalación nos dirigimos al repo de github a descargar mod security y en este nos dirigimos al instalador



Una vez lo ejecutamos tenemos lo siguiente

Continuamos e instalamos

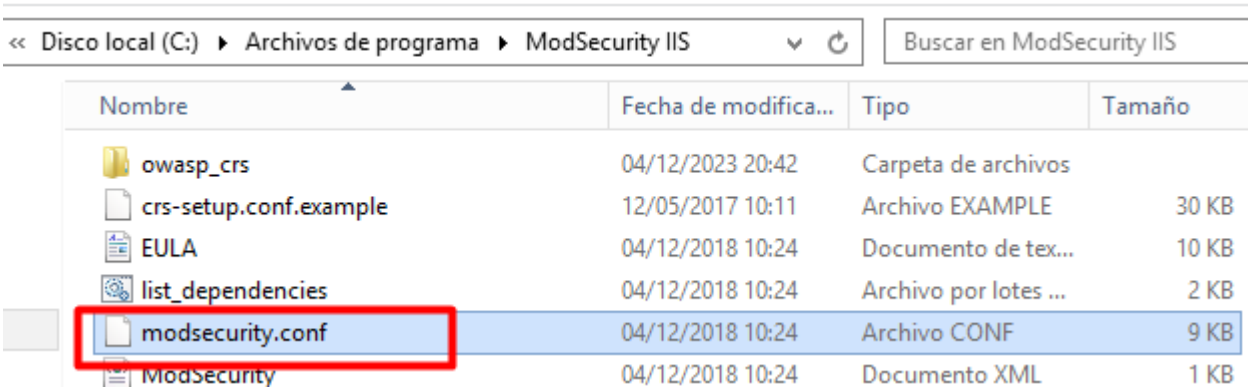


Una vez hecho esto comprobamos la instalación de este

```
C:\Users\Administrador>cd C:\Program Files\ModSecurity IIS

C:\Program Files\ModSecurity IIS>
```

Nos dirigimos a la carpeta de modsecurity y abrimos el siguiente archivo con WordPad



Una vez abierto modificamos el archivo

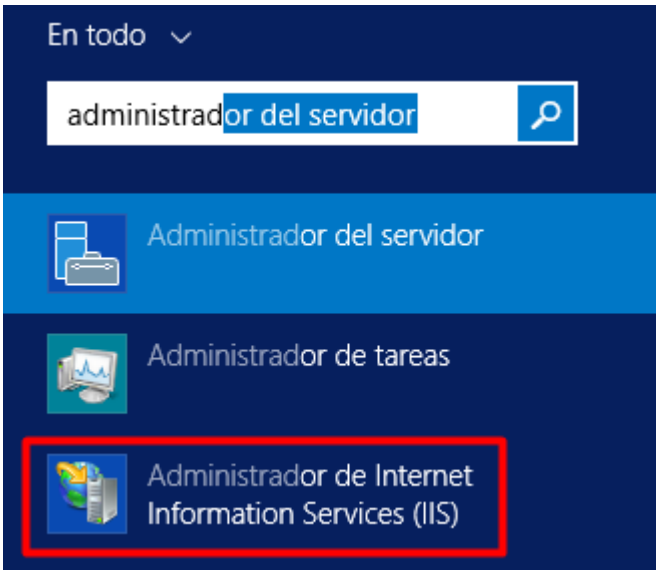
```
#     Rule engine
initialization ----------------------------

# Enable ModSecurity, attaching it to every
detection
# only to start with, because that minimise
post-installation
# disruption.
#
SecRuleEngine DetectionOnly
SecRuleEngine On
```

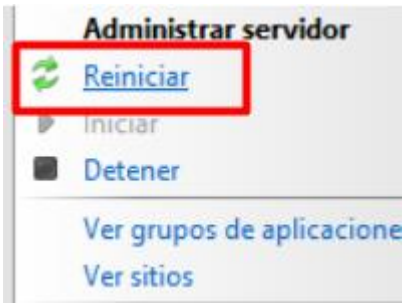
Volvemos al cmd y copiamos el siguiente comando

```
C:\Users\Administrador>cacls C:\inetpub\temp /e /p IIS_IUSRS:f
directorio procesado: C:\inetpub\temp
```

Buscamos la siguiente herramienta y la abrimos



Una vez dentro damos click derecho al ordenador y reiniciamos



Tras esto abrimos en nuestro buscador la siguiente IP que como resultado nos dará una interfaz