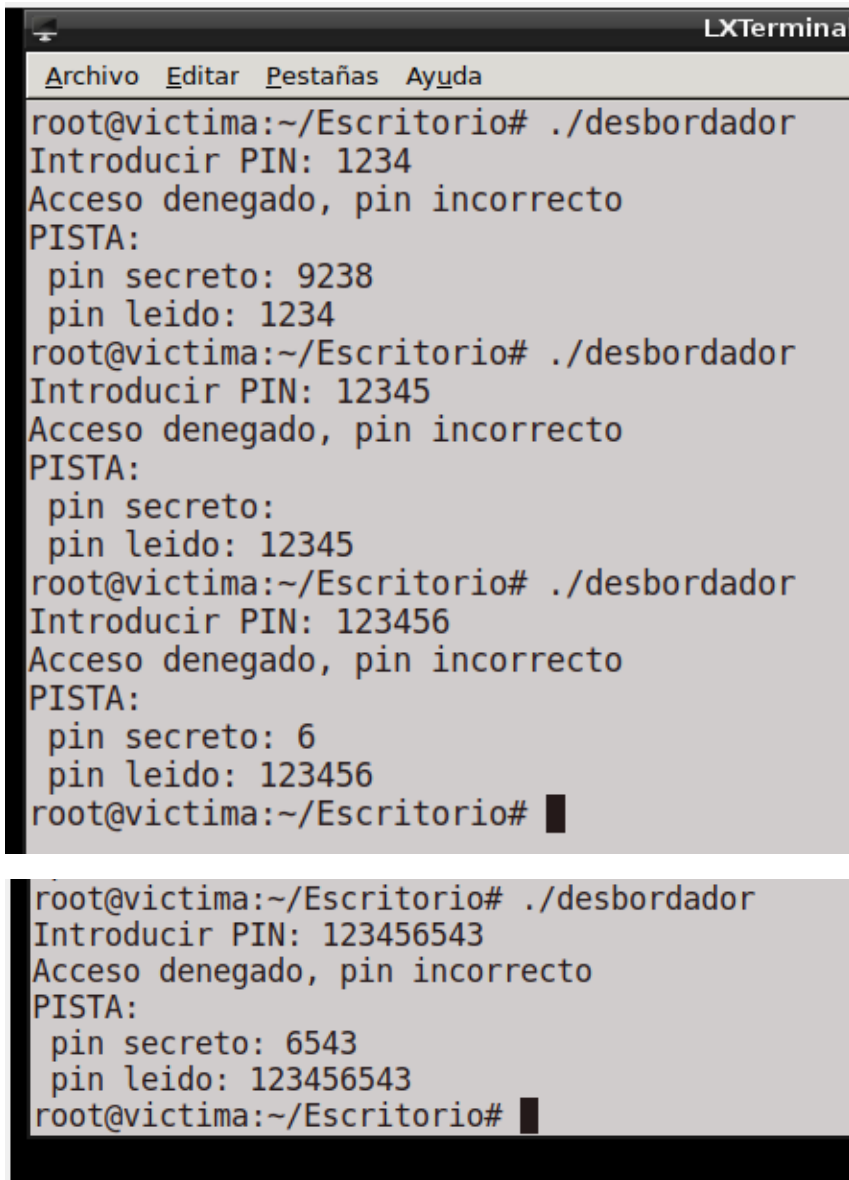


Práctica 3

VULNERABILIDADES WEB Y USO DE MOD-SECURITY

JACOBO MARTÍNEZ GÓMEZ

Tarea entregable (A)



```
LXTerminal
Archivo Editar Pestañas Ayuda
root@victima:~/Escritorio# ./desbordador
Introducir PIN: 1234
Acceso denegado, pin incorrecto
PISTA:
  pin secreto: 9238
  pin leído: 1234
root@victima:~/Escritorio# ./desbordador
Introducir PIN: 12345
Acceso denegado, pin incorrecto
PISTA:
  pin secreto:
  pin leído: 12345
root@victima:~/Escritorio# ./desbordador
Introducir PIN: 123456
Acceso denegado, pin incorrecto
PISTA:
  pin secreto: 6
  pin leído: 123456
root@victima:~/Escritorio# █

root@victima:~/Escritorio# ./desbordador
Introducir PIN: 123456543
Acceso denegado, pin incorrecto
PISTA:
  pin secreto: 6543
  pin leído: 123456543
root@victima:~/Escritorio# █
```

2. Al introducir un PIN de una longitud mayor a lo esperado es decir mas de 4 Bytes, y dado que los métodos gets no verifican el numero de caracteres introducidos, se produce un desbordamiento que sustituye el PIN almacenado, pudiendo sobrepasar así el control de acceso.
3. La protección de pila introduce valores aleatorios que se insertan antes de la dirección de retorno (stack canaries). Antes de recuperar la dirección de retorno se verifica el stack canary para ver si fue modificado previamente. Si es así también es probable que se haya modificado la dirección de retorno, por lo tanto se aborta la ejecución del programa.
4. La sustitución de gets(pin_leído) por fgets(pin_leído, 4, stdin) soluciona el problema de desbordamiento, ya que al limitar el tamaño del buffer a 4 Bytes no es posible que se sobreescriba el PIN secreto.

Tarea entregable (B)

Cross Site Scripting

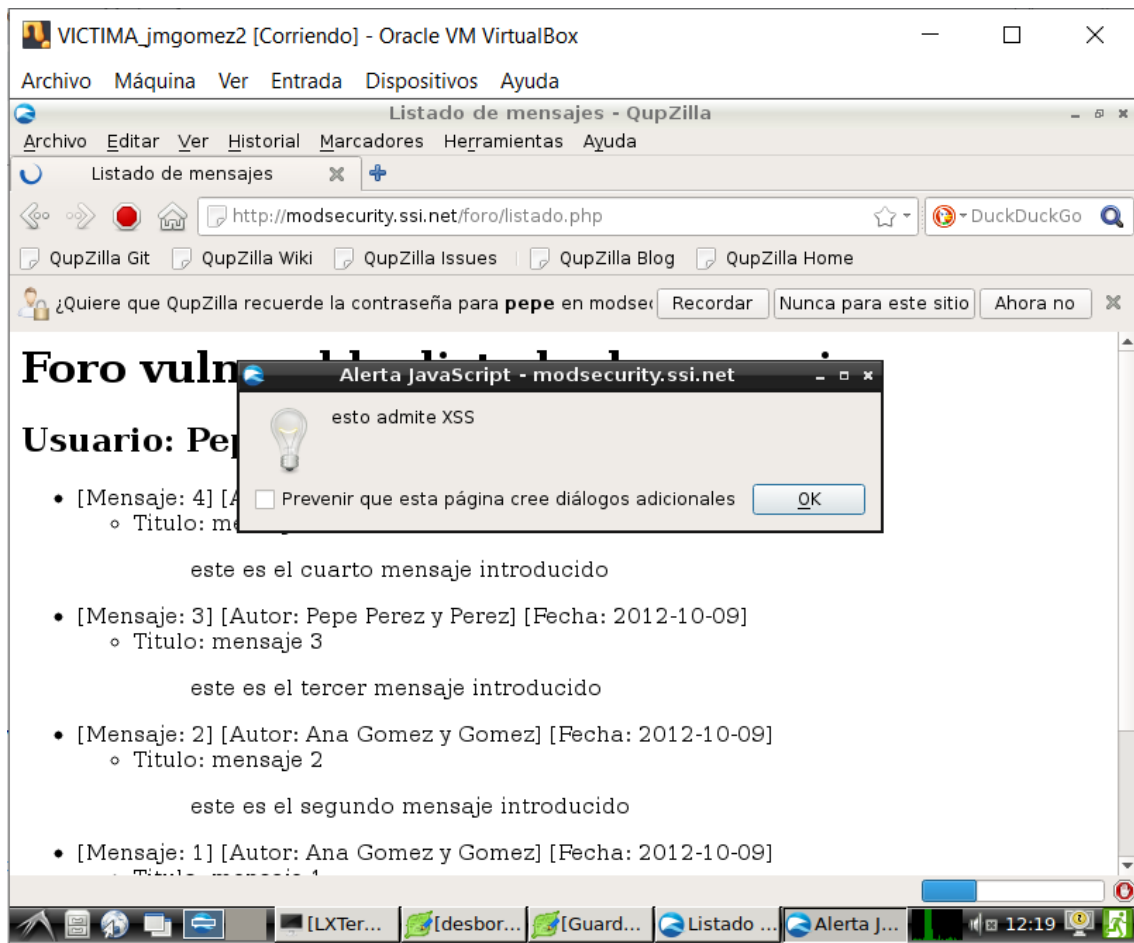
Inicialmente escribo un mensaje con etiquetas en negrita para comprobar que se puede introducir un script

- [Mensaje: 5] [Autor: Ana Gomez y Gomez] [Fecha: 2019-11-30]
 - Titulo: mensaje con texto en **negrita**

textoooooooooooo**textoooo**

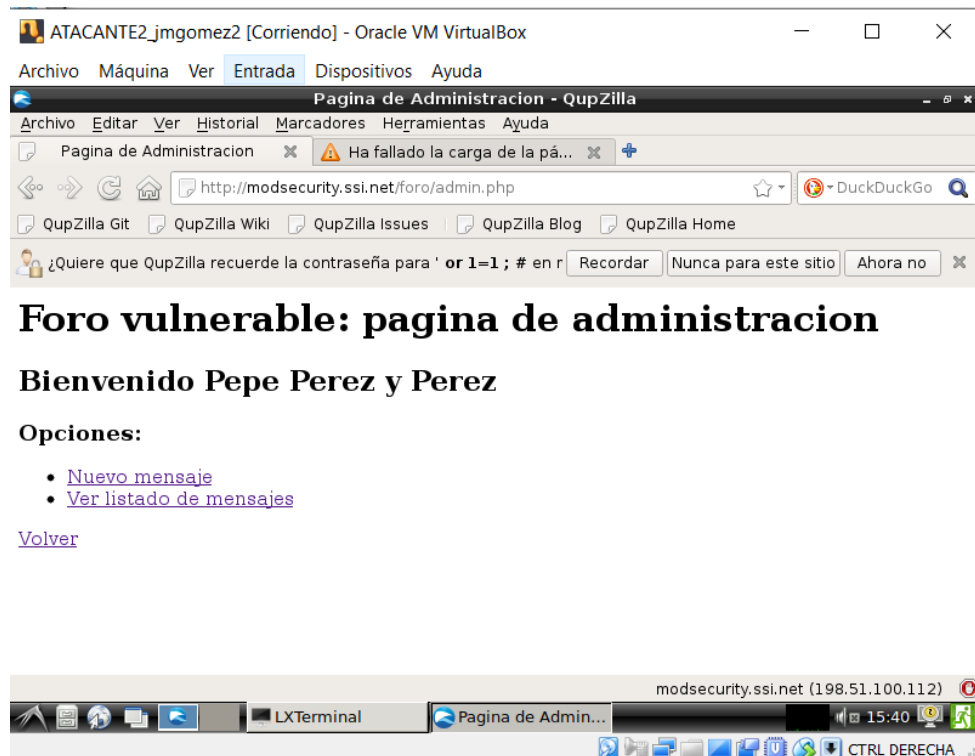
[Volver](#)

En el siguiente mensaje introducimos para comprobar que salta la alerta `<script> alert("esto admite XSS") </script>`



Inyección SQL

Probamos a acceder con una simple inyección de sql en el login:



Comprobamos que se puede acceder al foro sin credenciales de acceso. La sentencia que verifica las credenciales es la siguiente:

```
SELECT id, nombre FROM usuarios WHERE login = ' ".$login." ' AND pass = md5(' ".$password." ');
```

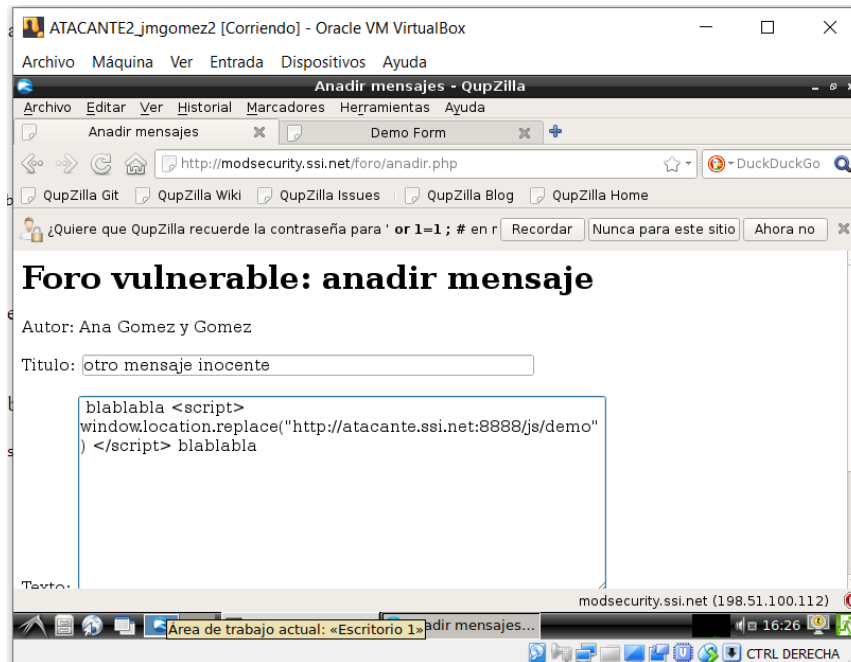
Al introducir esta secuencia: ' or 1=1 ; # en el campo usuario, provocamos que se ejecute la siguiente sentencia SQL:

```
SELECT id, nombre FROM usuarios WHERE login = ' ' or 1=1 ; # ' AND pass = md5(' ".$password." ');
```

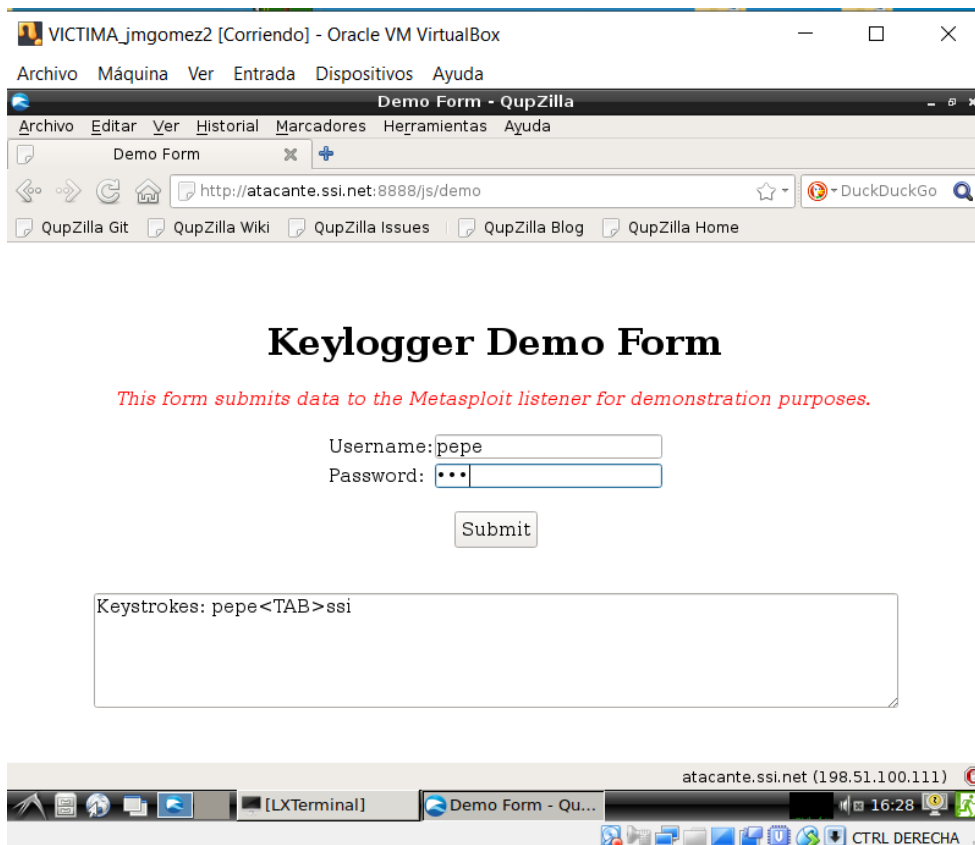
Esto se verifica siempre al ser 1=1 siempre verdad.

Ejercicio opcional:

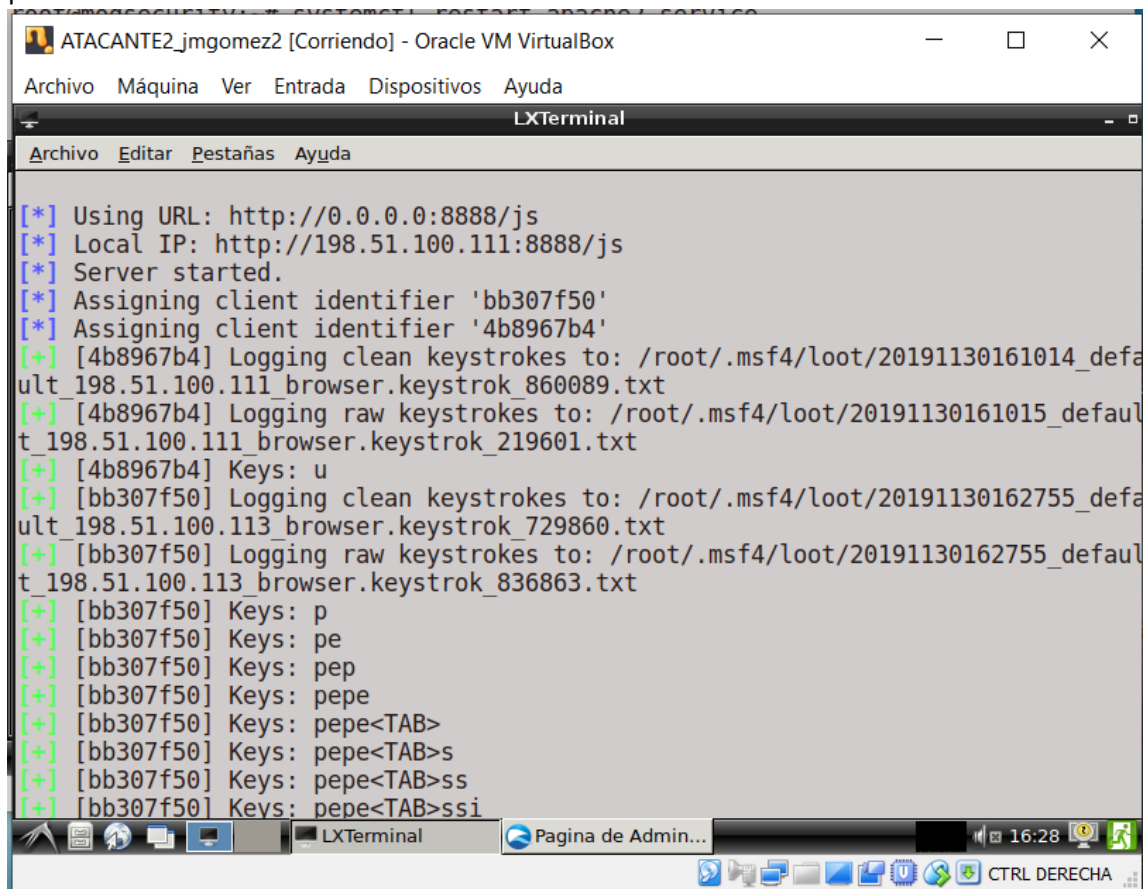
Escribimos un mensaje con el script hacia una dirección para recoger los datos de la victima:



Desde la victima entramos a la lista de mensajes y este nos redirige hacia una pagina demo de donde nos pide usuario y contraseña, esto lo que hace es que nos recupera toda la información y se la envía al atacante.



En el atacante podemos ver en el terminal todas las acciones de teclado que hemos usado para escribir la contraseña



```
ATACANTE2_jmgomez2 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
LXTerminal
Archivo  Editar  Pestañas  Ayuda
[*] Using URL: http://0.0.0.0:8888/js
[*] Local IP: http://198.51.100.111:8888/js
[*] Server started.
[*] Assigning client identifier 'bb307f50'
[*] Assigning client identifier '4b8967b4'
[+] [4b8967b4] Logging clean keystrokes to: /root/.msf4/loot/20191130161014_defaul
ult_198.51.100.111_browser.keystrok_860089.txt
[+] [4b8967b4] Logging raw keystrokes to: /root/.msf4/loot/20191130161015_defaul
t_198.51.100.111_browser.keystrok_219601.txt
[+] [4b8967b4] Keys: u
[+] [bb307f50] Logging clean keystrokes to: /root/.msf4/loot/20191130162755_defaul
ult_198.51.100.113_browser.keystrok_729860.txt
[+] [bb307f50] Logging raw keystrokes to: /root/.msf4/loot/20191130162755_defaul
t_198.51.100.113_browser.keystrok_836863.txt
[+] [bb307f50] Keys: p
[+] [bb307f50] Keys: pe
[+] [bb307f50] Keys: pep
[+] [bb307f50] Keys: pepe
[+] [bb307f50] Keys: pepe<TAB>
[+] [bb307f50] Keys: pepe<TAB>s
[+] [bb307f50] Keys: pepe<TAB>ss
[+] [bb307f50] Keys: pepe<TAB>ssi
LXTerminal
Pagina de Admin... 16:28 CTRL DERECHA
```

Para prevenir esto podemos evitar que se interpreten las tags html al presentar a información, haciendo este cambio en el código:

```
echo " <li> [Mensaje: $id] [Autor: $autor] [Fecha: $fecha]\n";
echo " <ul>\n";
echo " <li> Titulo: $titulo </li>\n";
echo " <blockquote>$mensaje</blockquote>\n";
echo " </ul>\n";
echo " </li>\n";
```

En el siguiente codigo:

```
echo " <li> [Mensaje: $id] [Autor: $autor] [Fecha: $fecha]\n";
echo " <ul>\n";
echo " <li> Titulo: ".strip_tags($titulo)." </li>\n";
echo " <blockquote>".strip_tags($mensaje)."</blockquote>\n";
echo " </ul>\n";
echo " </li>\n";
```

Por otro lado haciendo esta modificación evitando los tags en la sentencia sql también conseguiríamos que los tags de html no entraran en la BD:

```
$query = "INSERT INTO mensajes (id_autor, fecha, titulo, texto)";  
$query .= " VALUES ('$id_autor',NOW(),''."strip_tags($titulo)."',."strip_tags($mensaje)."'");  
$result = mysql_query($query, $db);
```

Tarea entregable (C)

Repetir las pruebas de inyección SQL y XSS sobre el foro y (opcionalmente) con DVWA.

XSS

Al comprobar de nuevo la inyección de XSS vemos que se ejecutan sin problemas porque el mod security esta configurado en modo detención, para únicamente registrar el ataque y no evitarlo. Se pueden observar las trazas de los ataques en el fichero error.log:

```
ARGS:mensaje. [file "/usr/share/modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "267"] [id "941160"] [rev "2"] [msg "NoScript XSS InjectionChecker: HTML Injection"] [data "Matched Data: <script found within ARGS:mensaje: <script> alert(\\x22esto admite XSS\\x22) </script>\\x0d\\x0a"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "1"] [accuracy "8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "OWASP_CRS/WEB_ATTACK/XSS"] [tag "WASCTC/WASC-8"] [tag "WASCTC/WASC-22"] [tag "OWASP_TOP_10/A3"] [tag "OWASP_AppSensor/IE1"] [tag "CAPEC-242"] [hostname "modsecurity.ssi.net"] [uri "/foro/insertar_mensaje.php"] [unique_id "XeLT4cYzZHAAABJ0b7kAAAAB"], referer: http://modsecurity.ssi.net/foro/anadir.php
```

```
[Sat Nov 30 21:41:05.553515 2019] [:error] [pid 4724] [client 198.51.100.111:42392] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "57"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 15)"] [severity "CRITICAL"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "modsecurity.ssi.net"] [uri "/foro/insertar_mensaje.php"] [unique_id "XeLT4cYzZHAAABJ0b7kAAAAB"], referer: http://modsecurity.ssi.net/foro/anadir.php
```

```
[Sat Nov 30 21:41:05.554864 2019] [:error] [pid 4724] [client 198.51.100.111:42392] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 15 - SQLI=0,XSS=15,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): NoScript XSS InjectionChecker: HTML Injection"] [tag "event-correlation"] [hostname "modsecurity.ssi.net"] [uri "/foro/insertar_mensaje.php"] [unique_id "XeLT4cYzZHAAABJ0b7kAAAAB"], referer: http://modsecurity.ssi.net/foro/anadir.php
```

SQL

Lo mismo pasa al hacer una inyección de SQL

```
[Sat Nov 30 22:30:25.823532 2019] [:error] [pid 4729] [client 198.51.100.111:42398] [client 198.51.100.111] ModSecurity: Warning. detected SQLi using libinjection with fingerprint 's&1;c' [file "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "68"] [id "942100"] [rev "1"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: s&1;c found within ARGS:login: ' or 1=1 ; #"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "1"] [accuracy "8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/foro/login.php"] [unique_id "XeLfccYzZHAAABJ5gQwAAAAG"], referer: http://modsecurity.ssi.net/foro/index.php
```

```
[Sat Nov 30 22:30:25.823673 2019] [:error] [pid 4729] [client 198.51.100.111:42398] [client 198.51.100.111] ModSecurity: Warning. detected SQLi using libinjection with fingerprint 's&1;' [file "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "68"] [id "942100"] [rev "1"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: s&1; found within ARGS:login: ' or 1=1 ; "] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "1"] [accuracy "8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/foro/login.php"] [unique_id "XeLfccYzZHAAABJ5gQwAAAAG"], referer: http://modsecurity.ssi.net/foro/index.php
```

```
[Sat Nov 30 22:30:25.823961 2019] [:error] [pid 4729] [client 198.51.100.111:42398] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "57"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 10)"] [severity "CRITICAL"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "modsecurity.ssi.net"] [uri "/foro/login.php"] [unique_id "XeLfccYzZHAAABJ5gQwAAAAG"], referer: http://modsecurity.ssi.net/foro/index.php
```

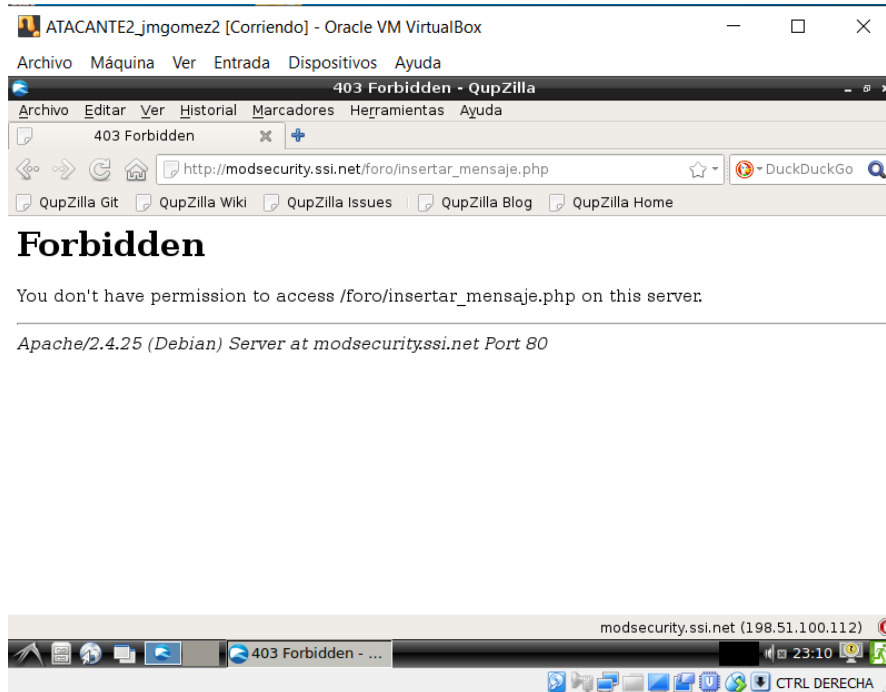
```
[Sat Nov 30 22:30:25.825684 2019] [:error] [pid 4729] [client 198.51.100.111:42398] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 10 - SQLI=10,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): SQL Injection Attack Detected via libinjection"] [tag "event-correlation"] [hostname "modsecurity.ssi.net"] [uri "/foro/login.php"] [unique_id "XeLfccYzZHAAABJ5gQwAAAAG"], referer: http://modsecurity.ssi.net/foro/index.php
```


Tarea entregable (D)

Una vez hecho el cambio en el modsecurity en la regla SecRuleEngine, volvemos a hacer las comprobaciones para XSS y SQL

XSS

Cuando creamos un mensaje nuevo con un script no nos deja guardarlo y nos salta ese error:

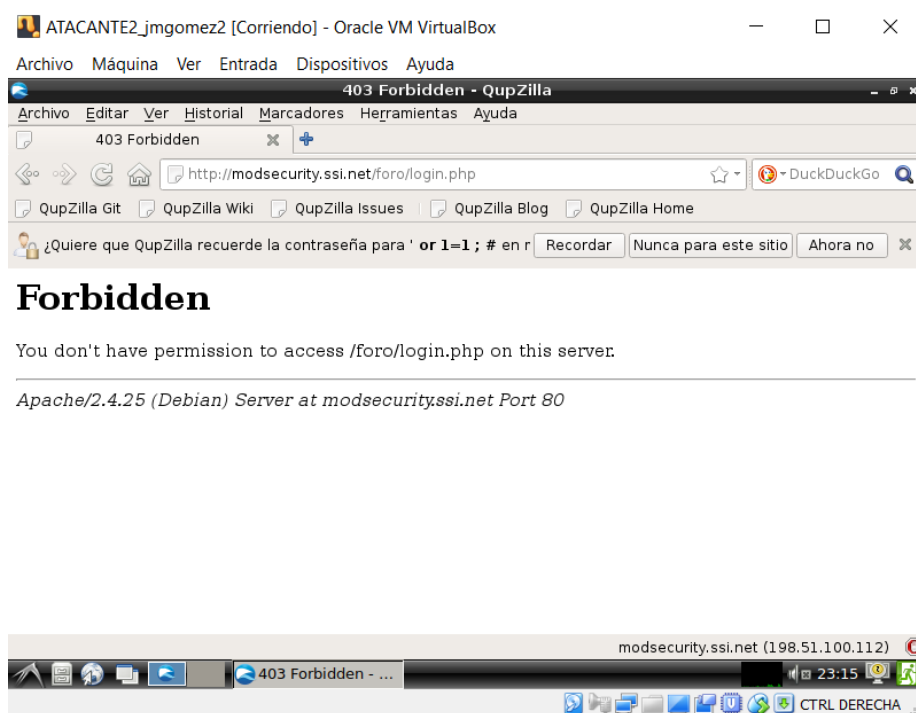


```
[Sat Nov 30 22:49:09.048218 2019] [:error] [pid 5009] [client 198.51.100.111:42406] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 15 - SQLI=0,XSS=15,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): NoScript XSS InjectionChecker: HTML Injection"] [tag "event-correlation"] [hostname "modsecurity.ssi.net"] [uri "/foro/insertar_mensaje.php"] [unique_id "XeLj1cYzZHAAABORGAMAAAF"], referer: http://modsecurity.ssi.net/foro/anadir.php
```

```
[Sat Nov 30 23:15:17.020968 2019] [:error] [pid 5010] [client 198.51.100.111:42410] [client 198.51.100.111] ModSecurity: Warning. detected SQLi using libinjection with fingerprint 's&1;c' [file "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "68"] [id "942100"] [rev "1"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: s&1;c found within ARGS:login: ' or 1=1 ; #"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "1"] [accuracy "8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "OWASP_CRS/WEB_ATTACK/SQL_INJECTION"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"] [tag "PCI/6.5.2"] [hostname "modsecurity.ssi.net"] [uri "/foro/login.php"] [unique_id "XeLp9cYzZHAAABOSf6kAAAAG"], referer: http://modsecurity.ssi.net/foro/index.php
```

SQL

Nos pasa lo mismo cuando queremos hacer un sql injection para entrar en la aplicación



```
[Sat Nov 30 23:15:17.021397 2019] [:error] [pid 5010] [client 198.51.100.111:42410] [client 198.51.100.111] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "57"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 10)"] [severity "CRITICAL"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "modsecurity.ssi.net"] [uri "/foro/login.php"] [unique_id "XeLp9cYzZHAAABOSf6kAAAAG"], referer: http://modsecurity.ssi.net/foro/index.php
```

```
[Sat Nov 30 23:15:17.021709 2019] [:error] [pid 5010] [client 198.51.100.111:42410] [client 198.51.100.111] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 10 - SQLI=10,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): SQL Injection Attack Detected via libinjection"] [tag "event-correlation"] [hostname "modsecurity.ssi.net"] [uri "/foro/login.php"] [unique_id "XeLp9cYzZHAAABOSf6kAAAAG"], referer: http://modsecurity.ssi.net/foro/index.php
```