WAF

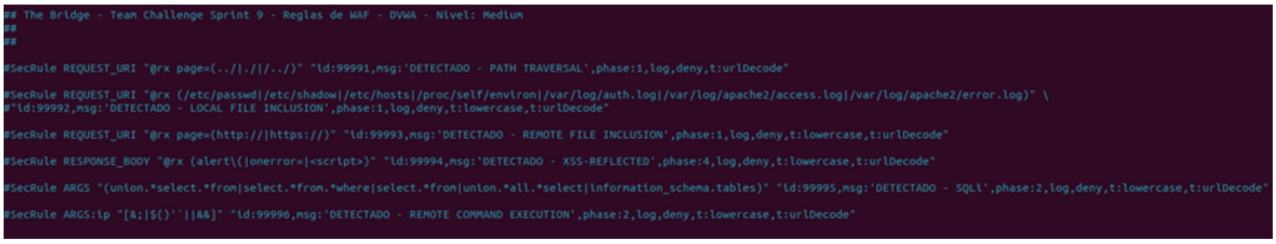
-CREACIÓN DE REGLAS EN MODSECURITY

-DVWA - LEVEL: MEDIUM

Team Challenge-U1S9- Jose Maria Jimenez

Creación de reglas en ModSecurity en la máquina RedWeb para su implementación en el recurso DVWA alojada en esta misma.

A continuación se muestra una imagen de las reglas que se piden en el ejercicio:



Path Traversal:
SecRule REQUEST_URI "@rx page=(../|./|/../)" "id:99991,msg:'DETECTADO - PATH TRAVERSAL',phase:1,log,deny,t:urlDecode"

Local File Inclusion:
SecRule REQUEST_URI "@rx (/etc/passwd|/etc/shadow|/etc/hosts|/proc/self/environ|/var/log/auth.log|/var/log/apache2/access.log|/var/log/apache2/error.log)" "id:99992,msg:'DETECTADO - LOCAL FILE INCLUSION',phase:1,log,deny,t:lowercase,t:urlDecode"

Remote File Inclusion:
SecRule REQUEST_URI "@rx page=(http:///|https:///)" "id:99993,msg:'DETECTADO - REMOTE FILE INCLUSION',phase:1,log,deny,t:lowercase,t:urlDecode"

Cross Site Scripting - Reflected:
SecRule RESPONSE_BODY "@rx (alert\(|onerror=|<script>)" "id:99994,msg:'DETECTADO - XSS-REFLECTED',phase:4,log,deny,t:lowercase,t:urlDecode"

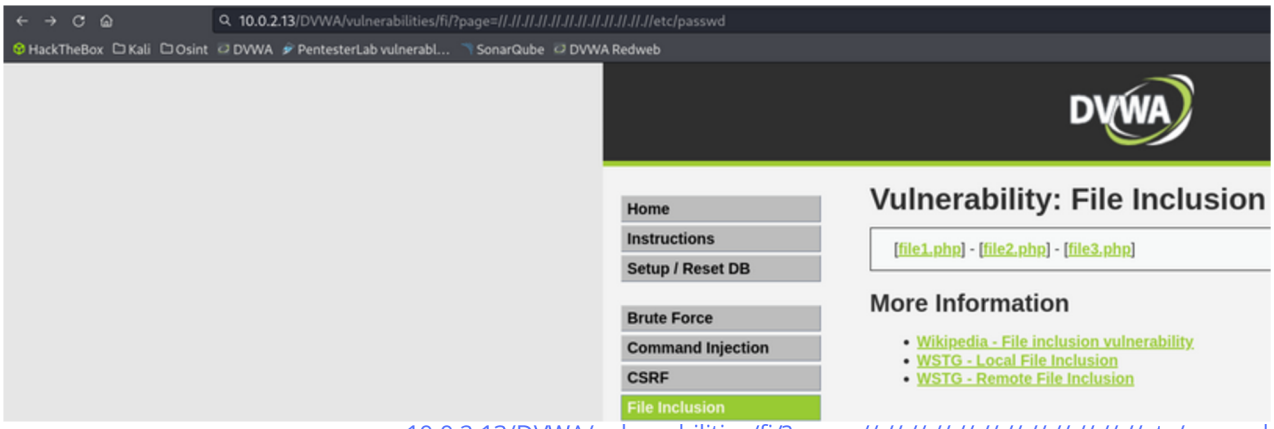
SQL Inyection:
SecRule ARGS "(union.*select.*from|select.*from.*where|select.*from|union.*all.*select|information_schema.tables)" "id:99995,msg:'DETECTADO - SQLi',phase:2,log,deny,t:lowercase,t:urlDecode"

Remote Command Execution:
SecRule ARGS:ip "[&;|$()'`||&&]" "id:99996,msg:'DETECTADO - REMOTE COMMAND EXECUTION',phase:2,log,deny,t:lowercase,t:urlDecode"

-Path Traversal:

Intento de Path Traversal desde la máquina Kali a DVWA denegado por la regla:

- SecRule REQUEST_URI "@rx page=(../|./|/../)" "id:99991,msg:'DETECTADO - PATH TRAVERSAL',phase:1,log,deny,t:urlDecode"



10.0.2.13/DVWA/vulnerabilities/fi/?page=//.//.//.//.//.//.//.//.//.//.//etc/passwd

Información del log de ModSecurity:

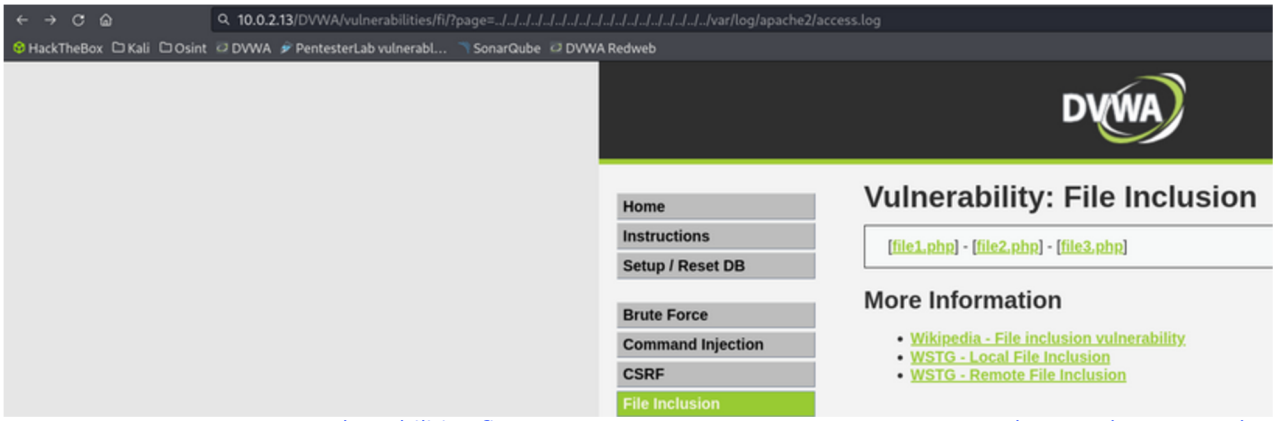
```
vboxuser@redweb:~$ sudo cat /var/log/apache2/modsec_audit.log

--0ff4f036-A--
[30/Jul/2024:12:13:47.493454 +0200] Zqi82xLsye90as1WsqEvigAAAAA 10.0.2.14 32928 10.0.2.13 80
--0ff4f036-B--
GET /DVWA/vulnerabilities/fi/?page=.//.//.//.//.//.//.//.//.//.//.//etc/passwd HTTP/1.1
Host: 10.0.2.13
```

```
--e43d5f0b-H--
Message: Access denied with code 403 (phase 1). Pattern match "page=(../|./|/../)" at REQUEST_URI. [file "/home/vboxuser/waf_rule.conf"] [line "24"] [id
"99991"] [msg "DETECTADO - PATH TRAVERSAL"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 10.0.2.14] ModSecurity: Access denied with code 403 (phase 1). Pattern match "page=(..
/|./|/../)" at REQUEST_URI. [file "/home/vboxuser/waf_rule.conf"] [line "24"] [id "99991"] [msg "DETECTADO - PATH TRAVERSAL"] [hostname "10.0.2.13"] [uri
 "/DVWA/vulnerabilities/fi/"] [unique_id "ZqpJbzzpjp6AFobajqJllgAAAAQ"]
Action: Intercepted (phase 1)
```

-Local File Inclusion:

Intento de Local File Intrusion desde la máquina Kali a DVWA denegado por la regla:

- SecRule REQUEST_URI "@rx (/etc/passwd|/etc/shadow|/etc/hosts|/proc/self/environ|/var/log/auth.log|/var/log/apache2/access.log|/var/log/apache2/error.log)" "id:99992,msg:'DETECTADO - LOCAL FILE INCLUSION',phase:1,log,deny,t:lowercase,t:urlDecode"



10.0.2.13/DVWA/vulnerabilities/fi/?page=../../../../../../../../../../../../../../../../../../var/log/apache2/access.log

Información del log de ModSecurity:

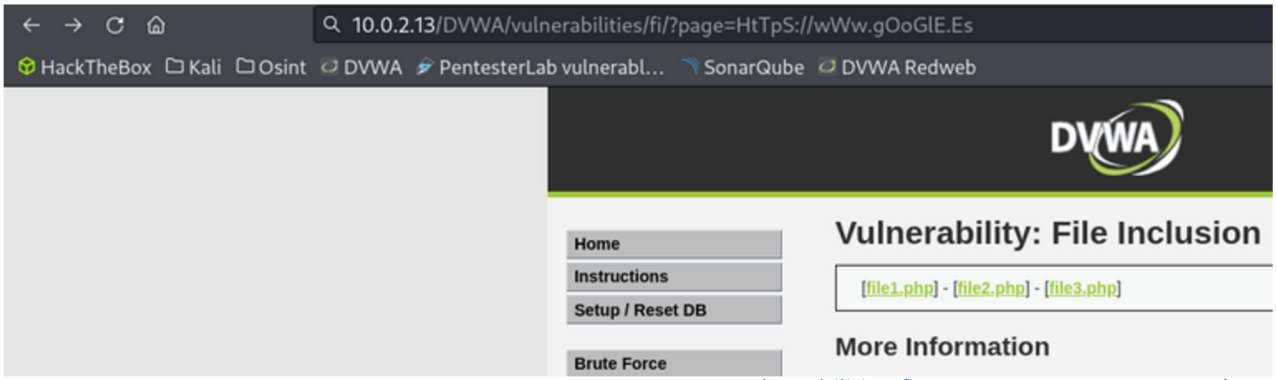
```
vboxuser@redweb:~$ sudo cat /var/log/apache2/modsec_audit.log

--f847bd37-A--
[30/Jul/2024:12:30:18.036654 +0200] ZqjAukhsXOPbX5tXgIhJHAAAAAA 10.0.2.14 38150 10.0.2.13 80
--f847bd37-B--
GET /DVWA/vulnerabilities/fi/?page=../../../../../../../../../../../../../../../../../../var/log/apache2/access.log HTTP/1.1
Host: 10.0.2.13
```

```
--f847bd37-H--
Message: Access denied with code 403 (phase 1). Pattern match "(/etc/passwd|/etc/shadow|/etc/hosts|/proc/self/environ|/var/log/auth.log|/var/log/apache2/access.log|/var/log/apache2/error.log)" at REQUEST_URI. [file "/home/vboxuser/waf_rule.conf"] [line "26"] [id "99992"] [msg "DETECTADO - LOCAL FILE INCLUSION"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 10.0.2.14] ModSecurity: Access denied with code 403 (phase 1). Pattern match "(/etc/passwd|/etc/shadow|/etc/hosts|/proc/self/environ|/var/log/auth.log|/var/log/apache2/access.log|/var/log/apache2/error.log)" at REQUEST_URI. [file "/home/vboxuser/waf_rule.conf"] [line "26"] [id "99992"] [msg "DETECTADO - LOCAL FILE INCLUSION"] [hostname "10.0.2.13"] [uri "/DVWA/vulnerabilities/fi/"] [unique_id "ZqjAukhsXOPbX5tXgIhJHAAAAAA"]
Action: Intercepted (phase 1)
```

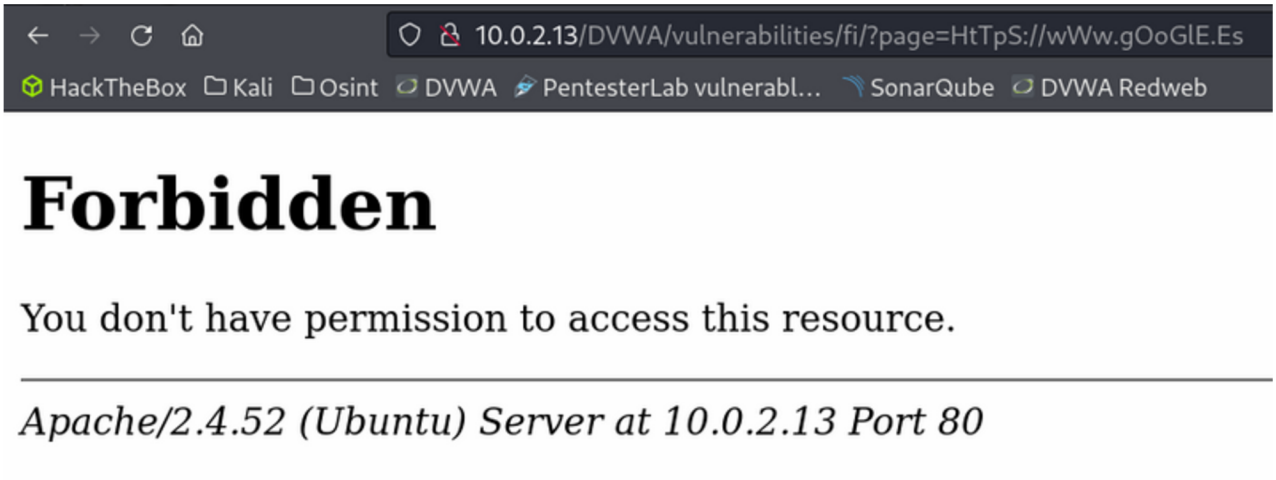
-Remote File Inclusion:

Intento de Remote File Intrusion desde la máquina Kali a DVWA denegado por la regla:

- SecRule REQUEST_URI "@rx page=(http://|https://)" "id:99993,msg:'DETECTADO - REMOTE FILE INCLUSION',phase:1,log,deny,t:lowercase,t:urlDecode"



10.0.2.13/DVWA/vulnerabilities/fi/?page=HtTpS://wWw.gOoGlE.Es



Información del log de ModSecurity:

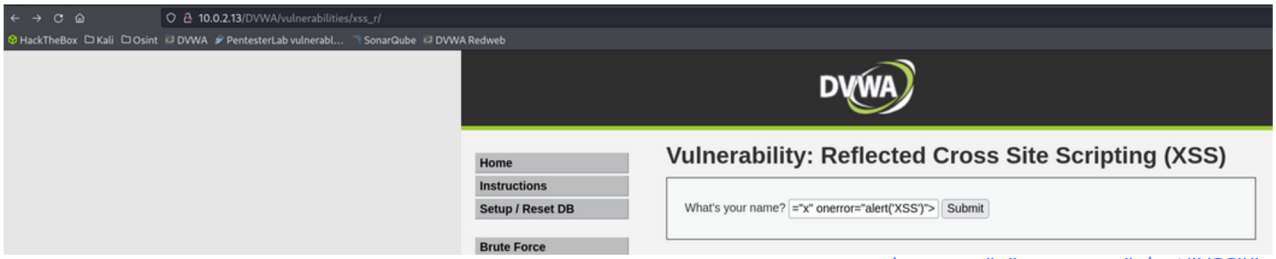
```
vboxuser@redweb:~$ sudo cat /var/log/apache2/modsec_audit.log

--55390711-A--
[30/Jul/2024:12:53:06.193587 +0200] ZqjGErljF-bEJHLavhL0uwAAAAA 10.0.2.14 38018 10.0.2.13 80
--55390711-B--
GET /DVWA/vulnerabilities/fi/?page=HtTpS://wWw.gOoGlE.Es HTTP/1.1
Host: 10.0.2.13
```

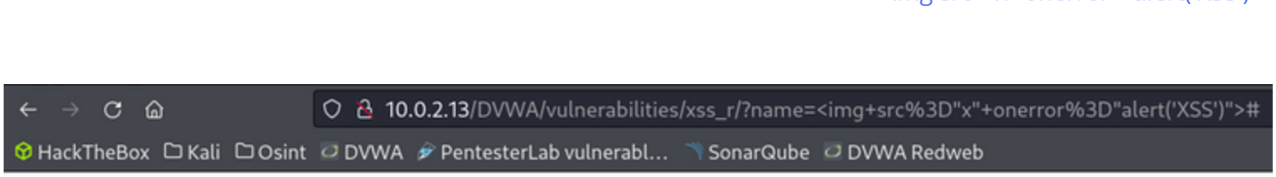
```
--55390711-H--
Message: Access denied with code 403 (phase 1). Pattern match "page=(http:///|https:///)" at REQUEST_URI. [file "/home/vboxuser/waf_rule.conf"] [line "28"] [
id "99993"] [msg "DETECTADO - REMOTE FILE INCLUSION"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 10.0.2.14] ModSecurity: Access denied with code 403 (phase 1). Pattern match "page=(http
:///|https:///)" at REQUEST_URI. [file "/home/vboxuser/waf_rule.conf"] [line "28"] [id "99993"] [msg "DETECTADO - REMOTE FILE INCLUSION"] [hostname "10.0.2.1
3"] [uri "/DVWA/vulnerabilities/fi/"] [unique_id "ZqjGErljF-bEJHLavhL0uwAAAAA"]
Action: Intercepted (phase 1)
```

-XSS Reflected:

Intento de XSS Relflected desde la máquina Kali a DVWA denegado por la regla:

- SecRule RESPONSE_BODY "@rx (alert\(|onerror=|<script>)" "id:99994,msg:'DETECTADO - XSS-REFLECTED',phase:4,log,deny,t:lowercase,t:urlDecode"





Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.0.2.13 Port 80

Información del log de ModSecurity:

```
vboxuser@redweb:~$ sudo cat /var/log/apache2/modsec_audit.log
[sudo] contraseña para vboxuser:

--6f983e60-A--
[30/Jul/2024:18:06:45.598926 +0200] ZqkPlQ2jl_PmDqbFFErFtwAAAAU 10.0.2.14 60998 10.0.2.13 80
--6f983e60-B--
GET /DVWA/vulnerabilities/xss_r/?name=%3Cimg+src%3D%22x%22+onerror%3D%22alert%28%27XSS%27%29%22%3E HTTP/1.1
Host: 10.0.2.13
```

```
--10c97479-H--
Message: Access denied with code 403 (phase 4). Pattern match "(alert\\(|onerror=|<script>)" at RESPONSE_BODY. [file "/home/vboxuser/waf_rule.conf"] [line "30"] [id "99994"] [msg "DETECTADO - XSS-REFLECTED"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 10.0.2.14] ModSecurity: Access denied with code 403 (phase 4). Pattern match "(alert\\\\\\\\(|onerror=|<script>)" at RESPONSE_BODY. [file "/home/vboxuser/waf_rule.conf"] [line "30"] [id "99994"] [msg "DETECTADO - XSS-REFLECTED"] [hostname "10.0.2.13"] [uri "/DVWA/vulnerabilities/xss_r/index.php"] [unique_id "ZqkPlQ2jl_PmDqbFFErFuAAAAAU"]
Action: Intercepted (phase 4)
```

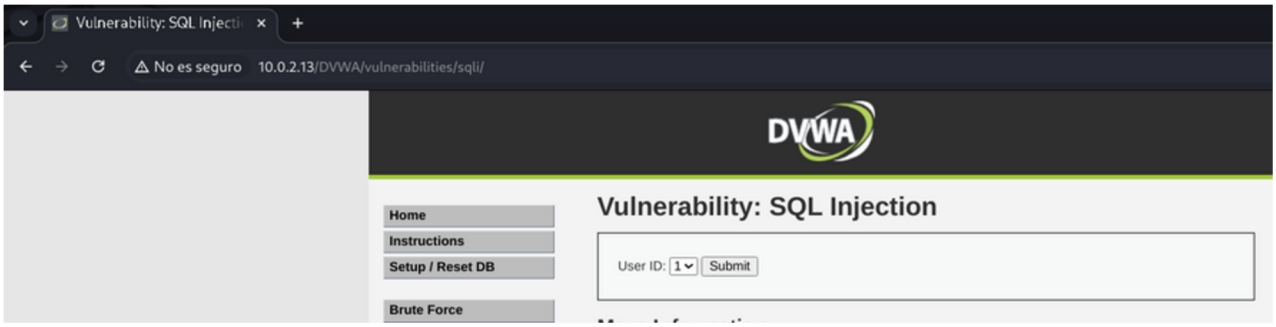
-SQLi

Intento de SQLi desde la máquina Kali a DVWA denegado por la regla:

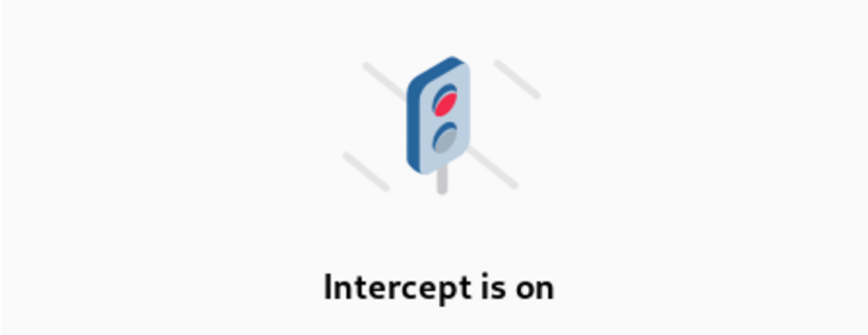
- SecRule ARGS "(union.*select.*from|select.*from.*where|select.*from|union.*all.*select|information_schema.tables)" "id:99995,msg:'DETECTADO - SQLi',phase:2,log,deny,t:lowercase,t:urlDecode"

A continuación se muestran los pasos para verificar que la regla en ModSecurity funciona correctamente:

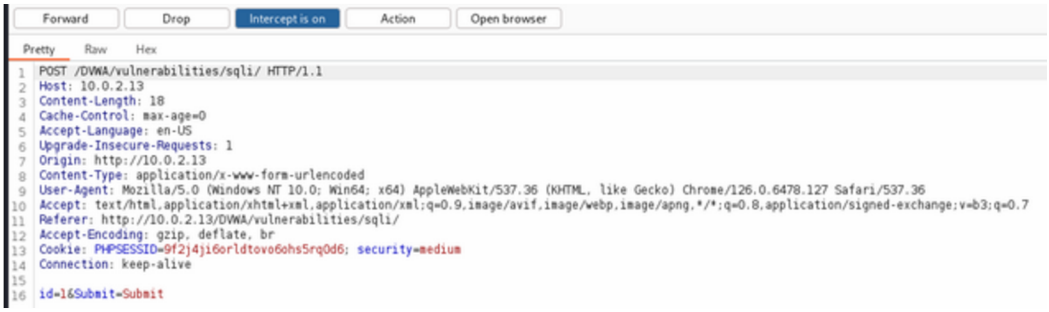
Sección de la vulnerabilidad SQL Inyection en el navegador de BurpSuite.



Interceptación del tráfico y pulso en el botón Submit de la captura anterior para obtener el ID del usuario 1.



Tráfico interceptado al hacer la consulta del ID 1.

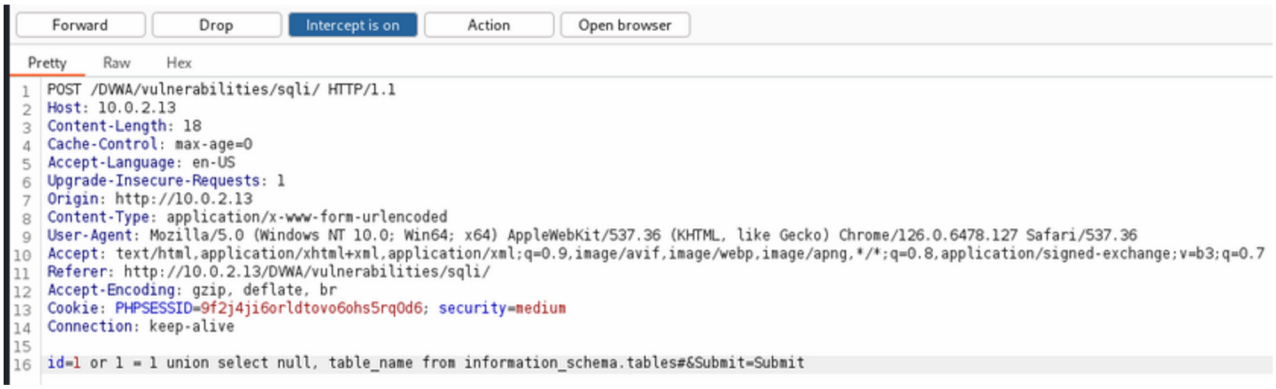


Edición de la consulta para después enviarla y obtener información de la base de datos con el código:

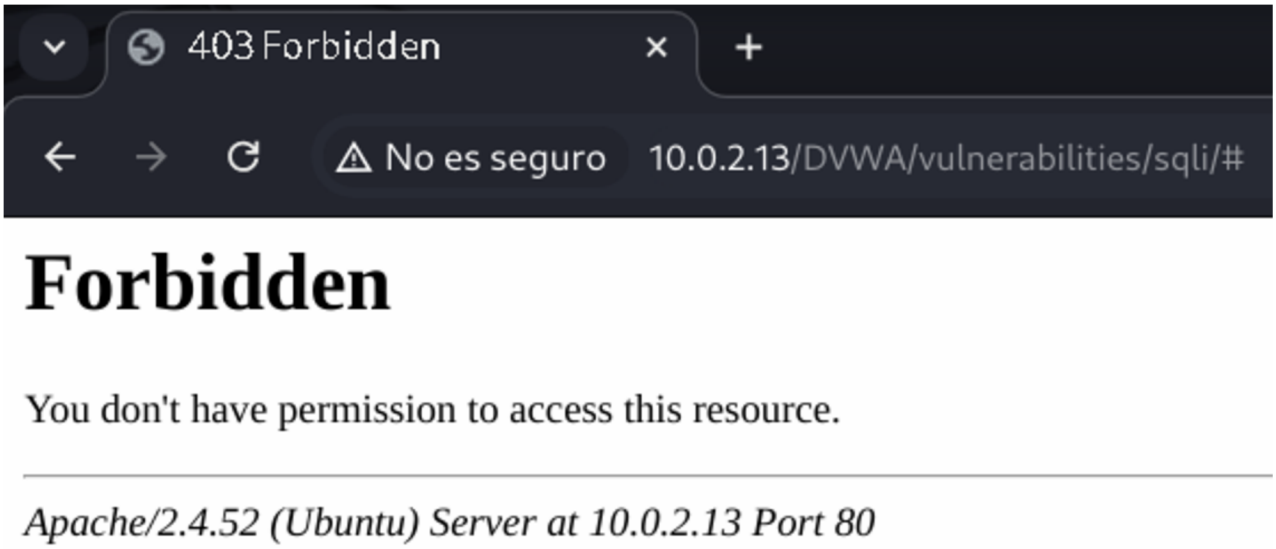
- or 1 = 1 union select null, table_name from information_schema.tables#

También se ha comprobado con:

- 1 or 1 = 1 union select user,password from users#



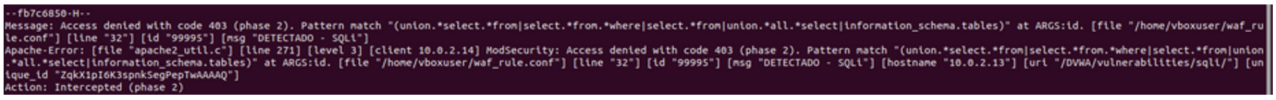
Pulso el botón de Forward para dejar pasar el tráfico con la consulta modificada y verifico que la regla está denegando el recurso solicitado:



Información del log de ModSecurity:

```
vboxuser@redweb:~$ sudo cat /var/log/apache2/modsec_audit.log
[sudo] contraseña para vboxuser:

--fb7c6850-A--
[30/Jul/2024:18:39:48.257308 +0200] ZqkXVM2zXKikkxq-f5CXmQAAAAI 10.0.2.14 58046 10.0.2.13 80
--fb7c6850-B--
POST /DVWA/vulnerabilities/sqli/ HTTP/1.1
Host: 10.0.2.13
```

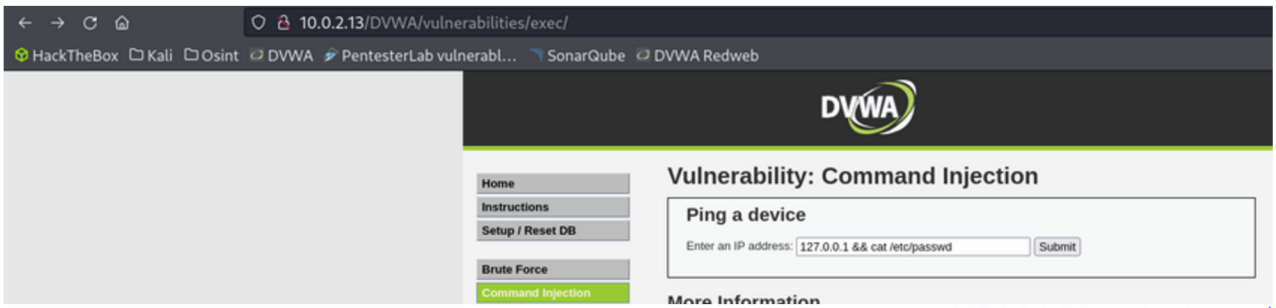
```
--fb7c6850-C--
id=1 or 1 = 1 union select null, table_name from information_schema.tables#&Submit=Submit
--fb7c6850-F--
HTTP/1.1 403 Forbidden
Content-Length: 274
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```



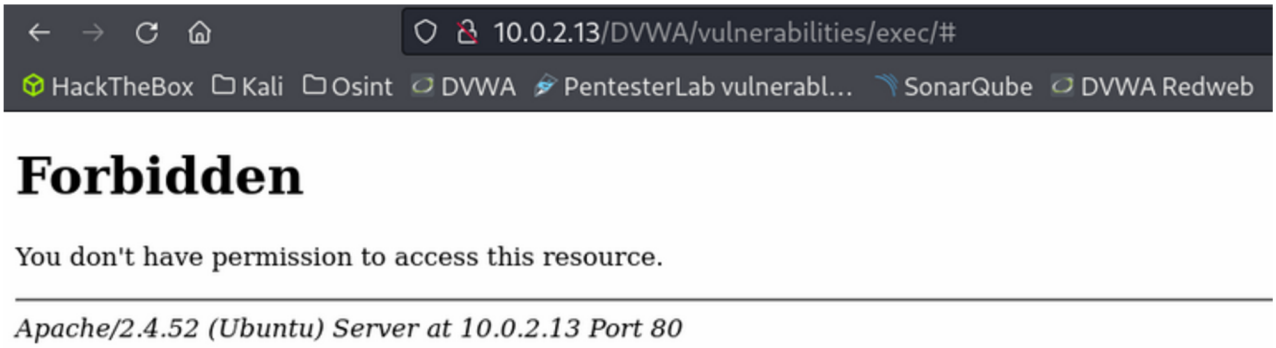
-Remote Command Execution:

Intento de Remote Command Execution desde la máquina Kali a DVWA denegado por la regla:

- SecRule ARGS:ip "[&;|$()'`||&&]" "id:99996,msg:'DETECTADO - REMOTE COMMAND EXECUTION',phase:2,log,deny,t:lowercase,t:urlDecode"



127.0.0.1 && cat /etc/passwd



Información del log de ModSecurity:

```
vboxuser@redweb:~$ sudo cat /var/log/apache2/modsec_audit.log
[sudo] contraseña para vboxuser:

--247ad64e-A--
[30/Jul/2024:22:29:26.513762 +0200] ZqlNJmg55fZwcWJU3WlHUwAAAAA 10.0.2.14 57892 10.0.2.13 80
--247ad64e-B--
POST /DVWA/vulnerabilities/exec/ HTTP/1.1
Host: 10.0.2.13
```

```
--247ad64e-H--
Message: Access denied with code 403 (phase 2). Pattern match "[&;|$()'`||&&]" at ARGS:ip. [file "/home/vboxuser/waf_rule.conf"] [line "34"] [id "99996"]
 [msg "DETECTADO - REMOTE COMMAND EXECUTION"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 10.0.2.14] ModSecurity: Access denied with code 403 (phase 2). Pattern match "[&;|$()'
`||&&]" at ARGS:ip. [file "/home/vboxuser/waf_rule.conf"] [line "34"] [id "99996"] [msg "DETECTADO - REMOTE COMMAND EXECUTION"] [hostname "10.0.2.13"] [u
ri "/DVWA/vulnerabilities/exec/"] [unique_id "ZqlNJmg55fZwcWJU3WlHUwAAAAA"]
Action: Intercepted (phase 2)
```