



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:

```
## The Bridge - Team Challenge Sprint 9 - Reglas de WAF - DVWA - Nivel: Medium
##
##SecRule REQUEST_URI "@rx page=(..|.|/|/.)" "id:99991,msg:'DETECTADO - PATH TRAVERSAL',phase:1,log,deny,t:urlDecode"
##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"
##SecRule REQUEST_URI "@rx page=(http://|https://)" "id:99993,msg:'DETECTADO - REMOTE FILE INCLUSION',phase:1,log,deny,t:lowercase,t:urlDecode"
##SecRule RESPONSE_BODY "@rx (alert\(|onerror=|\<script>|)" "id:99994,msg:'DETECTADO - XSS-REFLECTED',phase:4,log,deny,t:lowercase,t:urlDecode"
##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"
##SecRule ARGS:ip "[&;|$()`| |&&]" "id:99996,msg:'DETECTADO - REMOTE COMMAND EXECUTION',phase:2,log,deny,t:lowercase,t:urlDecode"
```

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 Injection:

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"

The screenshot shows a browser window with the URL `10.0.2.13/DVWA/vulnerabilities/fi/?page=../../../../etc/passwd`. The DVWA logo is at the top right. On the left, a sidebar menu has 'File Inclusion' highlighted in green. The main content area says 'Vulnerability: File Inclusion' and lists '[file1.php] - [file2.php] - [file3.php]'. Below that is a 'More Information' section with links to 'Wikipedia - File inclusion vulnerability', 'WSTG - Local File Inclusion', and 'WSTG - Remote File Inclusion'. At the bottom of the page, the same URL is repeated.

The screenshot shows a browser window with the URL `10.0.2.13/DVWA/vulnerabilities/fi/?page=../../../../etc/passwd`. The Apache error message 'Forbidden' is displayed prominently. Below it, the text 'You don't have permission to access this resource.' is shown.

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
--0ff4f036-A--
[30/Jul/2024:12:13:47.493454 +0200] Zqi82xLsyey90as1WsqEvigAAAAAA 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 "ZqpJbzpzjp6AfobajqJlgAAAAQ"]
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"

The screenshot shows the DVWA File Inclusion page. The URL in the address bar is `10.0.2.13/DVWA/vulnerabilities/fi/?page=../../../../../../../../var/log/apache2/access.log`. The sidebar menu has 'File Inclusion' selected. The main content area displays the DVWA logo and the title 'Vulnerability: File Inclusion'. Below it, there's a link to '[file1.php] - [file2.php] - [file3.php]'. Under 'More Information', there are links to 'Wikipedia - File inclusion vulnerability', 'WSTG - Local File Inclusion', and 'WSTG - Remote File Inclusion'.

The screenshot shows the DVWA Forbidden page. The URL in the address bar is `10.0.2.13/DVWA/vulnerabilities/fi/?page=../../../../../../../../var/log/apache2/access.log`. The main content area displays the word 'Forbidden' in large bold letters, followed by the message 'You don't have permission to access this resource.'

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
--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/ac
cess.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/pass
wd|/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/vboxus
er/waf_rule.conf"] [line "26"] [id "99992"] [msg "DETECTADO - LOCAL FILE INCLUSION"] [hostname "10.0.2.13"] [uri "/DVWA/vulnerabilities/fi/"] [unique_id "Z
qjAukhsXOPbX5tXgIhJHAAAAAA"]
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"

The screenshot shows a DVWA session with the URL `10.0.2.13/DVWA/vulnerabilities/fi/?page=HtTpS://wWw.gOoGlE.Es`. The page displays a 'Vulnerability: File Inclusion' section with three links: [file1.php], [file2.php], and [file3.php]. Below this, there's a 'More Information' section with a link to the same URL. The browser status bar also shows the full URL.

The screenshot shows a DVWA session with the URL `10.0.2.13/DVWA/vulnerabilities/fi/?page=HtTpS://wWw.gOoGlE.Es`. The page displays a large 'Forbidden' error message. The browser status bar shows the full URL.

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
--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 "10.0.2.13"] [uri "/DVWA/vulnerabilities/fi/"] [unique_id "ZqjGErljF-bEJHLavhL0uwAAAAA"]
Action: Intercepted (phase 1)
```

-XSS Reflected:

Intento de XSS Reflected 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"

The screenshot shows a DVWA session on port 80. The URL is 10.0.2.13/DVWA/vulnerabilities/xss_r/. The page title is 'Vulnerability: Reflected Cross Site Scripting (XSS)'. On the left, there's a sidebar with 'Home' selected and other options like 'Instructions', 'Setup / Reset DB', and 'Brute Force'. The main content area has a form with the placeholder 'What's your name?'. Below the form, a blue link reads ''. The browser's status bar at the bottom shows the full URL and the status code #.

The screenshot shows a DVWA session on port 80. The URL is 10.0.2.13/DVWA/vulnerabilities/xss_r/?name=<img+src%3D"x"+onerror%3D"alert('XSS')">. The page displays a large 'Forbidden' header and the message 'You don't have permission to access this resource.' The browser's status bar at the bottom shows the full URL and the status code #.

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"]
D"
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"] [url "/DVWA/vulnerabilities/xss_r/index.php"] [unique_id "ZqkPlQ2jl_PmDqbFFErFuAAAAAU"]
Action: Intercepted (phase 4)
```

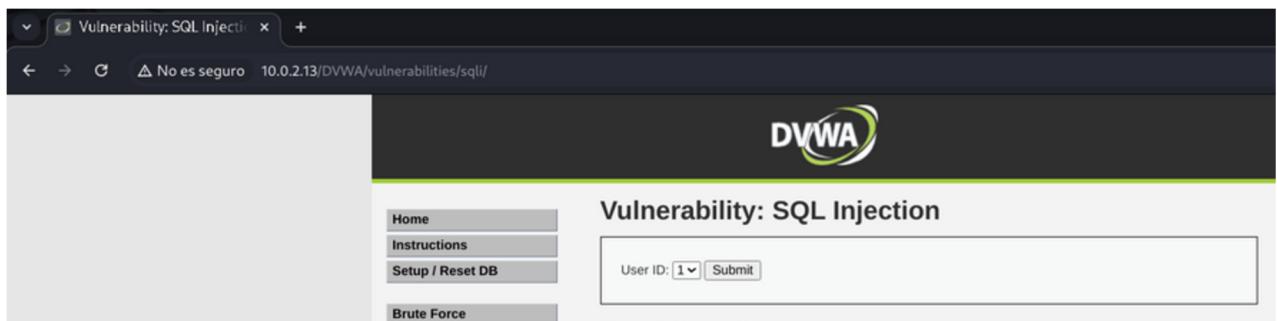
-SQLi

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 Injection 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.

```
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /DVWA/vulnerabilities/sql/ HTTP/1.1
2 Host: 10.0.2.13
3 Content-Length: 18
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://10.0.2.13
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://10.0.2.13/DVWA/vulnerabilities/sql/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=9f2j4j16orltdtovo6ohs5rq0d6; security=medium
14 Connection: keep-alive
15
16 id=1&Submit=Submit
```

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:

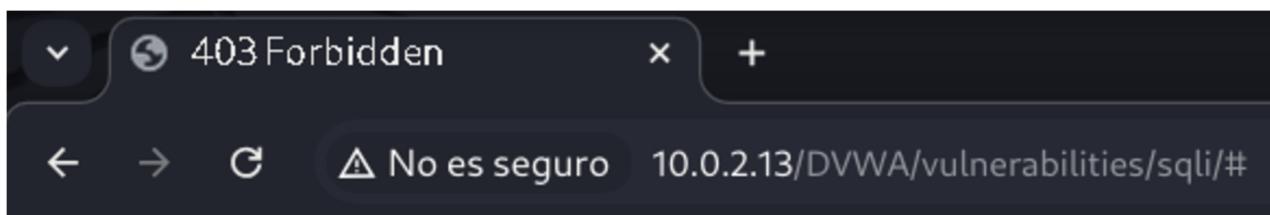
- 1 or 1 = 1 union select user,password from users#



The screenshot shows a NetworkMiner capture window. At the top, there are buttons for 'Forward', 'Drop', 'Intercept is on' (which is selected), 'Action', and 'Open browser'. Below the buttons, there are tabs for 'Pretty', 'Raw', and 'Hex'. The 'Pretty' tab displays the following POST request:

```
1 POST /DVWA/vulnerabilities/sqli/ HTTP/1.1
2 Host: 10.0.2.13
3 Content-Length: 18
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://10.0.2.13
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://10.0.2.13/DVWA/vulnerabilities/sqli/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=9f2j4ji6orltdtovo6ohs5rq0d6; security=medium
14 Connection: keep-alive
15
16 id=1 or 1 = 1 union select null, table_name from information_schema.tables#&Submit=Submit
```

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



Forbidden

You don't have permission to access this resource.

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
```

```
--fb7c6850-H--
Message: Access denied with code 403 (phase 2). Pattern match "(union.*select.*from|select.*from.*where|select.*from|union.*all.*select|information_schema.tables)" at ARGS:id. [file "/home/vboxuser/waf_rule.conf"] [line "32"] [id "99995"] [msg "DETECTADO - SQLi"]
Apache-Error: [file "/home/vboxuser/waf_rule.conf"] [line 32] [id "99995"] [msg "DETECTADO - SQLi"] [hostname "10.0.2.13"] [url "/DVWA/vulnerabilities/sqli/"] [unique_id "ZqkXipI6X3spn5SepPepTwAAAAQ"]
Action: Intercepted (phase 2)
```

-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"

The screenshot shows the DVWA Command Injection page. In the input field, the user has entered "127.0.0.1 && cat /etc/passwd". The page displays a success message: "127.0.0.1 && cat /etc/passwd".

The screenshot shows a "Forbidden" page from DVWA. The message reads: "You don't have permission to access this resource."

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:

--247ad64e-A--
[30/Jul/2024:22:29:26.513762 +0200] ZqlNjng55fZwcWJU3WlHUwAAAAA 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"] [uri "/DVWA/vulnerabilities/exec/"] [unique_id "ZqlNjng55fZwcWJU3WlHUwAAAAA"]
Action: Intercepted (phase 2)
```