RELATÓRIO TÉCNICO

Relatório Técnico de Coleta e Análise de Evidências

Autor: Fellipe Syllos

Data: 28/09/2025

Ambiente: Laboratório Docker - ModSecurity CRS + DVWA + Kali Linux

Escola: Vai na Web & Kensei CyberSec

1. Sumário Executivo

Este relatório tem como objetivo apresentar a coleta, análise e interpretação das evidências obtidas a partir do ambiente de monitoramento e defesa configurado durante o projeto prático do módulo 2 de Defesa e Monitoramento, disponibilizado pela **Escola Vai na Web** em parceria com a **Kensei CyberSec**. O foco foi o uso de um **Web Application Firewall (WAF)** baseado no **ModSecurity com OWASP Core Rule Set (CRS)**, integrado a um ambiente Docker contendo o **DVWA**, **Kali Linux** e **Dozzle**.

Durante o processo, realizei testes de exploração controlada para observar como o WAF reagiria a tentativas de ataques comuns, como **SQL Injection** e **Cross-Site Scripting (XSS)**. As respostas do sistema foram devidamente registradas e analisadas, resultando em bloqueios automáticos (código 403), conforme esperado.

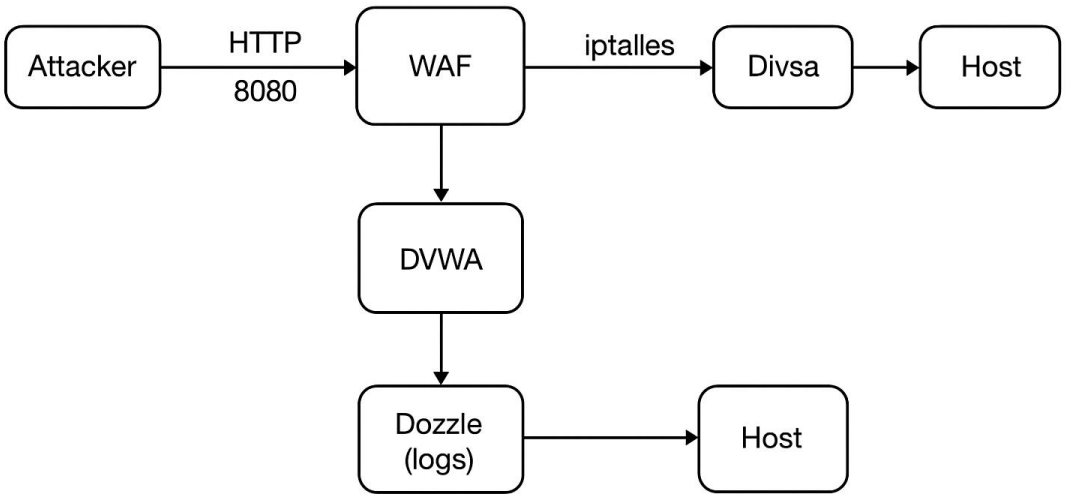
O objetivo principal desta atividade foi comprovar a eficácia do WAF na detecção e bloqueio de ameaças, bem como consolidar a prática de coleta estruturada de evidências digitais.

2. Objetivo e Escopo

O objetivo deste exercício foi validar a eficácia do ModSecurity CRS na mitigação de ataques típicos de camada web. O escopo incluiu a proteção de uma aplicação DVWA hospedada em contêiner Docker, com ataques realizados a partir de uma máquina Kali Linux. O foco foi a observação dos logs e respostas HTTP durante o modo ‘blocking’.

3. Arquitetura

O ambiente foi configurado em uma rede Docker simulando o fluxo entre atacante, WAF e aplicação. A topologia foi descrita conforme o diagrama a seguir:



3.1 Inventário de Ativos

Durante o experimento, quatro contêineres principais foram utilizados:

Contêiner	Imagem Base	Função
waf_modsec	owasp/modsecurity-crs:nginx-alpine	Proxy reverso com ModSecurity e CRS configurados.
dvwa	vulnerables/web-dvwa	Aplicativo vulnerável para simulação de ataques web.
dozzle	amir20/dozzle:latest	Visualização em tempo real dos logs dos contêineres.
kali_lab35	labs-kali_lab35	Ambiente de ataque controlado para execução dos testes de penetração.

Esses ativos foram executados em ambiente Docker Desktop, com integração total entre as redes internas configuradas pelo docker-compose.

4. Metodologia

A metodologia seguiu as etapas de detecção, bloqueio e resposta. Foram aplicadas requisições maliciosas controladas, com análise posterior dos logs em modo ‘blocking’. O sucesso foi determinado pelo retorno HTTP 403 e registro das regras do CRS.

5. Execução e Evidências

Os ataques simulados incluíram SQL Injection e XSS. Ambos foram detectados e bloqueados pelo ModSecurity CRS, gerando alertas correspondentes no log.

Figura 2 - Evidência de execução SQL Injection (bloqueio 403).

Figura 3 - Evidência de execução XSS (bloqueio 403).

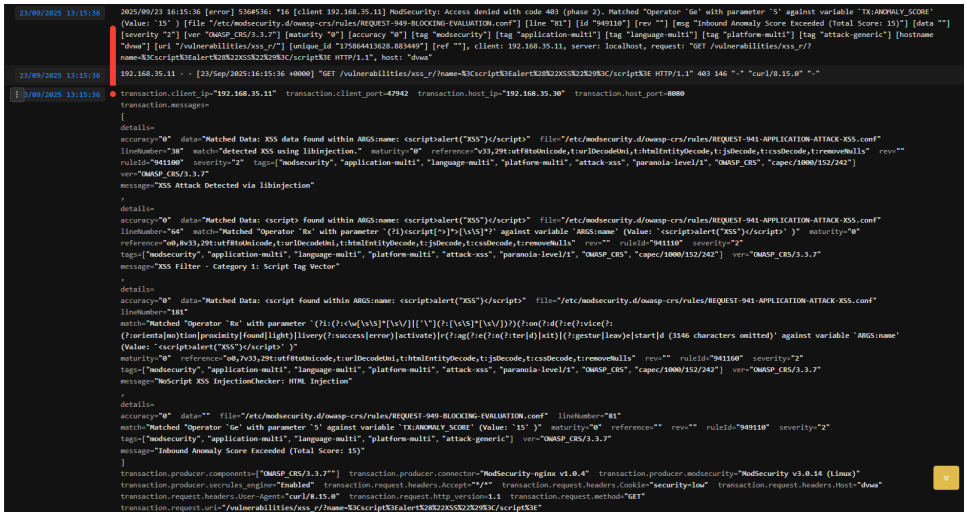


Figura 4 - Visualização adicional dos logs ModSecurity.

6. Resposta a Incidente (NIST IR)

A resposta seguiu o ciclo do NIST IR:

- **Detecção:** Alertas do ModSecurity identificaram padrões de SQLi e XSS.
- **Contenção:** O WAF bloqueou os acessos, retornando código 403.
- **Erradicação:** Nenhum impacto residual foi detectado.
- **Recuperação:** O serviço permaneceu íntegro e funcional.
- **Lições aprendidas:** O CRS demonstrou eficácia no modo ‘blocking’, validando as políticas de mitigação.

7. Recomendações

Com base na análise 80/20, recomenda-se:

- Ativar o modo ‘anomaly scoring’ com thresholds ajustados.
- Implementar monitoramento contínuo dos logs.
- Integrar alertas do ModSecurity ao SIEM corporativo.
- Revisar periodicamente as regras CRS.
- Realizar simulações regulares de ataque.

8. Conclusão

O laboratório atingiu seus objetivos, comprovando a capacidade de defesa do WAF frente a ataques web. O ModSecurity CRS atuou com precisão, bloqueando ameaças de SQLi e XSS em tempo real. A experiência reforça a importância da defesa em profundidade e da análise proativa de logs.

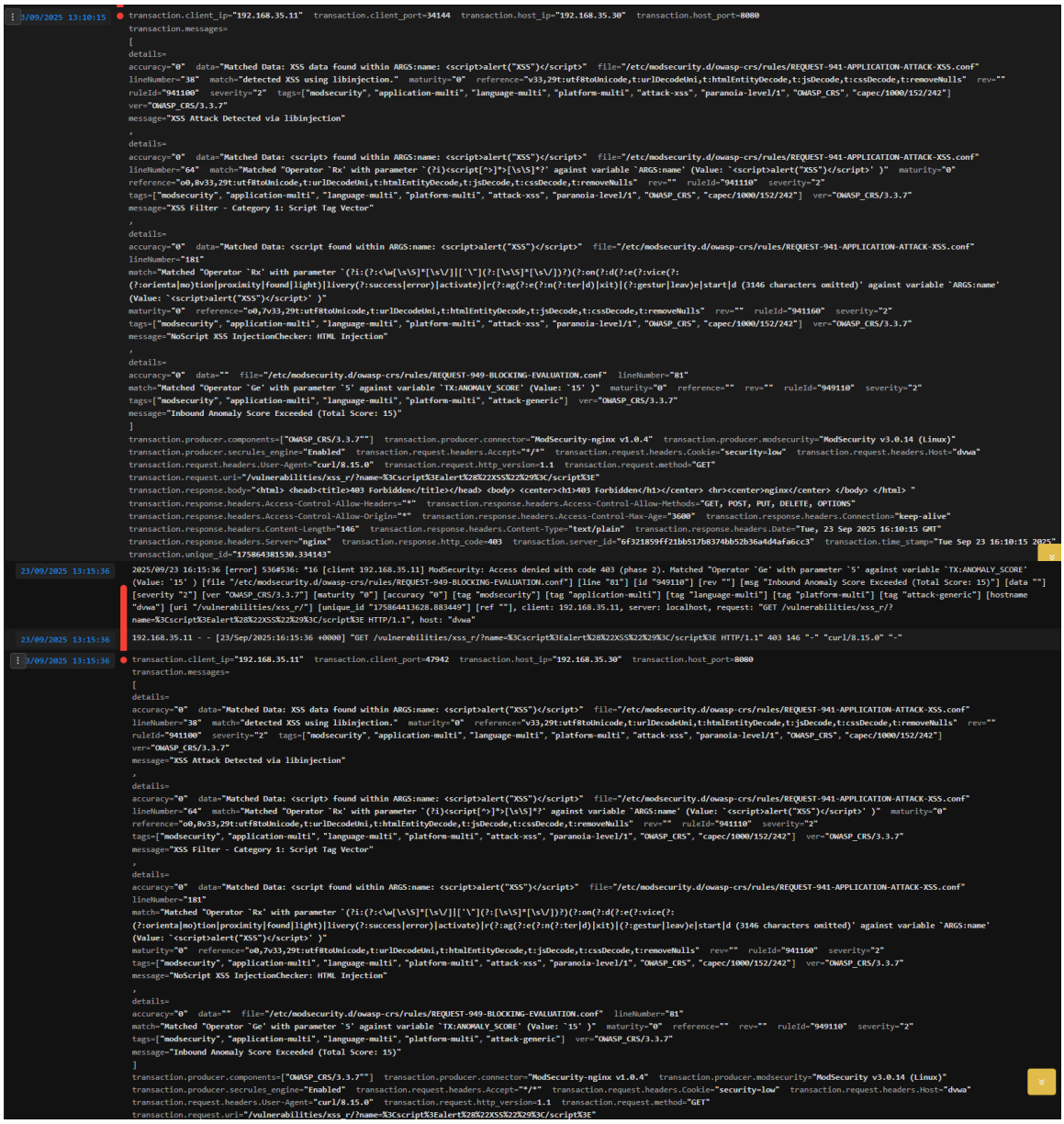
Anexos

Para melhor visualização clique aqui

```
PS C:\Users> docker psacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs>
CONTAINER ID   IMAGE                                COMMAND                  CREATED         STATUS                   PORTS                                       NAMES
d9656d4f9f06   owasp/modsecurity-crs:nginx-alpine   "/docker-entrypoint.…"   4 minutes ago   Up 4 minutes (healthy)   0.0.0.0:8080->8080/tcp, [::]:8080->8080/tcp   waf_modsec
2ebc5467d9ba   labs-kali_lab35                      "/bin/bash"              4 minutes ago   Up 4 minutes
               kali_lab35
b5d3db6252e7   amir20/dozzle:latest                 "/dozzle"                4 minutes ago   Up 4 minutes             0.0.0.0:9999->8080/tcp, [::]:9999->8080/tcp   dozzle
0c7d47180f4f   vulnerables/web-dvwa                 "/main.sh"               4 minutes ago   Up 4 minutes             80/tcp
               dvwa
PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> ls


    Diretório: C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        20/09/2025     17:26                scripts
-a----        20/09/2025     16:48           1509 docker-compose.yml
-a----        20/09/2025     16:48            218 Dockerfile.kali

PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> docker exec -it kali_lab35 bash
┌──(root㉿2ebc5467d9ba)-[/]
└─# curl -s http://waf_modsec:8080 | head -5
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>

┌──(root㉿2ebc5467d9ba)-[/]
└─# nmap -sS -sV waf_modsec
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 15:27 UTC
Nmap scan report for waf_modsec (192.168.35.30)
Host is up (0.0000090s latency).
rDNS record for 192.168.35.30: waf_modsec.labs_labnet35
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
8080/tcp open  http     nginx
8443/tcp open  ssl/http nginx
MAC Address: 06:FD:41:E9:B0:32 (Unknown)
PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> docker exec -it kali_lab35 bash
┌──(root㉿2ebc5467d9ba)-[/]
└─# curl -s http://waf_modsec:8080 | head -5
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>

┌──(root㉿2ebc5467d9ba)-[/]
└─# nmap -sS -sV waf_modsec
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 15:27 UTC
Nmap scan report for waf_modsec (192.168.35.30)
Host is up (0.0000090s latency).
rDNS record for 192.168.35.30: waf_modsec.labs_labnet35
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
8080/tcp open  http     nginx
8443/tcp open  ssl/http nginx
MAC Address: 06:FD:41:E9:B0:32 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds

┌──(root㉿2ebc5467d9ba)-[/]
└─# exit
```

```
PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit" -H "Host: dvwa" -H "Cookie: PHPSESSID=test; security=low" -w "Status: %{http_code}`n"
>>
Status: 302                                                                                          docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E" -H "Host: dvwa" -H "Cookie: security=low" -w "Status: %{http_code}\n"
Status: 302
PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> notepad.exe .\docker-compose.yml
PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> docker compose up -d --force-recreate waf_modsec
time="2025-09-23T13:09:14-03:00" level=warning msg="C:\\Users\\55219\\formacao-cybersec\\modulo2-defesa-monitoramento\\projeto-final\\opcao1-hands-on\\labs\\docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 2/2
 ✓ Container dvwa        Running                                                                                0.0s
 ✓ Container waf_modsec  Started                                                                                1.8s
PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit" -H "Host: dvwa" -H "Cookie: PHPSESSID=test; security=low" -w "Status: %{http_code}`n"
>>
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx</center>
</body>
</html>
Status: 403
PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E" -H "Host: dvwa" -H "Cookie: security=low" -w "Status: %{http_code}\n"
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx</center>
ty "2"] [ver "OWASP_CRS/3.3.7"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "dvwa"] [uri "/vulnerabilities/sqli/"] [unique_id "175864379645.492229"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1", host: "dvwa"
2025/09/23 16:10:15 [error] 534#534: *3 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `15' ) [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "81"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 15)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.3.7"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "dvwa"] [uri "/vulnerabilities/xss_r/"] [unique_id "175864381530.334143"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1", host: "dvwa"
2025/09/23 16:15:36 [error] 536#536: *16 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `15' ) [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "81"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 15)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.3.7"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "dvwa"] [uri "/vulnerabilities/xss_r/"] [unique_id "175864413628.883449"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1", host: "dvwa"
PS C:\Users\55219\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs>
```

```
waf_modsec   owasp/modsecurity-crs:nginx-alpine

23/09/2025 13:09:17   /docker-entrypoint.sh: Ignoring /docker-entrypoint.d/configure-rules.v3.conf
23/09/2025 13:09:17   /docker-entrypoint.sh: Ignoring /docker-entrypoint.d/configure-rules.v4.conf
23/09/2025 13:09:17   /docker-entrypoint.sh: Configuration complete; ready for start up
23/09/2025 13:09:17   2025/09/23 16:09:17 [warn] 1#1: "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/nginx/conf/server.crt"
23/09/2025 13:09:17   nginx: [warn] "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/nginx/conf/server.crt"
23/09/2025 13:09:17   2025/09/23 16:09:17 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remote: 0/926/0)
23/09/2025 13:09:17   2025/09/23 16:09:17 [notice] 1#1: libmodsecurity3 version 3.0.14
23/09/2025 13:09:56   2025/09/23 16:09:56 [error] 533#533: *2 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `5' ) [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "81"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 5)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.3.7"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "dvwa"] [uri "/vulnerabilities/sqli/"] [unique_id "175864379645.492229"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1", host: "dvwa"
23/09/2025 13:09:56   192.168.35.11 - - [23/Sep/2025:16:09:56 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
23/09/2025 13:09:56   transaction.client_ip="192.168.35.11"  transaction.client_port=48814  transaction.host_ip="192.168.35.30"  transaction.host_port=8080
transaction.messages=
[
details=
accuracy="0"  data="Matched Data: s&sos found within ARGS:id: 1' OR '1'='1'-- -"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"  lineNumber="46"
match="detected SQLi using libinjection."  maturity="0"  reference="v30,17"  rev=""  ruleId="942100"  severity="2"
tags=["application-multi", "language-multi", "platform-multi", "attack-sqli", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/248/66", "PCI/6.5.2"]  ver="OWASP_CRS/3.3.7"
message="SQL Injection Attack Detected via libinjection"
,
details=
accuracy="0"  data=""  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"  lineNumber="81"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `5' )"  maturity="0"  reference=""  rev=""  ruleId="949110"  severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-generic"]  ver="OWASP_CRS/3.3.7"
message="Inbound Anomaly Score Exceeded (Total Score: 5)"
]
transaction.producer.components=["OWASP_CRS/3.3.7""]  transaction.producer.connector="ModSecurity-nginx v1.0.4"  transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"
transaction.producer.secrules_engine="Enabled"  transaction.request.headers.Accept="*/*"  transaction.request.headers.Cookie="PHPSESSID=test; security=low"  transaction.request.headers.Host="dvwa"
transaction.request.headers.User-Agent="curl/8.15.0"  transaction.request.http_version=1.1  transaction.request.method="GET"
transaction.request.uri="/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit"
transaction.response.body="<html> <head><title>403 Forbidden</title></head> <body> <center><h1>403 Forbidden</h1></center> <hr><center>nginx</center> </body> </html> "
transaction.response.headers.Access-Control-Allow-Headers="*"  transaction.response.headers.Access-Control-Allow-Methods="GET, POST, PUT, DELETE, OPTIONS"
transaction.response.headers.Access-Control-Allow-Origin="*"  transaction.response.headers.Access-Control-Max-Age="3600"  transaction.response.headers.Connection="keep-alive"
transaction.response.headers.Content-Length="146"  transaction.response.headers.Content-Type="text/plain"  transaction.response.headers.Date="Tue, 23 Sep 2025 16:09:56 GMT"
transaction.response.headers.Server="nginx"  transaction.response.http_code=403  transaction.server_id="6f321859ff21bb517b8374bb52b36a4d4afa6cc3"  transaction.time_stamp="Tue Sep 23 16:09:56 2025"
transaction.unique_id="175864379645.492229"
23/09/2025 13:10:15   2025/09/23 16:10:15 [error] 534#534: *3 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `15' ) [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "81"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 15)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.3.7"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "dvwa"] [uri "/vulnerabilities/xss_r/"] [unique_id "175864381530.334143"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1", host: "dvwa"
23/09/2025 13:10:15   192.168.35.11 - - [23/Sep/2025:16:10:15 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
```


3/09/2025 13:10:15
transaction.client_ip="192.168.35.11" transaction.client_port=34144 transaction.host_ip="192.168.35.30" transaction.host_port=8080
transaction.messages=
[
details=
accuracy="0" data="Matched Data: XSS data found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="38" match="detected XSS using libinjection." maturity="0" reference="v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev=""
ruleId="941100" severity="2" tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"]
ver="OWASP_CRS/3.3.7"
message="XSS Attack Detected via libinjection"
,
details=
accuracy="0" data="Matched Data: <script> found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="64" match="Matched "Operator `Rx' with parameter `(?i)<script[^>]*>[\s\S]*?' against variable `ARGS:name' (Value: `<script>alert("XSS")</script>')" maturity="0"
reference="o0,8v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev="" ruleId="941110" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"] ver="OWASP_CRS/3.3.7"
message="XSS Filter - Category 1: Script Tag Vector"
,
details=
accuracy="0" data="Matched Data: <script found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="181"
match="Matched "Operator `Rx' with parameter `(?i:(?:<\w[\s\S]*[\s\/][`\"](?:[\s\S]*[\s\/])?)(?:on(?:d(?:e(?:vice(?:
(?:orienta|mo)tion|proximity|found|light)|livery(?:success|error)|activate)|r(?:ag(?:e(?:n(?:ter|d)|xit)|(?:gestur|leav)e|start|d (3146 characters omitted)' against variable `ARGS:name'
(Value: `<script>alert("XSS")</script>')"
maturity="0" reference="o0,7v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev="" ruleId="941160" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"] ver="OWASP_CRS/3.3.7"
message="NoScript XSS InjectionChecker: HTML Injection"
,
details=
accuracy="0" data="" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf" lineNumber="81"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `15')" maturity="0" reference="" rev="" ruleId="949110" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-generic"] ver="OWASP_CRS/3.3.7"
message="Inbound Anomaly Score Exceeded (Total Score: 15)"
]
transaction.producer.components=["OWASP_CRS/3.3.7""] transaction.producer.connector="ModSecurity-nginx v1.0.4" transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"
transaction.producer.secrules_engine="Enabled" transaction.request.headers.Accept="*/*" transaction.request.headers.Cookie="security=low" transaction.request.headers.Host="dvwa"
transaction.request.headers.User-Agent="curl/8.15.0" transaction.request.http_version=1.1 transaction.request.method="GET"
transaction.request.uri="/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E"
transaction.response.body="<html> <head><title>403 Forbidden</title></head> <body> <h1>403 Forbidden</h1> <hr> nginx </body> </html> "
transaction.response.headers.Access-Control-Allow-Headers="*" transaction.response.headers.Access-Control-Allow-Methods="GET, POST, PUT, DELETE, OPTIONS"
transaction.response.headers.Access-Control-Allow-Origin="*" transaction.response.headers.Access-Control-Max-Age="3600" transaction.response.headers.Connection="keep-alive"
transaction.response.headers.Content-Length="146" transaction.response.headers.Content-Type="text/plain" transaction.response.headers.Date="Tue, 23 Sep 2025 16:10:15 GMT"
transaction.response.headers.Server="nginx" transaction.response.http_code=403 transaction.server_id="6f321859ff21bb517b8374bb52b36a4d4afa6cc3" transaction.time_stamp="Tue Sep 23 16:10:15 2025"
transaction.unique_id="175864381530.334143"
23/09/2025 13:15:36
2025/09/23 16:15:36 [error] 536#536: *16 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE'
(Value: `15') [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "81"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 15)"] [data ""]
[severity "2"] [ver "OWASP_CRS/3.3.7"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname
"dvwa"] [uri "/vulnerabilities/xss_r/"] [unique_id "175864413628.883449"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/xss_r/?
name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1", host: "dvwa"
23/09/2025 13:15:36
192.168.35.11 - - [23/Sep/2025:16:15:36 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
3/09/2025 13:15:36
transaction.client_ip="192.168.35.11" transaction.client_port=47942 transaction.host_ip="192.168.35.30" transaction.host_port=8080
transaction.messages=
[
details=
accuracy="0" data="Matched Data: XSS data found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="38" match="detected XSS using libinjection." maturity="0" reference="v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev=""
ruleId="941100" severity="2" tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"]
ver="OWASP_CRS/3.3.7"
message="XSS Attack Detected via libinjection"
,
details=
accuracy="0" data="Matched Data: <script> found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="64" match="Matched "Operator `Rx' with parameter `(?i)<script[^>]*>[\s\S]*?' against variable `ARGS:name' (Value: `<script>alert("XSS")</script>')" maturity="0"
reference="o0,8v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev="" ruleId="941110" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"] ver="OWASP_CRS/3.3.7"
message="XSS Filter - Category 1: Script Tag Vector"
,
details=
accuracy="0" data="Matched Data: <script found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="181"
match="Matched "Operator `Rx' with parameter `(?i:(?:<\w[\s\S]*[\s\/][`\"](?:[\s\S]*[\s\/])?)(?:on(?:d(?:e(?:vice(?:
(?:orienta|mo)tion|proximity|found|light)|livery(?:success|error)|activate)|r(?:ag(?:e(?:n(?:ter|d)|xit)|(?:gestur|leav)e|start|d (3146 characters omitted)' against variable `ARGS:name'
(Value: `<script>alert("XSS")</script>')"
maturity="0" reference="o0,7v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev="" ruleId="941160" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"] ver="OWASP_CRS/3.3.7"
message="NoScript XSS InjectionChecker: HTML Injection"
,
details=
accuracy="0" data="" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf" lineNumber="81"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `15')" maturity="0" reference="" rev="" ruleId="949110" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-generic"] ver="OWASP_CRS/3.3.7"
message="Inbound Anomaly Score Exceeded (Total Score: 15)"
]
transaction.producer.components=["OWASP_CRS/3.3.7""] transaction.producer.connector="ModSecurity-nginx v1.0.4" transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"
transaction.producer.secrules_engine="Enabled" transaction.request.headers.Accept="*/*" transaction.request.headers.Cookie="security=low" transaction.request.headers.Host="dvwa"
transaction.request.headers.User-Agent="curl/8.15.0" transaction.request.http_version=1.1 transaction.request.method="GET"
transaction.request.uri="/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E"


3/09/2025 13:15:36
transaction.client_ip="192.168.35.11" transaction.client_port=47942 transaction.host_ip="192.168.35.30" transaction.host_port=8080
transaction.messages=
[
details=
accuracy="0" data="Matched Data: XSS data found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="38" match="detected XSS using libinjection." maturity="0" reference="v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev=""
ruleId="941100" severity="2" tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"]
ver="OWASP_CRS/3.3.7"
message="XSS Attack Detected via libinjection"
,
details=
accuracy="0" data="Matched Data: <script> found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="64" match="Matched "Operator `Rx' with parameter `(?i)<script[^>]*>[\s\S]*?' against variable `ARGS:name' (Value: `<script>alert("XSS")</script>')" maturity="0"
reference="o0,8v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev="" ruleId="941110" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"] ver="OWASP_CRS/3.3.7"
message="XSS Filter - Category 1: Script Tag Vector"
,
details=
accuracy="0" data="Matched Data: <script found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="181"
match="Matched "Operator `Rx' with parameter `(?i:(?:<\w[\s\S]*[\s\/][`\"](?:[\s\S]*[\s\/])?)(?:on(?:d(?:e(?:vice(?:
(?:orienta|mo)tion|proximity|found|light)|livery(?:success|error)|activate)|r(?:ag(?:e(?:n(?:ter|d)|xit)|(?:gestur|leav)e|start|d (3146 characters omitted)' against variable `ARGS:name'
(Value: `<script>alert("XSS")</script>')"
maturity="0" reference="o0,7v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls" rev="" ruleId="941160" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "paranoia-level/1", "OWASP_CRS", "capec/1000/152/242"] ver="OWASP_CRS/3.3.7"
message="NoScript XSS InjectionChecker: HTML Injection"
,
details=
accuracy="0" data="" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf" lineNumber="81"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `15')" maturity="0" reference="" rev="" ruleId="949110" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-generic"] ver="OWASP_CRS/3.3.7"
message="Inbound Anomaly Score Exceeded (Total Score: 15)"
]
transaction.producer.components=["OWASP_CRS/3.3.7""] transaction.producer.connector="ModSecurity-nginx v1.0.4" transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"
transaction.producer.secrules_engine="Enabled" transaction.request.headers.Accept="*/*" transaction.request.headers.Cookie="security=low" transaction.request.headers.Host="dvwa"
transaction.request.headers.User-Agent="curl/8.15.0" transaction.request.http_version=1.1 transaction.request.method="GET"
transaction.request.uri="/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E"
transaction.response.body="<html> <head><title>403 Forbidden</title></head> <body> <h1>403 Forbidden</h1> <hr> nginx </body> </html> "
transaction.response.headers.Access-Control-Allow-Headers="*" transaction.response.headers.Access-Control-Allow-Methods="GET, POST, PUT, DELETE, OPTIONS"
transaction.response.headers.Access-Control-Allow-Origin="*" transaction.response.headers.Access-Control-Max-Age="3600" transaction.response.headers.Connection="keep-alive"
transaction.response.headers.Content-Length="146" transaction.response.headers.Content-Type="text/plain" transaction.response.headers.Date="Tue, 23 Sep 2025 16:15:36 GMT"
transaction.response.headers.Server="nginx" transaction.response.http_code=403 transaction.server_id="6f321859ff21bb517b8374bb52b36a4d4af a6cc3" transaction.time_stamp="Tue Sep 23 16:15:36 2025"
transaction.unique_id="175864413628.883449"
24/09/2025 15:48:43
192.168.35.1 - - [24/Sep/2025:18:48:43 +0000] "GET /security.php HTTP/1.1" 200 2106 "http://localhost:8080/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36" "-"
24/09/2025 15:48:44
192.168.35.1 - - [24/Sep/2025:18:48:44 +0000] "GET /dvwa/css/main.css HTTP/1.1" 200 1109 "http://localhost:8080/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36" "-"
24/09/2025 15:48:44
192.168.35.1 - - [24/Sep/2025:18:48:44 +0000] "GET /dvwa/images/logo.png HTTP/1.1" 200 5044 "http://localhost:8080/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36" "-"
24/09/2025 15:48:44
192.168.35.1 - - [24/Sep/2025:18:48:44 +0000] "GET /dvwa/images/lock.png HTTP/1.1" 200 761 "http://localhost:8080/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36" "-"
24/09/2025 15:48:44
192.168.35.1 - - [24/Sep/2025:18:48:44 +0000] "GET /dvwa/js/dvwaPage.js HTTP/1.1" 200 466 "http://localhost:8080/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36" "-"
24/09/2025 15:48:44
192.168.35.1 - - [24/Sep/2025:18:48:44 +0000] "GET /dvwa/js/add_event_listeners.js HTTP/1.1" 200 276 "http://localhost:8080/security.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36" "-"