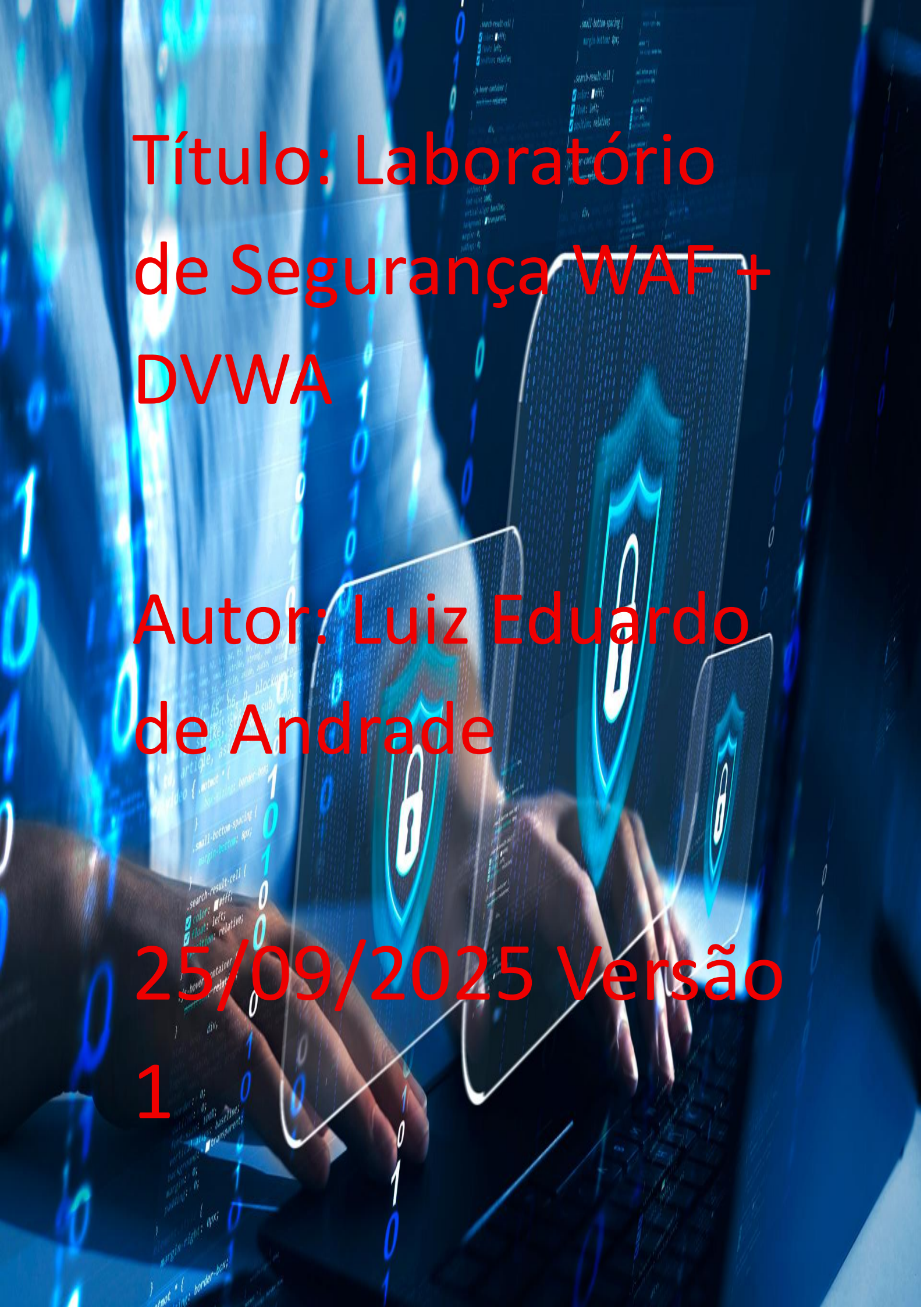


Título: Laboratório de Segurança WAF + DVWA

Autor: Luiz Eduardo de Andrade

25/09/2025 Versão 1

RELATÓRIO – Opção 1 (Hands-on)

Grupo: · Data: <2025-09-29>

1. Sumário Executivo

- Visão geral do ambiente, ataques simulados e nível de proteção alcançado.

Temos 3 redes (DVWA – a rede vulnerável, o DOZZLE que mostra os logs em tempo real e a Kali-Linux para realizar os ataques).

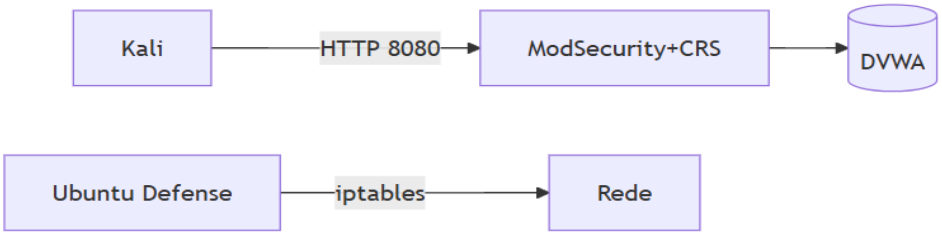
Demonstramos os ataques SQL Injection (SQLi) e Cross-Site Scripting (XSS) podem ser detectados através de uma regra do WAF e também serem bloqueados através de uma outra regra, estes ataques podem ser devastadores para os aplicativos Web seus bancos de dados e seu site podendo até ter a extração de dados.

Implantamos um WAF e regras para que estes ataques de SQLi e XSS essas medidas visam reduzir riscos operacionais e melhorar a segurança geral da rede

2. Objetivo e Escopo

- O que foi defendido, o que foi atacado, limites do exercício.
- Foi realizado o scan da máquina Kali para a máqina DVWA e foi verificado que há duas portas abertas: 8080/tcp open http nginx e 8443/tcp open ssl/http nginx o ataque foi realizado na máquina DVWA vulnerável
- Foram utilizados o Cross-Site Scripting (XSS) e o SQL Injection (SQLI) na porta 8080 para ataque em um cenário houve apenas a detecção e no outro o bloqueio.
- Os limites do exercício seria apenas utilizar XSS e SQLi.

3. Arquitetura (Diagrama)



- Descreva camadas e fluxos.

4. Metodologia

- Passos executados (detecção → bloqueio → resposta), critérios de sucesso.
- Os containers foram criados e executados no Ubuntu 24.04, depois no arquivo docker-compose.yml começamos com o modo de detecção deleto o # e alinho o comando MOD_SEC_RULE =DetectionOnly, o modo de bloqueio mantenho com o # para ele não ser executado e que mostra que os ataques de SQL Injection e de Cross-Site Scripting estão acontecendo mas que não há o bloqueio apenas o log mostra o código 302 de redirecionamento e mostrando que o ataque foi efetivado.
- Vamos novamente no arquivo docker-compose.yml e agora vamos retirar o # do modo de bloqueio MOD_SEC_RULE_ENGINE=on e alinhar e vamos colocar o # no modo de detecção, neste caso os ataques de SQL Injection e de Cross-Site Scripting são bloqueados e mostra o código 403 de Forbidden (Proibido) e evitando efetivamente o ataque.

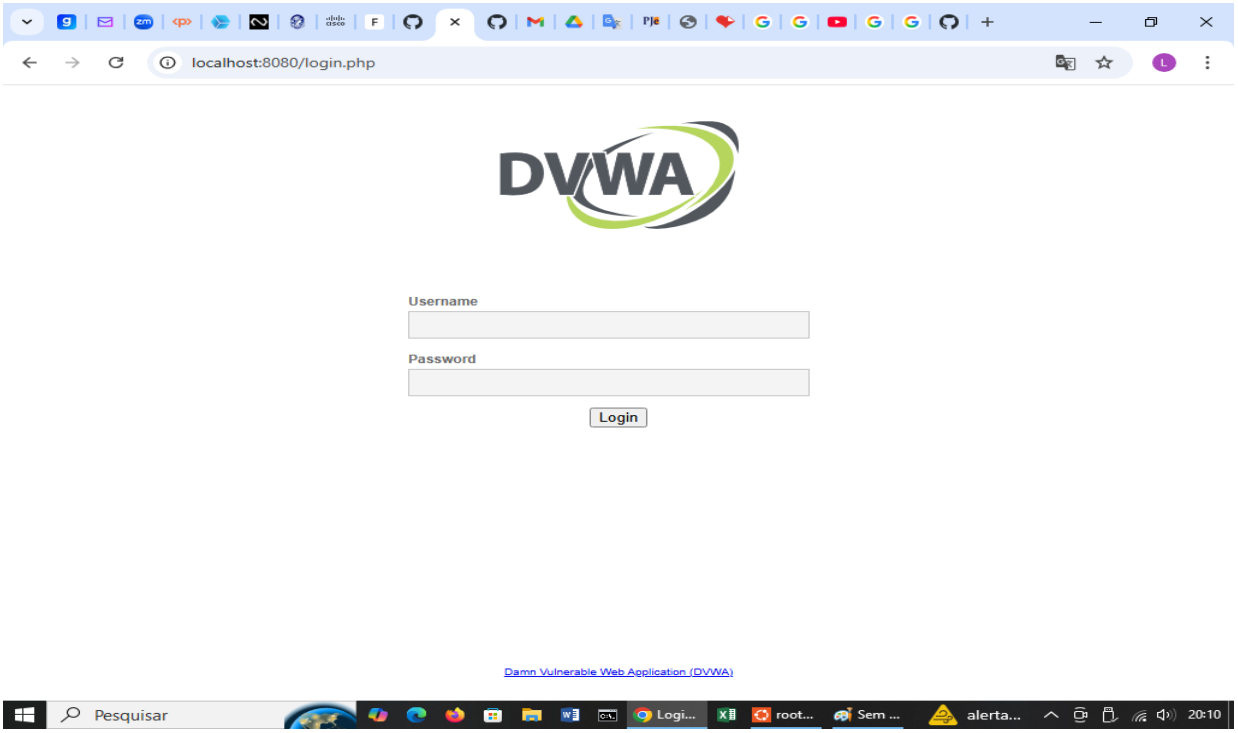
5. Execução e Evidências

- SQLi e XSS (detalhes, prints, resultados)
- Modo blocking (403 + logs CRS)
- iptables/tcpdump, tuning, decisões

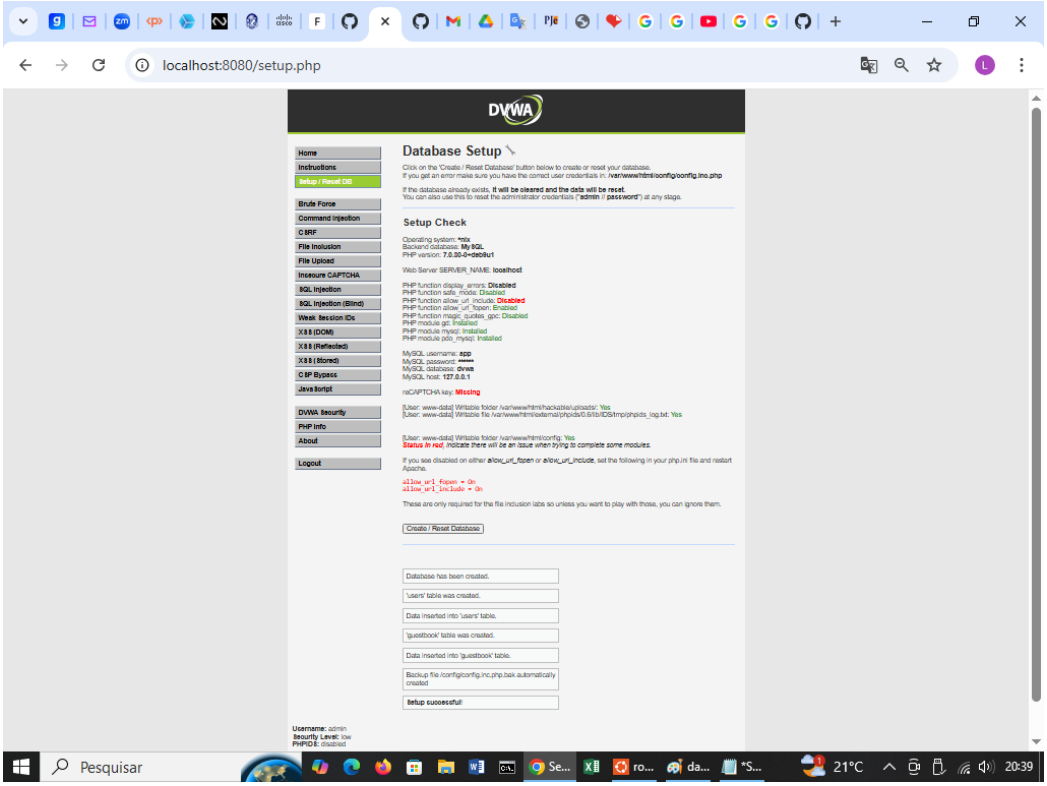
Os 4 cointainers rodando no Ubuntu: O WAF, O DVWA, o DOZZLE e o Kali_lab35

```
root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs
 => [kali_lab35 internal] load metadata for docker.io/kalilinux/kali-rolling:latest                                  0.0s
 => [kali_lab35 internal] load .dockerignore                                                                          0.0s
 => => transferring context: 2B                                                                                       0.0s
 => [kali_lab35 1/2] FROM docker.io/kalilinux/kali-rolling:latest                                                     0.0s
 => CACHED [kali_lab35 2/2] RUN apt-get update && DEBIAN_FRONTEND=noninteractive apt-get install -y     nmap gobu      0.0s
 => [kali_lab35] exporting to image                                                                                   0.0s
 => => exporting layers                                                                                               0.0s
 => => writing image sha256:0313b2fd9524d0031c7b8a08c550842855f778e81000f0ff3308ade4d676a4d6                          0.0s
 => => naming to docker.io/library/labs-kali_lab35                                                                    0.0s
 => [kali_lab35] resolving provenance for metadata file                                                               0.0s
[+] Running 6/6
 ✔ kali_lab35              Built                                                                                      0.0s
 ✔ Network labs_labnet35   Created                                                                                    0.1s
 ✔ Container dozzle        Started                                                                                    0.7s
 ✔ Container kali_lab35    Started                                                                                    0.7s
 ✔ Container dvwa          Started                                                                                    0.6s
 ✔ Container waf_modsec    Started                                                                                    0.9s
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs# docker
ps
CONTAINER ID   IMAGE                                  COMMAND                  CREATED          STATUS                    PORTS
                                          NAMES
3cdb10e6c216   owasp/modsecurity-crs:nginx-alpine     "/docker-entrypoint.…"   30 minutes ago   Up 30 minutes (healthy)   0.0.0
.0:8080->8080/tcp, [::]:8080->8080/tcp    waf_modsec
5a2ce0cb12d9   vulnerables/web-dvwa                   "/main.sh"               30 minutes ago   Up 30 minutes             80/tc
p                                         dvwa
1df440ae206b   amir20/dozzle:latest                   "/dozzle"                30 minutes ago   Up 30 minutes             0.0.0
.0:9999->8080/tcp, [::]:9999->8080/tcp    dozzle
3dfc92e0ce4c   labs-kali_lab35                        "/bin/bash"              30 minutes ago   Up 30 minutes
                                          kali_lab35
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs#
```

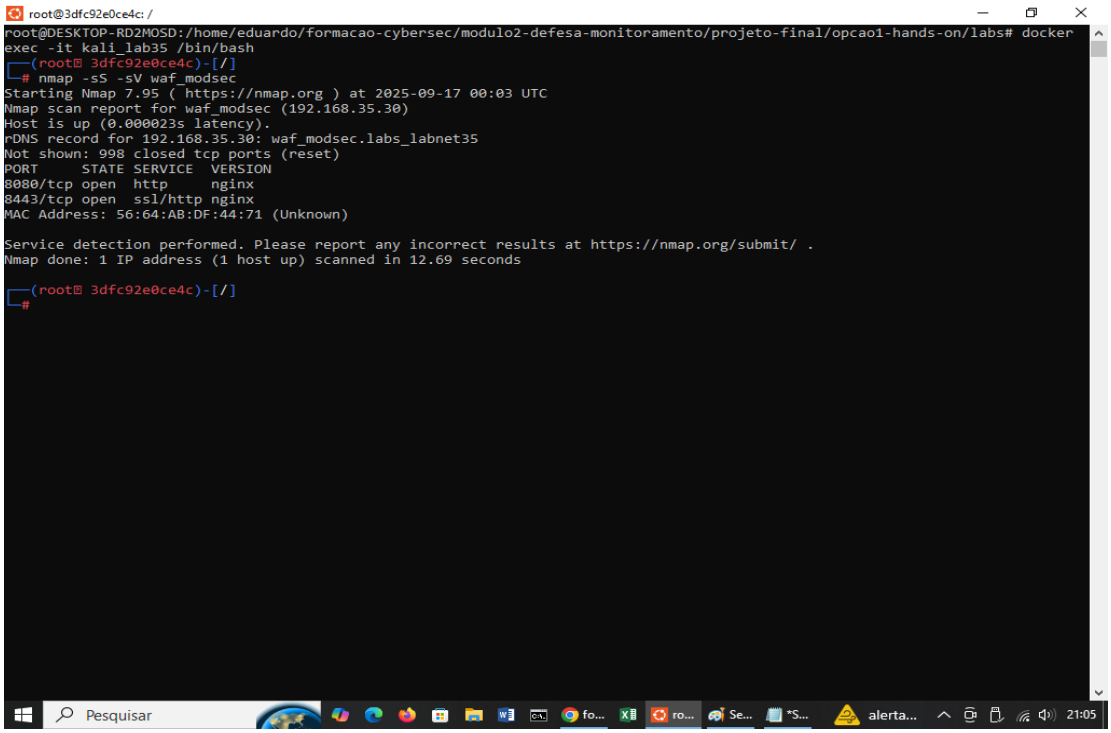
Interface gráfica do DVWA



Resetando o BD do DVWA



No terminal do Kali Linux foi realizado um NMAP no WAF através do comando docker exec -it kali_lab35 e foram encontradas as portas 8080 e 8443 abertas



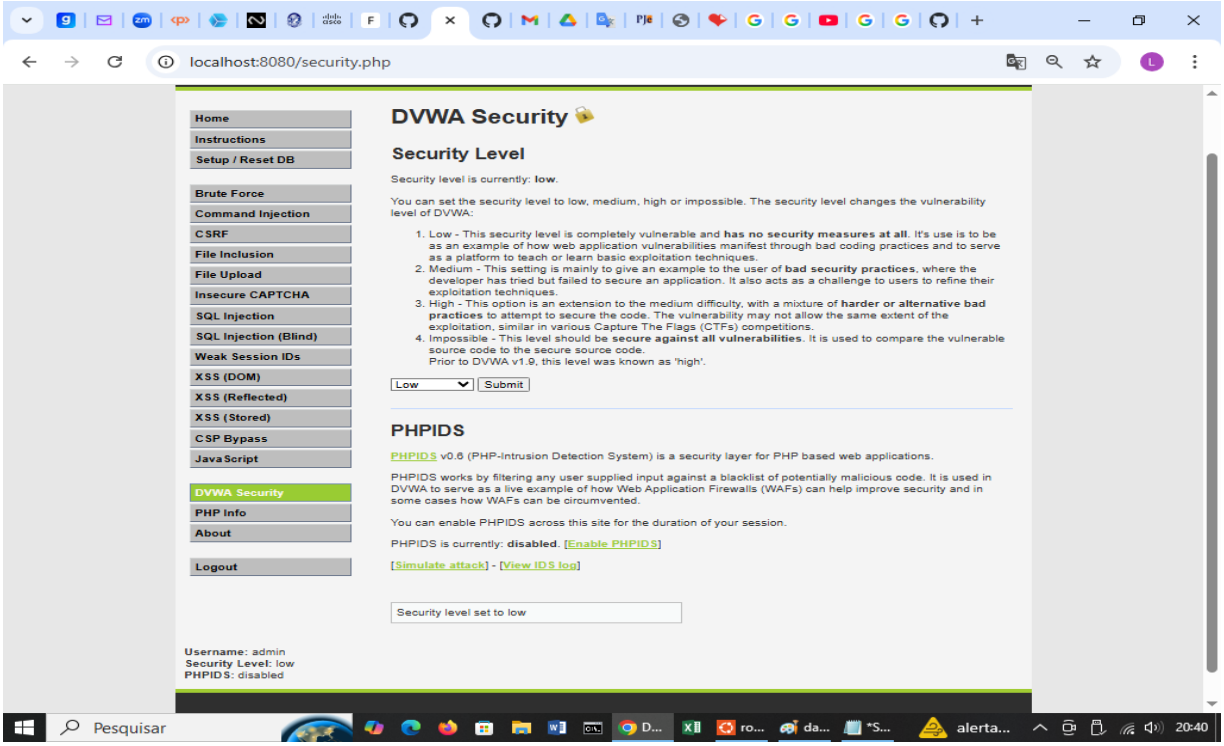
Modificamos o arquivo docker-compose.yml coloca-se o # quando não queremos que o comando seja realizado por exemplo # MODSEC_RULE_ENGINE=On deixamos apenas o modo de detecção ativo e será ele que será executado.

```
root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs
  GNU nano 7.2                                   docker-compose.yml *
version: "3.9"

services:
  kali_lab35:
    build:
      context: .
      dockerfile: Dockerfile.kali
    container_name: kali_lab35
    tty: true
    volumes:
      - ./scripts:/scripts
    networks:
      labnet35:
        ipv4_address: 192.168.35.11

  waf_modsec:
    image: owasp/modsecurity-crs:nginx-alpine
    container_name: waf_modsec
    environment:
      - BACKEND=http://dvwa:80        # para onde o WAF faz proxy_pass
      - SERVER_NAME=localhost         # hostname do WAF
      # MODSEC_RULE_ENGINE=On  # modo blocking (bloqueia ataques)
      - MODSEC_RULE_ENGINE=DetectionOnly
      # Níveis de paranoia (afinam detecção/bloqueio):
      - BLOCKING_PARANOIA=1
      - DETECTION_PARANOIA=1
    depends_on:
      - dvwa
    ports:
      - "8080:8080"                   # atenção: 8080:8080 (default da imagem OWASP)
    networks:
      labnet35:
        ipv4_address: 192.168.35.30

  dvwa:
    image: vulnerables/web-dvwa
    container_name: dvwa
    networks:
      labnet35:
        ipv4_address: 192.168.35.40

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy
```

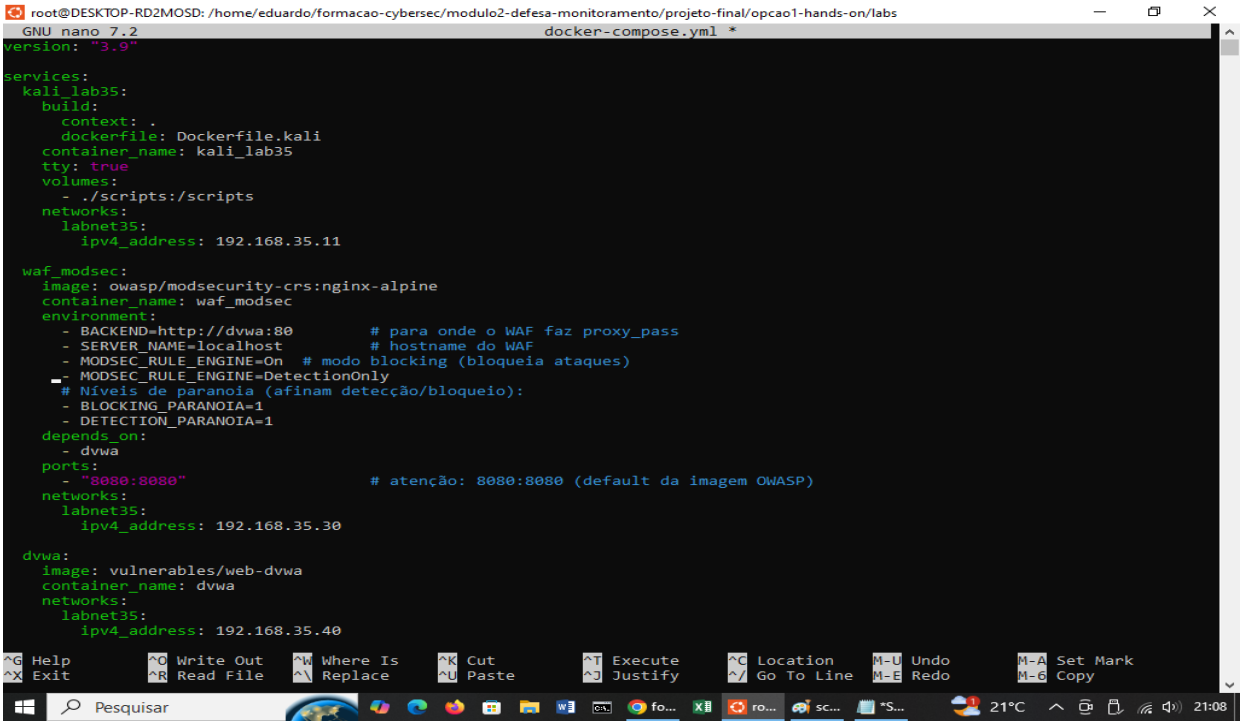
Depois temos que reiniciar o WAF para que as modificações sejam realizadas com o comando docker composse up -d –force-recreate waf-modsec

```
root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs# docker
exec -it kali_lab35 /bin/bash
┌──(root㉿ 3dfc92e0ce4c)-[/]
└─# nmap -sS -sV waf_modsec
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 00:03 UTC
Nmap scan report for waf_modsec (192.168.35.30)
Host is up (0.000023s 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: 56:64:AB:DF:44:71 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.69 seconds

┌──(root㉿ 3dfc92e0ce4c)-[/]
└─# exit
exit
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs# ls
Dockerfile.kali  docker-compose.yml  scripts
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs# nano do
cker-compose.yml
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs# docker
compose up -d --force-recreate waf_modsec
WARN[0000] /home/eduardo/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                                                                    1.1s
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs#
```

Configuramos o DVWA para a segurança low (baixa)



Depois de reiniciarmos o WAF enviamos o código de Cross-Site Scripting (XSS) no terminal lembrando que estamos apenas no modo detecção:



O comando do XSS é:

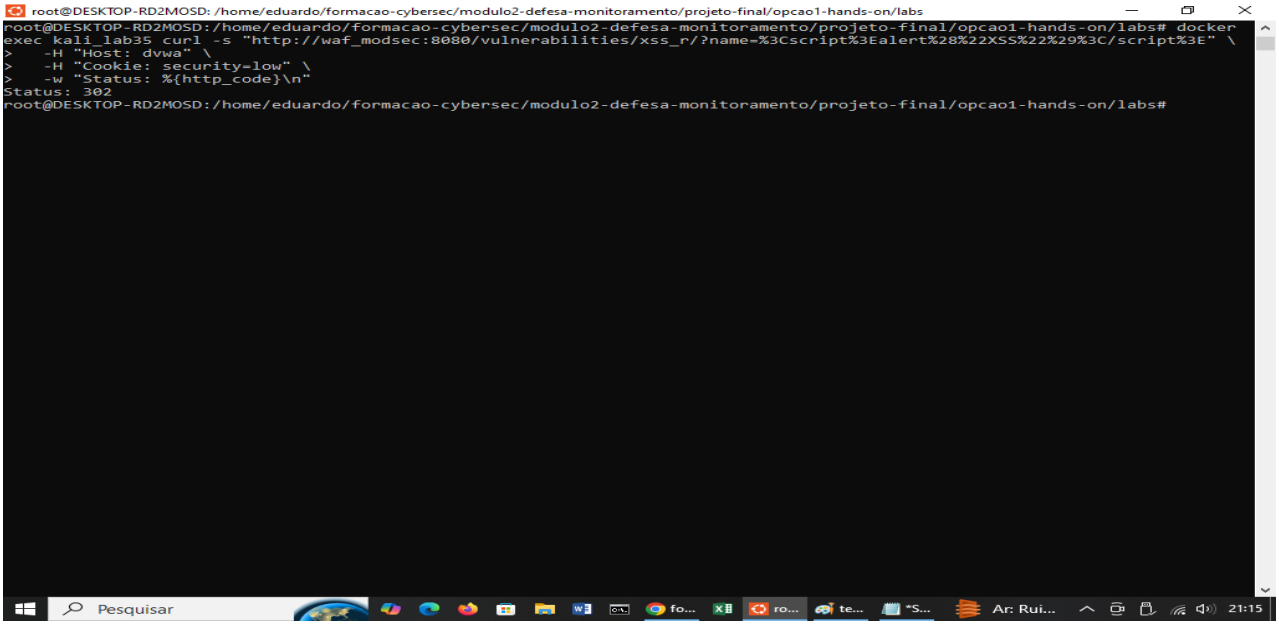
docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E" \

  -H "Host: dvwa" \

  -H "Cookie: security=low" \

  -w "Status: %{http_code}\n"

Vemos que o xss foi realizado com sucesso, ele detectou, mas não bloqueou por isso temos o código 302 (redirecionamento)



Agora enviamos o código de SQL Injection:

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"

Acontece o mesmo com o SQLi ele é detectado mas não bloqueado por este motivo temos o código 302 (redirecionamento)

```
root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs
root@DESKTOP-RD2MOSD:/home/eduardo/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 "H>    -H "Host: dvwa" \
>    -H "Cookie: PHPSESSID=test; security=low" \
>    -w "Status: %{http_code}\n"
Status: 302
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs#
```

No docker-compose.yml agora está ativado o modo de bloqueio, reiniciamos novamente o waf e colocamos o código de SQL Injection:

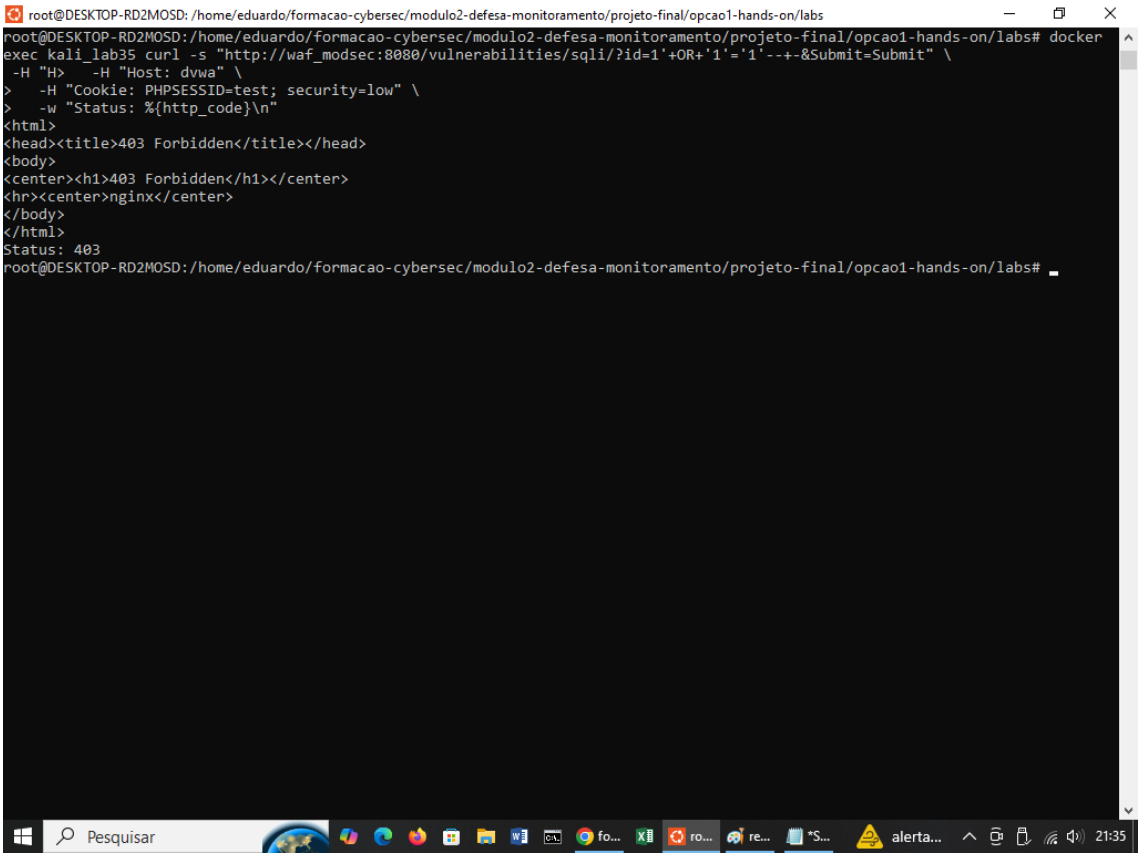
```
root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs
  GNU nano 7.2                                   docker-compose.yml *
version: "3.9"

services:
  kali_lab35:
    build:
      context: .
      dockerfile: Dockerfile.kali
    container_name: kali_lab35
    tty: true
    volumes:
      - ./scripts:/scripts
    networks:
      labnet35:
        ipv4_address: 192.168.35.11

  waf_modsec:
    image: owasp/modsecurity-crs:nginx-alpine
    container_name: waf_modsec
    environment:
      - BACKEND=http://dvwa:80        # para onde o WAF faz proxy_pass
      - SERVER_NAME=localhost         # hostname do WAF
      - MODSEC_RULE_ENGINE=On  # modo blocking (bloqueia ataques)
      # - MODSEC_RULE_ENGINE=DetectionOnly
      # Níveis de paranoia (afinam detecção/bloqueio):
      - BLOCKING_PARANOIA=1
      - DETECTION_PARANOIA=1
    depends_on:
      - dvwa
    ports:
      - "8080:8080"                   # atenção: 8080:8080 (default da imagem OWASP)
    networks:
      labnet35:
        ipv4_address: 192.168.35.30

  dvwa:
    image: vulnerables/web-dvwa
    container_name: dvwa
    networks:
      labnet35:
        ipv4_address: 192.168.35.40

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy
```

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"



Vemos que o acesso é negado pois ele bloqueou a tentativa de ataque de SQL Injection (SQLi) e retorna o código 403 Forbidden (Proibido)

Utilizamos o XSS com o seguinte código:

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" \

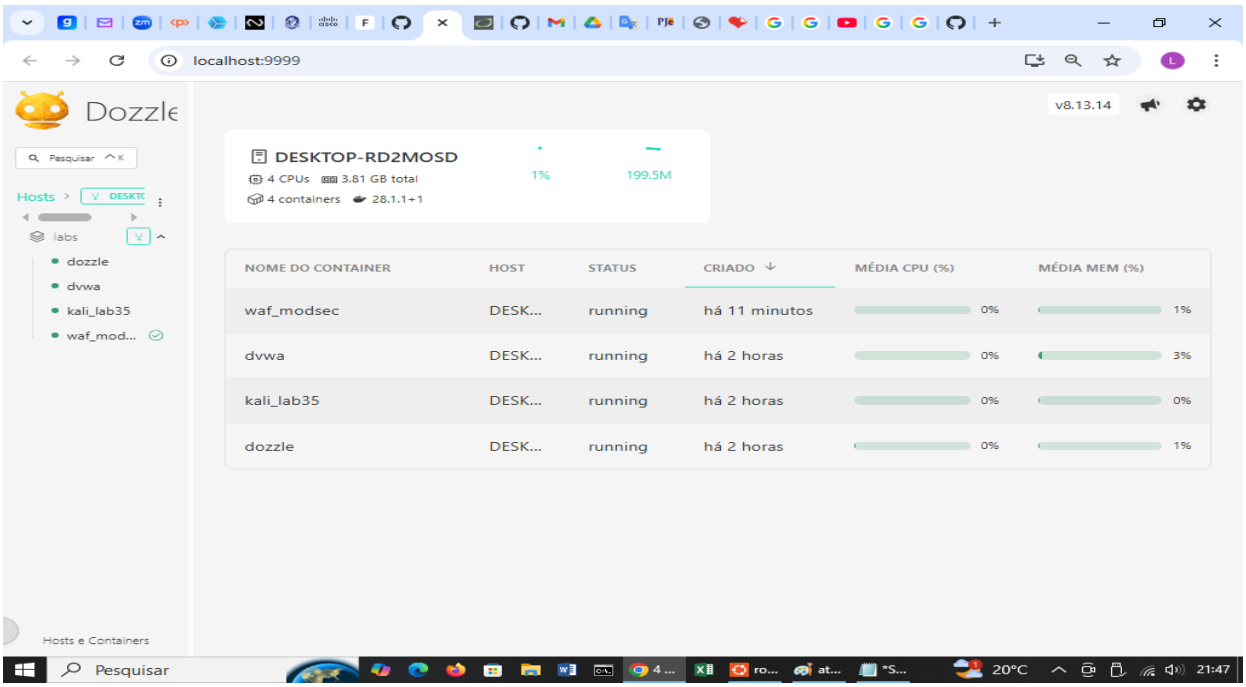
-H "Cookie: security=low" \

-w "Status: %{http_code}\n"

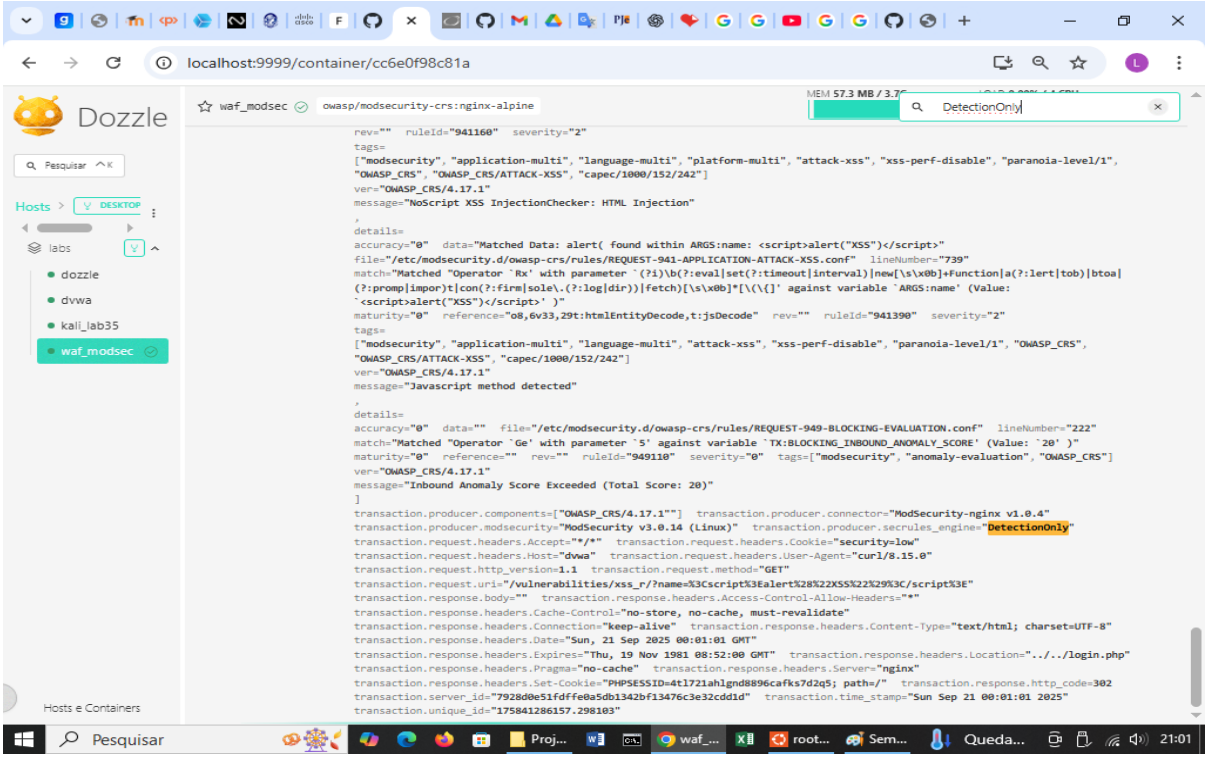
```
root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs# docker
exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%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>
</body>
</html>
Status: 403
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs#
```

Vemos que o acesso é negado pois ele bloqueou a tentativa de ataque de Cross-Site Scripting (XSS) e retorna o código 403 Forbidden (Proibido)

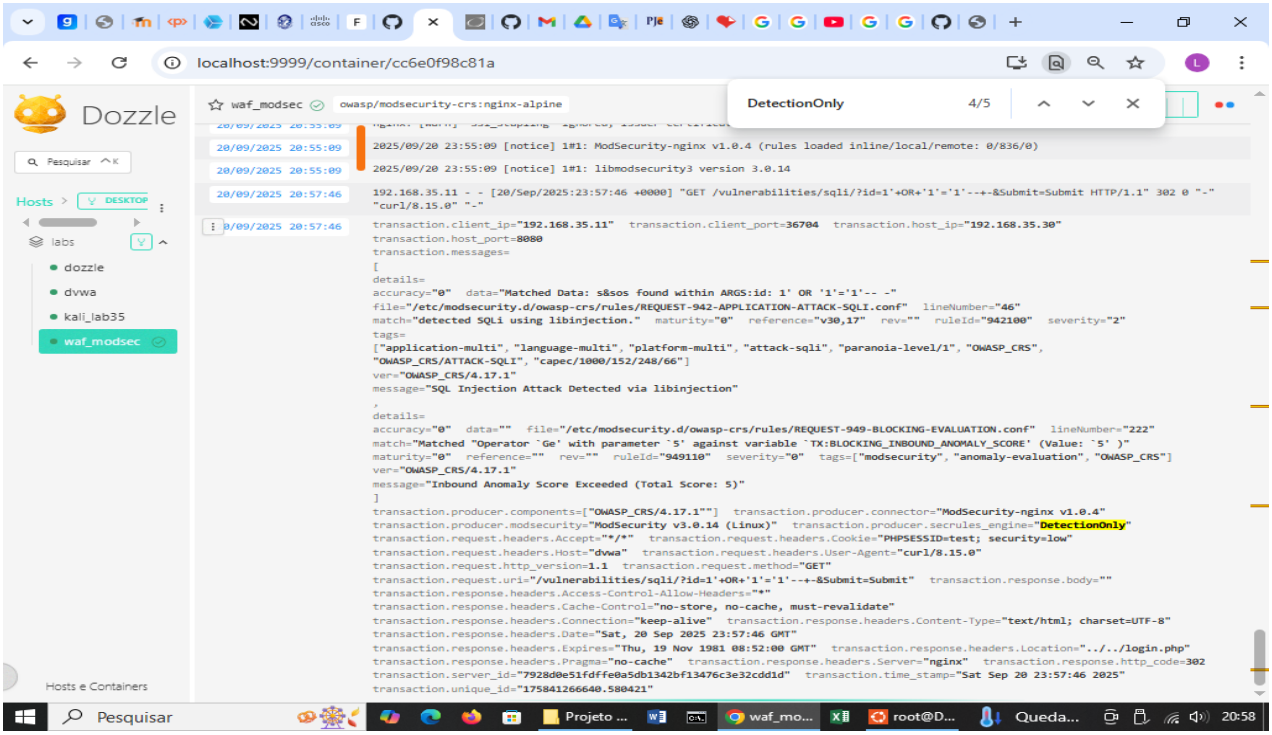
Acessar a plataforma Dozzle através da browser: http://localhost:9999 e escolher o container do waf_modsec para ver os logs em tempo real



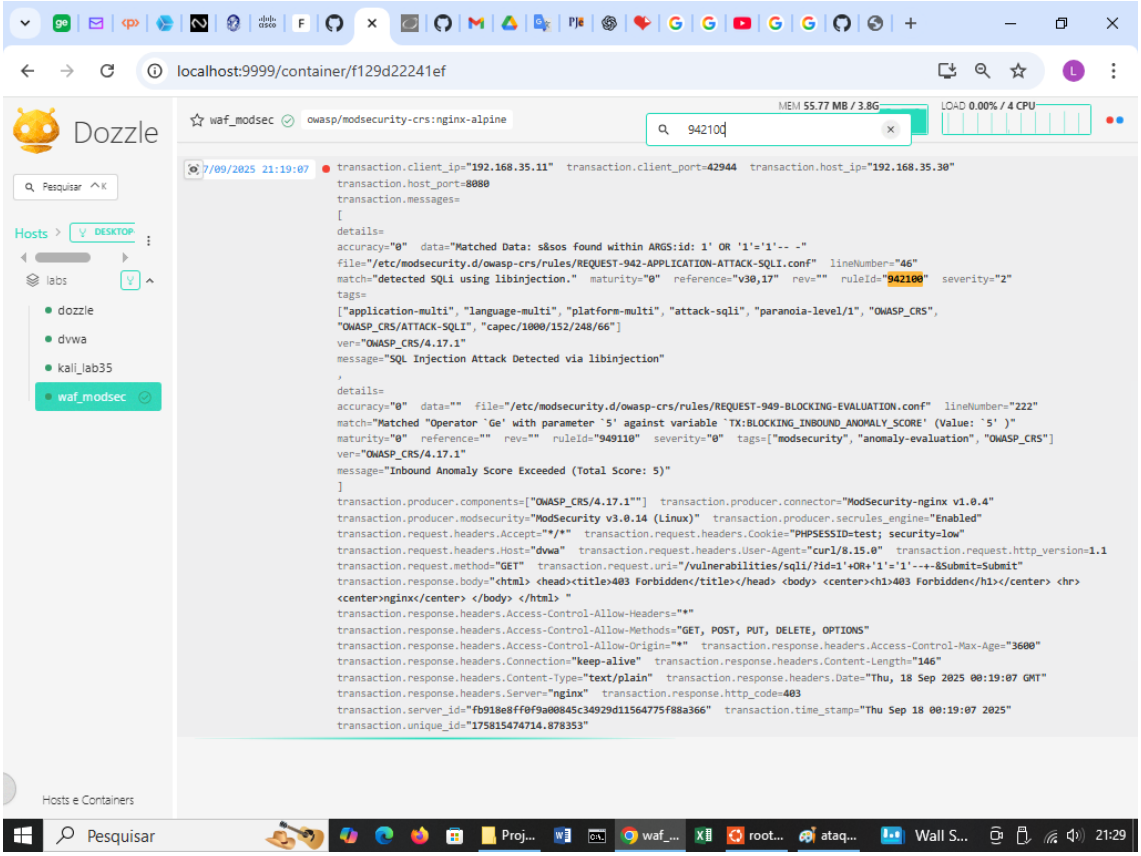
Informações importantes "secrules_engine":"DetectionOnly" em XSS

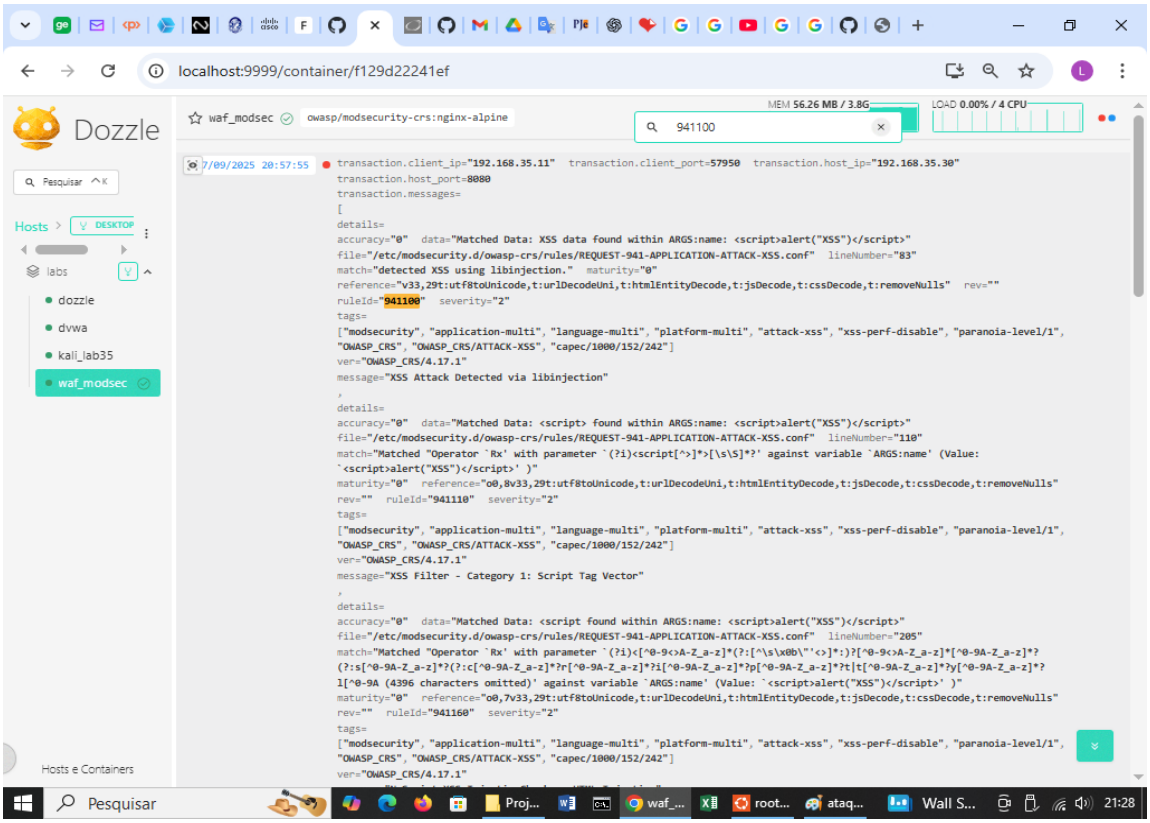


Informações importantes "secrules_engine":"DetectionOnly" em SQLi

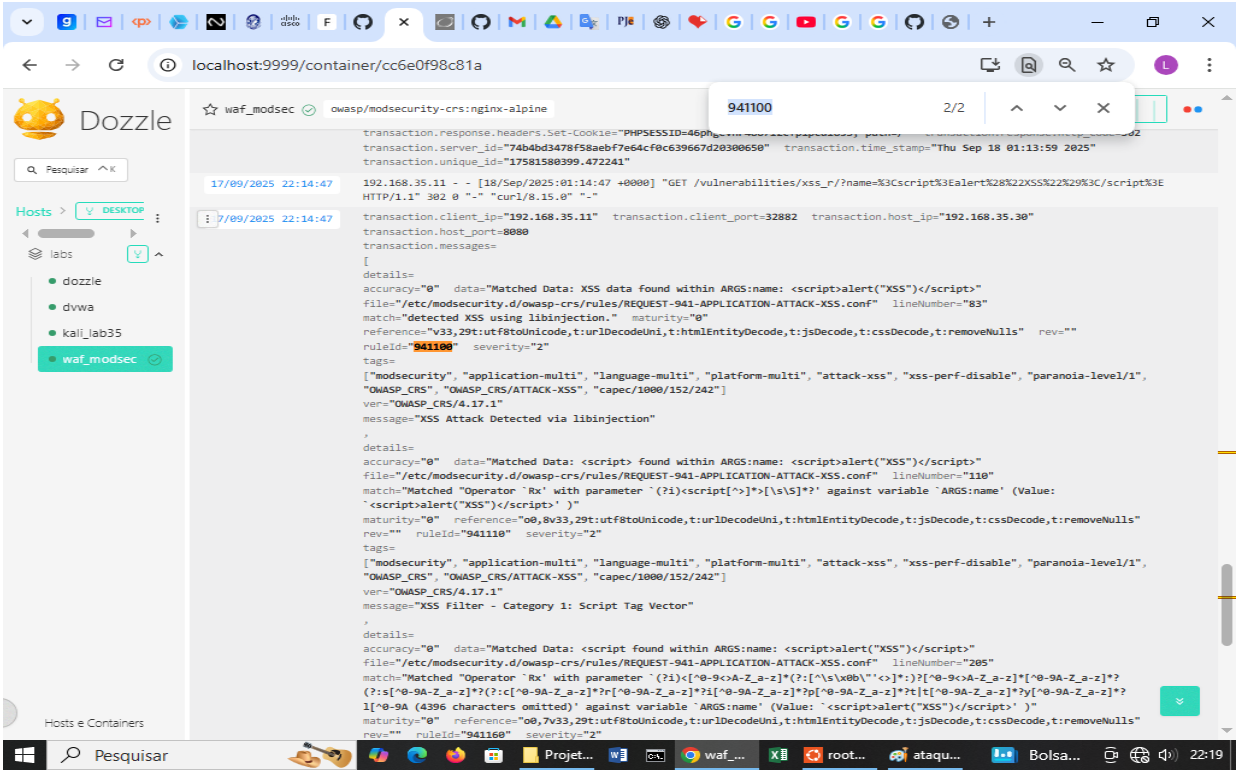


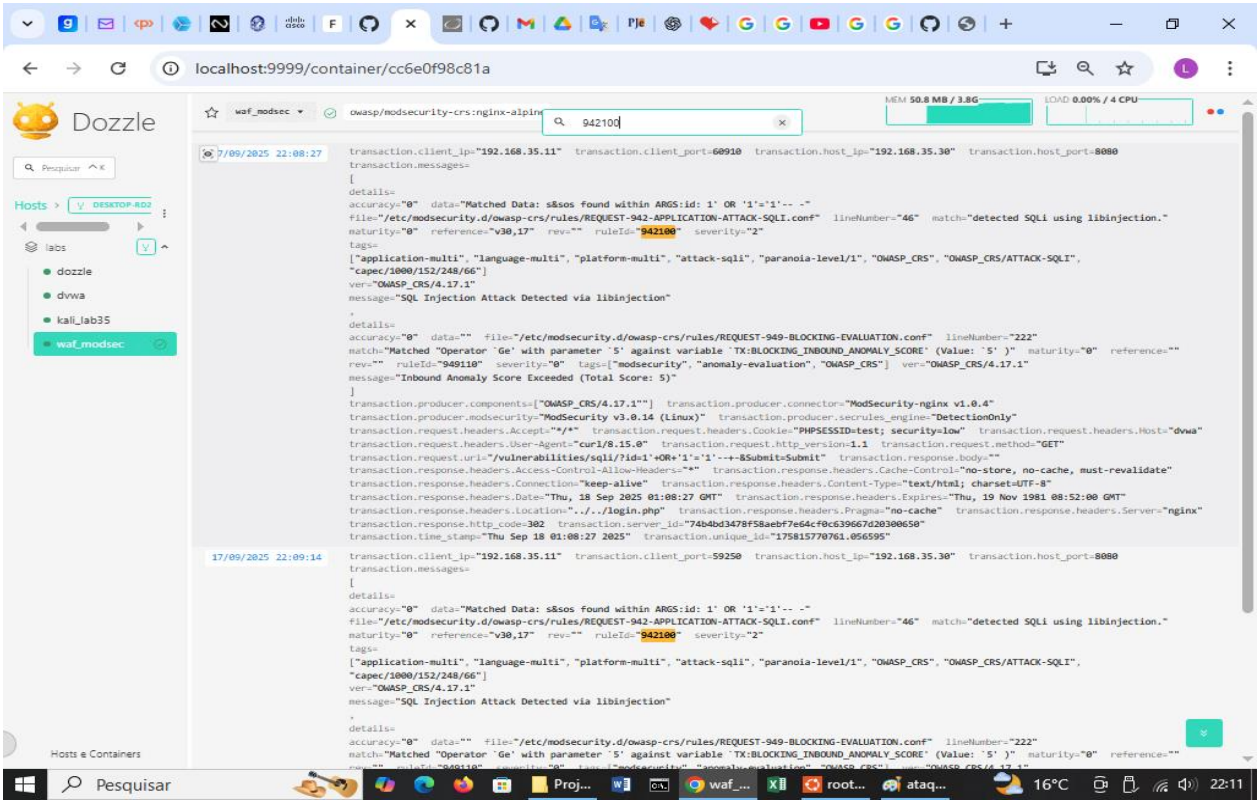
Informações importantes Rule IDs: 942100 (SQLi), 941100 (XSS) bloqueados



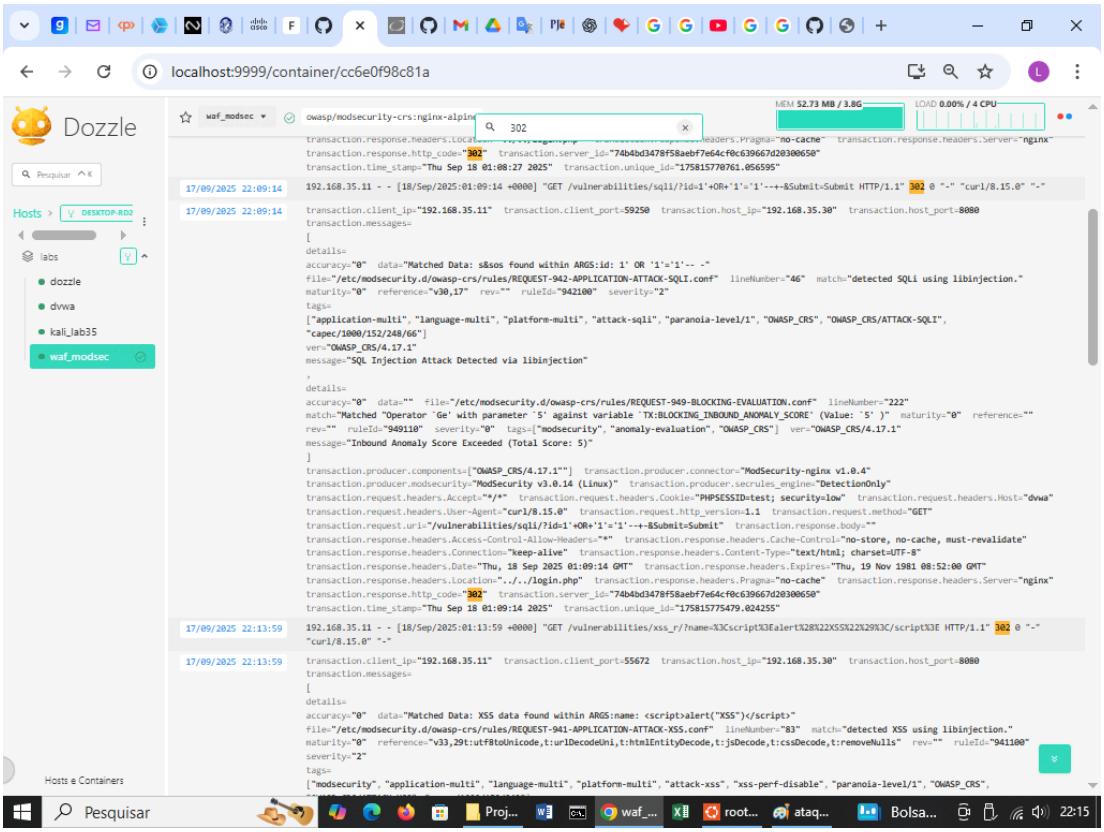


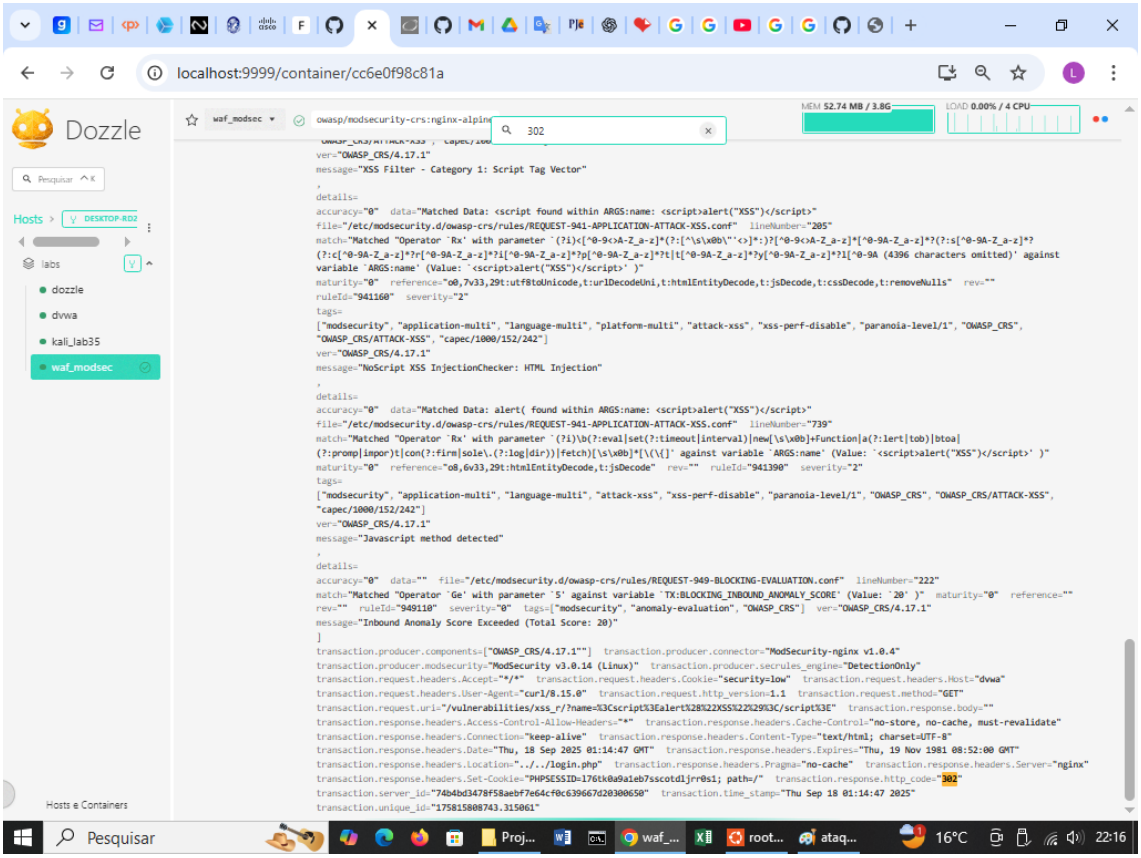
Informações importantes Rule IDs: 942100 (SQLi), 941100 (XSS) detectados mas não bloqueados

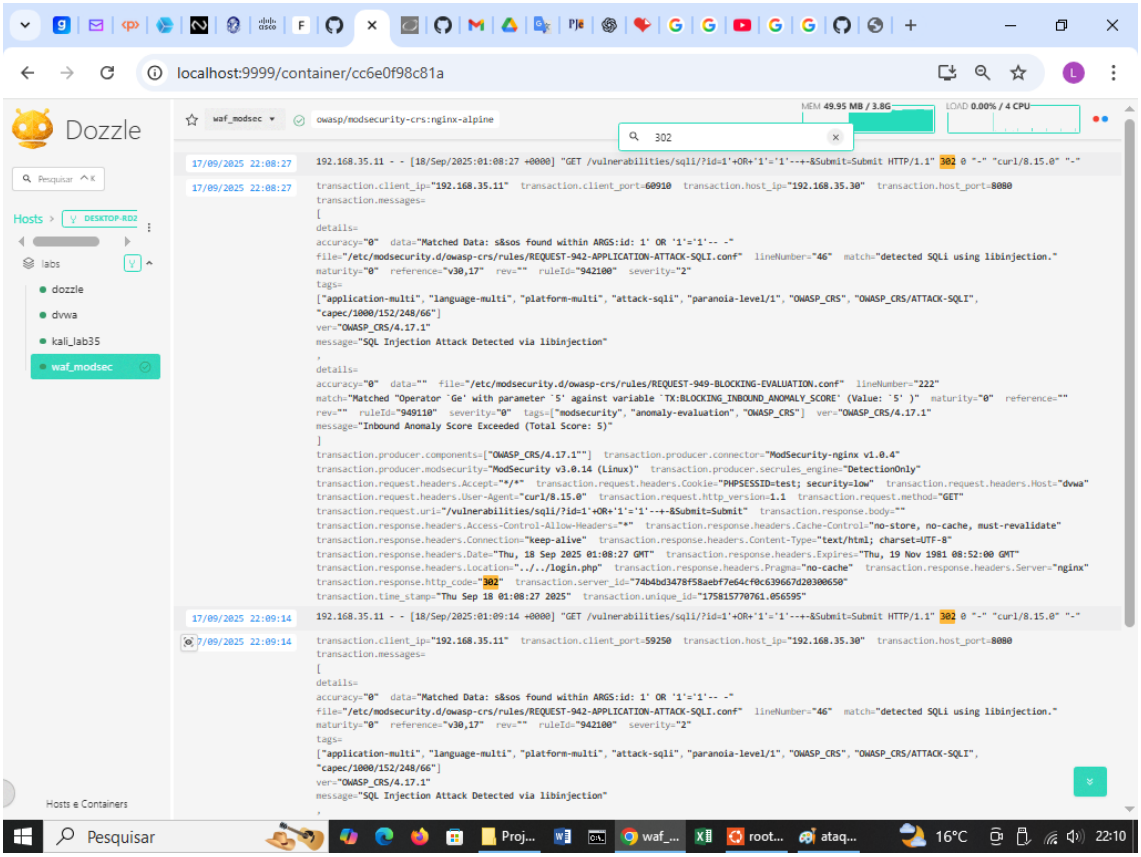


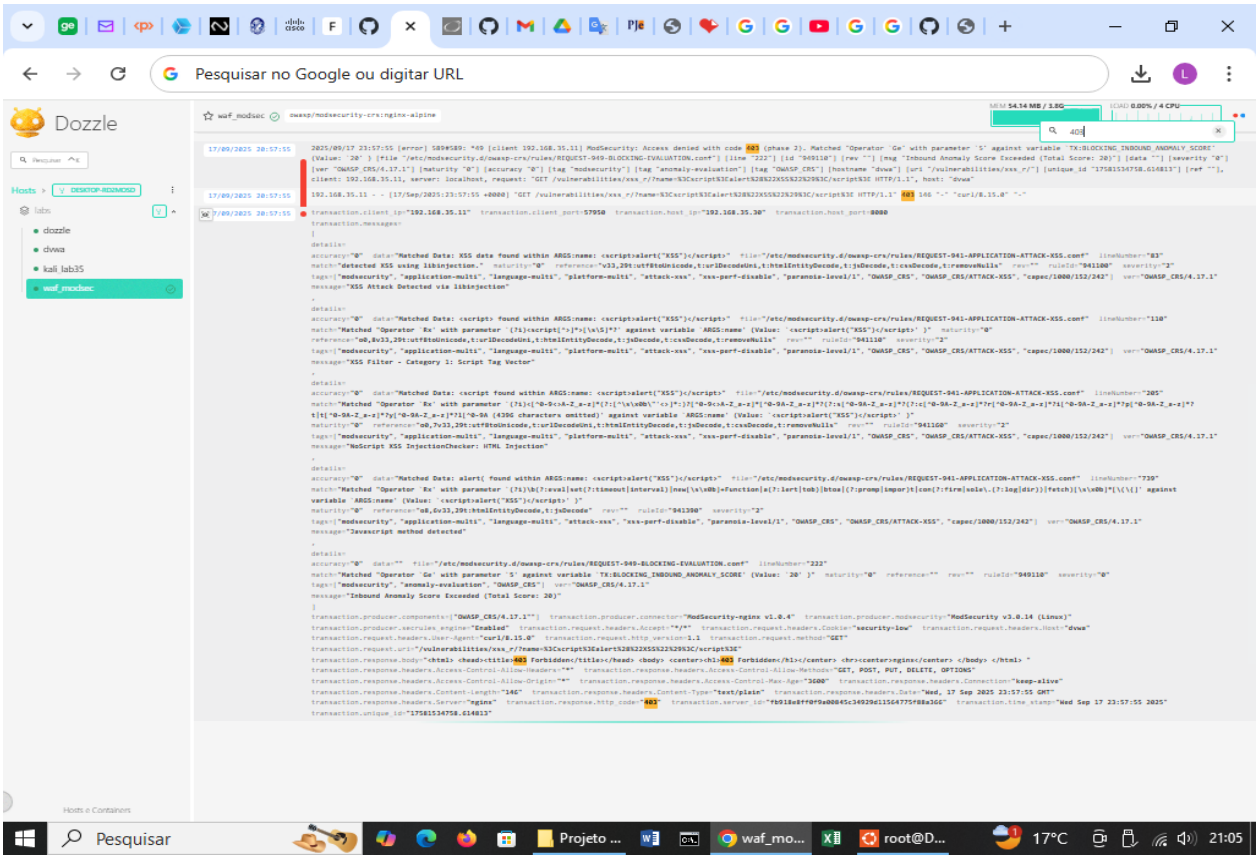


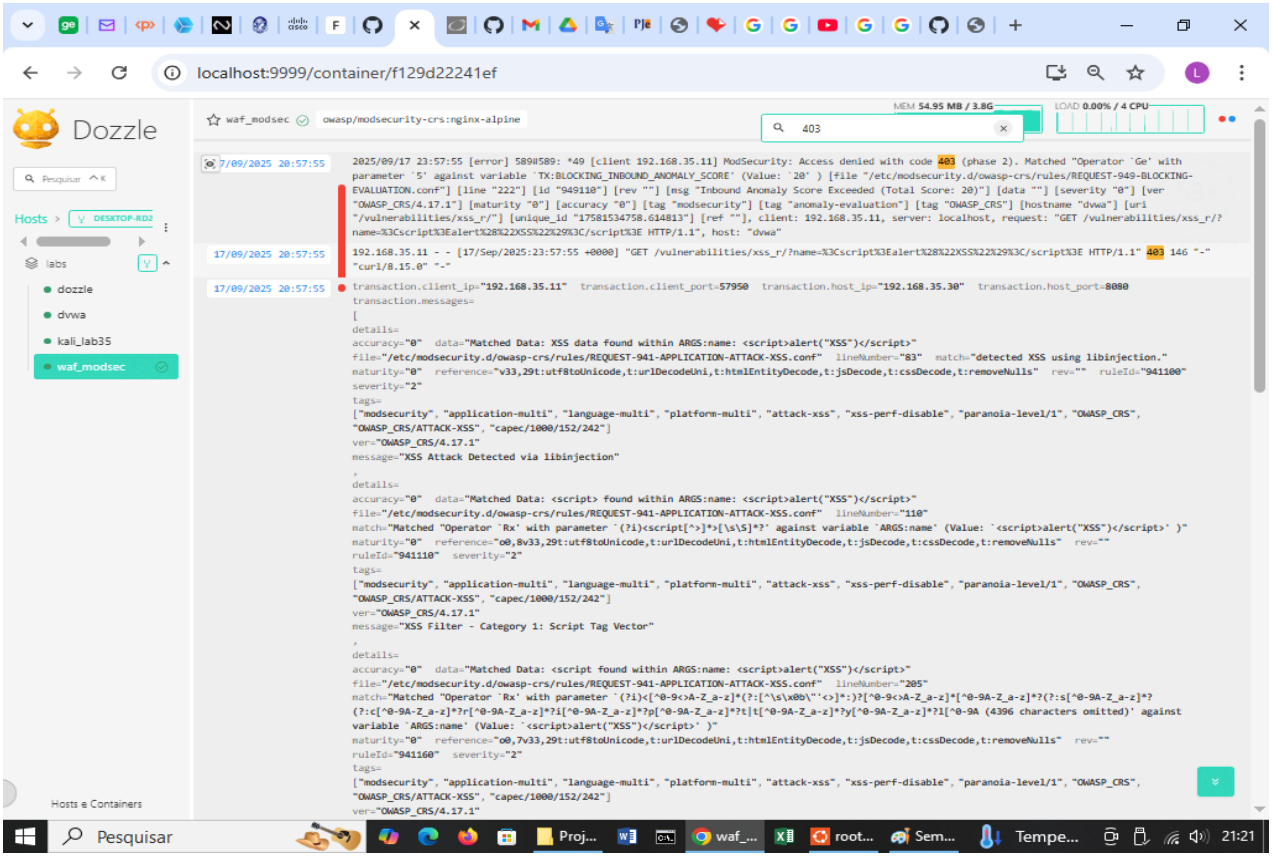
Informações importantes HTTP Status Codes: 302 (detecção) vs 403 (bloqueio)

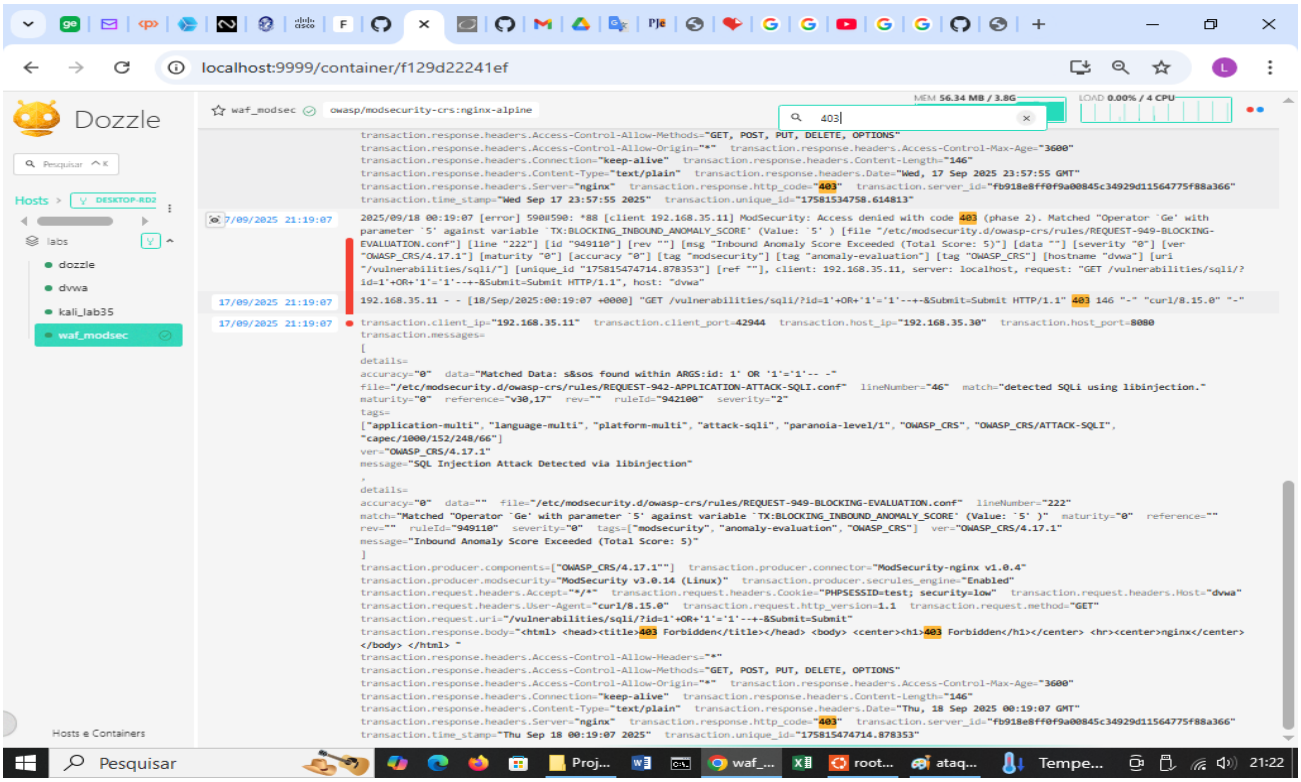





localhost:9999/container/cc6e0f98c81a
Dozzle
waf_modsec
owasp/modsecurity-crs:nginx-alpine
302
17/09/2025 22:08:27
192.168.35.11 - - [18/Sep/2025:01:08:27 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 302 0 "-" "curl/8.15.0" "-"
transaction.client_ip="192.168.35.11" transaction.client_port=60910 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", "OWASP_CRS/ATTACK-SQLI",
"capec/1000/152/248/66"]
ver="OWASP_CRS/4.17.1"
message="SQL Injection Attack Detected via libinjection"
,
details=
accuracy="0" data="" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf" lineNumber="222"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `5')" maturity="0" reference=""
rev="" ruleId="949110" severity="0" tags=["modsecurity", "anomaly-evaluation", "OWASP_CRS"] ver="OWASP_CRS/4.17.1"
message="Inbound Anomaly Score Exceeded (Total Score: 5)"
]
transaction.producer.components=["OWASP_CRS/4.17.1""] transaction.producer.connector="ModSecurity-nginx v1.0.4"
transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)" transaction.producer.secrules_engine="DetectionOnly"
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=""
transaction.response.headers.Access-Control-Allow-Headers="*" transaction.response.headers.Cache-Control="no-store, no-cache, must-revalidate"
transaction.response.headers.Connection="keep-alive" transaction.response.headers.Content-Type="text/html; charset=UTF-8"
transaction.response.headers.Date="Thu, 18 Sep 2025 01:08:27 GMT" transaction.response.headers.Expires="Thu, 19 Nov 1981 08:52:00 GMT"
transaction.response.headers.Location="../../login.php" transaction.response.headers.Pragma="no-cache" transaction.response.headers.Server="nginx"
transaction.response.http_code="302" transaction.server_id="74b4bd3478f58aebf7e64cf0c639667d20300650"
transaction.time_stamp="Thu Sep 18 01:08:27 2025" transaction.unique_id="175815770761.056595"
17/09/2025 22:09:14
192.168.35.11 - - [18/Sep/2025:01:09:14 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 302 0 "-" "curl/8.15.0" "-"
transaction.client_ip="192.168.35.11" transaction.client_port=59250 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", "OWASP_CRS/ATTACK-SQLI",
"capec/1000/152/248/66"]
ver="OWASP_CRS/4.17.1"
message="SQL Injection Attack Detected via libinjection"
Hosts e Containers
Pesquisar


Pesquisar no Google ou digitar URL
Dozzle
waf_modsec
owasp/modsecurity-crs:nginx-alpine
403
17/09/2025 20:57:55
transaction.client_ip="192.168.35.11" transaction.client_port=57950 transaction.host_ip="192.168.35.30" transaction.host_port=8080
Hosts e Containers
Pesquisar

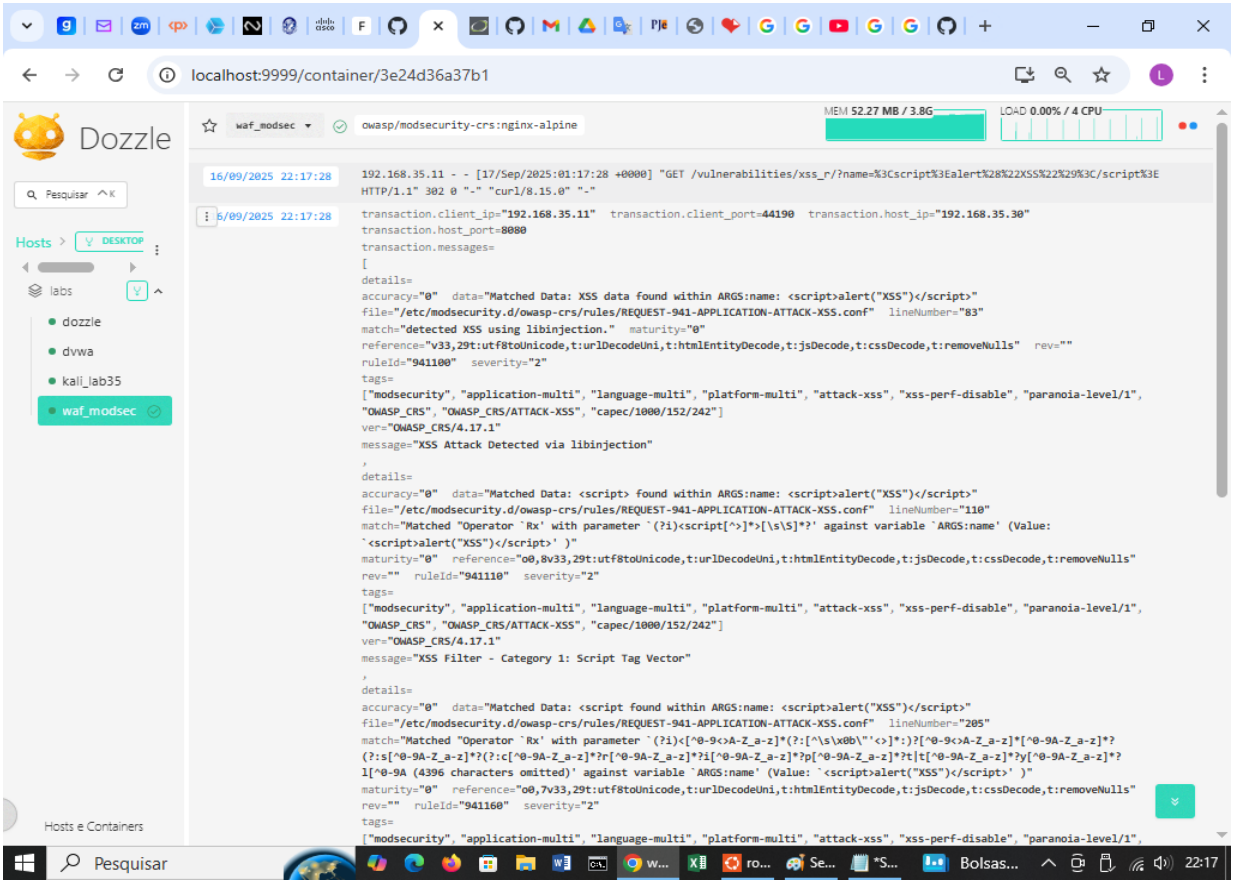

localhost:9999/container/f129d22241ef
Dozzle
waf_modsec
owasp/modsecurity-crs:nginx-alpine
403
MEM 54.95 MB / 3.8G
LOAD 0.00% / 4 CPU
Hosts
DESKTOP-RD2
labs
dozzle
dvwa
kali_lab35
waf_modsec
Hosts e Containers
7/09/2025 20:57:55
2025/09/17 23:57:55 [error] 589#589: *49 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `20') [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 20)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.17.1"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/xss_r/"] [unique_id "17581534758.614813"] [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"
17/09/2025 20:57:55
192.168.35.11 - - [17/Sep/2025:23:57:55 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
17/09/2025 20:57:55
transaction.client_ip="192.168.35.11" transaction.client_port=57950 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="83" 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", "xss-perf-disable", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-XSS", "capec/1000/152/242"]
ver="OWASP_CRS/4.17.1"
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="110"
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", "xss-perf-disable", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-XSS", "capec/1000/152/242"]
ver="OWASP_CRS/4.17.1"
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="205"
match="Matched "Operator `Rx' with parameter `(?i)<[^0-9<>A-Z_a-z]*(?:[^\s\x0b\"'<>]*:)?[^0-9<>A-Z_a-z]*[^0-9A-Z_a-z]*?(?:s[^0-9A-Z_a-z]*?(?:c[^0-9A-Z_a-z]*?r[^0-9A-Z_a-z]*?i[^0-9A-Z_a-z]*?p[^0-9A-Z_a-z]*?t|t[^0-9A-Z_a-z]*?y[^0-9A-Z_a-z]*?l[^0-9A (4396 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", "xss-perf-disable", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-XSS", "capec/1000/152/242"]
ver="OWASP_CRS/4.17.1"
Pesquisar
Proj...
waf_...
root...
Sem...
Tempe...
21:21


localhost:9999/container/f129d22241ef
Dozzle
waf_modsec
owasp/modsecurity-crs:nginx-alpine
403
MEM 56.34 MB / 3.8G
LOAD 0.00% / 4 CPU
Hosts
DESKTOP-RD2
labs
dozzle
dvwa
kali_lab35
waf_modsec
Hosts e Containers
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="Wed, 17 Sep 2025 23:57:55 GMT"
transaction.response.headers.Server="nginx" transaction.response.http_code="403" transaction.server_id="fb918e8ff0f9a00845c34929d11564775f88a366"
transaction.time_stamp="Wed Sep 17 23:57:55 2025" transaction.unique_id="17581534758.614813"
7/09/2025 21:19:07
2025/09/18 00:19:07 [error] 590#590: *88 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `5') [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 5)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.17.1"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/sqli/"] [unique_id "175815474714.878353"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1", host: "dvwa"
17/09/2025 21:19:07
192.168.35.11 - - [18/Sep/2025:00:19:07 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
17/09/2025 21:19:07
transaction.client_ip="192.168.35.11" transaction.client_port=42944 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", "OWASP_CRS/ATTACK-SQLI", "capec/1000/152/248/66"]
ver="OWASP_CRS/4.17.1"
message="SQL Injection Attack Detected via libinjection"
,
details=
accuracy="0" data="" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf" lineNumber="222"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `5')" maturity="0" reference=""
rev="" ruleId="949110" severity="0" tags=["modsecurity", "anomaly-evaluation", "OWASP_CRS"] ver="OWASP_CRS/4.17.1"
message="Inbound Anomaly Score Exceeded (Total Score: 5)"
]
transaction.producer.components=["OWASP_CRS/4.17.1""] 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> <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="Thu, 18 Sep 2025 00:19:07 GMT"
transaction.response.headers.Server="nginx" transaction.response.http_code="403" transaction.server_id="fb918e8ff0f9a00845c34929d11564775f88a366"
transaction.time_stamp="Thu Sep 18 00:19:07 2025" transaction.unique_id="175815474714.878353"
Pesquisar
Proj...
waf_...
root...
ataq...
Tempe...
21:22

Logs detalhados:

```
root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs# docker
logs waf_modsec --tail 50 > logs_waf_evidencias.txt
2025/09/17 01:22:07 [warn] 1#1: "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/nginx/conf/server.
crt"
nginx: [warn] "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/nginx/conf/server.crt"
2025/09/17 01:22:07 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remote: 0/836/0)
2025/09/17 01:22:07 [notice] 1#1: libmodsecurity3 version 3.0.14
2025/09/17 01:22:14 [error] 590#590: *1 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "O
perator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `5' ) [file "/etc/modsecurity.d/
owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceed
ed (Total Score: 5)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.17.1"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [ta
g "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/sqli/"] [unique_id "175807213478.692518"]
[ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit H
TTP/1.1", host: "dvwa"
2025/09/17 01:22:46 [error] 591#591: *3 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "O
perator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `5' ) [file "/etc/modsecurity.d/
owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceed
ed (Total Score: 5)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.17.1"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [ta
g "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/sqli/"] [unique_id "175807216649.455418"]
[ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit H
TTP/1.1", host: "dvwa"
2025/09/17 01:23:09 [error] 592#592: *4 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "O
perator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `5' ) [file "/etc/modsecurity.d/
owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceed
ed (Total Score: 5)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.17.1"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [ta
g "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/sqli/"] [unique_id "175807218993.776954"]
[ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit H
TTP/1.1", host: "dvwa"
2025/09/17 01:25:06 [error] 593#593: *9 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "O
perator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `20' ) [file "/etc/modsecurity.d
/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Excee
ded (Total Score: 20)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.17.1"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [
tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/xss_r/"] [unique_id "175807230647.575115
"] [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"
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs#
```

Dozzle mostrando logs de detecção XSS e SQLi



localhost:9999/container/3e24d36a37b1

Dozzle

waf_modsec — owasp/modsecurity-crs:nginx-alpine

MEM 48.3 MB / 3.8G — LOAD 0.00% / 4 CPU

Hosts — DESKTOP

labs
- dozzle
- dvwa
- kali_lab35
- waf_modsec

Hosts e Containers

16/09/2025 22:13:43

```
192.168.35.11 - - [17/Sep/2025:01:13:43 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 302 0 "-"
"curl/8.15.0" "-"
```

6/09/2025 22:13:43


```
transaction.client_ip="192.168.35.11"  transaction.client_port=52880  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",
"OWASP_CRS/ATTACK-SQLI", "capec/1000/152/248/66"]
ver="OWASP_CRS/4.17.1"
message="SQL Injection Attack Detected via libinjection"
,
details=
accuracy="0"  data=""  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"  lineNumber="222"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `5' )"
maturity="0"  reference=""  rev=""  ruleId="949110"  severity="0"  tags=["modsecurity", "anomaly-evaluation", "OWASP_CRS"]
ver="OWASP_CRS/4.17.1"
message="Inbound Anomaly Score Exceeded (Total Score: 5)"
]
transaction.producer.components=["OWASP_CRS/4.17.1""]  transaction.producer.connector="ModSecurity-nginx v1.0.4"
transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"  transaction.producer.secrules_engine="DetectionOnly"
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=""  transaction.response.headers.Access-Control-Allow-Headers="*"
transaction.response.headers.Cache-Control="no-store, no-cache, must-revalidate"
transaction.response.headers.Connection="keep-alive"  transaction.response.headers.Content-Type="text/html; charset=UTF-8"
transaction.response.headers.Date="Wed, 17 Sep 2025 01:13:43 GMT"
transaction.response.headers.Expires="Thu, 19 Nov 1981 08:52:00 GMT"  transaction.response.headers.Location="../../login.php"
transaction.response.headers.Pragma="no-cache"  transaction.response.headers.Server="nginx"  transaction.response.http_code=302
transaction.server_id="3baee462b5ae063c7b692d9c9fe6332151894bfc"  transaction.time_stamp="Wed Sep 17 01:13:43 2025"
transaction.unique_id="175807162339.254368"
```


Pesquisar — 20°C — 22:12

localhost:9999/container/3e24d36a37b1

Dozzle

waf_modsec — owasp/modsecurity-crs:nginx-alpine

MEM 52.49 MB / 3.8G — LOAD 0.00% / 4 CPU

Hosts — DESKTOP

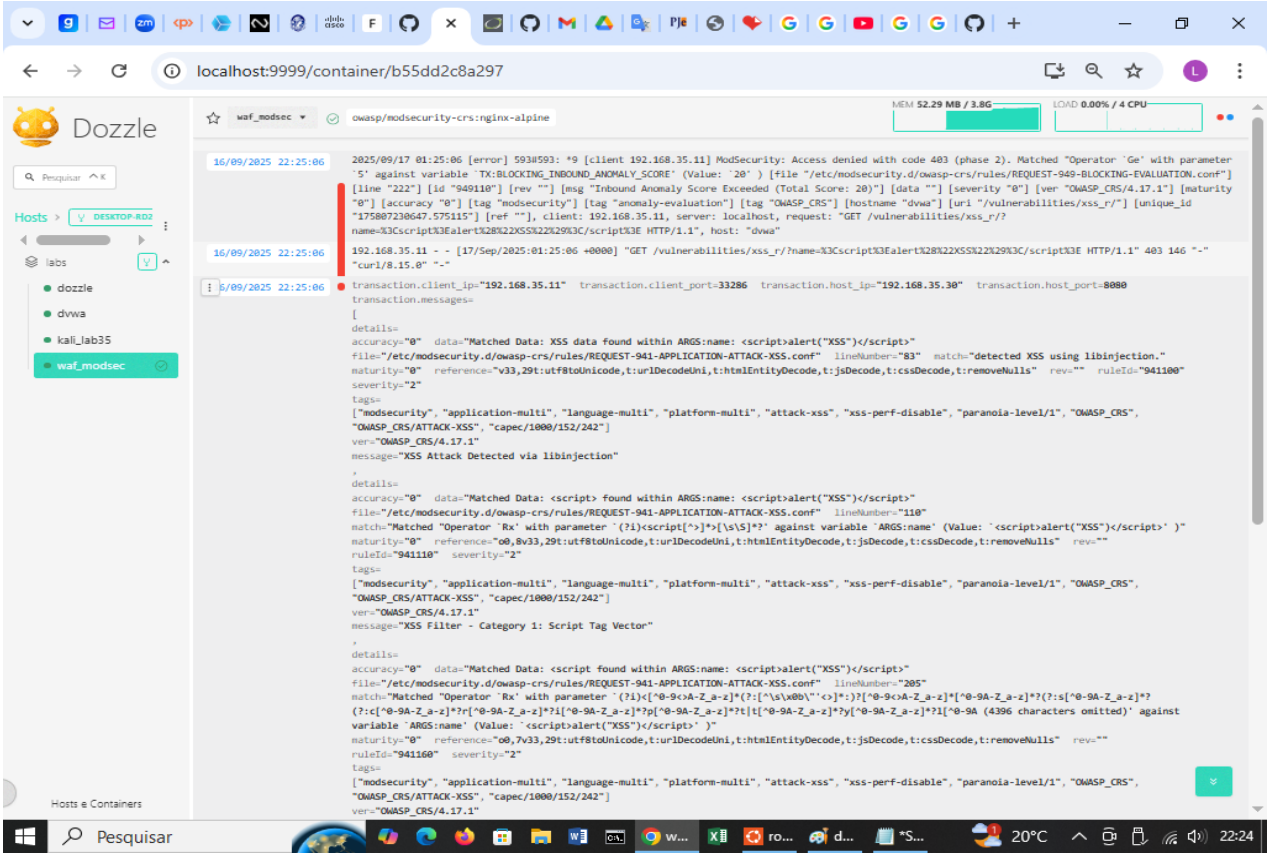
labs
- dozzle
- dvwa
- kali_lab35
- waf_modsec

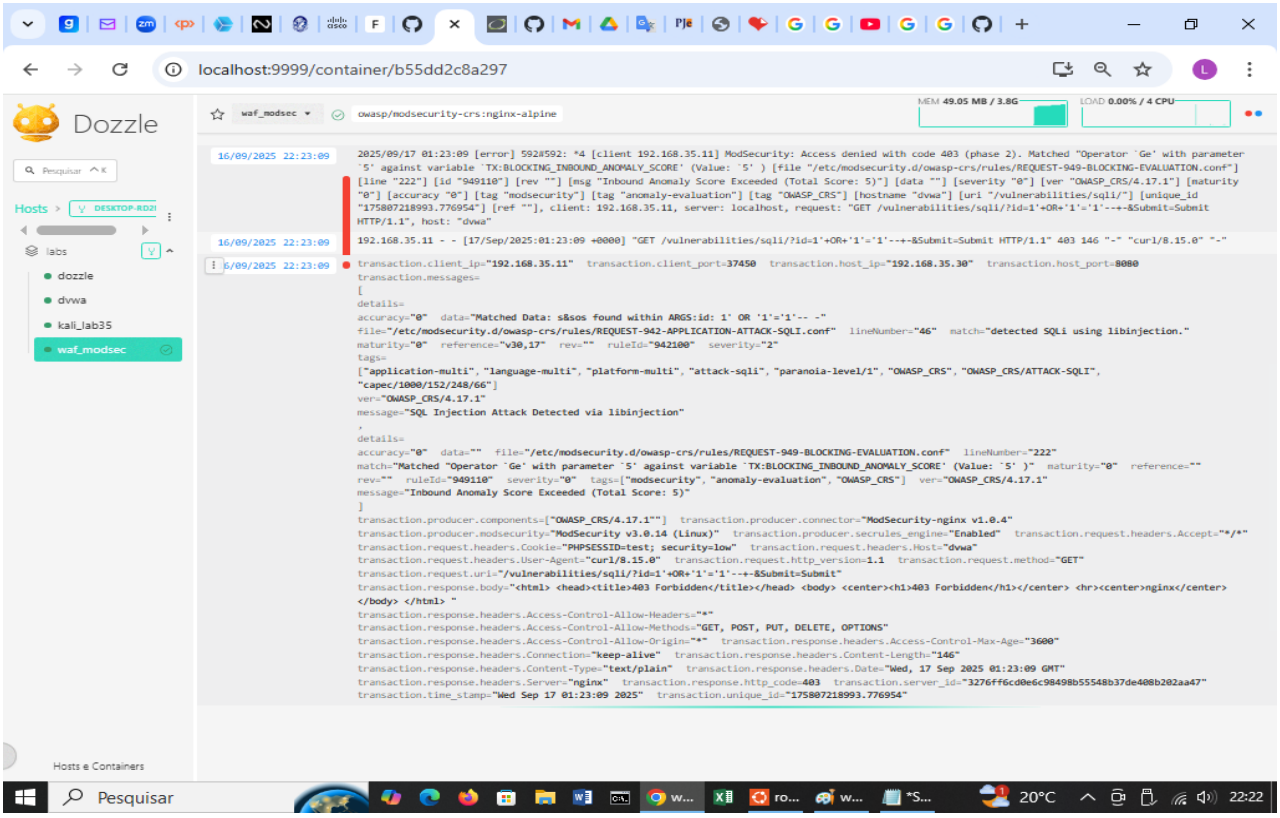
Hosts e Containers

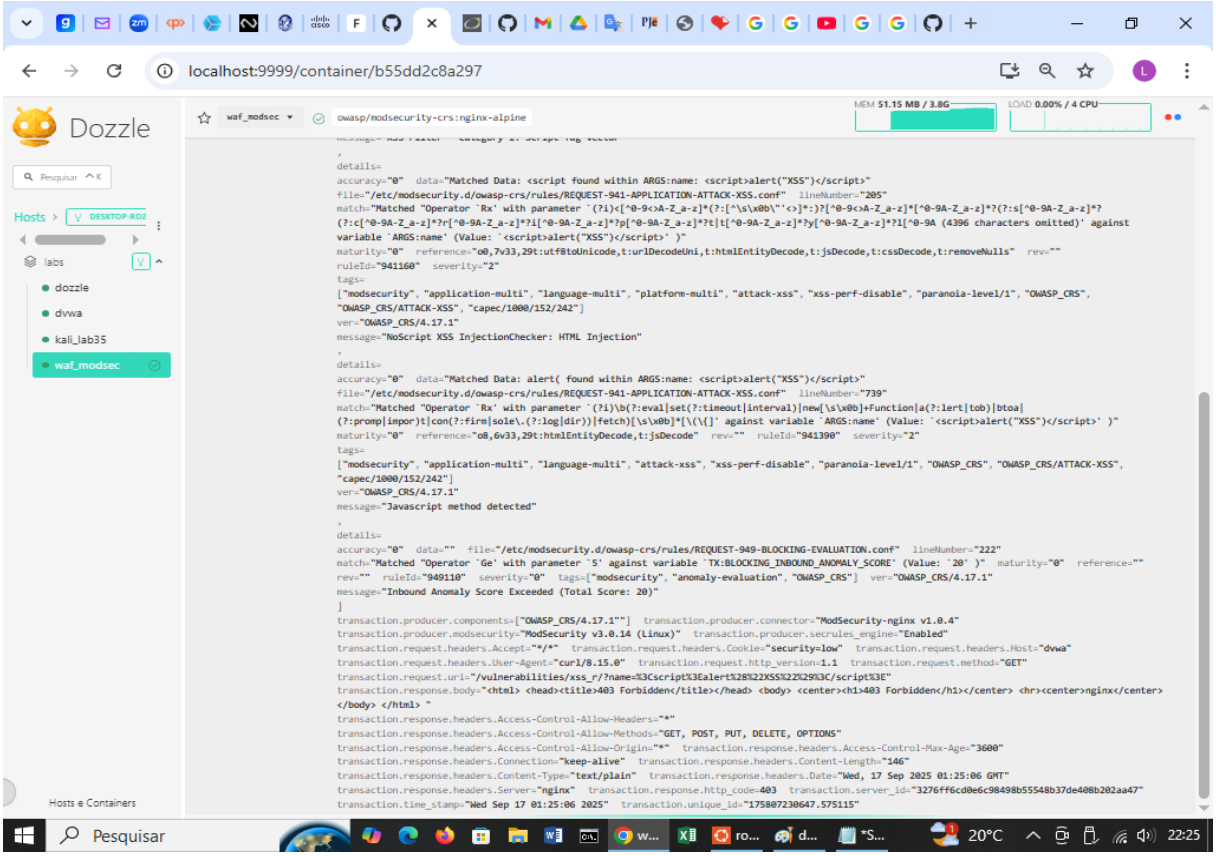

```
rev=""  ruleId="941160"  severity="2"
tags=
["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-xss", "xss-perf-disable", "paranoia-level/1",
"OWASP_CRS", "OWASP_CRS/ATTACK-XSS", "capec/1000/152/242"]
ver="OWASP_CRS/4.17.1"
message="NoScript XSS InjectionChecker: HTML Injection"
,
details=
accuracy="0"  data="Matched Data: alert( found within ARGS:name: <script>alert("XSS")</script>"
file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"  lineNumber="739"
match="Matched "Operator `Rx' with parameter `(?i)\b(?:eval|set(?:timeout|interval)|new[\s\x0b]+Function|a(?:lert|tob)|btoa|
(?:promp|impor)t|con(?:firm|sole\.(?:log|dir))|fetch)[\s\x0b]*[\(\{]' against variable `ARGS:name' (Value:
`<script>alert("XSS")</script>' )"
maturity="0"  reference="o8,6v33,29t:htmlEntityDecode,t:jsDecode"  rev=""  ruleId="941390"  severity="2"
tags=
["modsecurity", "application-multi", "language-multi", "attack-xss", "xss-perf-disable", "paranoia-level/1", "OWASP_CRS",
"OWASP_CRS/ATTACK-XSS", "capec/1000/152/242"]
ver="OWASP_CRS/4.17.1"
message="Javascript method detected"
,
details=
accuracy="0"  data=""  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"  lineNumber="222"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `20' )"
maturity="0"  reference=""  rev=""  ruleId="949110"  severity="0"  tags=["modsecurity", "anomaly-evaluation", "OWASP_CRS"]
ver="OWASP_CRS/4.17.1"
message="Inbound Anomaly Score Exceeded (Total Score: 20)"
]
transaction.producer.components=["OWASP_CRS/4.17.1""]  transaction.producer.connector="ModSecurity-nginx v1.0.4"
transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"  transaction.producer.secrules_engine="DetectionOnly"
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=""  transaction.response.headers.Access-Control-Allow-Headers="*"
transaction.response.headers.Cache-Control="no-store, no-cache, must-revalidate"
transaction.response.headers.Connection="keep-alive"  transaction.response.headers.Content-Type="text/html; charset=UTF-8"
transaction.response.headers.Date="Wed, 17 Sep 2025 01:17:28 GMT"
transaction.response.headers.Expires="Thu, 19 Nov 1981 08:52:00 GMT"  transaction.response.headers.Location="../../login.php"
transaction.response.headers.Pragma="no-cache"  transaction.response.headers.Server="nginx"
transaction.response.headers.Set-Cookie="PHPSESSID=bnf14b111msrtn3dl7cniajln7; path=/"  transaction.response.http_code=302
transaction.server_id="3baee462b5ae063c7b692d9c9fe6332151894bfc"  transaction.time_stamp="Wed Sep 17 01:17:28 2025"
transaction.unique_id="175807184894.988158"
```


Pesquisar — Bolsas... — 22:18

Dozzle mostrando logs de bloqueio de XSS e SQLi







6. Resposta a Incidente (NIST IR)

- Detecção, Contenção, Erradicação, Recuperação, Lições Aprendidas

FASE 2: DETECÇÃO E ANÁLISE

2.1 Indicadores de Comprometimento (IoCs)

Cenário Específico: Segue os detalhes dos IoCs do laboratório

- Indicador 1 – Ataque ao banco de dados através do SQL Injection (SQLI)
- Indicador 2 – Site comprometido devido ao Cross-Site Scripting (XSS)
- Indicador 3 – Modificações do banco de dados, exclusão, inclusão ou alteração
- Indicador 4 – Alteração do site para conseguir dados de quem o acessa.

2.2 Fontes de Detecção

- **Logs de Sistema:** Windows Event Logs, Syslog
- **Logs de Rede:** Firewall, IPS/IDS, DNS
- **Logs de Aplicação:** Web servers, Databases
- **Usuários:** Relatos de funcionários/clientes
- **Terceiros:** Threat intelligence, fornecedores

2.3 Processo de Análise Inicial

Passo 1: Validação do Incidente (< 15 min)

```
# Comandos para verificação inicial
Verificar logs de eventos
Verificar a integridade do banco de dados
Verificar se o site está comprometido
```

Passo 2: Classificação (< 30 min)

- **Severidade:** Crítico
- **Impacto:** Confidencialidade/Integridade
- **Categoria:** XSS e SQLi
- **Urgência:** Imediata

Passo 3: Coleta de Evidências Iniciais

- Screenshots de alertas/sistemas afetados
- Logs relevantes preservados
- Tráfego de rede capturado
- Depoimentos iniciais coletados

2.4 Escalação e Ativação

Critérios de Escalação

- Impacto em sistemas críticos
- Exposição de dados sensíveis
- Paralisação de operações
- Repercussão midiática potencial
- Valor financeiro envolvido > R$ 10 milhões

Processo de Ativação do CSIRT

1. **Detecção inicial** → Analista de plantão
2. **Validação** → Líder técnico (< 15 min)
3. **Escalação** → Coordenador CSIRT (< 30 min)
4. **Ativação completa** → Toda a equipe (< 1 hora)

⚡ FASE 3: CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

3.1 Contenção Imediata (< 1 hora)

Objetivos

- Parar a propagação do incidente
- Preservar evidências
- Manter sistemas críticos funcionando
- Minimizar impacto nos negócios

Ações de Contenção - [Cenário Específico]

```
# Comandos de contenção específicos
Isolar a máquina que contém o arquivo malicioso
Se o site estiver comprometido tira-lo do ar
Tirar o acesso ao banco de dados para evitar maior comprometimento
```

Checklist de Contenção:

- Restaurar os backups validados
- Subir os sistemas com imagens limpas e sem vírus ou qualquer tipo de malware que prejudique o sistema e volte a ter problemas
- Verificar por onde o malware entrou e como ele conseguiu invadir o site e o banco de dados
- Porque não conseguimos evitar o XSS e o SQLi
- Comunicação às partes interessadas
- Documentação das ações realizadas

3.2 Coleta de Evidências Forenses

Ordem de Volatilidade (RFC 3227)

1. **Memória RAM** → Mais volátil
2. **Estado do sistema** → Processos, conexões
3. **Disco rígido** → Arquivos, logs
4. **Logs remotos** → SIEM, syslog
5. **Configurações** → Menos volátil

Procedimentos de Coleta

```
# Exemplo de comandos forenses
Fazer a coleta de dados dos logs
Verificar de onde partiu o ataque
Algum dado foi exfiltrado?
Quais dados foram modificados, excluídos ou adicionados?
Verificar os dados do site o que foi modificado para que o script conseguisse
o acesso
```

3.3 Erradicação (< 4 horas)

Identificação da Causa Raiz

- Vetor de ataque identificado
- Vulnerabilidade explorada mapeada
- Timeline de comprometimento estabelecida
- Extensão do comprometimento avaliada

Ações de Erradicação

- Ação específica 1 – Proteger a entrada contra SQL Injection (SQLI)
- Ação específica 2 – Proteger o site contra Cross-Site Scripting (XSS)
- Ação específica 3 – Instalar um IPS para bloquear os ataques
- Ação específica 4 – Instalar um WAF.

3.4 Recuperação (< 8 horas)

Plano de Recuperação

1. **Sistemas Críticos** (Prioridade 1)
    - Site do DVWA vulnerável
    - Banco de Dados MySQL

2. **Sistemas Importantes** (Prioridade 2)
    - WAF
    - Firewall

Validação da Recuperação

- Funcionalidade restaurada
- Performance normal
- Conectividade verificada
- Dados íntegros
- Usuários conseguem acessar

📝 FASE 4: ATIVIDADES PÓS-INCIDENTE

4.1 Relatório de Incidente

Resumo Executivo

- **Tipo de Incidente:** SQLi e XSS
- **Data/Hora:** 25/09 as 04:00 25/09 12:00
- **Duração:** 8 horas
- **Sistemas Afetados:** Site do DVWA, Banco de Dados
- **Impacto:** Impacto Total no site, modificação do banco de dados, informações não confiáveis, site invadido conseguindo informações do cliente
- **Custo Estimado:** R$ 100 milhões

Timeline Detalhada

Timestamp	Evento	Responsável	Evidência
04:00:00	XSS	Luiz Eduardo de Andrade	https://doi.org/10.6028/NIST.SP.800-63-4

Timestamp	Evento	Responsável	Evidência
04:00:00	SQLi	Luiz Eduardo de Andrade	https://doi.org/10.6028/NIST.IR.7682

4.2 Lições Aprendidas

O que funcionou bem?

- Backups testados e em diversos lugares diferentes
- Plano de Recuperação de Desastres
- Plano de Continuidade de Negócios

O que precisa melhorar?

- Regras de Firewall mais restritivas
- Proteção na entrada dos dados para evitar SQLi e XSS
- Treinamentos constantes com a equipe sobre a Segurança dos Dados e não clicar em links suspeitos sempre consultar a equipe de TI quando tiver dúvidas sobre algum link recebido por e-mail ou em uma página da internet.

Recomendações

1. **Prevenção:**
    - Treinamentos regulares para funcionários
    - Instalar IPS para o bloqueio de malwares conhecidos
2. **Detecção:**
    - Investir em SIEM e SOAR para verificar eventos suspeitos.
    - Ter um SOC 24/7 para tomar as ações o mais rápido possível

3. **Resposta:**
    - Resposta mais rápida quando o sistema for comprometido
    - Equipe melhor preparada para lidar com incidentes graves

4.3 Plano de Ação

Ação	Responsável	Prazo	Status
Fazer o saneamento da entrada de dados	Carla Maria	29/09/2025	Concluído
Instalar IPS para bloquear os ataques	Luiz Eduardo de Andrade	29/09/2025	Concluído

7. Recomendações (80/20)

- Top 5 ações com esforço vs. Impacto

Ação	Impacto	Facilidade	Prioridade
Bloquear SQLi e XSS nas entradas do usuário	Alto	Alta	Alta
Instalar Firewall	Alto	Média	Alta
Instalar WAF	Alto	Baixo	Alta
Bloquear tentativas de ip externos ao servidor web quando for identificado um ataque	Alto	Média	Alta
Configurar regras de Firewall	Alto	Baixa	Média

8. Conclusão

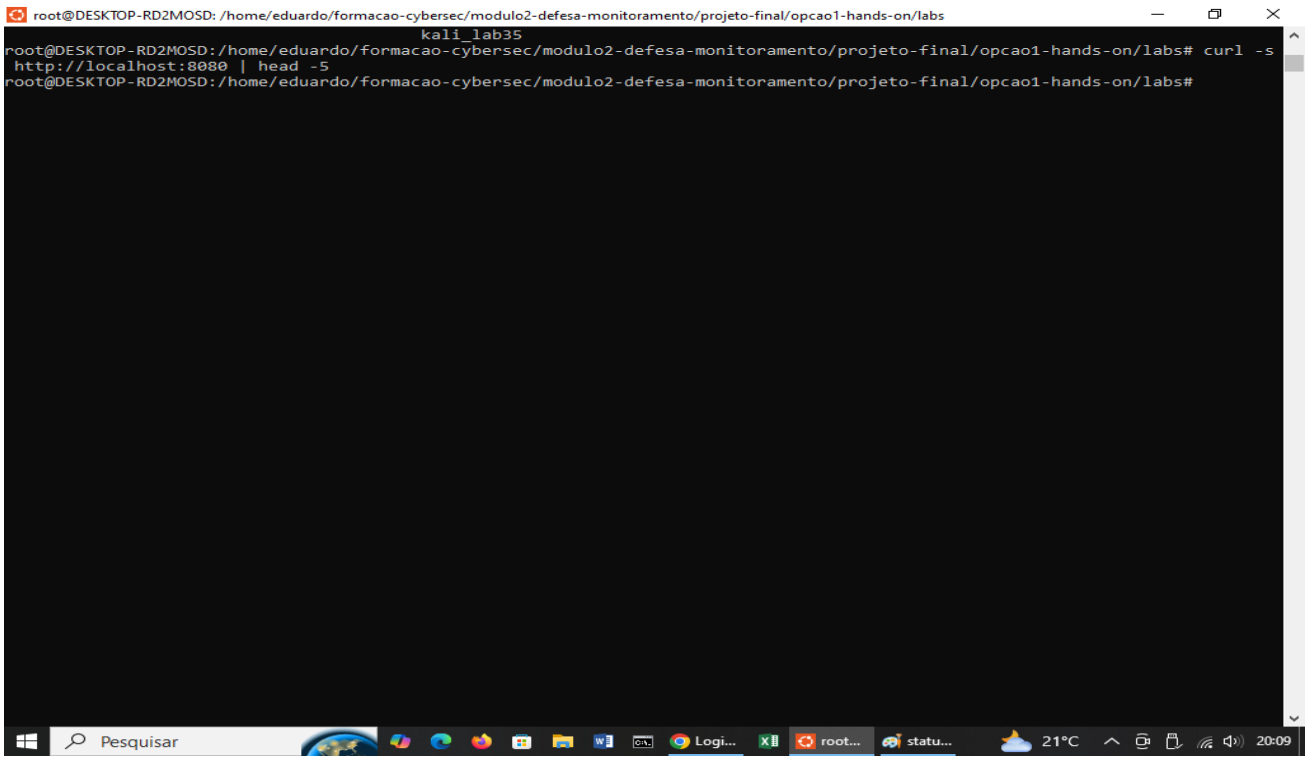
- Maturidade demonstrada e próximos passos

Realizados os scripts de XSS E SQLi e vemos que o WAF detectou e bloqueou os ataques isso é necessário para que os aplicativos WEB funcionem corretamente, precisamos evitar que estes ataques infectem o nosso site e prejudiquem o nosso sistema, o nosso banco de dados e a nossa reputação.

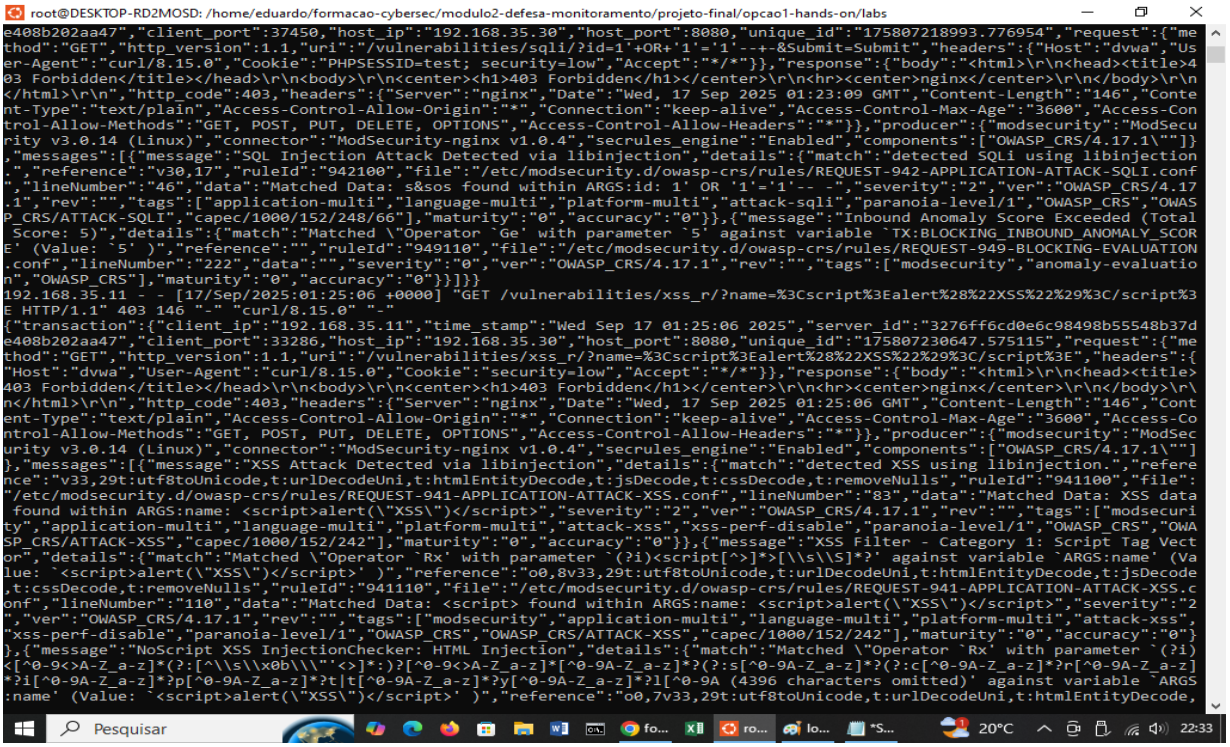
Anexos

- Configs, logs, scripts

Teste de DVWA no terminal através do comando curl -s http://localhost:8080 | head 5

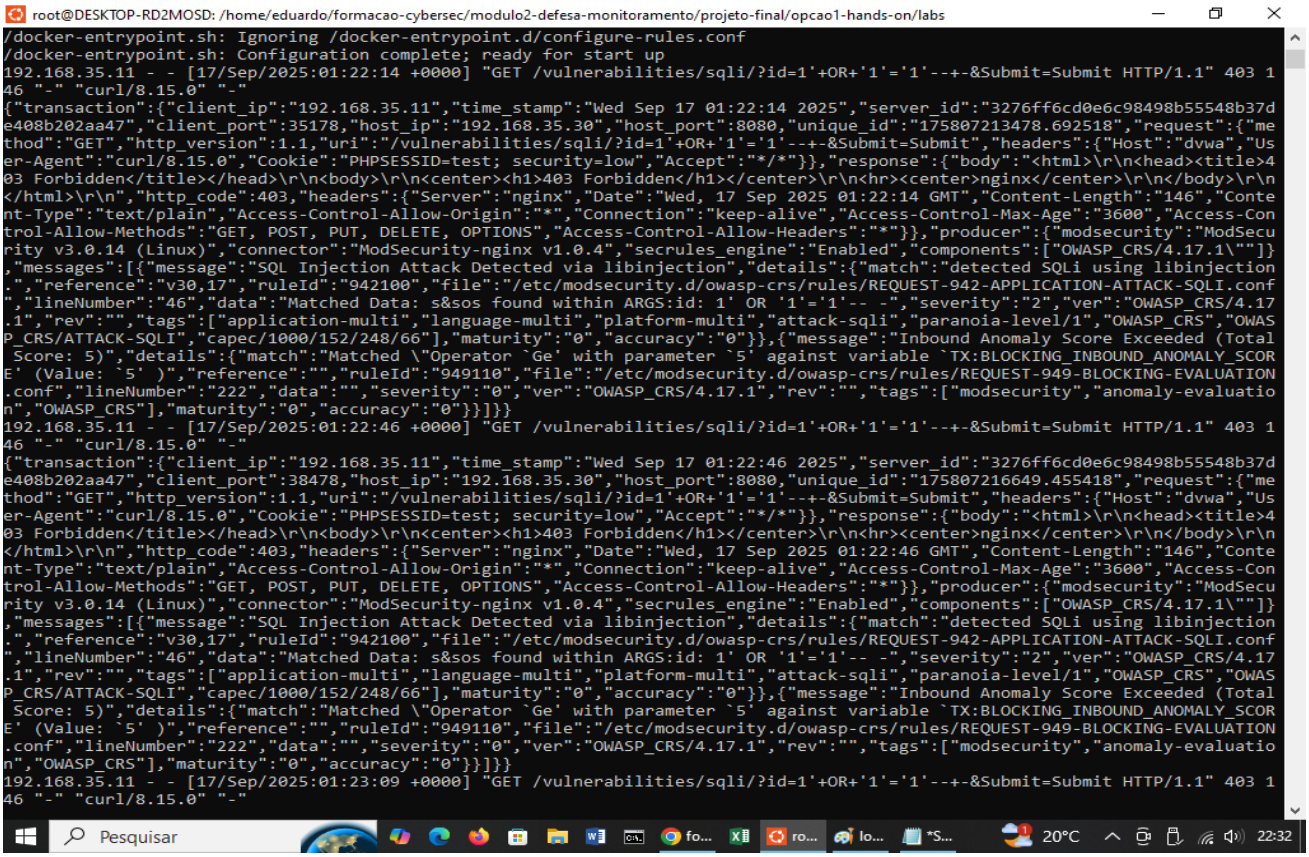


Segue os prints dos Logs do WAF através do comando cat logs_waf_evidencias.txt


root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs

```
e408b202aa47","client_port":37450,"host_ip":"192.168.35.30","host_port":8080,"unique_id":"175807218993.776954","request":{"me
thod":"GET","http_version":1.1,"uri":"/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit","headers":{"Host":"dvwa","Us
er-Agent":"curl/8.15.0","Cookie":"PHPSESSID=test; security=low","Accept":"*/*"}},"response":{"body":"<html>\r\n<head><title>4
03 Forbidden</title></head>\r\n<body>\r\n<center><h1>403 Forbidden</h1></center>\r\n<hr><center>nginx</center>\r\n</body>\r\n
</html>\r\n","http_code":403,"headers":{"Server":"nginx","Date":"Wed, 17 Sep 2025 01:23:09 GMT","Content-Length":"146","Conte
nt-Type":"text/plain","Access-Control-Allow-Origin":"*","Connection":"keep-alive","Access-Control-Max-Age":"3600","Access-Con
trol-Allow-Methods":"GET, POST, PUT, DELETE, OPTIONS","Access-Control-Allow-Headers":"*"}},"producer":{"modsecurity":"ModSecu
rity v3.0.14 (Linux)","connector":"ModSecurity-nginx v1.0.4","secrules_engine":"Enabled","components":["OWASP_CRS/4.17.1\""]}
,"messages":[{"message":"SQL Injection Attack Detected via libinjection","details":{"match":"detected SQLi using libinjection
.","reference":"v30,17","ruleId":"942100","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf
","lineNumber":"46","data":"Matched Data: s&sos found within ARGS:id: 1' OR '1'='1'-- -","severity":"2","ver":"OWASP_CRS/4.17
.1","rev":"","tags":["application-multi","language-multi","platform-multi","attack-sqli","paranoia-level/1","OWASP_CRS","OWAS
P_CRS/ATTACK-SQLI","capec/1000/152/248/66"],"maturity":"0","accuracy":"0"}},{"message":"Inbound Anomaly Score Exceeded (Total
 Score: 5)","details":{"match":"Matched \"Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCOR
E' (Value: `5' )","reference":"","ruleId":"949110","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION
.conf","lineNumber":"222","data":"","severity":"0","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modsecurity","anomaly-evaluatio
n","OWASP_CRS"],"maturity":"0","accuracy":"0"}}]}}
192.168.35.11 - - [17/Sep/2025:01:25:06 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3
E HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
{"transaction":{"client_ip":"192.168.35.11","time_stamp":"Wed Sep 17 01:25:06 2025","server_id":"3276ff6cd0e6c98498b55548b37d
e408b202aa47","client_port":33286,"host_ip":"192.168.35.30","host_port":8080,"unique_id":"175807230647.575115","request":{"me
thod":"GET","http_version":1.1,"uri":"/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E","headers":{
"Host":"dvwa","User-Agent":"curl/8.15.0","Cookie":"security=low","Accept":"*/*"}},"response":{"body":"<html>\r\n<head><title>
403 Forbidden</title></head>\r\n<body>\r\n<center><h1>403 Forbidden</h1></center>\r\n<hr><center>nginx</center>\r\n</body>\r\
n</html>\r\n","http_code":403,"headers":{"Server":"nginx","Date":"Wed, 17 Sep 2025 01:25:06 GMT","Content-Length":"146","Cont
ent-Type":"text/plain","Access-Control-Allow-Origin":"*","Connection":"keep-alive","Access-Control-Max-Age":"3600","Access-Co
ntrol-Allow-Methods":"GET, POST, PUT, DELETE, OPTIONS","Access-Control-Allow-Headers":"*"}},"producer":{"modsecurity":"ModSec
urity v3.0.14 (Linux)","connector":"ModSecurity-nginx v1.0.4","secrules_engine":"Enabled","components":["OWASP_CRS/4.17.1\""]
},"messages":[{"message":"XSS Attack Detected via libinjection","details":{"match":"detected XSS using libinjection.","refere
nce":"v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls","ruleId":"941100","file":
"/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf","lineNumber":"83","data":"Matched Data: XSS data
 found within ARGS:name: <script>alert(\"XSS\")</script>","severity":"2","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modsecuri
ty","application-multi","language-multi","platform-multi","attack-xss","xss-perf-disable","paranoia-level/1","OWASP_CRS","OWA
SP_CRS/ATTACK-XSS","capec/1000/152/242"],"maturity":"0","accuracy":"0"}},{"message":"XSS Filter - Category 1: Script Tag Vect
or","details":{"match":"Matched \"Operator `Rx' with parameter `(?i)<script[^>]*>[\\s\\S]*?' against variable `ARGS:name' (Va
lue: `<script>alert(\"XSS\")</script>' )","reference":"o0,8v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode
,t:cssDecode,t:removeNulls","ruleId":"941110","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.c
onf","lineNumber":"110","data":"Matched Data: <script> found within ARGS:name: <script>alert(\"XSS\")</script>","severity":"2
","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modsecurity","application-multi","language-multi","platform-multi","attack-xss",
"xss-perf-disable","paranoia-level/1","OWASP_CRS","OWASP_CRS/ATTACK-XSS","capec/1000/152/242"],"maturity":"0","accuracy":"0"}
},{"message":"NoScript XSS InjectionChecker: HTML Injection","details":{"match":"Matched \"Operator `Rx' with parameter `(?i)
<[^0-9<>A-Z_a-z]*(?:[^\\s\\x0b\\\"'<>]*:)?[^0-9<>A-Z_a-z]*[^0-9A-Z_a-z]*?(?:s[^0-9A-Z_a-z]*?(?:c[^0-9A-Z_a-z]*?r[^0-9A-Z_a-z]
*?i[^0-9A-Z_a-z]*?p[^0-9A-Z_a-z]*?t|t[^0-9A-Z_a-z]*?y[^0-9A-Z_a-z]*?l[^0-9A (4396 characters omitted)' against variable `ARGS
:name' (Value: `<script>alert(\"XSS\")</script>' )","reference":"o0,7v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,
```

Pesquisar 20°C 22:33


root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs

```
/docker-entrypoint.sh: Ignoring /docker-entrypoint.d/configure-rules.conf
/docker-entrypoint.sh: Configuration complete; ready for start up
192.168.35.11 - - [17/Sep/2025:01:22:14 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 403 1
46 "-" "curl/8.15.0" "-"
{"transaction":{"client_ip":"192.168.35.11","time_stamp":"Wed Sep 17 01:22:14 2025","server_id":"3276ff6cd0e6c98498b55548b37d
e408b202aa47","client_port":35178,"host_ip":"192.168.35.30","host_port":8080,"unique_id":"175807213478.692518","request":{"me
thod":"GET","http_version":1.1,"uri":"/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit","headers":{"Host":"dvwa","Us
er-Agent":"curl/8.15.0","Cookie":"PHPSESSID=test; security=low","Accept":"*/*"}},"response":{"body":"<html>\r\n<head><title>4
03 Forbidden</title></head>\r\n<body>\r\n<center><h1>403 Forbidden</h1></center>\r\n<hr><center>nginx</center>\r\n</body>\r\n
</html>\r\n","http_code":403,"headers":{"Server":"nginx","Date":"Wed, 17 Sep 2025 01:22:14 GMT","Content-Length":"146","Conte
nt-Type":"text/plain","Access-Control-Allow-Origin":"*","Connection":"keep-alive","Access-Control-Max-Age":"3600","Access-Con
trol-Allow-Methods":"GET, POST, PUT, DELETE, OPTIONS","Access-Control-Allow-Headers":"*"}},"producer":{"modsecurity":"ModSecu
rity v3.0.14 (Linux)","connector":"ModSecurity-nginx v1.0.4","secrules_engine":"Enabled","components":["OWASP_CRS/4.17.1\""]}
,"messages":[{"message":"SQL Injection Attack Detected via libinjection","details":{"match":"detected SQLi using libinjection
.","reference":"v30,17","ruleId":"942100","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf
","lineNumber":"46","data":"Matched Data: s&sos found within ARGS:id: 1' OR '1'='1'-- -","severity":"2","ver":"OWASP_CRS/4.17
.1","rev":"","tags":["application-multi","language-multi","platform-multi","attack-sqli","paranoia-level/1","OWASP_CRS","OWAS
P_CRS/ATTACK-SQLI","capec/1000/152/248/66"],"maturity":"0","accuracy":"0"}},{"message":"Inbound Anomaly Score Exceeded (Total
 Score: 5)","details":{"match":"Matched \"Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCOR
E' (Value: `5' )","reference":"","ruleId":"949110","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION
.conf","lineNumber":"222","data":"","severity":"0","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modsecurity","anomaly-evaluatio
n","OWASP_CRS"],"maturity":"0","accuracy":"0"}}]}}
192.168.35.11 - - [17/Sep/2025:01:22:46 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 403 1
46 "-" "curl/8.15.0" "-"
{"transaction":{"client_ip":"192.168.35.11","time_stamp":"Wed Sep 17 01:22:46 2025","server_id":"3276ff6cd0e6c98498b55548b37d
e408b202aa47","client_port":38478,"host_ip":"192.168.35.30","host_port":8080,"unique_id":"175807216649.455418","request":{"me
thod":"GET","http_version":1.1,"uri":"/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit","headers":{"Host":"dvwa","Us
er-Agent":"curl/8.15.0","Cookie":"PHPSESSID=test; security=low","Accept":"*/*"}},"response":{"body":"<html>\r\n<head><title>4
03 Forbidden</title></head>\r\n<body>\r\n<center><h1>403 Forbidden</h1></center>\r\n<hr><center>nginx</center>\r\n</body>\r\n
</html>\r\n","http_code":403,"headers":{"Server":"nginx","Date":"Wed, 17 Sep 2025 01:22:46 GMT","Content-Length":"146","Conte
nt-Type":"text/plain","Access-Control-Allow-Origin":"*","Connection":"keep-alive","Access-Control-Max-Age":"3600","Access-Con
trol-Allow-Methods":"GET, POST, PUT, DELETE, OPTIONS","Access-Control-Allow-Headers":"*"}},"producer":{"modsecurity":"ModSecu
rity v3.0.14 (Linux)","connector":"ModSecurity-nginx v1.0.4","secrules_engine":"Enabled","components":["OWASP_CRS/4.17.1\""]}
,"messages":[{"message":"SQL Injection Attack Detected via libinjection","details":{"match":"detected SQLi using libinjection
.","reference":"v30,17","ruleId":"942100","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf
","lineNumber":"46","data":"Matched Data: s&sos found within ARGS:id: 1' OR '1'='1'-- -","severity":"2","ver":"OWASP_CRS/4.17
.1","rev":"","tags":["application-multi","language-multi","platform-multi","attack-sqli","paranoia-level/1","OWASP_CRS","OWAS
P_CRS/ATTACK-SQLI","capec/1000/152/248/66"],"maturity":"0","accuracy":"0"}},{"message":"Inbound Anomaly Score Exceeded (Total
 Score: 5)","details":{"match":"Matched \"Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCOR
E' (Value: `5' )","reference":"","ruleId":"949110","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION
.conf","lineNumber":"222","data":"","severity":"0","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modsecurity","anomaly-evaluatio
n","OWASP_CRS"],"maturity":"0","accuracy":"0"}}]}}
192.168.35.11 - - [17/Sep/2025:01:23:09 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 403 1
46 "-" "curl/8.15.0" "-"
```

Pesquisar 20°C 22:32

root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs

```
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs# cat log
s_waf_evidencias.txt
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/proxy_backend.conf.template to /etc/nginx/incl
udes/proxy_backend.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/cors.conf.template to /etc/nginx/includes/cors
.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/nginx.conf.template to /etc/nginx/nginx.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/modsecurity.conf.template to /etc/nginx/conf.d/m
odsecurity.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/logging.conf.template to /etc/nginx/conf.d/loggi
ng.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/default.conf.template to /etc/nginx/conf.d/defau
lt.conf
/docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-processes.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/90-copy-modsecurity-config.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/91-update-resolver.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/92-update-real_ip.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/93-update-proxy-ssl-config.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/94-activate-plugins.sh
# # #
Running CRS plugin activation
- - -

- - -
Finished CRS plugin activation
# # #

/docker-entrypoint.sh: Launching /docker-entrypoint.d/95-configure-rules.sh
# # #
Running CRS rule configuration
- - -
Configuring 900000 for BLOCKING_PARANOIA with blocking_paranoia_level=1
Configuring 900001 for DETECTION_PARANOIA with detection_paranoia_level=1
Configuring 900110 for ANOMALY_INBOUND with inbound_anomaly_score_threshold=5
Configuring 900110 for ANOMALY_OUTBOUND with outbound_anomaly_score_threshold=4
- - -
Finished CRS rule configuration
# # #

/docker-entrypoint.sh: Ignoring /docker-entrypoint.d/configure-rules.conf
/docker-entrypoint.sh: Configuration complete; ready for start up
192.168.35.11 - - [17/Sep/2025:01:22:14 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 403 1
46 "-" "curl/8.15.0" "-"
{"transaction":{"client_ip":"192.168.35.11","time_stamp":"Wed Sep 17 01:22:14 2025","server_id":"3276ff6cd0e6c98498b55548b37d
```

Pesquisar 20°C 22:31

root@DESKTOP-RD2MOSD: /home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs

```
E HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
{"transaction":{"client_ip":"192.168.35.11","time_stamp":"Wed Sep 17 01:25:06 2025","server_id":"3276ff6cd0e6c98498b55548b37d
e408b202aa47","client_port":33286,"host_ip":"192.168.35.30","host_port":8080,"unique_id":"175807230647.575115","request":{"me
thod":"GET","http_version":1.1,"uri":"/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E","headers":{
"Host":"dvwa","User-Agent":"curl/8.15.0","Cookie":"security=low","Accept":"*/*"}},"response":{"body":"<html>\r\n<head><title>
403 Forbidden</title></head>\r\n<body>\r\n<center><h1>403 Forbidden</h1></center>\r\n<hr><center>nginx</center>\r\n</body>\r\
n</html>\r\n","http_code":403,"headers":{"Server":"nginx","Date":"Wed, 17 Sep 2025 01:25:06 GMT","Content-Length":"146","Cont
ent-Type":"text/plain","Access-Control-Allow-Origin":"*","Connection":"keep-alive","Access-Control-Max-Age":"3600","Access-Co
ntrol-Allow-Methods":"GET, POST, PUT, DELETE, OPTIONS","Access-Control-Allow-Headers":"*"}},"producer":{"modsecurity":"ModSec
urity v3.0.14 (Linux)","connector":"ModSecurity-nginx v1.0.4","secrules_engine":"Enabled","components":["OWASP_CRS/4.17.1\""]
},"messages":[{"message":"XSS Attack Detected via libinjection","details":{"match":"detected XSS using libinjection.","refere
nce":"v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode,t:cssDecode,t:removeNulls","ruleId":"941100","file":
"/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf","lineNumber":"83","data":"Matched Data: XSS data
 found within ARGS:name: <script>alert(\"XSS\")</script>","severity":"2","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modsecuri
ty","application-multi","language-multi","platform-multi","attack-xss","xss-perf-disable","paranoia-level/1","OWASP_CRS","OWA
SP_CRS/ATTACK-XSS","capec/1000/152/242"],"maturity":"0","accuracy":"0"}},{"message":"XSS Filter - Category 1: Script Tag Vect
or","details":{"match":"Matched \"Operator `Rx' with parameter `(?i)<script[^>]*>[\\s\\S]*?' against variable `ARGS:name' (Va
lue: `<script>alert(\"XSS\")</script>' )","reference":"o0,8v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,t:jsDecode
,t:cssDecode,t:removeNulls","ruleId":"941110","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.c
onf","lineNumber":"110","data":"Matched Data: <script> found within ARGS:name: <script>alert(\"XSS\")</script>","severity":"2
","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modsecurity","application-multi","language-multi","platform-multi","attack-xss",
"xss-perf-disable","paranoia-level/1","OWASP_CRS","OWASP_CRS/ATTACK-XSS","capec/1000/152/242"],"maturity":"0","accuracy":"0"}
},{"message":"NoScript XSS InjectionChecker: HTML Injection","details":{"match":"Matched \"Operator `Rx' with parameter `(?i)
<[^0-9<>A-Z_a-z]*(?:[^\\s\\x0b\\\"'<>]*:)?[^0-9<>A-Z_a-z]*[^0-9A-Z_a-z]*?(?:s[^0-9A-Z_a-z]*?(?:c[^0-9A-Z_a-z]*?r[^0-9A-Z_a-z]
*?i[^0-9A-Z_a-z]*?p[^0-9A-Z_a-z]*?t|t[^0-9A-Z_a-z]*?y[^0-9A-Z_a-z]*?l[^0-9A (4396 characters omitted)' against variable `ARGS
:name' (Value: `<script>alert(\"XSS\")</script>' )","reference":"o0,7v33,29t:utf8toUnicode,t:urlDecodeUni,t:htmlEntityDecode,
t:jsDecode,t:cssDecode,t:removeNulls","ruleId":"941160","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-AT
TACK-XSS.conf","lineNumber":"205","data":"Matched Data: <script found within ARGS:name: <script>alert(\"XSS\")</script>","sev
erity":"2","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modsecurity","application-multi","language-multi","platform-multi","att
ack-xss","xss-perf-disable","paranoia-level/1","OWASP_CRS","OWASP_CRS/ATTACK-XSS","capec/1000/152/242"],"maturity":"0","accur
acy":"0"}},{"message":"Javascript method detected","details":{"match":"Matched \"Operator `Rx' with parameter `(?i)\\b(?:eval
|set(?:timeout|interval)|new[\\s\\x0b]+Function|a(?:lert|tob)|btoa|(?:promp|impor)t|con(?:firm|sole\\.(?:log|dir))|fetch)[\\s
\\x0b]*[\\(\\{]' against variable `ARGS:name' (Value: `<script>alert(\"XSS\")</script>' )","reference":"o8,6v33,29t:htmlEntit
yDecode,t:jsDecode","ruleId":"941390","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf","li
neNumber":"739","data":"Matched Data: alert( found within ARGS:name: <script>alert(\"XSS\")</script>","severity":"2","ver":"O
WASP_CRS/4.17.1","rev":"","tags":["modsecurity","application-multi","language-multi","attack-xss","xss-perf-disable","paranoi
a-level/1","OWASP_CRS","OWASP_CRS/ATTACK-XSS","capec/1000/152/242"],"maturity":"0","accuracy":"0"}},{"message":"Inbound Anoma
ly Score Exceeded (Total Score: 20)","details":{"match":"Matched \"Operator `Ge' with parameter `5' against variable `TX:BLOC
KING_INBOUND_ANOMALY_SCORE' (Value: `20' )","reference":"","ruleId":"949110","file":"/etc/modsecurity.d/owasp-crs/rules/REQUE
ST-949-BLOCKING-EVALUATION.conf","lineNumber":"222","data":"","severity":"0","ver":"OWASP_CRS/4.17.1","rev":"","tags":["modse
curity","anomaly-evaluation","OWASP_CRS"],"maturity":"0","accuracy":"0"}}]}}
root@DESKTOP-RD2MOSD:/home/eduardo/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs#
```

Pesquisar 20°C 22:34