RELATÓRIO – Opção 1 (Hands-on)

Nome: Waldecy Façanha Oliveira Junior

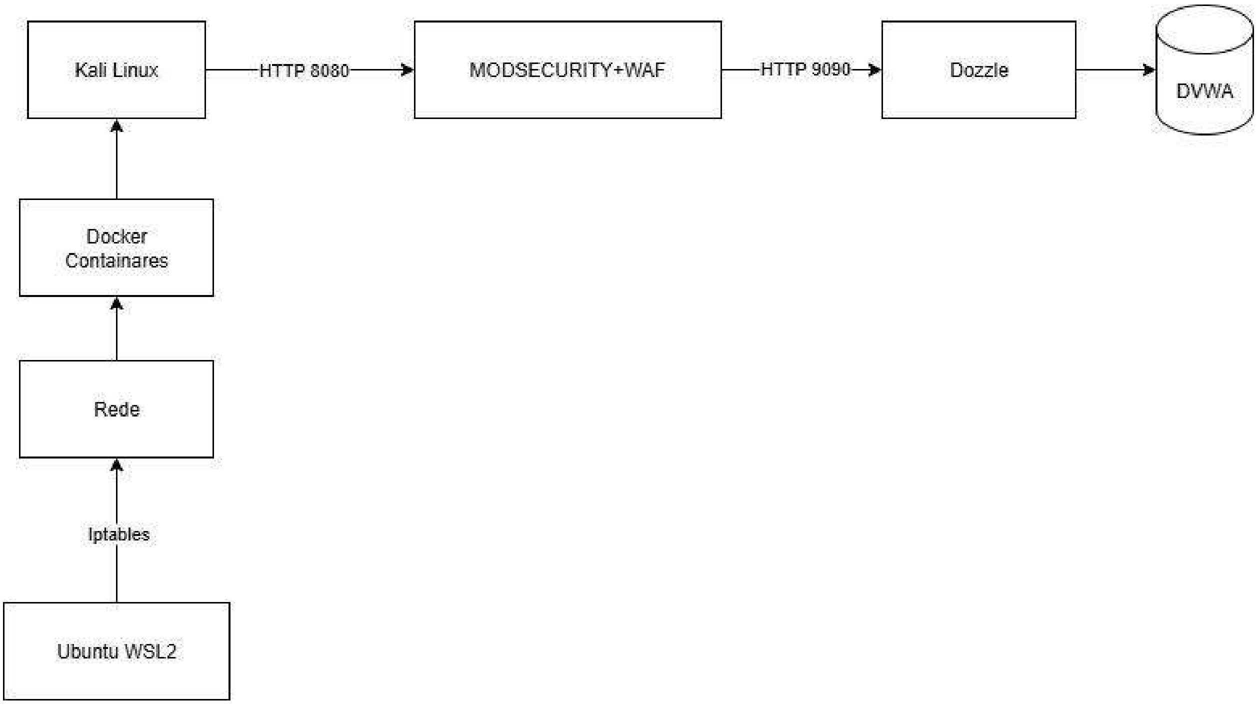
Data: 25/09/2025

1. Sumário Executivo

2. Objetivo e Escopo

- O que foi defendido, o que foi atacado, limites do exercício.
- O que foi defendido, a aplicação Web DVWA que roda na porta 8080 através do Mod Security+Waf contra invasões e acessos externos, ele fica na entrada da aplicação protegendo, e tem o Dozzle uma interface de monitoramento de logs em tempo real. Tem um container atacante Kali Linux que tem várias ferramentas pentester onde é usado para ataques, escalonamneto de privilégios, DDOs, SQli, XSS etc.

3. Arquitetura (Diagrama)



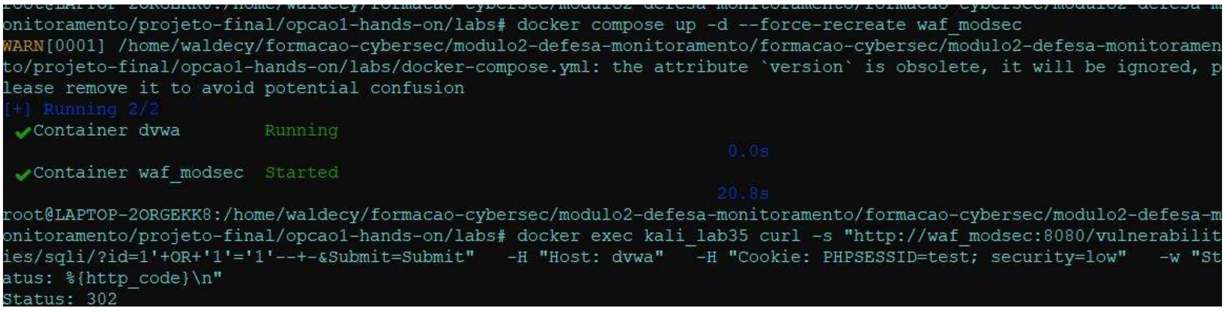
- Kali Linux é uma aplicação atacante através do protocolo da internet HTTP na porta 8080 tem acesso a aplicação vulnerável DVWA onde tem um firewall na entrada MODSECURITY+WAF para proteger que estiver configurado para proteger de ataques de invasores.
- Ubuntu para entrar na rede tem o Iptables um firewall para Sistemas Linux que serve para proteção entre o Sistema operacional e a rede.

4. Metodologia

- Passos executados (detecção → bloqueio → resposta), critérios de sucesso.
- É usado o MODSECURITY+WAF para bloqueios de ataques
- Dozzle ferramenta de monitoramento de logs, Ips, tráfego de redes e ataques
- É usado para proteger de ataques e acessos indevidos ao sistema web, o MODSECURITY+WAF e configurar o docker-compose.yml no arquivo através de editor de texto: Vscode, bloco de notas, Vim e Nano,
- `O # para desativar a função`
- `- MODSEC_RULE_ENGINE=On (modo bloqueio de ataques)`
- `- MODSEC_RULE_ENGINE=DetectionOnly  (modo detecção)`

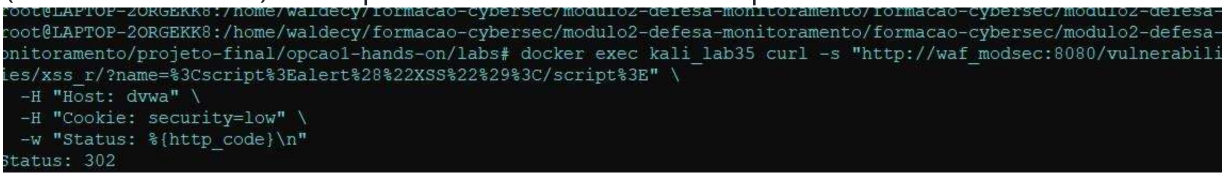
5. Execução e Evidências

- Print de execução do SQLI sem proteção de (MODSECURITY+WAF): Status 302 (redirecionamento) - Ataque detectado mas não bloqueado

- 

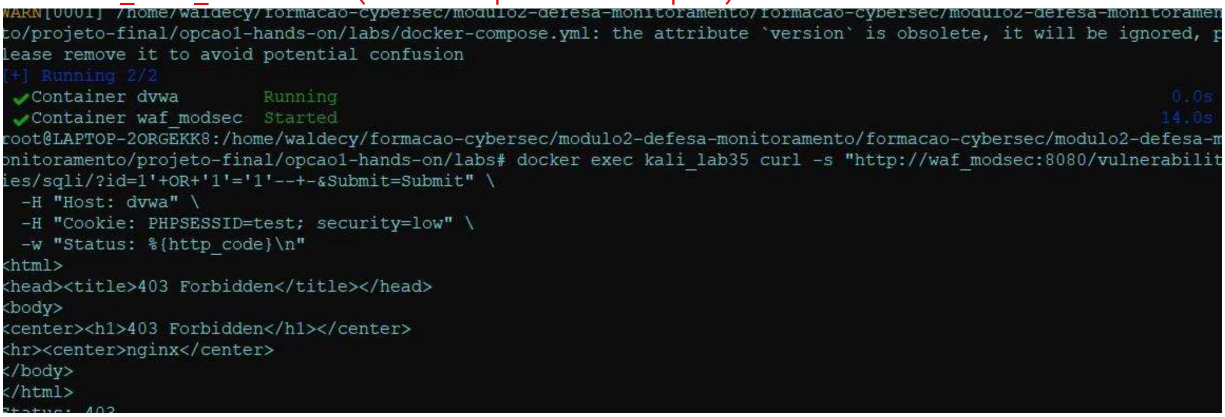
```
root@LAPTOP-2ORGEKK8:/home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-m
onitoramento/projeto-final/opcao1-hands-on/labs# docker compose up -d --force-recreate waf_modsec
WARN[0001] /home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-monitoramen
to/projeto-final/opcao1-hands-on/labs/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, p
lease remove it to avoid potential confusion
[+] Running 2/2
 ✔Container dvwa         Running
                                                                         0.0s
 ✔Container waf_modsec   Started
                                                                        20.8s
root@LAPTOP-2ORGEKK8:/home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-m
onitoramento/projeto-final/opcao1-hands-on/labs# docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilit
ies/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit"   -H "Host: dvwa"   -H "Cookie: PHPSESSID=test; security=low"   -w "St
atus: %{http_code}\n"
Status: 302
```

- Print de execução do XSS sem proteção de (MODSECURITY+WAF): Status 302 (redirecionamento) - Ataque detectado mas não bloqueado

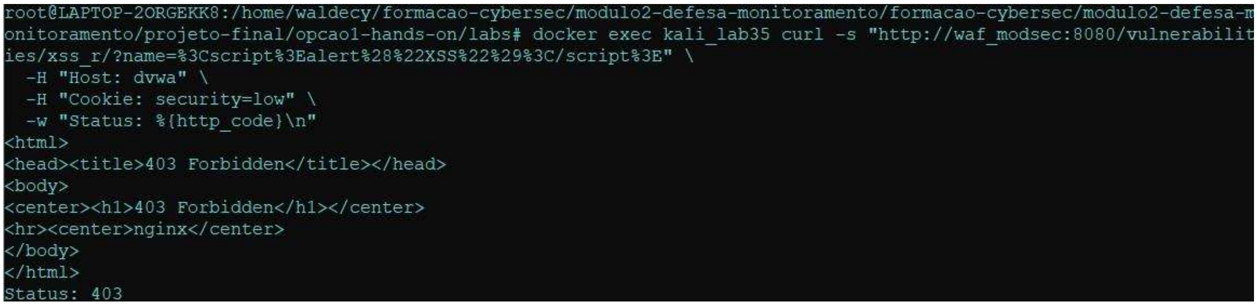
- 

```
root@LAPTOP-2ORGEKK8:/home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-
root@LAPTOP-2ORGEKK8:/home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-
onitoramento/projeto-final/opcao1-hands-on/labs# docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabili
ies/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
```

- Configurar o WAF para o modo blocking: Edite o arquivo `docker-compose.yml` e altere para:
- - MODSEC_RULE_ENGINE=On (modo bloqueio de ataques)



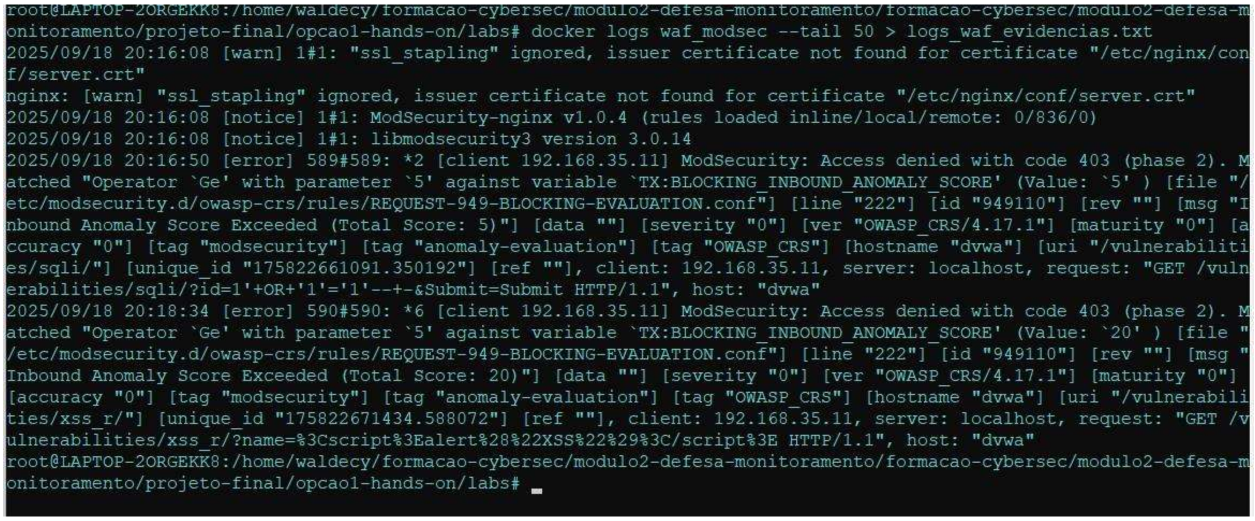
```
WARN[0001] /home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-monitoramen
to/projeto-final/opcao1-hands-on/labs/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, p
lease remove it to avoid potential confusion
[+] Running 2/2
 ✔Container dvwa         Running                                                                                0.0s
 ✔Container waf_modsec   Started                                                                               14.0s
root@LAPTOP-2ORGEKK8:/home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-m
onitoramento/projeto-final/opcao1-hands-on/labs# docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilit
ies/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
```



```
root@LAPTOP-2ORGEKK8:/home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-m
onitoramento/projeto-final/opcao1-hands-on/labs# docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilit
ies/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
```

- Foi usado na proteção da aplicação vulnerável (DVWA), MODSECURITY+WAF é um firewall para proteção de sistemas Web, editando o arquivo docker-compose.yml e alterar no código a configuração: ativando – MODSEC_RULE_ENGINE=ON (bloqueia os ataques).

  - MODSEC_RULE_ENGINE=DetectionOnly # (modo de detecção)
- Tem uma ferramenta de monitoramento de logs: Dozzle, monitora os Ips, tráfego de redes, ataques e bloqueios.
- Relatório de evidências do WAF:



```
root@LAPTOP-2ORGEKK8:/home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-m
onitoramento/projeto-final/opcao1-hands-on/labs# docker logs waf_modsec --tail 50 > logs_waf_evidencias.txt
2025/09/18 20:16:08 [warn] 1#1: "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/nginx/con
f/server.crt"
nginx: [warn] "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/nginx/conf/server.crt"
2025/09/18 20:16:08 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remote: 0/836/0)
2025/09/18 20:16:08 [notice] 1#1: libmodsecurity3 version 3.0.14
2025/09/18 20:16:50 [error] 589#589: *2 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). M
atched "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 "I
nbound Anomaly Score Exceeded (Total Score: 5)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.17.1"] [maturity "0"] [a
ccuracy "0"] [tag "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabiliti
es/sqli/"] [unique_id "175822661091.350192"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vuln
erabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1", host: "dvwa"
2025/09/18 20:18:34 [error] 590#590: *6 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). M
atched "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 "/vulnerabili
ties/xss_r/"] [unique_id "175822671434.588072"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /v
ulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1", host: "dvwa"
root@LAPTOP-2ORGEKK8:/home/waldecy/formacao-cybersec/modulo2-defesa-monitoramento/formacao-cybersec/modulo2-defesa-m
onitoramento/projeto-final/opcao1-hands-on/labs#
```

6. Resposta a Incidente (NIST IR)

- Detecção, Contenção, Erradicação, Recuperação, Lições Aprendidas
- Detecção: através da ferramentas de logs Dozzle que detecta a defesa e ataques, IP, protocolos de redes e todos os containar.
- Contenção: através de configurações do Sistema e MODSECURITY+WAF Firewall Web que bloqueia IPs e ataques externos aos Sistemas Web.
- Recuperação dos Sistemas a funcionar normalmente
- Lições Aprendidas: Temos que configurar da forma ideal aplicativos e Sistemas Web e usar Firewall na entrada para proteger de acesso indevidos e ataques.

7. Recomendações (80/20)

Ação	Impacto	Facilidade	Prioridade
DVWA	Alta	Alta	Alta
Dozzle	Média	Média	Alta
Docker	Média	Baixa	Baixa
Kali Linux	Alta	Alta	Alta
MODSECURITY+WAF	Alta	Alta	Alta

8. Conclusão

- Que devemos configurar de forma eficiente nossos Sistemas Web e aplicativos atráves de configurações, Firewall de entrada WAF, ferramentas de monitoramento Dozzle etc.

10. Anexos

- Configs, logs, scripts
- **Configuração Inicial:**
- docker --version

□ docker-compose –version

□ **Navegar para o diretório do lab**

□ Cd ./labs

□ **Arquivos Necessários dentro da pasta Labs**

□ labs/

```
labs/
├── docker-compose.yml
├── Dockerfile.kali
├── scripts/
│   ├── attack_script.sh
│   └── monitor_defense.sh
└── README.md
```

Subindo todos os containers:

```
docker compose up -d –build
```

Verificar o status dos containars:

```
Docker ps
```

Resultado os containars rodando

```
CONTAINER ID   IMAGE                               PORTS                    NAMES
xxxxxxxxxx     owasp/modsecurity-crs:nginx-alpine  0.0.0.0:8080->8080/tcp  waf_modsec
xxxxxxxxxx     labs-kali_lab35                                               kali_lab35
xxxxxxxxxx     vulnerables/web-dvwa                80/tcp                    dvwa
xxxxxxxxxx     amir20/dozzle:latest                0.0.0.0:9999->8080/tcp  dozzle
```

Testar Conectividade

```
curl -s http://localhost:8080 | head -5
```

Se funcionar: Você verá HTML do DVWA **Se não funcionar:** Veja a seção Solução de Problemas

Configuração do DVWA

. Acessar DVWA no Navegador

Abra seu navegador e vá para: **http://localhost:8080**

. Fazer Login

- **Usuário:** `admin`
- **Senha:** `password`

. Configurar Banco de Dados

Após login, clique em **"Setup"** (menu lateral)
Clique em **"Create / Reset Database"**
Aguarde a mensagem de sucesso

. Configurar Nível de Segurança

Clique em **"DVWA Security"** (menu lateral)
Selecione **"Low"**
Clique em **"Submit"**

Importante: Mantenha o navegador aberto para manter a sessão ativa!

Reconhecimento (Nmap)

. Entrar no Container Kali

```
docker exec -it kali_lab35 /bin/bash
```

Executar Scan Nmap

```
nmap -sS -sV waf_modsec
```

Resultado esperado:

```
PORT     STATE SERVICE  VERSION
8080/tcp open  http     nginx
8443/tcp open  ssl/http nginx
```

3. Sair do Container

```
exit
```

Explicação: O nmap identifica que o WAF está rodando nginx nas portas 8080 (HTTP) e 8443 (HTTPS).

Teste no Modo Detecção

Configurar WAF para Modo Detecção

Edite o arquivo `docker-compose.yml` e certifique-se de que a linha esteja assim:

```
- MODSEC_RULE_ENGINE=DetectionOnly  # modo detecção apenas
```

Recriar o Container WAF

```
docker compose up -d --force-recreate waf_modsec
```

. Testar Ataque SQLi (Deve Passar)

```
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"
```

Resultado esperado: Status 302 (redirecionamento) - **ATAQUE DETECTADO MAS NÃO BLOQUEADO**

. Testar Ataque XSS (Deve Passar)

```
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"
```

Resultado esperado: Status 302 (redirecionamento) - **ATAQUE DETECTADO MAS NÃO BLOQUEADO**

Teste no Modo Blocking

Configurar WAF para Modo Blocking

Edite o arquivo `docker-compose.yml` e altere para:

```
- MODSEC_RULE_ENGINE=On  # modo blocking (bloqueia ataques)
```

Recriar o Container WAF

```
docker compose up -d --force-recreate waf_modsec
```

Testar Ataque SQLi (Deve ser Bloqueado)

```
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"
```

Resultado esperado: Status 403 + página "403 Forbidden" - ATAQUE BLOQUEADO!

Testar Ataque XSS (Deve ser Bloqueado)

```
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"
```

Resultado esperado: Status 403 + página "403 Forbidden" - **ATAQUE BLOQUEADO!**

Monitoramento com Dozzle

Acessar Interface Dozzle

Abra seu navegador e vá para: **http://localhost:9999**

Fazer Login no Dozzle

- **Usuário:** `admin`
- **Senha:** `admin`

Visualizar Logs do WAF

1. Clique no container **"waf_modsec"**
2. Observe os logs em tempo real
3. Execute novos ataques e veja as detecções aparecerem

Analisar Logs Estruturados

Procure por estas informações importantes:

- `"secrules_engine":"DetectionOnly"` ou `"secrules_engine":"Enabled"`
- **Rule IDs:** 942100 (SQLi), 941100 (XSS)
- **HTTP Status Codes:** 302 (detecção) vs 403 (bloqueio)

Coleta de Evidências

Capturar Logs Detalhados

```
docker logs waf_modsec --tail 50 > logs_waf_evidencias.txt
```

Fazer Screenshots

Capture telas do:

- Dozzle mostrando logs de detecção
- Dozzle mostrando logs de bloqueio
- Resultado do nmap
- Páginas 403 Forbidden

Documentar Timeline NIST IR

1. **Detecção:** Timestamp dos logs de detecção
2. **Análise:** Identificação dos tipos de ataque
3. **Contenção:** Ativação do modo blocking
4. **Erradicação:** Bloqueio efetivo dos ataques

🛠 Solução de Problemas

Container não sobe

```
# Verificar logs de erro
docker logs waf_modsec
docker logs dvwa

# Recriar tudo do zero
```

```
docker compose down
docker compose up -d --build
```

DVWA não carrega

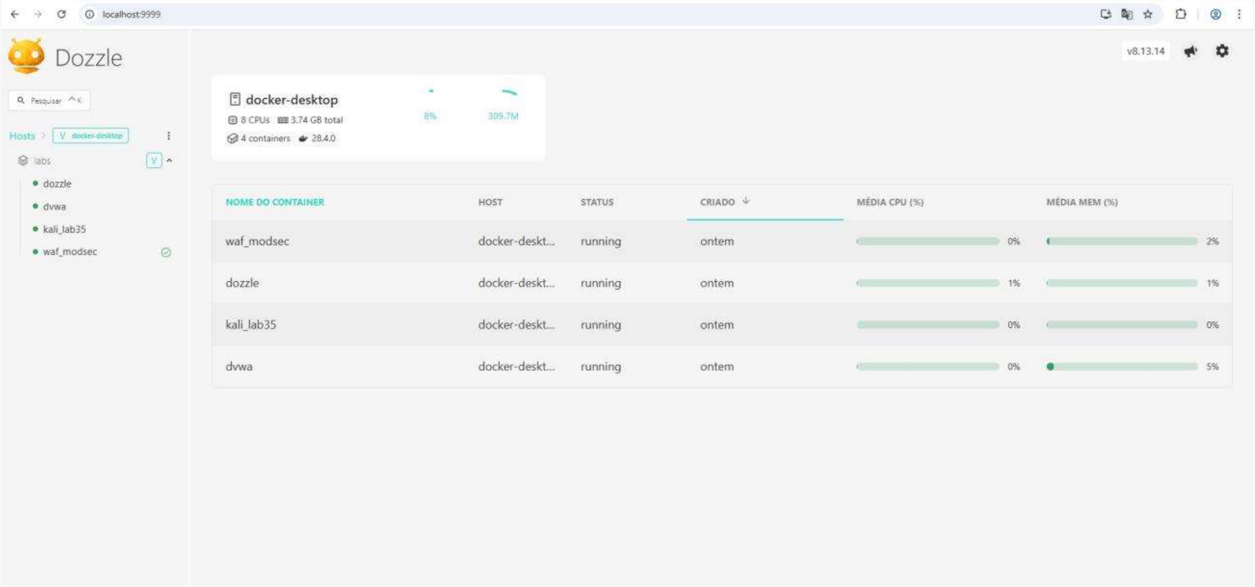
```
# Verificar se header Host está correto
curl -v "http://localhost:8080/login.php" -H "Host: dvwa"
```

WAF não bloqueia

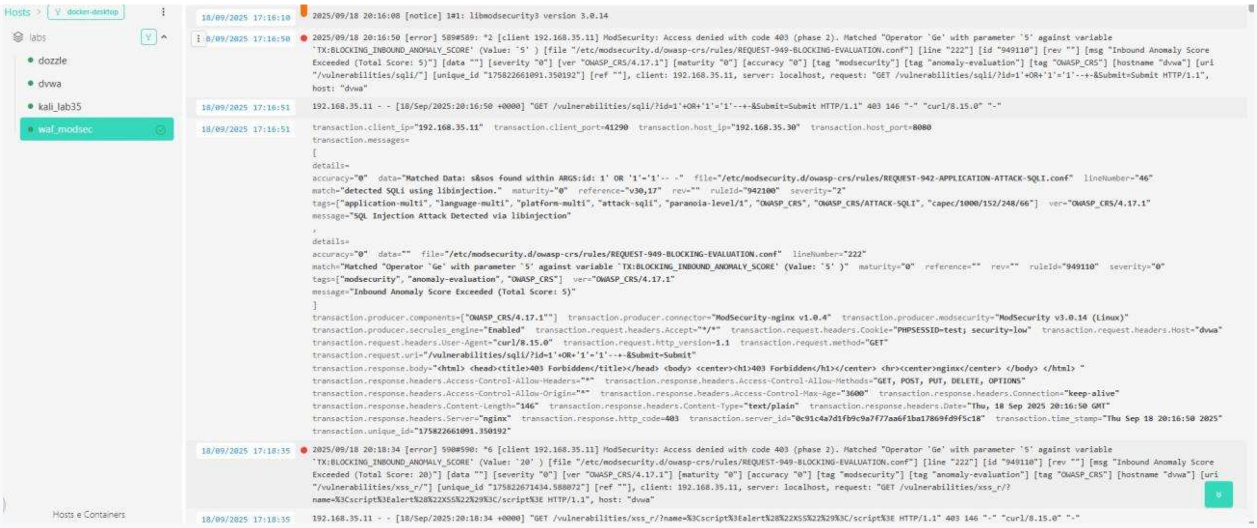
```
# Verificar configuração
docker exec waf_modsec env | grep MODSEC_RULE_ENGINE

# Deve mostrar: MODSEC_RULE_ENGINE=On (para blocking)
```

Dozzle não acessa

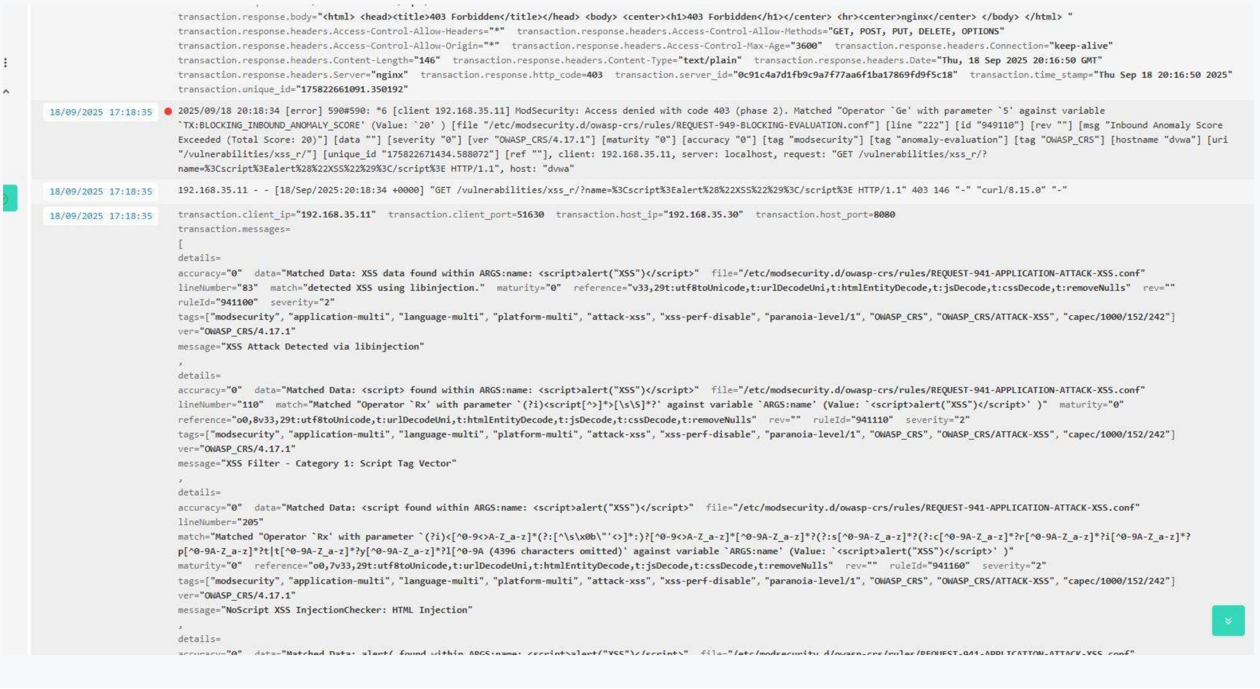
```
# Verificar se porta está disponível
docker ps | grep dozzle

# Deve mostrar: 0.0.0.0:9999->8080/tcp
```



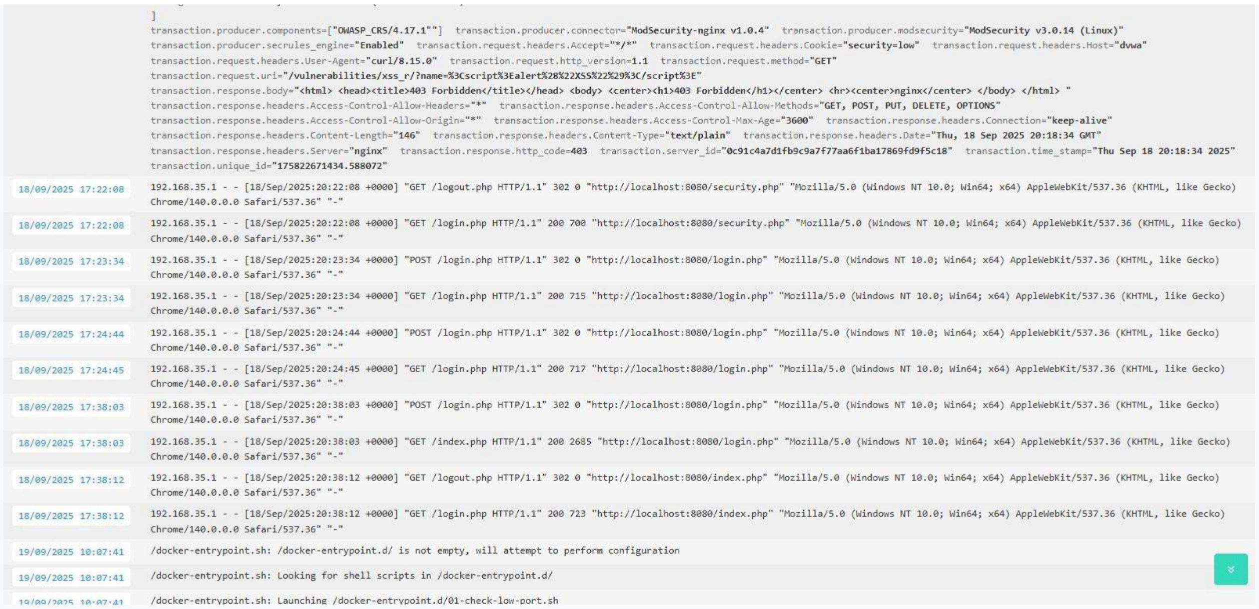
NOME DO CONTAINER	HOST	STATUS	CRIADO ↓	MÉDIA CPU (%)	MÉDIA MEM (%)
waf_modsec	docker-deskt...	running	ontem	0%	2%
dozzle	docker-deskt...	running	ontem	1%	1%
kali_lab35	docker-deskt...	running	ontem	0%	0%
dvwa	docker-deskt...	running	ontem	0%	5%



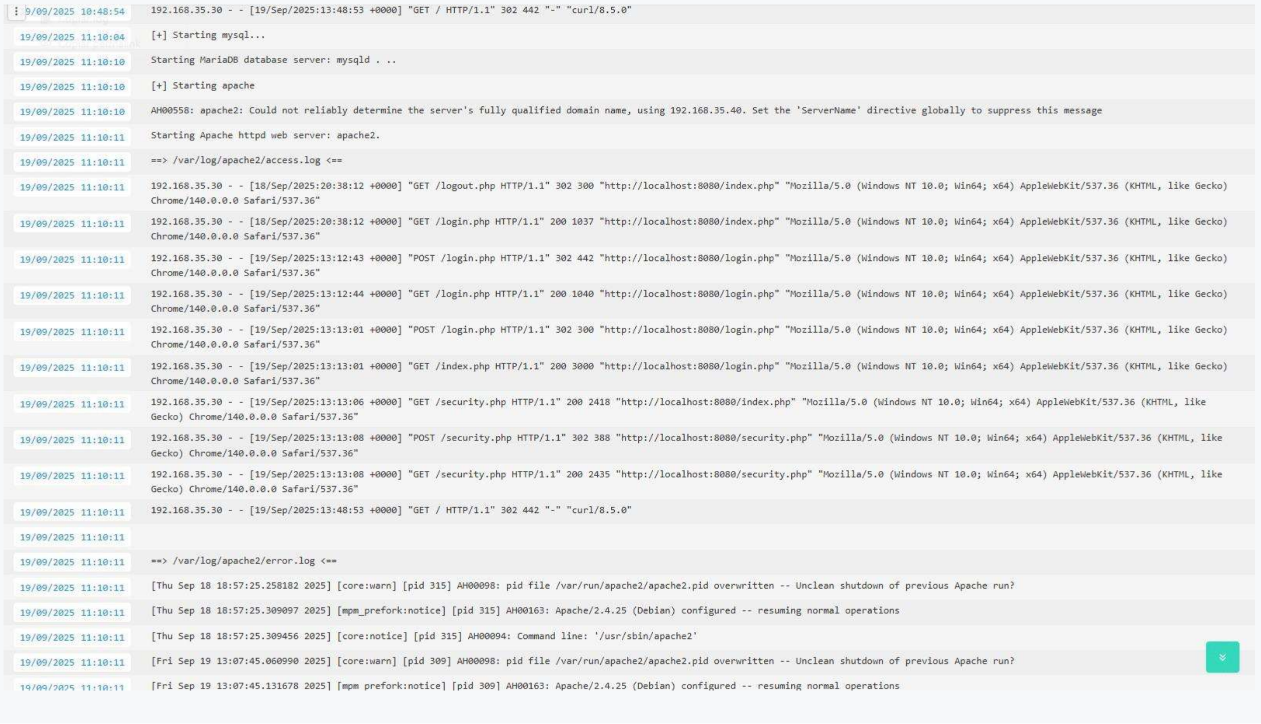
```
18/09/2025 17:16:10  2025/09/18 20:16:08 [notice] 1#1: libmodsecurity3 version 3.0.14
18/09/2025 17:16:50  2025/09/18 20:16:50 [error] 589#589: *2 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge' with parameter `5' against variable
                     `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 "175822661091.350192"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1",
                     host: "dvwa"
18/09/2025 17:16:51  192.168.35.11 - - [18/Sep/2025:20:16:50 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
18/09/2025 17:16:51  transaction.client_ip="192.168.35.11"  transaction.client_port=41290  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> <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="Thu, 18 Sep 2025 20:16:50 GMT"
                     transaction.response.headers.Server="nginx"  transaction.response.http_code=403  transaction.server_id="0c91c4a7d1fb9c9a7f77aa6f1ba17869fd9f5c18"  transaction.time_stamp="Thu Sep 18 20:16:50 2025"
                     transaction.unique_id="175822661091.350192"
18/09/2025 17:18:35  2025/09/18 20:18:34 [error] 590#590: *6 [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 "175822671434.588072"] [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"
18/09/2025 17:18:35  192.168.35.11 - - [18/Sep/2025:20:18:34 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
```



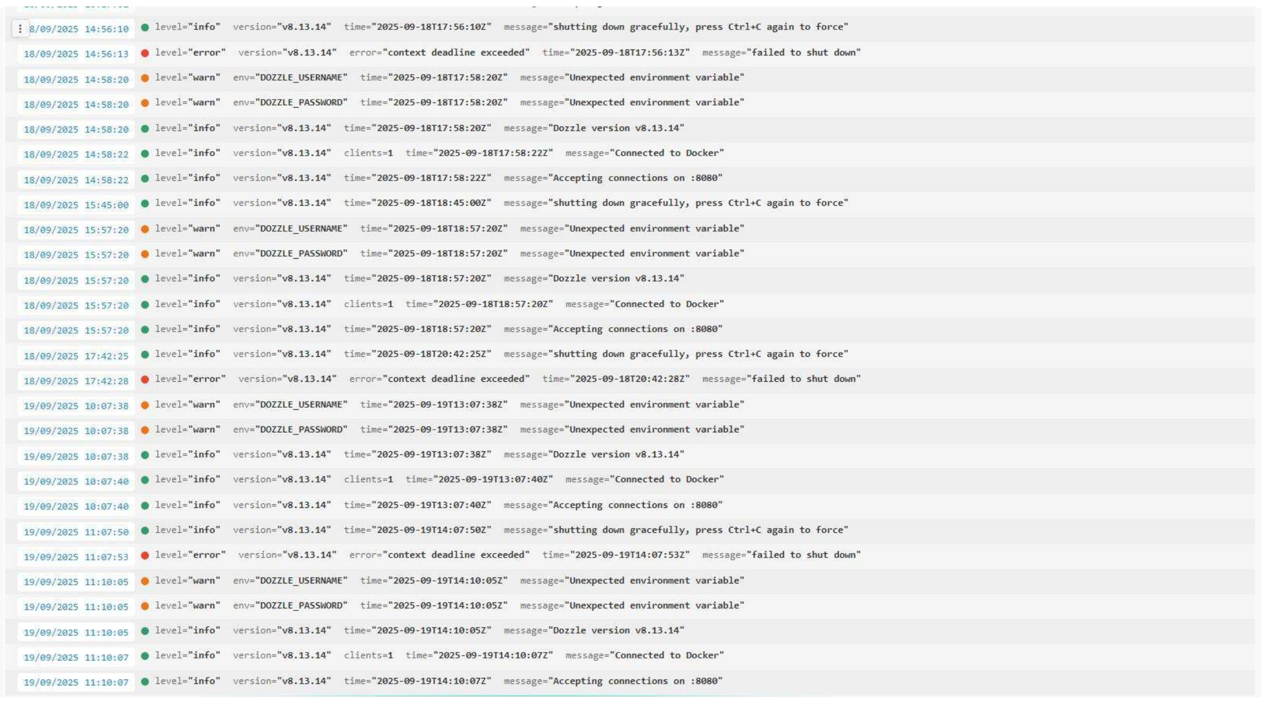
```
                     transaction.response.body="<html> <head><title>403 Forbidden</title></head> <body> <center><h1>403 Forbidden</h1></center> <hr><center>nginx</center> </body> </html> "
                     transaction.response.headers.Access-Control-Allow-Headers="*"  transaction.response.headers.Access-Control-Allow-Methods="GET, 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="Thu, 18 Sep 2025 20:16:50 GMT"
                     transaction.response.headers.Server="nginx"  transaction.response.http_code=403  transaction.server_id="0c91c4a7d1fb9c9a7f77aa6f1ba17869fd9f5c18"  transaction.time_stamp="Thu Sep 18 20:16:50 2025"
                     transaction.unique_id="175822661091.350192"
18/09/2025 17:18:35  2025/09/18 20:18:34 [error] 590#590: *6 [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 "175822671434.588072"] [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"
18/09/2025 17:18:35  192.168.35.11 - - [18/Sep/2025:20:18:34 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"
18/09/2025 17:18:35  transaction.client_ip="192.168.35.11"  transaction.client_port=51630  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"
                     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"
```



```
                      ]
                      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="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> <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="Thu, 18 Sep 2025 20:18:34 GMT"
                      transaction.response.headers.Server="nginx"  transaction.response.http_code=403  transaction.server_id="0c91c4a7d1fb9c9a7f77aa6f1ba17869fd9f5c18"  transaction.time_stamp="Thu Sep 18 20:18:34 2025"
                      transaction.unique_id="175822671434.588072"
18/09/2025 17:22:08   192.168.35.1 - - [18/Sep/2025:20:22:08 +0000] "GET /logout.php HTTP/1.1" 302 0 "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" "-"
18/09/2025 17:22:08   192.168.35.1 - - [18/Sep/2025:20:22:08 +0000] "GET /login.php HTTP/1.1" 200 700 "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" "-"
18/09/2025 17:23:34   192.168.35.1 - - [18/Sep/2025:20:23:34 +0000] "POST /login.php HTTP/1.1" 302 0 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36" "-"
18/09/2025 17:23:34   192.168.35.1 - - [18/Sep/2025:20:23:34 +0000] "GET /login.php HTTP/1.1" 200 715 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36" "-"
18/09/2025 17:24:44   192.168.35.1 - - [18/Sep/2025:20:24:44 +0000] "POST /login.php HTTP/1.1" 302 0 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36" "-"
18/09/2025 17:24:45   192.168.35.1 - - [18/Sep/2025:20:24:45 +0000] "GET /login.php HTTP/1.1" 200 717 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36" "-"
18/09/2025 17:38:03   192.168.35.1 - - [18/Sep/2025:20:38:03 +0000] "POST /login.php HTTP/1.1" 302 0 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36" "-"
18/09/2025 17:38:03   192.168.35.1 - - [18/Sep/2025:20:38:03 +0000] "GET /index.php HTTP/1.1" 200 2685 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36" "-"
18/09/2025 17:38:12   192.168.35.1 - - [18/Sep/2025:20:38:12 +0000] "GET /logout.php HTTP/1.1" 302 0 "http://localhost:8080/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36" "-"
18/09/2025 17:38:12   192.168.35.1 - - [18/Sep/2025:20:38:12 +0000] "GET /login.php HTTP/1.1" 200 723 "http://localhost:8080/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36" "-"
19/09/2025 10:07:41   /docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
19/09/2025 10:07:41   /docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
19/09/2025 10:07:41   /docker-entrypoint.sh: Launching /docker-entrypoint.d/01-check-low-port.sh
```



```
9/09/2025 10:48:54    192.168.35.30 - - [19/Sep/2025:13:48:53 +0000] "GET / HTTP/1.1" 302 442 "-" "curl/8.5.0"
19/09/2025 11:10:04   [+] Starting mysql...
19/09/2025 11:10:10   Starting MariaDB database server: mysqld . ..
19/09/2025 11:10:10   [+] Starting apache
19/09/2025 11:10:10   AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 192.168.35.40. Set the 'ServerName' directive globally to suppress this message
19/09/2025 11:10:11   Starting Apache httpd web server: apache2.
19/09/2025 11:10:11   ==> /var/log/apache2/access.log <==
19/09/2025 11:10:11   192.168.35.30 - - [18/Sep/2025:20:38:12 +0000] "GET /logout.php HTTP/1.1" 302 300 "http://localhost:8080/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36"
19/09/2025 11:10:11   192.168.35.30 - - [18/Sep/2025:20:38:12 +0000] "GET /login.php HTTP/1.1" 200 1037 "http://localhost:8080/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36"
19/09/2025 11:10:11   192.168.35.30 - - [19/Sep/2025:13:12:43 +0000] "POST /login.php HTTP/1.1" 302 442 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36"
19/09/2025 11:10:11   192.168.35.30 - - [19/Sep/2025:13:12:44 +0000] "GET /login.php HTTP/1.1" 200 1040 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36"
19/09/2025 11:10:11   192.168.35.30 - - [19/Sep/2025:13:13:01 +0000] "POST /login.php HTTP/1.1" 302 300 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36"
19/09/2025 11:10:11   192.168.35.30 - - [19/Sep/2025:13:13:01 +0000] "GET /index.php HTTP/1.1" 200 3000 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
                      Chrome/140.0.0.0 Safari/537.36"
19/09/2025 11:10:11   192.168.35.30 - - [19/Sep/2025:13:13:06 +0000] "GET /security.php HTTP/1.1" 200 2418 "http://localhost:8080/index.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
                      Gecko) Chrome/140.0.0.0 Safari/537.36"
19/09/2025 11:10:11   192.168.35.30 - - [19/Sep/2025:13:13:08 +0000] "POST /security.php HTTP/1.1" 302 388 "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"
19/09/2025 11:10:11   192.168.35.30 - - [19/Sep/2025:13:13:08 +0000] "GET /security.php HTTP/1.1" 200 2435 "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"
19/09/2025 11:10:11   192.168.35.30 - - [19/Sep/2025:13:48:53 +0000] "GET / HTTP/1.1" 302 442 "-" "curl/8.5.0"
19/09/2025 11:10:11
19/09/2025 11:10:11   ==> /var/log/apache2/error.log <==
19/09/2025 11:10:11   [Thu Sep 18 18:57:25.258182 2025] [core:warn] [pid 315] AH00098: pid file /var/run/apache2/apache2.pid overwritten -- Unclean shutdown of previous Apache run?
19/09/2025 11:10:11   [Thu Sep 18 18:57:25.309097 2025] [mpm_prefork:notice] [pid 315] AH00163: Apache/2.4.25 (Debian) configured -- resuming normal operations
19/09/2025 11:10:11   [Thu Sep 18 18:57:25.309456 2025] [core:notice] [pid 315] AH00094: Command line: '/usr/sbin/apache2'
19/09/2025 11:10:11   [Fri Sep 19 13:07:45.060990 2025] [core:warn] [pid 309] AH00098: pid file /var/run/apache2/apache2.pid overwritten -- Unclean shutdown of previous Apache run?
19/09/2025 11:10:11   [Fri Sep 19 13:07:45.131678 2025] [mpm_prefork:notice] [pid 309] AH00163: Apache/2.4.25 (Debian) configured -- resuming normal operations
```



```
⋮ 8/09/2025 14:56:10  ● level="info"   version="v8.13.14"   time="2025-09-18T17:56:10Z"   message="shutting down gracefully, press Ctrl+C again to force"
18/09/2025 14:56:13  ● level="error"   version="v8.13.14"   error="context deadline exceeded"   time="2025-09-18T17:56:13Z"   message="failed to shut down"
18/09/2025 14:58:20  ● level="warn"   env="DOZZLE_USERNAME"   time="2025-09-18T17:58:20Z"   message="Unexpected environment variable"
18/09/2025 14:58:20  ● level="warn"   env="DOZZLE_PASSWORD"   time="2025-09-18T17:58:20Z"   message="Unexpected environment variable"
18/09/2025 14:58:20  ● level="info"   version="v8.13.14"   time="2025-09-18T17:58:20Z"   message="Dozzle version v8.13.14"
18/09/2025 14:58:22  ● level="info"   version="v8.13.14"   clients=1   time="2025-09-18T17:58:22Z"   message="Connected to Docker"
18/09/2025 14:58:22  ● level="info"   version="v8.13.14"   time="2025-09-18T17:58:22Z"   message="Accepting connections on :8080"
18/09/2025 15:45:00  ● level="info"   version="v8.13.14"   time="2025-09-18T18:45:00Z"   message="shutting down gracefully, press Ctrl+C again to force"
18/09/2025 15:57:20  ● level="warn"   env="DOZZLE_USERNAME"   time="2025-09-18T18:57:20Z"   message="Unexpected environment variable"
18/09/2025 15:57:20  ● level="warn"   env="DOZZLE_PASSWORD"   time="2025-09-18T18:57:20Z"   message="Unexpected environment variable"
18/09/2025 15:57:20  ● level="info"   version="v8.13.14"   time="2025-09-18T18:57:20Z"   message="Dozzle version v8.13.14"
18/09/2025 15:57:20  ● level="info"   version="v8.13.14"   clients=1   time="2025-09-18T18:57:20Z"   message="Connected to Docker"
18/09/2025 15:57:20  ● level="info"   version="v8.13.14"   time="2025-09-18T18:57:20Z"   message="Accepting connections on :8080"
18/09/2025 17:42:25  ● level="info"   version="v8.13.14"   time="2025-09-18T20:42:25Z"   message="shutting down gracefully, press Ctrl+C again to force"
18/09/2025 17:42:28  ● level="error"   version="v8.13.14"   error="context deadline exceeded"   time="2025-09-18T20:42:28Z"   message="failed to shut down"
19/09/2025 10:07:38  ● level="warn"   env="DOZZLE_USERNAME"   time="2025-09-19T13:07:38Z"   message="Unexpected environment variable"
19/09/2025 10:07:38  ● level="warn"   env="DOZZLE_PASSWORD"   time="2025-09-19T13:07:38Z"   message="Unexpected environment variable"
19/09/2025 10:07:38  ● level="info"   version="v8.13.14"   time="2025-09-19T13:07:38Z"   message="Dozzle version v8.13.14"
19/09/2025 10:07:40  ● level="info"   version="v8.13.14"   clients=1   time="2025-09-19T13:07:40Z"   message="Connected to Docker"
19/09/2025 10:07:40  ● level="info"   version="v8.13.14"   time="2025-09-19T13:07:40Z"   message="Accepting connections on :8080"
19/09/2025 11:07:50  ● level="info"   version="v8.13.14"   time="2025-09-19T14:07:50Z"   message="shutting down gracefully, press Ctrl+C again to force"
19/09/2025 11:07:53  ● level="error"   version="v8.13.14"   error="context deadline exceeded"   time="2025-09-19T14:07:53Z"   message="failed to shut down"
19/09/2025 11:10:05  ● level="warn"   env="DOZZLE_USERNAME"   time="2025-09-19T14:10:05Z"   message="Unexpected environment variable"
19/09/2025 11:10:05  ● level="warn"   env="DOZZLE_PASSWORD"   time="2025-09-19T14:10:05Z"   message="Unexpected environment variable"
19/09/2025 11:10:05  ● level="info"   version="v8.13.14"   time="2025-09-19T14:10:05Z"   message="Dozzle version v8.13.14"
19/09/2025 11:10:07  ● level="info"   version="v8.13.14"   clients=1   time="2025-09-19T14:10:07Z"   message="Connected to Docker"
19/09/2025 11:10:07  ● level="info"   version="v8.13.14"   time="2025-09-19T14:10:07Z"   message="Accepting connections on :8080"
```