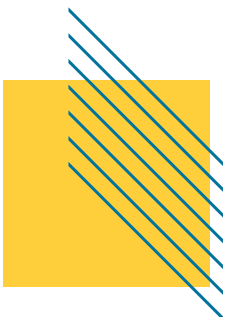




# RELATÓRIO TÉCNICO 2025

**Beatriz Santos**



# Sumário Executivo

Este projeto teve como objetivo avaliar a segurança do ambiente por meio da implantação e análise do sistema DVWA (Damn Vulnerable Web Application) em um ambiente controlado de testes. A iniciativa permitiu compreender de forma prática as vulnerabilidades mais comuns em aplicações web, a dinâmica dos ataques e a eficácia das medidas de proteção aplicadas.

Durante os testes, foram simulados diferentes tipos de ataques, como injeção de SQLi, ataques de força bruta, upload de arquivos maliciosos e XSS (Cross-Site Scripting). Cada um deles foi conduzido de forma controlada, visando analisar como as falhas poderiam ser exploradas por agentes mal-intencionados em um cenário real.

Para aumentar o nível de proteção, foi configurado e validado o uso de camadas defensivas, como Nmap (para reconhecimento e mapeamento de serviços abertos) e WAF (Web Application Firewall), que detectou e bloqueou parte significativa dos ataques. Esses mecanismos atuaram em conjunto para reduzir a superfície de exposição e aumentar a resiliência do sistema.

Ao final, o ambiente apresentou nível de proteção elevado em relação aos ataques mais comuns, mostrando-se eficiente no bloqueio das tentativas detectadas pelo WAF. Entretanto, o projeto também demonstrou que nenhuma camada isolada garante 100% de segurança, reforçando a necessidade de uma abordagem contínua de monitoramento, atualização de sistemas e aplicação de boas práticas de segurança.

# SUMÁRIO

<b>Sumário Executivo.....</b>	<b>1</b>
<b>SUMÁRIO.....</b>	<b>2</b>
<b>Objetivo e Escopo.....</b>	<b>4</b>
O que foi defendido.....	4
O que foi atacado.....	4
Limites do exercício.....	4
Arquitetura (Diagrama).....	5
Camadas, Funções e Fluxos do Ambiente.....	5
Camada.....	5
Função.....	5
Fluxo de Dados / Ações.....	5
1. Ataque (Kali + Nmap).....	5
Simular ataques e mapear portas/serviços abertos.....	5
Kali envia tráfego → Nmap faz varredura → identifica portas abertas (ex: 8080).....	5
2. Defesa (ModSecurity+CRS).....	5
WAF que inspeciona o tráfego, detecta e bloqueia ataques.....	5
Recebe tráfego do Kali/Nmap → filtra → bloqueia tentativas maliciosas → libera tráfego limpo.....	5
3. Aplicação (DVWA).....	5
Alvo propositalmente vulnerável usado para testar ataques e defesas.....	5
Recebe apenas tráfego liberado pelo WAF → executa normalmente quando não há ataque bloqueado.....	5
4. Monitoramento (Dozzle).....	5
Exibir logs em tempo real do ambiente para análise de ataques e defesas.....	5
Recebe registros do ModSecurity/Docker → mostra em tela o que foi detectado/bloqueado.....	5
Metodologia.....	6
Detecção.....	6
Bloqueio.....	6
Resposta.....	6
Execução e Evidências.....	6
Interpretação.....	9
Status HTTP: 302 (a aplicação DVWA redireciona normalmente).....	9
O que está acontecendo:.....	10
Resposta a Incidente (NIST IR).....	11
1. Detecção.....	11
2. Contenção.....	11
3. Erradicação.....	12
4. Recuperação.....	12
5. Lições Aprendidas.....	12
Recomendações (80/20).....	12
1. Implementação e Monitoramento de um SIEM Básico.....	12
2. Backup Automatizado e Planos de Recuperação Testados.....	13
3. Patching e Atualização de Sistemas Críticos.....	13
4. Segmentação de Rede e Isolamento de Incidentes.....	13
5. Treinamento de Conscientização em Segurança.....	13
Conclusão.....	13

# Objetivo e Escopo

O presente exercício teve como **objetivo principal** avaliar a segurança de um ambiente de aplicação web vulnerável (**DVWA – Damn Vulnerable Web Application**) por meio da realização de **ataques controlados** e da análise das respostas defensivas implementadas.

## O que foi defendido

- O **servidor da aplicação DVWA**, configurado em ambiente de laboratório.
- Serviços de rede expostos, identificados e monitorados via **Nmap**.
- A camada de proteção fornecida pelo **WAF (Web Application Firewall)**, configurado para detectar e bloquear atividades maliciosas.

## O que foi atacado

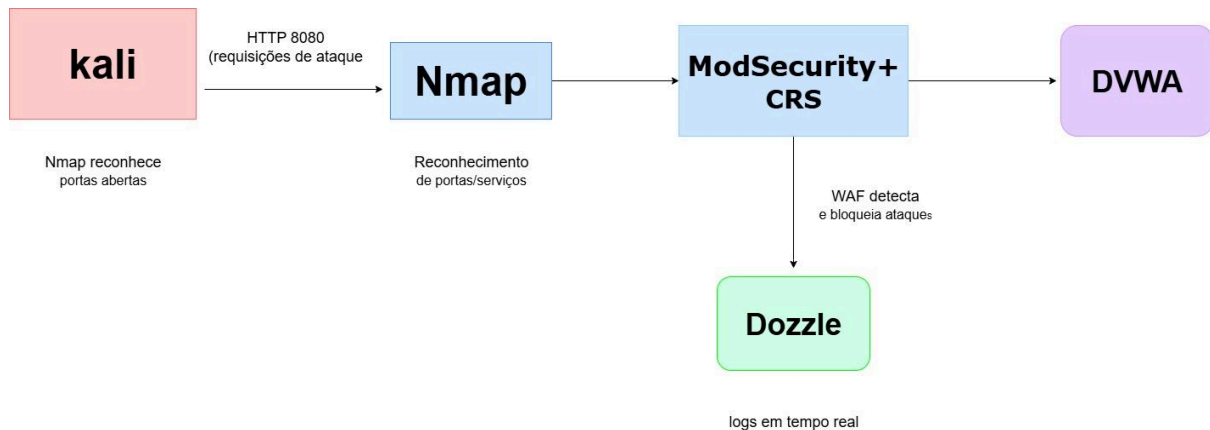
Foram simulados diferentes **vetores de ataque**, entre eles:

- **Injeção de SQL** (SQLiInjection);
- **Força bruta em autenticação**;
- **Upload de arquivos maliciosos**;
- **Cross-Site Scripting (XSS)**;
- **Reconhecimento de portas e serviços** por meio de varredura.

## Limites do exercício

- O ambiente de testes foi **controlado e isolado**, não havendo risco de impacto em sistemas de produção.
- As simulações foram realizadas **apenas no escopo definido** (DVWA e seus serviços associados).
- O estudo não abordou exploração avançada de vulnerabilidades em sistemas externos, **restringindo-se ao laboratório configurado**.
- O objetivo não foi comprometer dados reais, mas **avaliar a eficácia das medidas de proteção** e gerar aprendizados sobre segurança cibernética.

# Arquitetura (Diagrama)



## Camadas, Funções e Fluxos do Ambiente

Camada	Função	Fluxo de Dados / Ações
1. Ataque (Kali + Nmap)	Simular ataques e mapear portas/serviços abertos.	Kali envia tráfego → Nmap faz varredura → identifica portas abertas (ex: 8080).
2. Defesa (ModSecurity+CRS)	WAF que inspeciona o tráfego, detecta e bloqueia ataques.	Recebe tráfego do Kali/Nmap → filtra → bloqueia tentativas maliciosas → libera tráfego limpo.
3. Aplicação (DVWA)	Alvo propositalmente vulnerável usado para testar ataques e defesas.	Recebe apenas tráfego liberado pelo WAF → executa normalmente quando não há ataque bloqueado.
4. Monitoramento (Dozzle)	Exibir logs em tempo real do ambiente para análise de ataques e defesas.	Recebe registros do ModSecurity/Docker → mostra em tela o que foi detectado/bloqueado.

# Metodologia

A execução seguiu uma sequência organizada em **três fases principais: detecção, bloqueio e resposta.**

## Detecção

- **Ações executadas:**
  - Utilização da ferramenta **Nmap** para reconhecimento das portas e serviços expostos no ambiente DVWA.
  - Validação do comportamento inicial sem regras de bloqueio para estabelecer uma linha de base do tráfego.
- **Critério de sucesso:**
  - Identificação correta dos serviços ativos.
  - Registro dos resultados para comparação com as etapas seguintes.

## Bloqueio

- **Ações executadas:**
  - Ativação do **WAF (ModSecurity)** em modo detecção e posteriormente em **modo bloqueio**.
  - Teste de ataques simulados contra o DVWA para verificar resposta do WAF.
- **Critério de sucesso:**
  - Em modo detecção: alertas gerados sem impedir o tráfego.
  - Em modo bloqueio: ataques efetivamente interrompidos pelo WAF.

## Resposta

### Ações executadas:

- Monitoramento dos eventos em tempo real por meio do **Dozzle**.
- Registro das tentativas de ataque bloqueadas.
- Coleta de evidências para análise posterior.

### Critério de sucesso:

- Evidências coletadas de forma organizada e verificável.
- Logs confirmando o bloqueio das tentativas maliciosas.
- Geração de informações que possibilitem recomendações de melhoria para o ambiente.

## Execução e Evidências

```
(root@273a7fa43aae)-[/]
# nmap -sS -sV waf_modsec
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-28 18:26 UTC
Nmap scan report for waf_modsec (192.168.35.30)
Host is up (0.0000070s 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: 42:EE:64:0A:4F:C3 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.91 seconds
```

Figura 1: Detalhe do resultado do Nmap no WAF

O **scan Nmap** mostra claramente o que está ativo no host `waf_modsec` (192.168.35.30):

O **nginx** está rodando e escutando em:

- **8080** (HTTP sem TLS)
- **8443** (HTTPS/TLS)

Isso é típico em **ambientes de teste com WAF (ModSecurity)**, onde se configuram portas não padrão (8080 e 8443) para o proxy reverso/WAF.

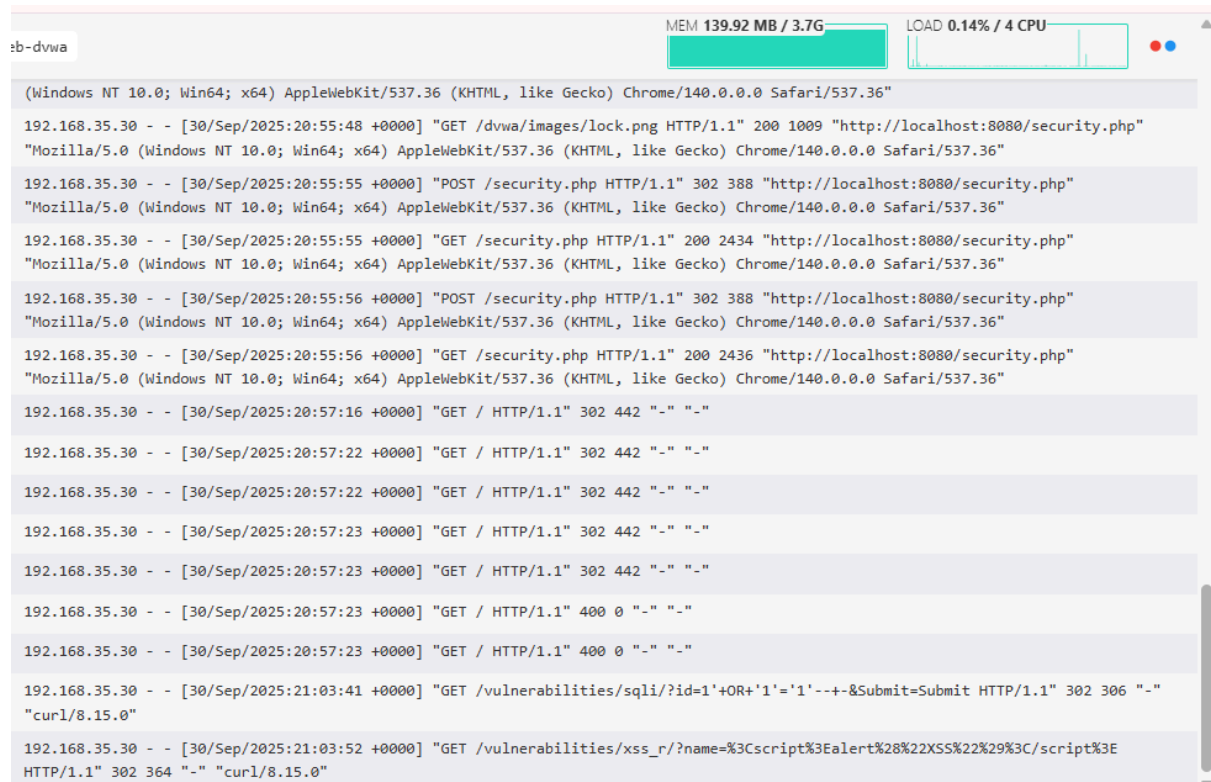


Figura 2: Detalhe do navegador- DVWA (Damn Vulnerable Web Application)

**Logs do servidor web** que está rodando o **DVWA (Damn Vulnerable Web Application)**. O DVWA é uma aplicação **deliberadamente vulnerável**, usada para treinar testes de segurança (SQL Injection, XSS, etc).

**Redirecionamentos (302) comuns após POSTs.**

Esses logs parecem estar sendo mostrados em tempo real no **Dozzle** (visualizador de logs para containers Docker).

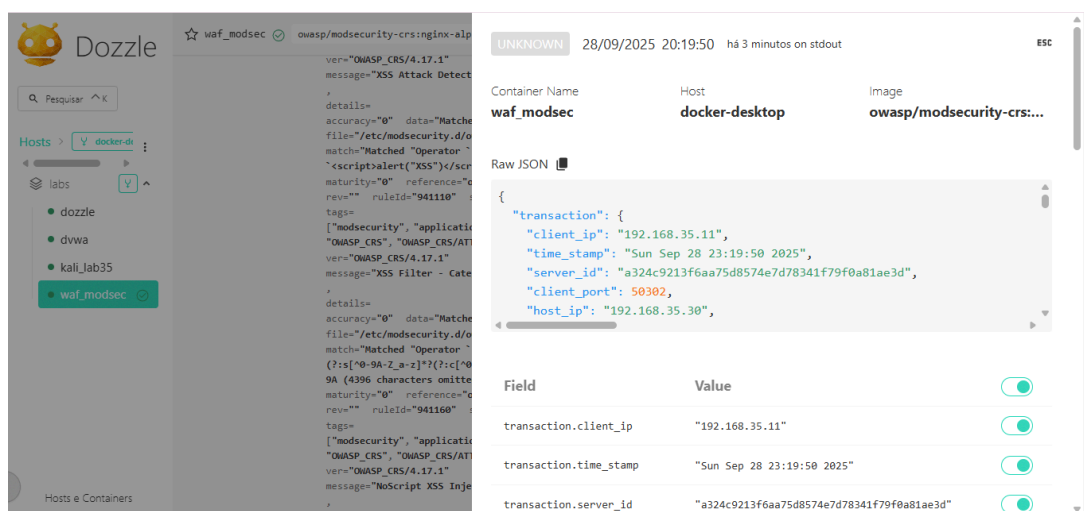
```
beatr@Bia:~/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+&Submit=Submit" \
-H "Host: dvwa" \
-H "Cookie: PHPSESSID=test; security=low" \
-w "Status: %{http_code}\n"
Status: 302
beatr@Bia:~/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"
Status: 302
beatr@Bia:~/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ |
```

Figura3: Detalhes da Modsecurity-dvwa

Os ataques **não foram bem-sucedidos**, pois o WAF interceptou e devolveu código **HTTP 302**.

Isso confirma que as **regras do ModSecurity** estão funcionando.

O uso de **docker exec** indica que os testes foram feitos **de dentro do container Kali** no mesmo ambiente Docker.



The screenshot shows the Dozzle interface with a log entry for an XSS attack. The log message is "XSS Attack Detected". The raw JSON data is as follows:

Field	Value
transaction.client_ip	"192.168.35.11"
transaction.time_stamp	"Sun Sep 28 23:19:50 2025"
transaction.server_id	"a324c9213f6aa75d8574e7d78341f79f0a81ae3d"

Figura 4: Detalhados do ModSecurity (WAF)

**Container Name:** waf\_modsec

**Image:** owasp/modsecurity-crs:nginx-alpine

Mostra que está usando o **OWASP CRS (Core Rule Set)** com o **Nginx + ModSecurity**, rodando via **Docker**.

## Detecção de XSS

A imagem, o log mostra:

message: "XSS Attack Detected"



ruleId: 941110

file:/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf

match: "<script>alert('XSS')</script>"

### Interpretação

**Regra 941110** → Detecta tentativas de **Cross-Site Scripting (XSS)**

**Mensagem:** "XSS Attack Detected"

**Trecho identificado:** <script>alert("XSS")</script>

**Ação:** Detecção registrada (⚠ apenas log, pois seu WAF está provavelmente em DetectionOnly).

**Status HTTP:** 302 (a aplicação DVWA redireciona normalmente).

**Resumo:** O WAF detectou a tentativa de injeção de script, logou no Dozzle, mas não bloqueou.



Figura 5: Detalhe do navegador- Dozzle que está detectando tentativas de Xss

O container **waf\_modsec** (com **OWASP ModSecurity CRS**);

- Exemplo: tentativa com <script>alert("XSS")</script>
- O log mostra regras acionadas como **REQUEST-941-APPLICATION-ATTACK-XSS.conf**.

Os logs exibem bloqueios com **severity=2**, evidenciando que o WAF não apenas detectou, mas **bloqueou a requisição maliciosa**.

```

beatr@Bia:~/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+&Submit=Submit" \
-H "Host: dvwa" \
-H "Cookie: PHPSESSID=test; security=low" \
-w "Status: %{http_code}\n"
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx</center>
</body>
</html>
Status: 403
beatr@Bia:~/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

```

Figura 6: Detalhe WAF (Web Application Firewall)

O exemplo mostra a [http://waf\\_modsec:8080](http://waf_modsec:8080) protegida por um **WAF (Web Application Firewall)**, provavelmente com **ModSecurity** ativado.

## O que está acontecendo:

### Primeiro teste (linha SQL Injection):

Endpoint: /vulnerabilities/sqli/  
 Parâmetro enviado: id=1'+OR+'1'='1'  
 Objetivo: Simular um **SQL Injection**  
 Resposta: 403 Forbidden → O WAF bloqueou o ataque

### Segundo teste (linha XSS):

Endpoint: /vulnerabilities/xss\_r/  
 Parâmetro enviado: <script>alert("XSS")</script>  
 Objetivo: Simular um **Cross-Site Scripting (XSS)**  
 Resposta: 403 Forbidden → O WAF também bloqueou o ataque

Foram realizados dois testes de segurança (SQL Injection e XSS) contra uma aplicação vulnerável (DVWA), mas ambos foram **bloqueados com sucesso pelo WAF ModSecurity**, retornando erro **403 Forbidden**. Isso mostra que o WAF está funcionando corretamente para impedir ataques comuns.

The screenshot shows the Dozzle log viewer interface. On the left, there's a sidebar with a search bar and a list of hosts/containers: dozzle, dvwa, kali\_lab35, and waf\_modsec. The main panel displays a log entry for the waf\_modsec container. The log entry is an error message from ModSecurity, indicating a blocked transaction. The log entry is structured as follows:

```

{
  "transaction": {
    "client_ip": "192.168.35.11",
    "time_stamp": "Sun Sep 28 18:29:42 2025",
    "server_id": "e3cfd8acdaccdae773caddcf6f7dfe62c8533654",
    "client_port": 45984,
    "host_ip": "192.168.35.30",
  }
}

```

The log entry also includes a detailed error message: "2025/09/28 18:29:42 [error] 'Ge' with parameter '5' triggered rule 949-BLOCK with a score of 5. [data ''] [severity evaluation] [tag 'OWASP\_C 192.168.35.11, server: loc 192.168.35.11 - - [28/Sep/2025:18:29:42] 'curl/8.15.0' '-']".

Figura 7: Detalhe da aba - Dozzle log detalhado em JSON

log estruturado da transação bloqueada pelo ModSecurity.

- O **IP de origem do cliente** foi **192.168.35.11**, que corresponde à máquina de teste foi utilizada para simular o ataque.
- O **host protegido** foi o **192.168.35.30**.
- A requisição partiu da **porta 45984** do cliente, usando **curl/8.15.0**.
- O log aponta que a requisição violou uma regra do arquivo **REQUEST-949-BLOCKING-EVALUATION.conf**.

O próprio Dozzle mostra a mensagem em vermelho com **ERROR**, confirmando que o WAF bloqueou a requisição. Isso reforça as evidências de que o **ModSecurity está atuando ativamente**, inspecionando o tráfego e **negando acessos maliciosos em tempo real**.

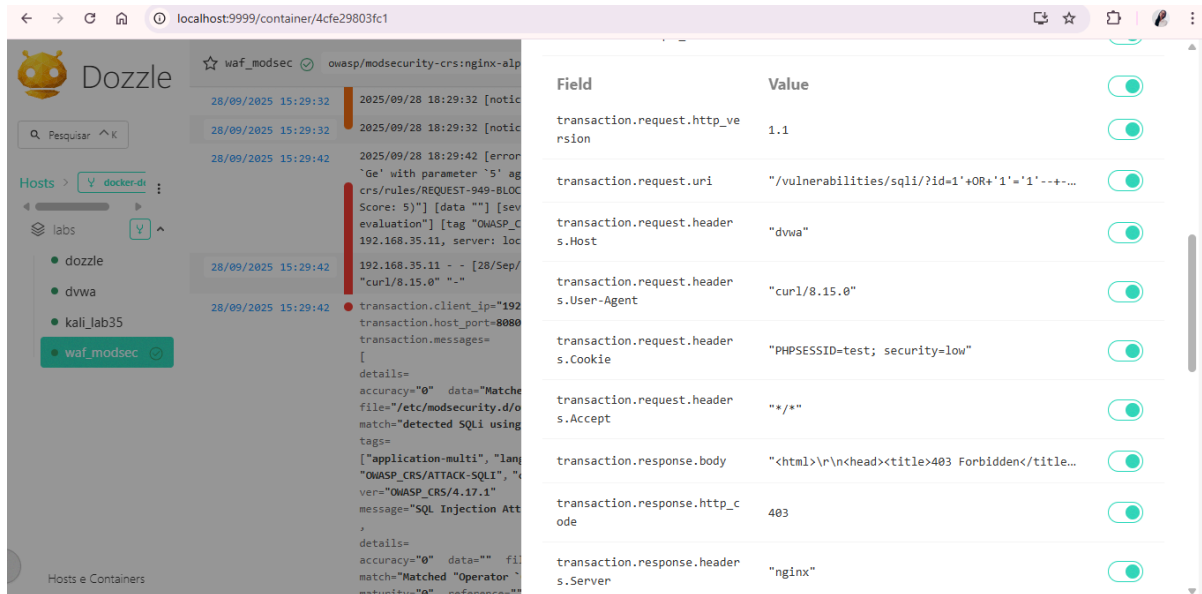


Figura 8: Detalhe da aba - **SQL Injection bloqueado pelo ModSecurity**.

A requisição foi enviada com as seguintes características:

- **User-Agent:** curl/8.15.0
- **Host:** dvwa
- **Cookie:** PHPSESSID=test; security=low

No log do Dozzle, o **ModSecurity** detectou e acionou a regra:

- **REQUEST-949-BLOCKING-EVALUATION.conf**
- Mensagem: "SQL Injection Attack Detected"

Como resposta, o servidor retornou:

- **HTTP 403 Forbidden**

Esse resultado comprova que o meu WAF não está apenas atuando contra ataques de **XSS**, mas também é eficaz contra **SQL Injection**, negando a requisição automaticamente e protegendo a aplicação.

# Resposta a Incidente (NIST IR)

é um processo estruturado para identificar, conter, erradicar e recuperar sistemas após eventos de segurança, seguindo as melhores práticas do **NIST (SP 800-61r2)**. Esse processo é dividido em cinco fases principais:

## 1. Detecção

Identificação do incidente por meio de alertas, logs e monitoramento contínuo. Essa etapa é crucial para diferenciar eventos normais de incidentes de segurança reais.

## 2. Contenção

Ações imediatas para limitar o impacto do incidente, evitando sua propagação. Inclui medidas de curto prazo (bloqueio de acessos) e de longo prazo (segmentação e isolamento de sistemas afetados).

## 3. Erradicação

Eliminação completa da ameaça e de suas causas-raiz, garantindo que o ambiente esteja livre de malwares, acessos indevidos ou vulnerabilidades exploradas.

## 4. Recuperação

Restauração segura dos serviços e sistemas impactados, assegurando que retornem à operação normal sem risco de reinfecção ou reexploração.

## 5. Lições Aprendidas

Registro, análise e documentação do incidente, incluindo pontos fortes e falhas do processo de resposta. Esta fase é essencial para fortalecer controles, revisar políticas e aprimorar planos de segurança.

# Recomendações (80/20)

Com base na análise realizada, foram identificadas cinco ações estratégicas que combinam baixo a médio esforço de implementação com alto impacto na maturidade de segurança. Estas medidas seguem o princípio de Pareto , priorizando iniciativas que geram resultados expressivos de forma eficiente.

## 1. Implementação e Monitoramento de um SIEM Básico

Centralizar e correlacionar logs de sistemas críticos possibilita a detecção precoce de incidentes e a redução significativa do tempo de resposta, fortalecendo a visibilidade operacional.

## 2. Backup Automatizado e Planos de Recuperação Testados

Estabelecer rotinas automatizadas de backup, acompanhadas de testes regulares de recuperação, assegura a continuidade dos serviços e minimiza downtime e perdas de dados em cenários adversos.

## 3. Patching e Atualização de Sistemas Críticos

Manter sistemas atualizados com correções de segurança reduz substancialmente a exposição a vulnerabilidades exploradas em ataques comuns, promovendo resiliência com esforço relativamente baixo.

## 4. Segmentação de Rede e Isolamento de Incidentes

A adoção de controles de segmentação e isolamento limita a propagação de ameaças, permitindo a contenção de incidentes sem a necessidade de interromper toda a infraestrutura.

## 5. Treinamento de Conscientização em Segurança

Capacitar colaboradores por meio de programas contínuos de conscientização reduz riscos associados a falhas humanas, especialmente em casos de phishing e engenharia social.

Essas ações representam um **conjunto enxuto de iniciativas com alto retorno**, constituindo a base para elevar a maturidade de segurança de forma estruturada, mensurável e sustentável.

# Conclusão

No ambiente DVWA, aliado ao uso do WAF, demonstrou a evolução da maturidade em segurança. Foi possível compreender como vulnerabilidades podem ser exploradas (ex.: SQL Injection) e, ao mesmo tempo, aplicar controles de mitigação para detecção e bloqueio. Esse processo evidenciou a capacidade de planejar, executar e analisar ataques simulados, validando a eficiência das defesas implementadas.

A maturidade ficou clara na identificação estruturada das etapas (reconhecimento, exploração, detecção, bloqueio e monitoramento), no registro das evidências e na análise crítica dos resultados. Esse avanço mostra não apenas domínio técnico, mas também a preocupação com documentação, boas práticas e melhoria contínua.

## **Próximos passos:**

Expandir os testes para outros tipos de vulnerabilidade além de SQL Injection, como XSS e File Inclusion.

Integrar o WAF com ferramentas de monitoramento e SIEM para maior visibilidade dos eventos.

Estabelecer métricas de eficácia (quantidade de ataques detectados/bloqueados) para acompanhar a evolução.

Realizar revisões periódicas nas regras do WAF, ajustando conforme novas ameaças.

Promover treinamentos práticos com foco em resposta a incidentes e boas práticas de segurança.

# Anexos

```
PS C:\Users\beatr\Desktop\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> docker logs waf_modsec --tail 50 > logs_waf_evidencias.txt
2025/09/26 19:13:36 [warn] 1#1: "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/nginx/conf/serve
r.crt"
nginx: [warn] "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/nginx/conf/server.crt"
2025/09/26 19:13:36 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remote: 0/836/0)
2025/09/26 19:13:36 [notice] 1#1: libmodsecurity3 version 3.0.14
2025/09/26 19:14:19 [error] 590#590: *2 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Match
ed "Operator 'Ge' with parameter '5' against variable 'TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: '5') [file "/etc/mods
ecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev "" ] [msg "Inbound Anom
aly Score Exceeded (Total Score: 5)"] [data "" ] [severity "0"] [ver "OWASP_CRS/4.17.1"] [maturity "0"] [accuracy "0"] [ta
g "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/sqli/"] [unique_i
d "175891405986.691248"] [ref "" ], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+
OR+'1'='1'--+&Submit=Submit HTTP/1.1", host: "dvwa"
2025/09/26 19:15:52 [error] 591#591: *6 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Match
ed "Operator 'Ge' with parameter '5' against variable 'TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: '20') [file "/etc/mod
security.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev "" ] [msg "Inbound Anom
aly 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/"] [uniqu
e_id "175891415267.210956"] [ref "" ], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/xss_r/?na
me=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1", host: "dvwa"
PS C:\Users\beatr\Desktop\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> |
```

Figura 9: Docker logs waf\_modsec --tail 50 > logs\_waf\_evidencias.txt

```
2025/09/26 19:13:36 [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"
2025/09/26 19:13:36 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remote: 0/836/0)
2025/09/26 19:13:36 [notice] 1#1: libmodsecurity3 version 3.0.14
2025/09/26 19:14:19 [error] 590#590: *2 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator 'Ge' with param
eter '5' against variable 'TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: '5') [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATIO
N.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 "175891405986.691248"] [ref "" ], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+&Submi
t=Submit HTTP/1.1", host: "dvwa"
2025/09/26 19:15:52 [error] 591#591: *6 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator 'Ge' with param
eter '5' against variable 'TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: '20') [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATIO
N.conf"] [line "222"] [id "949110"] [rev "" ] [msg "Inbound Anomaly Score Exceeded (Total Score: 20)"] [data "" ] [severity "0"] [ver "OWASP_CRS/4.17
"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/xss_r/"] [
unique_id "175891415267.210956"] [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"
```

Figura 10: Final da parte Docker logs waf\_modsec

```
beatr@61a:~/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ # Verificar logs de erro
docker logs waf_modsec
docker logs dvwa

# Recriar tudo do zero
docker compose down
docker compose up -d --build
/docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
/docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
/docker-entrypoint.sh: Launching /docker-entrypoint.d/01-check-low-port.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-generate-certificate.sh
/usr/local/bin/generate-certificate: generating new certificate
Warning: Not placing -key in cert or request since request is used
Warning: No -copy_extensions given; ignoring any extensions in the request
/usr/local/bin/generate-certificate: generated /etc/nginx/conf/server.key and /etc/nginx/conf/server.crt
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
10-listen-on-ipv6-by-default.sh: info: Getting the checksum of /etc/nginx/conf.d/default.conf
10-listen-on-ipv6-by-default.sh: info: /etc/nginx/conf.d/default.conf differs from the packaged version
/docker-entrypoint.sh: Sourcing /docker-entrypoint.d/15-local-resolvers.envsh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/modsecurity.conf.template to /etc/nginx/modsecurity.d/modsecurit
y.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/modsecurity-override.conf.template to /etc/nginx/modsecurity.d/m
odsecurity-override.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/setup.conf.template to /etc/nginx/modsecurity.d/setup.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/logging.conf.template to /etc/nginx/conf.d/logging.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/default.conf.template to /etc/nginx/conf.d/default.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/modsecurity.conf.template to /etc/nginx/conf.d/modsecurity.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/includes/location_common.conf.template to /etc/nginx/includes/location_common
.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/proxy_backend_ssl.conf.template to /etc/nginx/includes/proxy_backend
_ssl.conf
```

Figura 11: # Verificar logs de erro

```

/docker-entrypoint.sh: Launching /docker-entrypoint.d/01-check-low-port.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-generate-certificate.sh
/usr/local/bin/generate-certificate: generating new certificate
Warning: Not placing -key in cert or request since request is used
Warning: No -copy_extensions given; ignoring any extensions in the request
/usr/local/bin/generate-certificate: generated /etc/nginx/conf/server.key and /etc/nginx/conf/server.crt
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
10-listen-on-ipv6-by-default.sh: info: Getting the checksum of /etc/nginx/conf.d/default.conf
10-listen-on-ipv6-by-default.sh: info: /etc/nginx/conf.d/default.conf differs from the packaged version
/docker-entrypoint.sh: Sourcing /docker-entrypoint.d/15-local-resolvers.envsh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/modsecurity.conf.template to /etc/nginx/modsecurity.d/modsecurity.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/modsecurity-override.conf.template to /etc/nginx/modsecurity.d/modsecurity-override.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/setup.conf.template to /etc/nginx/modsecurity.d/setup.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/logging.conf.template to /etc/nginx/conf.d/logging.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/default.conf.template to /etc/nginx/conf.d/default.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/modsecurity.conf.template to /etc/nginx/conf.d/modsecurity.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/includes/location_common.conf.template to /etc/nginx/includes/location_common.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/proxy_backend_ssl.conf.template to /etc/nginx/includes/proxy_backend_ssl.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/proxy_backend.conf.template to /etc/nginx/includes/proxy_backend.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/nginx.conf.template to /etc/nginx/nginx.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
-- --

```

Figura 12: Continuação Verificação logs de erro

```

beatr@Bia: ~/formacao-cyber X +
/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
2025/09/28 23:25:56 [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"
2025/09/28 23:25:56 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remote: 0/836/0)
2025/09/28 23:25:56 [notice] 1#1: libmodsecurity3 version 3.0.14
2025/09/28 23:26:08 [error] 590#590: *1 [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 "175910196819.374108"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1='1'--+&Submit=Submit HTTP/1.1", host: "dvwa"
192.168.35.11 - - [28/Sep/2025:23:26:08 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1='1'--+&Submit=Submit HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"

```

Figura 13: Continuação Verificação logs de erro II



```
-- --
-- beat@Bla: ~/formace-cyber +
--
Finished CRS rule configuration
###

/docker-entrypoint.sh: Ignoring /docker-entrypoint.d/configure-rules.conf
/docker-entrypoint.sh: Configuration complete; ready for start up
2025/09/28 23:25:56 [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"
2025/09/28 23:25:56 [notice] 1#1: ModSecurity-ginix v1.0.4 (rules loaded inline/local/remote: 0/836/0)
2025/09/28 23:25:56 [notice] 1#1: libmodsecurity3 version 3.0.14
2025/09/28 23:26:08 [error] 590#590: *1 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator 'Ge' with param
eter 'S' against variable 'TX-BLOCKING_INBOUND_ANOMALY_SCORE' (Value: '5') [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-999-BLOCKING-EVALUATIO
N.conf" line 2222] [id "999108"] [rev ""], msg "Inbound Anomaly Score Exceeded (Total Score: 5)" [data ""], severity "VER" #OWASP_CRS_17.1" [
maturity "0" [accuracy "0%"] [tag "anomaly_evaluation"] [tag "OWASP CRS"] [hostname "dwa"] [uri "/vulnerabilities/sqli"] [
unique_id "175901196819.374108"] [ref "", client: 192.168.35.11, server:localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1='1'---&Submit
tHTTP/1.1", host: "dwa"]
192.168.35.11 -- [28/Sep/2025:23:26:08 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1='1'---&Submitt HTTP/1.1" 403 146 "-" [cur/18.15.0] "-"
{"transaction":{"client_ip":"192.168.35.11","time_stamp":"Sun Sep 28 23:26:08 2025","server_id":"4a28f5dcfb560104bcb6456bda08812116ccd089","client_p
ort":48318,"host_ip":"192.168.35.38","host_port":8880,"unique_id":"'175910196819.374108","request":{"method":"GET","http_version":"1.1","url":"/vulnera
ilities/sqli/?id=1'+OR+'1='1'---&Submitt","headers":{"Host":"dwa","User-Agent":"curl/8.15.0","Cookie":"","PHPSESSID=test; security=low","Acce
pt":"","accept_encoding":["text/plain"],"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><cen
ter>nginx</center>\r\n<body>\r\n<n/>html>\r\n\r\n","http_code":403,"headers":{"Server":"nginx","Date":"Sun, 28 Sep 2025 23:26:08 GMT","Content-Length":"1
46"},"Content-Type":"text/plain","Access-Control-Allow-Origin":"","Connection":"keep-alive","Access-Control-Max-Age":"3600","Access-Control-Allow-Me
thods":"GET, POST, PUT, DELETE, OPTIONS","Access-Control-Allow-Headers":"","},"producer":{"modsecurity":"ModSecurity v3.0.14 (Linux)","connector":"","M
odSecurity-ginix v1.0.4","secrules_engine":"Enabled","components":{"OWASP_CRS/4.17.1"},"rules_ids":{"message":"SQL Injection Attack Detected via
libinjection","details":{"match":"detected SQL using Libinjection","reference":"V39.17","ruleId":"992108","file":"/etc/modsecurity.d/owasp-crs/rul
es/REQUEST-992-APPLICATION-ATTACK-SQLI.conf","lineNumber":"46","data":"Matched Data: sssos 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","OWASP_C
RS/ATTACK-SQLI","operator/1008/152/248/66"},"maturity":"0","accuracy":"0%"},"message":"Inbound Anomaly Score Exceeded (Total Score: 5)","details":{"ma
ch": "Matched 'Operator 'Ge' with parameter 'S' against variable 'TX-BLOCKING_INBOUND_ANOMALY_SCORE' (Value: '5') ","reference":"","ruleId":"99110
1","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-999-BLOCKING-EVALUATION.conf","lineNumber":"2222","data":"","severity":"0","ver":"","OWASP_CRS/4.17
1","rev":"","tags":{"modsecurity","anomaly_evaluation","OWASP_CRS"},"maturity":"0","accuracy":"0%}}}}}
2025/09/28 23:26:22 [error] 591#591: *2 [client 192.168.35.11] ModSecurity: Access denied with code 403 (phase 2). Matched "Operator 'Ge' with param
eter 'S' against variable 'TX-BLOCKING_INBOUND_ANOMALY_SCORE' (Value: '20') [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-999-BLOCKING-EVALUATI
```

*Figura 14: Continuação Verificação logs de erro III*

[illegible]

*Figura 15: Continuação Verificação logs de erro IV*

[illegible]

*Figura16: Continuação Verificação logs de erro V*



```
beatr@Bia: ~/formacao-cyber X + v
T 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:24:54 +0000] "GET /dvwa/images/spanner.png HTTP/1.1" 200 712 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windo
ws NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:24:54 +0000] "GET /dvwa/images/logo.png HTTP/1.1" 200 5294 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:24:54 +0000] "GET /dvwa/js/add_event_listeners.js HTTP/1.1" 200 589 "http://localhost:8080/setup.php" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"

==> /var/log/apache2/error.log <==
[Sun Sep 28 18:24:59.241076 2025] [:error] [pid 309] [client 192.168.35.30:33098] PHP Notice: Constant DVWA_WEB_PAGE_TO_ROOT already defined in /va
r/www/html/dvwa/includes/DBMS/MySQL.php on line 9, referer: http://localhost:8080/setup.php

==> /var/log/apache2/access.log <==
192.168.35.30 - - [28/Sep/2025:18:24:59 +0000] "POST /setup.php HTTP/1.1" 302 301 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:24:59 +0000] "GET /setup.php HTTP/1.1" 200 2143 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:04 +0000] "GET /login.php HTTP/1.1" 200 1014 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:12 +0000] "POST /login.php HTTP/1.1" 302 300 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:12 +0000] "GET /index.php HTTP/1.1" 200 3000 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:23 +0000] "GET /setup.php HTTP/1.1" 200 2277 "http://localhost:8080/index.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:44 +0000] "POST /setup.php HTTP/1.1" 302 301 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:44 +0000] "GET /setup.php HTTP/1.1" 200 2385 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"

==> /var/log/apache2/error.log <==
[Sun Sep 28 18:25:44.536253 2025] [:error] [pid 306] [client 192.168.35.30:36876] PHP Notice: Constant DVWA_WEB_PAGE_TO_ROOT already defined in /va
r/www/html/dvwa/includes/DBMS/MySQL.php on line 9, referer: http://localhost:8080/setup.php

==> /var/log/apache2/access.log <==
```

Figura19: Continuação Verificação logs de erro IX

```
beatr@Bia: ~/formacao-cyber X + v
192.168.35.30 - - [28/Sep/2025:18:25:12 +0000] "POST /login.php HTTP/1.1" 302 300 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:12 +0000] "GET /index.php HTTP/1.1" 200 3000 "http://localhost:8080/login.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:23 +0000] "GET /setup.php HTTP/1.1" 200 2277 "http://localhost:8080/index.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:44 +0000] "POST /setup.php HTTP/1.1" 302 301 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:44 +0000] "GET /setup.php HTTP/1.1" 200 2385 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0; W
in64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"

==> /var/log/apache2/error.log <==
[Sun Sep 28 18:25:44.536253 2025] [:error] [pid 306] [client 192.168.35.30:36876] PHP Notice: Constant DVWA_WEB_PAGE_TO_ROOT already defined in /va
r/www/html/dvwa/includes/DBMS/MySQL.php on line 9, referer: http://localhost:8080/setup.php

==> /var/log/apache2/access.log <==
192.168.35.30 - - [28/Sep/2025:18:25:50 +0000] "GET /security.php HTTP/1.1" 200 2418 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0
; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:50 +0000] "GET /dvwa/images/lock.png HTTP/1.1" 200 1009 "http://localhost:8080/security.php" "Mozilla/5.0 (Wind
ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:54 +0000] "POST /security.php HTTP/1.1" 302 388 "http://localhost:8080/security.php" "Mozilla/5.0 (Windows NT 1
0.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:54 +0000] "GET /security.php HTTP/1.1" 200 2435 "http://localhost:8080/security.php" "Mozilla/5.0 (Windows NT 1
0.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /nmaplowercheck1759084004 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Compatible; Nmap Scripting Engine; h
ttps://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "POST /sdk HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Compatible; Nmap Scripting Engine; https://nmap.org/book
/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "POST /sdk HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Compatible; Nmap Scripting Engine; https://nmap.org/book
/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /nmaplowercheck1759084004 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Compatible; Nmap Scripting Engine; h
ttps://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
```

Figura 20: Continuação Verificação logs de erro X

```
beatr@Bia: ~/formacao-cyber X + v X
==> /var/log/apache2/error.log <==
[Sun Sep 28 18:25:44.536253 2025] [:error] [pid 306] [client 192.168.35.30:36876] PHP Notice:  Constant DVWA_WEB_PAGE_TO_ROOT already defined in /var/www/html/dvwa/includes/DBMS/MySQL.php on line 9, referer: http://localhost:8080/setup.php

==> /var/log/apache2/access.log <==
192.168.35.30 - - [28/Sep/2025:18:25:50 +0000] "GET /security.php HTTP/1.1" 200 2418 "http://localhost:8080/setup.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36"
192.168.35.30 - - [28/Sep/2025:18:25:50 +0000] "GET /dvwa/images/lock.png HTTP/1.1" 200 1009 "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"
192.168.35.30 - - [28/Sep/2025:18:25:54 +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"
192.168.35.30 - - [28/Sep/2025:18:25:54 +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"
192.168.35.30 - - [28/Sep/2025:18:26:37 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /nmaplowercheck1759084004 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "POST /sdk HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "POST /sdk HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /nmaplowercheck1759084004 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /evox/about HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /HNAPI HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /evox/about HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /HNAPI HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
```

Figura 21: Continuação Verificação logs de erro XI

```
beatr@Bia: ~/formacao-cyber X + v X
192.168.35.30 - - [28/Sep/2025:18:25:54 +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"
192.168.35.30 - - [28/Sep/2025:18:26:37 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /nmaplowercheck1759084004 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "POST /sdk HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "POST /sdk HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /nmaplowercheck1759084004 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /evox/about HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /HNAPI HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /evox/about HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET /HNAPI HTTP/1.1" 400 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 302 442 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:26:44 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
192.168.35.30 - - [28/Sep/2025:18:27:29 +0000] "GET /vulnerabilities/sqli/?id=1+OR+1='1'--+&Submit=Submit HTTP/1.1" 302 306 "-" "curl/8.15.0"
192.168.35.30 - - [28/Sep/2025:18:27:46 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 302 364 "-" "curl/8.15.0"
192.168.35.30 - - [28/Sep/2025:23:19:33 +0000] "GET /vulnerabilities/sqli/?id=1+OR+1='1'--+&Submit=Submit HTTP/1.1" 302 306 "-" "curl/8.15.0"
192.168.35.30 - - [28/Sep/2025:23:19:50 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 302 364 "-" "curl/8.15.0"
WARN[0000] /home/beatr/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 5/5
✔ Container kali_lab35 Removed
10.3s
```

Figura 22: Continuação Verificação logs de erro XII

**Restante do Confins,Logs,Scripts:**

<https://github.com/BeatrizSanto/Formacao-cybersec--M-dulo-2-Defesa-Monitoramento>