

# RELATÓRIO DE LAB DE SEGURANÇA WAF + DVWA

---



**Título: Simulação de Ataques Controlados contra DVWA com  
Proteção WAF**

Data: 24/09/2025

Versão: 1.0

Responsável: Gonçalo Quissola Dala

## 1. Sumário Executivo

Este relatório avaliou a resiliência de uma aplicação vulnerável (DVWA) frente a ataques controlados, utilizando NGINX + ModSecurity + OWASP CRS como defesa.

- Ambiente: DVWA exposta a ataques OWASP Top 10.
- Ataques simulados: nmap, SQLi e XSS.
- Nível de proteção: Modo detecção (302) logou ataques; modo bloqueio (403) os impediu.
- Estado atual: Ambiente protegido com logs estruturados.

Conclusão: O WAF foi eficaz ao detectar e bloquear ataques críticos.

## 2. Objetivo e Escopo

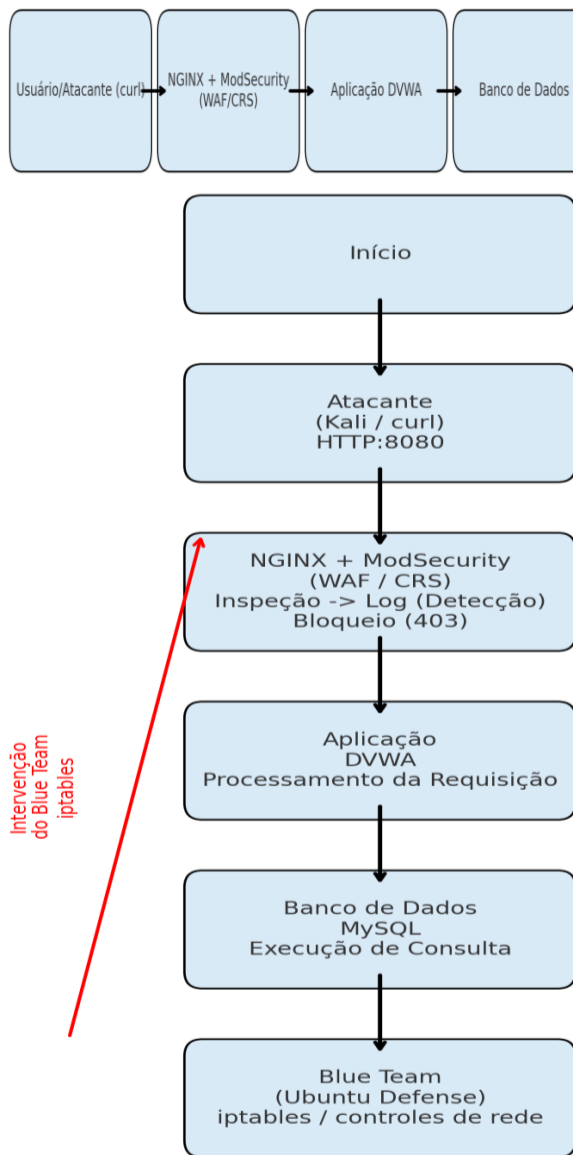
### Objetivo:

- Validar a eficácia do WAF na detecção e bloqueio de ataques comuns (SQLi e XSS).
- Demonstrar o ciclo completo de segurança: detecção, análise, contenção e resposta.

### Escopo:

- Aplicação alvo: DVWA (<http://dvwa>).
- Atacado: Endpoints SQLi (/sqli/) e XSS (/xss\_r refletido).
- Defendido: DVWA em Linux protegida por WAF.
- Quando: 17/09/2025. Onde: Laboratório controlado.
- Impacto: Risco de vazamento de dados e execução de código
- Ferramentas: ModSecurity v3.0.14, OWASP CRS 4.17.1, Nginx, curl, nmap.
- Limite: Testes realizados apenas em ambiente controlado, com configuração de paranoia nível 1, sem impacto produtivo.

### 3. Arquitetura (Diagrama)



Descrição:

Camadas:

- **Camada 1:** Cliente (IP: 192.168.35.11) envia requisições maliciosas.
- **Camada 2:** Nginx com ModSecurity atua como WAF, analisando e bloqueando ataques.
- **Camada 3:** Aplicação DVWA (IP: 192.168.35.30:8080) hospeda a aplicação vulnerável.

Fluxo:

1. Requisição HTTP → WAF (análise de regras CRS).
2. Se detectada ameaça → Bloqueio (403) e log estruturado.
3. Se for segura → Encaminhamento para DVWA, seguindo para o banco de dados.

Ativos:

- Servidor Web (NGINX+WAF).
- Aplicação DVWA (PHP/MySQL).
- Banco MySQL.
- Logs estruturados.

## 4. Metodologia

Passos executados:

1. **Reconhecimento:** Varredura com **nmap** → descoberta de portas abertas e serviços.
2. **Ataques controlados:** Execução de payloads SQLi e XSS.
3. **Deteccção:** WAF em modo *Detection Only*, registrando ataques (302).
4. **Bloqueio:** Ativação de modo *Blocking*, interrompendo ataques (403).
5. **Resposta:** Análise, contenção, erradicação e recuperação segundo NIST IR.

**CrITÉrios de sucesso:**

- WAF deve detectar SQLi e XSS via libinjection e regras CRS
- Bloqueio deve retornar HTTP 403 com log detalhado
- Score de anomalia deve exceder o threshold configurado (5 para inbound)

**Causa raiz:** vulnerabilidades DVWA.

**Ferramentas:** nmap, curl, ModSecurity, iptables/tcpdump.

## 5. Execução e Evidências

Reconhecimento (nmap): Serviços identificados.

SQL Injection:

- Modo Deteccção (302): Requisição logada.
- Modo Bloqueio (403): Negada, log SQL Injection Detected.

XSS:

- Modo Deteccção (302): Requisição logada.
- Modo Bloqueio (403): Negada, regras CRS acionadas.

**Notas operacionais e implicações (deteccção 302 vs bloqueio 403)**

- **Deteccção (302)**

Vantagem: visibilidade e coleta de inteligência sobre técnicas do atacante sem impactar usuários. Risco: ataques são observados em produção potencialmente permitindo exploração de janelas pequenas; ideal apenas em ambientes de teste ou durante tuning.

- **Bloqueio (403)**

Vantagem: previne exploração em tempo real; reduz risco de comprometimento.

Risco: risco de falsos positivos que podem bloquear usuários legítimos — mitiga-se com tuning (paranoia level, whitelists, rule exclusions).

6. Resposta a Incidente (NIST IR)

- Detecção: SQLi e XSS em logs.
- Análise: Ataques críticos OWASP Top 10.
- Contenção: Modo blocking (403).
- Erradicação: Regras CRS ativas.
- Recuperação: Serviço restaurado.

Timeline NIST IR

Fase	Timestamp	Ação
Detecção	17/Sep/2025 19:53:54	WAF detecta SQLi (regra 942100)
Análise	19:53:54	Identificado SQLi via libinjection
Contenção	19:53:54	Bloqueio imediato (HTTP 403)
Erradicação	19:53:54	Requisição maliciosa descartada
Recuperação	-	Serviço permaneceu estável
Lições	-	Monitorar antes de bloquear reduz falsos positivos, necessário tuning contínuo.

Tabela – Classificação dos Incidentes Ocorridos

Incidente	Data/Hora	Categoria	Severidade	Impacto CIA	Urgência	Priorização
SQLi	17/Sep/2025 19:53:54	CAT-01 Ataques Web application	SEV-3: Médio Ataque bloqueado	Confidencialidade (Médio) Integridade (Médio) Disponibilidade (Baixo)	Baixa Ataque contido Imediatamente	P4
XSS	17/Sep/2025 19:55:38	CAT-01 Ataques Web application	SEV-3: Médio Ataque bloqueado	Integridade (Médio) Confidencialidade (Baixo) Disponibilidade (Baixo)	Baixa Ataque contido Imediatamente	P4

## 7. Recomendações (80/20)

Ação	Esforço	Impacto	Tipo
Ativar WAF permanentemente em blocking	Médio	Alto	Permanente
Integrar SIEM para correlação de logs (ex.: Splunk, ELK)	Médio	Alto	Permanente
Criar playbooks de resposta rápida	Baixo	Médio	Permanente
Atualizar CRS e ModSecurity	Baixo	Alto	Permanente
Atualizar regras CRS regularmente Treinar equipe contra falsos positivos	Médio	Médio	Permanente

Próximos passos: dashboards, KPIs de segurança, ampliar para OWASP Top 10

- Testar ataques mais complexos (ex.: blind SQLi, XSS persistente).
- Ajustar regras para reduzir falsos positivos em produção.
- Automatizar resposta a incidentes com integração a ferramentas de orquestração.
- Implementar dashboard de monitoramento para visualização em tempo real.

## 8. Conclusão

O ambiente demonstrou **madureza operacional básica** na defesa contra ataques web comuns. O WAF foi eficaz na detecção e bloqueio de SQLi e XSS, com logs detalhados para análise forense. O plano de resposta a incidentes baseado no NIST permitiu classificar adequadamente os eventos ocorridos.

- Pontos fortes: Detecção, bloqueio, logs, logging estruturado.

- A melhorar: tuning contínuo, integração com SIEM.

## Anexos

Configs, logs, scripts, prints, evidências, políticas.

## Scripts:

SQL Injection (id=1' OR '1'='1'--).

XSS (<script>alert("XSS")</script>).

## Prints:

The first screenshot shows the initial configuration of the `waf_modsec` container. The log output includes the OWASP CRS ruleset version (4.17.1), the detected JavaScript method, and the inbound anomaly score (20). The container's memory usage is 49.96 MB and CPU usage is 6.58%.

The second screenshot shows the container's response to a request. The log output includes the request headers, the response headers, and the response body. The response body contains a 403 Forbidden status and a message indicating that the inbound anomaly score exceeded the total score of 20.

The third screenshot shows the container's response to a request. The log output includes the request headers, the response headers, and the response body. The response body contains a 403 Forbidden status and a message indicating that the inbound anomaly score exceeded the total score of 20.







## EVIDÊNCIAS TÉCNICAS

### Incidente SQLi (INC-20250917-001A)

Dados Técnicos:

- Source IP: 192.168.35.11
- URI: /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit
- HTTP Status: 403 (Bloqueado)
- Regra Acionada: 942100 - SQL Injection via libinjection
- Score de Anomalia: 5

### Incidente XSS (INC-20250917-001B)

Dados Técnicos:

- Source IP: 192.168.35.11
- URI: /vulnerabilities/xss\_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E
- HTTP Status: 403 (Bloqueado)
- Regras Acionadas: 941100, 941110, 941160, 941390
- Score de Anomalia: 20

## Glossario e Apêndice

Glossario (Termos e Definições)

Termo / Sigla	Definição
WAF	Web Application Firewall.
CRS	Core Rule Set (OWASP).
SQLi	SQL Injection.
XSS	Cross-Site Scripting.
Nmap	Scanner de portas e serviços.
302	HTTP redirect temporário – em detecção sem bloqueio.
403	HTTP Forbidden – bloqueio ativo pelo WAF.
CIA	Confidencialidade, Integridade, Disponibilidade.
NIST IR	Ciclo NIST: Detecção, Análise, Contenção, Erradicação, Recuperação.

Apêndice (Políticas NIST IR)

Categorias de Incidentes

Categoria	Descrição	Exemplo
CAT-01	Ataques Web Application	SQLi, XSS, LFI/RFI
CAT-02	Ataques de Rede	DDoS, Port Scanning
CAT-03	Acesso Não Autorizado	Bruteforce, Credential Stuffing
CAT-04	Vazamento de Dados	Exfiltração de informações sensíveis

Matriz de Urgência

Critério	Baixa	Média	Alta
Propagação	Isolado	Limitado	Em expansão
Impacto Negócio	Mínimo	Moderado	Severo
Exposição Legal	Nenhuma	Potencial	Imediata

Níveis de Severidade

Nível	Impacto	Exemplo
SEV-1 - Crítico	Comprometimento total do sistema	RCE, Data Breach em larga escala
SEV-2 – Alto	Comprometimento parcial	SQLi bem-sucedido, acesso a dados
SEV-3 – Médio	Tentativa de ataque bloqueada	SQLi/XSS bloqueados pelo WAF
SEV-4 - Baixo	Atividade suspeita	Scanning, tentativas leves

Matriz de Impacto CIA

Dimensão	Baixo	Médio	Alto
Confidencialidade	Dados públicos	Dados internos	Dados sensíveis/PII
Integridade	Alteração não crítica	Alteração parcial	Alteração crítica
Disponibilidade	Interrupção < 1h	Interrupção 1-4h	Interrupção > 4h

Matriz de Priorização

Severidade	Urgência Baixa	Urgência Média	Urgência Alta
SEV-1	P2	P1	P1 (Crítico)
SEV-2	P3	P2	P1
SEV-3	P4	P3	P2
SEV-4	P5	P4	P3

