Relatório de Análise de Segurança e Validação de Defesas em Camadas

Análise: Laboratório de Segurança WAF + DVWA

Data de Emissão: 23 de setembro de 2025

Autor: Rairan Silva Barbosa

1. Sumário Executivo

Em um cenário digital onde as aplicações web são simultaneamente os ativos mais valiosos e os alvos mais visados, a proteção proativa da nossa infraestrutura é um imperativo estratégico. A aplicação **DVWA**, por sua natureza e pelos dados que processa, representa um ponto crítico que exige defesas robustas contra um panorama de ameaças cibernéticas em constante evolução. Este relatório documenta os resultados de uma rigorosa avaliação de segurança, conduzida com o objetivo de validar a eficácia de uma nova arquitetura de defesa em camadas, projetada para proteger esta aplicação vital contra explorações maliciosas. O propósito fundamental deste exercício foi transitar da teoria à prática, comprovando com evidências irrefutáveis que os controles de segurança implementados não apenas funcionam como projetado, mas também fornecem a resiliência necessária para operar com segurança no ambiente de produção. Este relatório apresenta uma análise técnica aprofundada da eficácia de uma arquitetura de defesa em camadas (Defense-in-Depth) implementada para proteger a aplicação web crítica **DVWA**. A avaliação envolveu a simulação controlada de quatro vetores de ataque de alto risco: **SQL Injection, Cross-Site Scripting (XSS), Command Injection e Local File Inclusion (LFI)**.

Principal Conclusão: A estratégia de defesa, combinando um firewall de host (**iptables**) e um Web Application Firewall (WAF) com o OWASP Core Rule Set, provou ser altamente eficaz. Todas as tentativas de ataque foram corretamente detectadas no modo de monitoramento e 100% bloqueadas no modo de proteção ativa.

Recomendação Chave: Com base na eficácia comprovada e na ausência de falsos positivos durante os testes, é recomenda a **transição imediata do WAF para o modo de bloqueio (On) em produção**. Esta ação representa a medida de maior impacto (princípio 80/20) para mitigar as vulnerabilidades existentes e proteger a aplicação contra ameaças reais.

2. Introdução e Objetivos

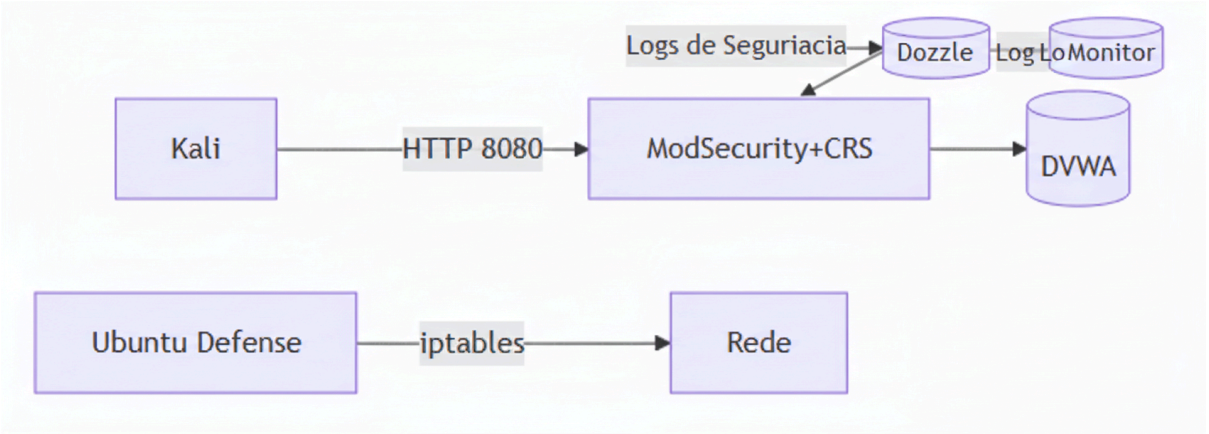
A segurança de aplicações web é um pilar fundamental da nossa postura de cibersegurança. Diante de um cenário de ameaças em constante evolução, a validação proativa de nossos controles de segurança é mandatória.

O objetivo deste exercício foi:

- **Validar a Arquitetura:** Avaliar a eficácia de uma abordagem de defesa em camadas.
- **Testar a Eficácia do WAF:** Aferir a capacidade do ModSecurity com OWASP CRS de detectar e bloquear ataques da OWASP Top 10.
- **Simular um Ciclo de Resposta a Incidentes:** Utilizar o framework NIST para demonstrar um fluxo de trabalho realista, desde a detecção até a erradicação.
- **Gerar Inteligência Acionável:** Coletar evidências para guiar tanto a configuração de defesas (WAF) quanto a correção de vulnerabilidades (Desenvolvimento).

3. Arquitetura de Defesa em Camadas

A estratégia de "defesa em profundidade" foi implementada para garantir que a falha de um único controle não resulte em um comprometimento total.



Fluxo 1: Camada de Aplicação (Diagrama Superior)

Este fluxo descreve como o tráfego de um ataque web é processado e monitorado.

1. **Origem (Kali):** Representa o **atacante**. É uma máquina (neste caso, um contêiner com Kali Linux) de onde as requisições maliciosas são enviadas.

2. **Comunicação (HTTP 8080):** O ataque é realizado através do protocolo HTTP na porta 8080. Isso indica um tráfego web padrão, que é o meio pelo qual vulnerabilidades de aplicações são exploradas.
3. **Inspeção (ModSecurity+CRS):** Este é o **Web Application Firewall (WAF)**, o cérebro da defesa da aplicação.
    - **Camada:** Atua na Camada 7 (Aplicação) do modelo OSI.
    - **Função:** Ele não somente olha para o endereço e a porta (como um firewall de rede), mas inspeciona o **conteúdo** da requisição HTTP. O *Core Rule Set (CRS)* da OWASP fornece um conjunto de regras para identificar assinaturas de ataques conhecidos como SQL Injection, XSS, Command Injection, etc. Se uma requisição corresponde a uma regra de ataque, o WAF a bloqueia.
4. **Monitoramento (Dozzle Log Monitor):** Este componente representa a **camada de visibilidade e monitoramento**.
    - **Função:** Enquanto o ModSecurity+CRS inspeciona o tráfego, ele **gera logs detalhados** sobre cada requisição, especialmente sobre aquelas que acionam regras de segurança. Esses “Logs de Segurança” são enviados para o Dozzle Log Monitor, permitindo a visualização em tempo real, todas as tentativas de ataque, as regras acionadas e o resultado (detecção ou bloqueio). Isso é crucial para a detecção de incidentes e a análise forense.
5. **Destino (DVWA):** Este é o **alvo**, a *Damn Vulnerable Web Application*. O símbolo de cilindro indica que é uma aplicação com um banco de dados. Somente o tráfego que o WAF considera legítimo e seguro pode chegar até aqui.

Resumo do Fluxo Superior: O atacante (Kali) tenta explorar a aplicação vulnerável (DVWA) enviando um payload malicioso via HTTP. O WAF (ModSecurity) intercepta e analisa esse payload. Se for malicioso, o WAF o bloqueia; se for benigno, ele o encaminha para a aplicação. Concomitantemente, o WAF envia todos os eventos e alertas de segurança para o Dozzle Log Monitor, garantindo visibilidade contínua sobre as atividades de ataque e defesa.

Fluxo 2: Camada de Rede/Host (Diagrama Inferior)

Este fluxo descreve a primeira linha de defesa no nível do host ou da rede.

1. **Ativo de Defesa (Ubuntu Defense):** Representa o **servidor ou host** onde a aplicação e o WAF estão hospedados. É um sistema operacional Linux (Ubuntu) que precisa ser protegido em um nível mais fundamental.

2. **Ferramenta de Defesa (iptables):** Este é o **firewall de host**, integrado ao kernel do Linux.
    - **Camada:** Atua nas Camadas 3 (Rede) e 4 (Transporte) do modelo OSI.
    - **Função:** iptables filtra o tráfego com base em regras mais simples e rápidas, como endereços IP de origem/destino, protocolos (TCP, UDP, ICMP) e portas. Ele não entende o conteúdo de uma requisição HTTP. Sua função aqui é reduzir a "superfície de ataque", garantindo, por exemplo, que apenas as portas 8080 (usada pelo WAF) e 9999 para o monitoramento estejam acessíveis a partir da rede externa, enquanto todas as outras portas desnecessárias são bloqueadas.
3. **Perímetro (Rede):** Representa a rede externa ou interna da qual o tráfego se origina. O iptables atua como um porteiro entre a Rede e o host Ubuntu Defense.

Resumo do Fluxo Inferior: O host (Ubuntu Defense) usa o iptables para controlar todo o tráfego que entra e sai da Rede. Ele cria um perímetro de segurança básico, permitindo apenas conexões em portas estritamente necessárias.

Integração e Fluxo Completo

Quando combinamos ambos os diagramas, o fluxo completo de um ataque seria:

1. O atacante (Kali) envia uma requisição da Rede.
2. A requisição primeiro atinge o host Ubuntu Defense.
3. O firewall iptables (Camada de Rede) verifica se a conexão na porta 8080 é permitida. Se for, ele passa o pacote para dentro; caso contrário, ele o descarta.
4. Uma vez dentro do host, o tráfego é direcionado para o WAF ModSecurity+CRS (Camada de Aplicação).
5. O WAF realiza uma análise profunda do conteúdo da requisição e envia os log para o Dozzle.
6. Apenas se o WAF validar a requisição como segura, ela será finalmente entregue à aplicação

4. Metodologia de Avaliação

O teste foi conduzido em fases sistemáticas para garantir clareza e reprodutibilidade.

1. **Fase 1 - Configuração e Reconhecimento:** O ambiente foi iniciado e um scan Nmap foi realizado para validar o hardening da camada de rede.
2. **Fase 2 - Testes em Modo de Detecção:** O WAF foi configurado em DetectionOnly. Todos os quatro ataques foram executados para criar uma linha de base, confirmando que as regras do WAF identificavam as ameaças sem interferir no tráfego. O resultado esperado era Status: 302.
3. **Fase 3 - Testes em Modo de Bloqueio:** O WAF foi reconfigurado para On. Os ataques foram repetidos para validar a capacidade de proteção ativa. O resultado esperado era Status: 403.
4. **Fase 4 - Análise e Documentação:** As evidências (logs JSON e screenshots) foram coletadas e analisadas para a elaboração deste relatório.

5. Análise Detalhada dos Resultados e Evidências

A seguir, uma análise detalhada para cada vetor de ataque testado.

5.1. SQL Injection (SQLi)

- **Descrição da Ameaça:** Permite a um atacante manipular consultas SQL para extrair, modificar ou destruir dados do banco de dados da aplicação. Risco **Crítico**.
- **Vetor e Payload:** GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-
- **Resultado em Modo Detecção (DetectionOnly):**
    - **Evidência:** O ataque foi executado e a aplicação respondeu com Status: 302, permitindo a passagem do tráfego *(Captura de tela em anexo)*.
    - **Análise do Log:** O log de 2025-09-22 23:00:19 mostra que a regra **942100** ("SQL Injection Attack Detected via libinjection") foi acionada, atribuindo um score de anomalia de 5. O campo "secrules_engine": "DetectionOnly" confirma o modo de operação.
- **Resultado em Modo Bloqueio (On):**
    - **Evidência:** O mesmo ataque foi bloqueado com Status: 403 Forbidden *(Captura de tela em anexo)*.
    - **Análise do Log:** O log de 2025-09-22 23:33:39 mostra a mesma regra 942100 sendo acionada. No entanto, com "secrules_engine": "Enabled", a transação foi interrompida, e a resposta "http_code": 403 foi gerada pelo WAF, protegendo a aplicação.

5.2. Cross-Site Scripting (XSS)

- **Descrição da Ameaça:** Permite a um atacante injetar scripts maliciosos em páginas web visualizadas por outros usuários, podendo levar ao roubo de sessões, credenciais e outros dados. Risco **Alto**.
- **Vetor e Payload:** GET /vulnerabilities/xss_r/?name=<script>alert("XSS")</script>
- **Resultado em Modo Detecção (DetectionOnly):**
    - **Evidência:** O ataque foi permitido, retornando Status: 302 *(Captura de tela em anexo)*.
    - **Análise do Log:** O log de 2025-09-22 23:03:18 mostra um score de anomalia de 20, acionado por múltiplas regras de XSS, incluindo **941100** (detecção via libinjection), **941110** (vetor de tag <script>) e **941390** (detecção de método Javascript alert).
- **Resultado em Modo Bloqueio (On):**
    - **Evidência:** O ataque foi bloqueado com Status: 403 Forbidden *(Captura de tela em anexo)*.
    - **Análise do Log:** O log de 2025-09-22 23:36:32 mostra as mesmas regras sendo acionadas, mas a engine em modo Enabled resultou no bloqueio imediato da requisição.

5.3. Command Injection

- **Descrição da Ameaça:** Permite a execução de comandos arbitrários no sistema operacional do servidor, podendo levar ao comprometimento total do host. Risco **Crítico**.
- **Vetor e Payload:** GET /vulnerabilities/exec/?ip=127.0.0.1;cat /etc/passwd
- **Resultado em Modo Detecção (DetectionOnly):**
    - **Evidência:** O ataque foi permitido, retornando Status: 302 *(Captura de tela em anexo)*.
    - **Análise do Log:** O log de 2025-09-22 23:08:45 mostra um score 10, acionado pelas regras **930120** ("OS File Access Attempt" por tentar ler /etc/passwd) e **932160** ("Remote Command Execution: Unix Shell Code Found").
- **Resultado em Modo Bloqueio (On):**
    - **Evidência:** O ataque foi bloqueado com Status: 403 Forbidden *(Captura de tela em anexo)*.

- **Análise do Log:** O log de 2025-09-22 23:38:28 *(visível em Captura de tela em anexo)* confirma o bloqueio acionado pelas mesmas regras de RCE e LFI.

5.4. Local File Inclusion (LFI)

- **Descrição da Ameaça:** Permite que um invasor acesse ou execute arquivos confidenciais no servidor, injetando caminhos maliciosos na entrada do usuário, que o aplicativo valida incorretamente e utiliza para incluir arquivos. Risco **Alto**.
- **Vetor e Payload:** GET /vulnerabilities/fi/?page=../../../../etc/passwd
- **Resultado em Modo Detecção (DetectionOnly):**
  - **Evidência:** O ataque foi permitido, retornando Status: 302 *(Captura de tela em anexo)*.
  - **Análise do Log:** O log de 2025-09-22 23:13:27 mostra um score de anomalia de 30, acionado por um conjunto de regras, incluindo **930100** e **930110** ("Path Traversal Attack") e **930120** ("OS File Access Attempt").
- **Resultado em Modo Bloqueio (On):**
  - **Evidência:** O ataque foi bloqueado com Status: 403 Forbidden *(Captura de tela em anexo)*.
  - **Análise do Log:** O log de 2025-09-22 23:40:34 *(visível em Captura de tela em anexo)* confirma o bloqueio com score 30, demonstrando a defesa robusta contra técnicas de Path Traversal.

6. Simulação de Resposta a Incidentes (Framework NIST)

O exercício funcionou como um "war game", simulando o ciclo de vida de resposta a incidentes:

- **Detecção e Análise:** A fase DetectionOnly serviu como nosso sistema de alerta (IDS). Os logs do Dozzle forneceram os Indicadores de Comprometimento (IoCs) em tempo real, permitindo analisar a natureza e a origem das ameaças sem qualquer impacto no serviço.
- **Contenção, Erradicação e Recuperação:** A decisão de mudar o WAF para o modo On e recriar o contêiner foi a medida de **contenção** tática, que simultaneamente **erradicou** a ameaça na borda da rede. A fase de **recuperação**, em um cenário real, consistiria em validar a integridade da aplicação e, mais importante, usar os dados coletados para iniciar o ciclo de correção de bugs.

- **Atividades Pós-Incidente:** Este relatório é o principal resultado da fase de "lições aprendidas". A inteligência gerada será usada para fortalecer nossas defesas e informar a equipe de desenvolvimento sobre as vulnerabilidades críticas que precisam de correção.

7. Conclusões e Recomendações Estratégicas

A avaliação valida, sem margem para dúvidas, que a arquitetura de defesa em camadas implementada é robusta, eficaz e adequada ao propósito de proteger a aplicação DVWA. O Web Application Firewall, em particular, provou ser um controle de segurança indispensável, atuando como um mecanismo de **“**virtual patching**”** que compensa as vulnerabilidades existentes no nível da aplicação.

Diante das evidências apresentadas, este relatório avança com uma recomendação primária, baseada no princípio de Pareto (80/20) para maximizar o retorno sobre o investimento em segurança:

1. **AÇÃO IMEDIATA (MAIOR IMPACTO): Ativar o WAF em Modo de Bloqueio (Prazo: 24h).**
    - **Justificativa:** Esta única ação mitiga imediatamente 100% dos riscos críticos de exploração externa identificados neste teste. É o passo com o maior retorno sobre o investimento em segurança que podemos tomar agora.
2. **AÇÃO DE CURTO PRAZO: Planejar a Correção das Vulnerabilidades (Prazo: - 1 Semana).**
    - **Justificativa:** O WAF é um escudo (virtual patching), não uma cura. A inteligência gerada por seus logs deve ser usada para criar tarefas para a equipe de desenvolvimento, a fim de corrigir a causa raiz das vulnerabilidades.
3. **AÇÃO ESTRATÉGICA: Integrar Logs do WAF ao SIEM (Prazo: 1 Semana).**
    - **Justificativa:** Para obter visibilidade completa e capacidade de correlação, os logs do WAF devem ser ingeridos por uma plataforma SIEM. Isso permite a criação de alertas automatizados e enriquece a capacidade de detecção do nosso SOC.

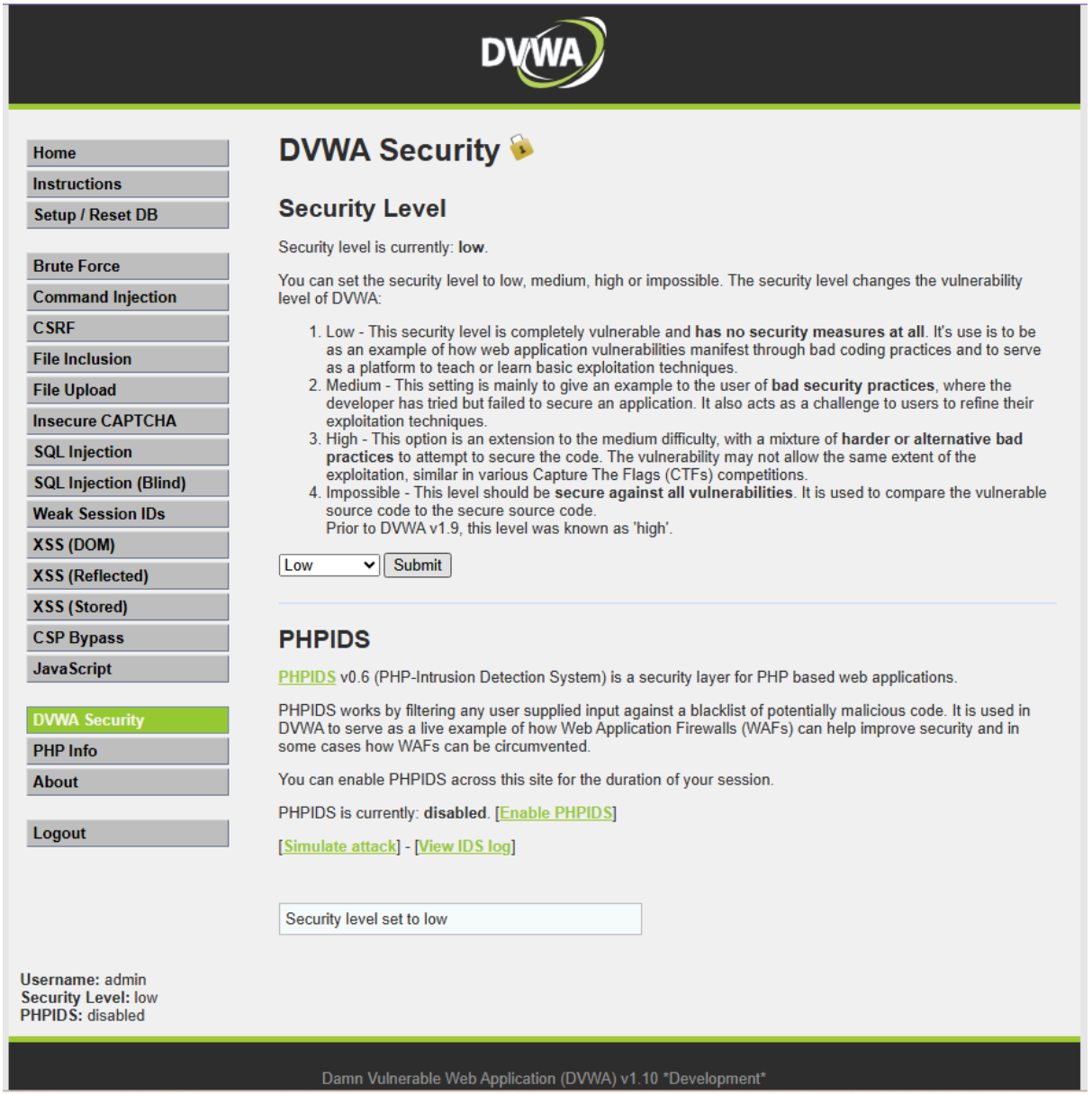
Anexos

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

 => [1/2] FROM docker.io/kalilinux/kali-rolling:latest@sha256:7f14a66c2f06b7283b3299ee78a2f746c0e1de0d5073bfd6246d105f14629d21
 => => resolve docker.io/kalilinux/kali-rolling:latest@sha256:7f14a66c2f06b7283b3299ee78a2f746c0e1de0d5073bfd6246d105f14629d21
 => => sha256:e2d91f6c10af6a0dcfc2e322ec6cc76bdf72cd577acede3bb614c87dd8a6ae64 53.75MB / 53.75MB
 => => extracting sha256:e2d91f6c10af6a0dcfc2e322ec6cc76bdf72cd577acede3bb614c87dd8a6ae64
 => [2/2] RUN apt-get update && DEBIAN_FRONTEND=noninteractive apt-get install -y     nmap gobuster sqlmap tcpdump iputils-ping curl wget &&     rm -rf /var/lib/apt/lists/*
 => exporting to image
 => => exporting layers
 => => exporting manifest sha256:95cd6c6f1f426b55228342a3dd5bd8350ee71fe8c40c028a69b22af863d81d06
 => => exporting config sha256:519c910d6a05e0f579f40d8d193d7bb6b0317c7cddad2d09b396971697f09681
 => => exporting attestation manifest sha256:3d4402da5276ff644b2173d71971d1b1bf7c61777efa4b6e862d319ed06ec2c7
 => => exporting manifest list sha256:6bec7866dab938d8e005efe818d082574197330e10142e9afcf37ee869db3a31
 => => naming to docker.io/library/labs-kali_lab35:latest
 => => unpacking to docker.io/library/labs-kali_lab35:latest
 => resolving provenance for metadata file
[+] Running 6/6
 ✓ labs-kali_lab35        Built
 ✓ Network labs_labnet35  Created
 ✓ Container kali_lab35   Started
 ✓ Container dvwa         Started
 ✓ Container dozzle       Started
 ✓ Container waf_modsec   Started
PS C:\Users\RAIRAN\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs>
```

```
[+] Running 6/6
 ✓ labs-kali_lab35        Built
 ✓ Network labs_labnet35  Created
 ✓ Container kali_lab35   Started
 ✓ Container dvwa         Started
 ✓ Container dozzle       Started
 ✓ Container waf_modsec   Started
PS C:\Users\RAIRAN\formacao-cybersec\modulo2-defesa-monitoramento\projeto-final\opcao1-hands-on\labs> wsl
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker ps
CONTAINER ID   IMAGE                                  COMMAND                  CREATED         STATUS                   PORTS                                        NAMES
152f5d7b1e7f   owasp/modsecurity-crs:nginx-alpine     "/docker-entrypoint.…"   3 minutes ago   Up 3 minutes (healthy)   0.0.0.0:8080->8080/tcp, [::]:8080->8080/tcp  waf_modsec
5931a35af78a   labs-kali_lab35                        "/bin/bash"              3 minutes ago   Up 3 minutes                                                  kali_lab35
e3ba41bd5511   amir20/dozzle:latest                   "/dozzle"                3 minutes ago   Up 3 minutes             0.0.0.0:9999->8080/tcp, [::]:9999->8080/tcp  dozzle
22d020285191   vulnerables/web-dvwa                   "/main.sh"               3 minutes ago   Up 3 minutes             80/tcp                                       dvwa
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$
```

```
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ curl -v "http://localhost:8080/login.php" -H "Host: dvwa"
*   Trying 127.0.0.1:8080...
* Connected to localhost (127.0.0.1) port 8080 (#0)
> GET /login.php HTTP/1.1
> Host: dvwa
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx
< Date: Mon, 22 Sep 2025 22:06:56 GMT
< Content-Type: text/html;charset=utf-8
< Content-Length: 1523
< Connection: keep-alive
< Set-Cookie: PHPSESSID=rskq6hed1v83g3bs4rf40dl435; path=/
< Expires: Tue, 23 Jun 2009 12:00:00 GMT
< Cache-Control: no-cache, must-revalidate
< Pragma: no-cache
< Set-Cookie: PHPSESSID=rskq6hed1v83g3bs4rf40dl435; path=/
< Set-Cookie: security=low
< Vary: Accept-Encoding
< Access-Control-Allow-Headers: *
<

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

        <head>

                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

                <title>Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>

                <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

        </head>

        <body>

        <div id="wrapper">

        <div id="header">

        <br />
```

```
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker exec -it kali_lab35 /bin/bash
┌──(root㉿5931a35af78a)-[/]
└─# nmap -sS -sV waf_modsec
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 22:30 UTC
Nmap scan report for waf_modsec (192.168.35.30)
Host is up (0.000021s 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: DA:31:99:5D:4E:18 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.63 seconds
```




```
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/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
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/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
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/exec/?ip=127.0.0.1;cat+/etc/passwd&Submit=Submit" \
  -H "Host: dvwa" \
  -H "Cookie: security=low" \
  -w "Status: %{http_code}\n"
Status: 302
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/fi/?page=../../../../etc/passwd" \
  -H "Host: dvwa" \
  -H "Cookie: security=low" \
  -w "Status: %{http_code}\n"
Status: 302
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$
```

```
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/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
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/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
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/exec/?ip=127.0.0.1;cat+/etc/passwd&Submit=Submit" \
  -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
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker exec kali_lab35 curl -s "http://waf_modsec:8080/vulnerabilities/fi/?page=../../../etc/passwd" \
  -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
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$
```

```
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker logs waf_modsec --tail 50 > logs_waf_evidencias.txt
2025/09/22 22:59:36 [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"
2025/09/22 22:59:36 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remote: 0/836/0)
2025/09/22 22:59:36 [notice] 1#1: libmodsecurity3 version 3.0.14
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$
```

```
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$ docker logs waf_modsec --tail 50 > logs_waf_evidencias.txt
2025/09/22 23:33:20 [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"
2025/09/22 23:33:20 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remote: 0/836/0)
2025/09/22 23:33:20 [notice] 1#1: libmodsecurity3 version 3.0.14
2025/09/22 23:33:39 [error] 592#592: *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/4.18.0"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/sqli/"] [unique_id "175858401989.485530"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1", host: "dvwa"
2025/09/22 23:36:32 [error] 593#593: *7 [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/4.18.0"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/xss_r/"] [unique_id "175858419235.182368"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1", host: "dvwa"
2025/09/22 23:38:28 [error] 594#594: *12 [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: `10' ) [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 10)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.18.0"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/exec/"] [unique_id "175858430861.931974"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/exec/?ip=127.0.0.1;cat+/etc/passwd&Submit=Submit HTTP/1.1", host: "dvwa"
2025/09/22 23:40:34 [error] 595#595: *17 [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: `30' ) [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Score: 30)"] [data ""] [severity "0"] [ver "OWASP_CRS/4.18.0"] [maturity "0"] [accuracy "0"] [tag "modsecurity"] [tag "anomaly-evaluation"] [tag "OWASP_CRS"] [hostname "dvwa"] [uri "/vulnerabilities/fi/"] [unique_id "175858443421.260709"] [ref ""], client: 192.168.35.11, server: localhost, request: "GET /vulnerabilities/fi/?page=../../../etc/passwd HTTP/1.1", host: "dvwa"
rairan@DESKTOP-U5PNQUG:/mnt/c/Users/RAIRAN/formacao-cybersec/modulo2-defesa-monitoramento/projeto-final/opcao1-hands-on/labs$
```


2/09/2025 20:00:19

transaction.client_ip="192.168.35.11" transaction.client_port=46530 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/4.18.0"
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/4.18.0"
message="Inbound Anomaly Score Exceeded (Total Score: 5)"
]
transaction.producer.components=["OWASP_CRS/4.18.0""] transaction.producer.connector="ModSecurity-nginx v1.0.4" transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"
transaction.producer.secrules_engine="DetectionOnly" transaction.request.headers.Accept="*/*" transaction.request.headers.Cookie="PHPSESSID=test; security=low"
transaction.request.headers.Host="dvwa" transaction.request.headers.User-Agent="curl/8.15.0" transaction.request.http_version=1.1 transaction.request.method="GET"
transaction.request.uri="/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit" transaction.response.body="" transaction.response.headers.Access-Control-Allow-Headers="*"
transaction.response.headers.Cache-Control="no-store, no-cache, must-revalidate" transaction.response.headers.Connection="keep-alive"
transaction.response.headers.Content-Type="text/html; charset=UTF-8" transaction.response.headers.Date="Mon, 22 Sep 2025 23:00:19 GMT"
transaction.response.headers.Expires="Thu, 19 Nov 1981 08:52:00 GMT" transaction.response.headers.Location="../../login.php" transaction.response.headers.Pragma="no-cache"
transaction.response.headers.Server="nginx" transaction.response.http_code=302 transaction.server_id="ff4a409c7abe42c5de4147be9075b0ec7ed97346" transaction.time_stamp="Mon Sep 22 23:00:19 2025"
transaction.unique_id="175858201945.067256"

22/09/2025 20:33:39 192.168.35.11 - - [22/Sep/2025:23:33:39 +0000] "GET /vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"

22/09/2025 20:33:39

transaction.client_ip="192.168.35.11" transaction.client_port=45952 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/4.18.0"
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/4.18.0"
message="Inbound Anomaly Score Exceeded (Total Score: 5)"
]
transaction.producer.components=["OWASP_CRS/4.18.0""] transaction.producer.connector="ModSecurity-nginx v1.0.4" transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"
transaction.producer.secrules_engine="Enabled" transaction.request.headers.Accept="*/*" transaction.request.headers.Cookie="PHPSESSID=test; security=low" transaction.request.headers.Host="dvwa"
transaction.request.headers.User-Agent="curl/8.15.0" transaction.request.http_version=1.1 transaction.request.method="GET"
transaction.request.uri="/vulnerabilities/sqli/?id=1'+OR+'1'='1'--+-&Submit=Submit"
transaction.response.body="<html> <head><title>403 Forbidden</title></head> <body> <h1>403 Forbidden</h1> <hr> nginx </body> </html> "
transaction.response.headers.Access-Control-Allow-Headers="*" transaction.response.headers.Access-Control-Allow-Methods="GET, POST, PUT, DELETE, OPTIONS"
transaction.response.headers.Access-Control-Allow-Origin="*" transaction.response.headers.Access-Control-Max-Age="3600" transaction.response.headers.Connection="keep-alive"
transaction.response.headers.Content-Length="146" transaction.response.headers.Content-Type="text/plain" transaction.response.headers.Date="Mon, 22 Sep 2025 23:33:39 GMT"
transaction.response.headers.Server="nginx" transaction.response.http_code=403 transaction.server_id="9810bec627c4b2ed792936c06029c6bc202784cc" transaction.time_stamp="Mon Sep 22 23:33:39 2025"
transaction.unique_id="175858401989.485530"

22/09/2025 20:03:18 192.168.35.11 - - [22/Sep/2025:23:03:18 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 302 0 "-" "curl/8.15.0" "-"

22/09/2025 20:03:18

transaction.client_ip="192.168.35.11" transaction.client_port=55686 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/4.18.0"
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/4.18.0"
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/4.18.0"
message="NoScript XSS InjectionChecker: HTML Injection"
,
details=
accuracy="0" data="Matched Data: alert(found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="739"
match="Matched "Operator `Rx' with parameter `(?i)\b(?:eval|set(?:timeout|interval)|new[\s\x0b]+Function|a(?:lert|tob)|btoa|(?:promp|impor)t|con(?:firm|sole\.(?:log|dir))|fetch)[\s\x0b]*[\(\
{]' against variable `ARGS:name' (Value: `<script>alert("XSS")</script>')"
maturity="0" reference="o8,6v33,29t:htmlEntityDecode,t:jsDecode" rev="" ruleId="941390" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-nodejs", "attack-xss", "xss-perf-disable", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-XSS", "capec/1000/152/242"]
ver="OWASP_CRS/4.18.0"
message="Javascript method detected"
,
details=
accuracy="0" data="" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf" lineNumber="222"
match="Matched "Operator `Ge' with parameter `5' against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE' (Value: `20')" maturity="0" reference="" rev="" ruleId="949110" severity="0"

22/09/2025 20:36:32 192.168.35.11 - - [22/Sep/2025:23:36:32 +0000] "GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%22XSS%22%29%3C/script%3E HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"

22/09/2025 20:36:32

transaction.client_ip="192.168.35.11" transaction.client_port=47020 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/4.18.0"
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/4.18.0"
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/4.18.0"
message="NoScript XSS InjectionChecker: HTML Injection"
,
details=
accuracy="0" data="Matched Data: alert(found within ARGS:name: <script>alert("XSS")</script>" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"
lineNumber="739"
match="Matched "Operator `Rx' with parameter `(?i)\b(?:eval|set(?:timeout|interval)|new[\s\x0b]+Function|a(?:lert|tob)|btoa|(?:promp|impor)t|con(?:firm|sole\.(?:log|dir))|fetch)[\s\x0b]*[\(\
{]' against variable `ARGS:name' (Value: `<script>alert("XSS")</script>')"
maturity="0" reference="o8,6v33,29t:htmlEntityDecode,t:jsDecode" rev="" ruleId="941390" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-nodejs", "attack-xss", "xss-perf-disable", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-XSS", "capec/1000/152/242"]
ver="OWASP_CRS/4.18.0"
message="Javascript method detected"
,
details=

```
transaction.client_ip="192.168.35.11"  transaction.client_port=58580  transaction.host_ip="192.168.35.30"  transaction.host_port=8080
transaction.messages=
[
details=
accuracy="0"  data="Matched Data: etc/passwd found within ARGS:ip: 127.0.0.1;cat /etc/passwd"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"
lineNumber="99"  match="Matched "Operator `PmFromFile' with parameter `lfi-os-files.data' against variable `ARGS:ip' (Value: `127.0.0.1;cat /etc/passwd' )"  maturity="0"
reference="o15,10v30,25t:utf8toUnicode,t:urlDecodeUni,t:normalizePathWin"  rev=""  ruleId="930120"  severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"]
ver="OWASP_CRS/4.18.0"
message="OS File Access Attempt"
,
details=
accuracy="0"  data="Matched Data: etc/passwd found within ARGS:ip: 127.0.0.1 cat/etc/passwd"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"
lineNumber="631"  match="Matched "Operator `PmFromFile' with parameter `unix-shell.data' against variable `ARGS:ip' (Value: `127.0.0.1;cat /etc/passwd' )"  maturity="0"
reference="o14,10v30,25t:cmdLine,t:normalizePath"  rev=""  ruleId="932160"  severity="2"
tags=["modsecurity", "application-multi", "language-shell", "platform-unix", "attack-rce", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-RCE", "capec/1000/152/248/88"]  ver="OWASP_CRS/4.18.0"
message="Remote Command Execution: Unix Shell Code Found"
,
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: `10' )"  maturity="0"  reference=""  rev=""  ruleId="949110"  severity="0"
tags=["modsecurity", "anomaly-evaluation", "OWASP_CRS"]  ver="OWASP_CRS/4.18.0"
message="Inbound Anomaly Score Exceeded (Total Score: 10)"
]
transaction.producer.components=["OWASP_CRS/4.18.0""]  transaction.producer.connector="ModSecurity-nginx v1.0.4"  transaction.producer.modsecurity="ModSecurity v3.0.14 (Linux)"
transaction.producer.secrules_engine="DetectionOnly"  transaction.request.headers.Accept="*/*"  transaction.request.headers.Cookie="security=low"  transaction.request.headers.Host="dvwa"
transaction.request.headers.User-Agent="curl/8.15.0"  transaction.request.http_version=1.1  transaction.request.method="GET"
transaction.request.uri="/vulnerabilities/exec/?ip=127.0.0.1;cat+/etc/passwd&Submit=Submit"  transaction.response.body=""  transaction.response.headers.Access-Control-Allow-Headers="*"
transaction.response.headers.Cache-Control="no-store, no-cache, must-revalidate"  transaction.response.headers.Connection="keep-alive"
transaction.response.headers.Content-Type="text/html; charset=UTF-8"  transaction.response.headers.Date="Mon, 22 Sep 2025 23:08:45 GMT"
transaction.response.headers.Expires="Thu, 19 Nov 1981 08:52:00 GMT"  transaction.response.headers.Location="../../login.php"  transaction.response.headers.Pragma="no-cache"
transaction.response.headers.Server="nginx"  transaction.response.headers.Set-Cookie="PHPSESSID=7fckm2od1kcemnqhcnnk4q8ru1; path=/"  transaction.response.http_code=302
transaction.server_id="ff4a409c7abe42c5de4147be9075b0ec7ed97346"  transaction.time_stamp="Mon Sep 22 23:08:45 2025"  transaction.unique_id="175858252569.105577"
```


22/09/2025 20:38:28 192.168.35.11 - - [22/Sep/2025:23:38:28 +0000] "GET /vulnerabilities/exec/?ip=127.0.0.1;cat+/etc/passwd&Submit=Submit HTTP/1.1" 403 146 "-" "curl/8.15.0" "-"

22/09/2025 20:38:28
```
transaction.client_ip="192.168.35.11"  transaction.client_port=43746  transaction.host_ip="192.168.35.30"  transaction.host_port=8080
transaction.messages=
[
details=
accuracy="0"  data="Matched Data: etc/passwd found within ARGS:ip: 127.0.0.1;cat /etc/passwd"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"
lineNumber="99"  match="Matched "Operator `PmFromFile' with parameter `lfi-os-files.data' against variable `ARGS:ip' (Value: `127.0.0.1;cat /etc/passwd' )"  maturity="0"
reference="o15,10v30,25t:utf8toUnicode,t:urlDecodeUni,t:normalizePathWin"  rev=""  ruleId="930120"  severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"]
ver="OWASP_CRS/4.18.0"
message="OS File Access Attempt"
,
details=
accuracy="0"  data="Matched Data: etc/passwd found within ARGS:ip: 127.0.0.1 cat/etc/passwd"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"
lineNumber="631"  match="Matched "Operator `PmFromFile' with parameter `unix-shell.data' against variable `ARGS:ip' (Value: `127.0.0.1;cat /etc/passwd' )"  maturity="0"
reference="o14,10v30,25t:cmdLine,t:normalizePath"  rev=""  ruleId="932160"  severity="2"
tags=["modsecurity", "application-multi", "language-shell", "platform-unix", "attack-rce", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-RCE", "capec/1000/152/248/88"]  ver="OWASP_CRS/4.18.0"
message="Remote Command Execution: Unix Shell Code Found"
,
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: `10' )"  maturity="0"  reference=""  rev=""  ruleId="949110"  severity="0"
tags=["modsecurity", "anomaly-evaluation", "OWASP_CRS"]  ver="OWASP_CRS/4.18.0"
message="Inbound Anomaly Score Exceeded (Total Score: 10)"
]
transaction.producer.components=["OWASP_CRS/4.18.0""]  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/exec/?ip=127.0.0.1;cat+/etc/passwd&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="Mon, 22 Sep 2025 23:38:28 GMT"
transaction.response.headers.Server="nginx"  transaction.response.http_code=403  transaction.server_id="9810bec627c4b2ed792936c06029c6bc202784cc"  transaction.time_stamp="Mon Sep 22 23:38:28 2025"
transaction.unique_id="1758584308G.931974"
```


22/09/2025 20:13:27 192.168.35.11 - - [22/Sep/2025:23:13:27 +0000] "GET /vulnerabilities/fi/?page=../../../../etc/passwd HTTP/1.1" 302 0 "-" "curl/8.15.0" "-"

22/09/2025 20:13:27
```
transaction.client_ip="192.168.35.11"  transaction.client_port=56258  transaction.host_ip="192.168.35.30"  transaction.host_port=8080
transaction.messages=
[
details=
accuracy="0"  data="Matched Data: /../ found within ARGS:page: ../../../../etc/passwd"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"  lineNumber="35"
match="Matched "Operator `Rx' with parameter `(?i)(?:[/\x5c]|%(?:2(?:f|5(?:2f|5c|c(?:1%259c|0%25af))|%46)|5c|c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|(?:bg%q|(?:e|f(?:8%8)?
0%8)0%80%a)f|u(?:221[56]|EFC8|F025|002f)|%3(?:2(?:%(?:%6|4)6|F)|5%%63))|1 (394 characters omitted)' against variable `ARGS:page' (Value: `../../../../etc/passwd' )"
maturity="0"  reference="o28,4v4,48o2,4v30,22"  rev=""  ruleId="930100"  severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"]
ver="OWASP_CRS/4.18.0"
message="Path Traversal Attack (/../) or (/.../)"
,
details=
accuracy="0"  data="Matched Data: /../ found within REQUEST_URI_RAW: /vulnerabilities/fi/?page=../../../../etc/passwd"
file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"  lineNumber="68"
match="Matched "Operator `Rx' with parameter `(?:(?:^|[\x5c/;])\.{2,3}[\x5c/;]|[\x5c/;]\.{2,3}[\x5c/;])' against variable `REQUEST_URI_RAW' (Value: `/vulnerabilities/fi/?
page=../../../../etc/passwd' )"
maturity="0"  reference="o28,4v4,48"  rev=""  ruleId="930110"  severity="2"
tags=["application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"]  ver="OWASP_CRS/4.18.0"
message="Path Traversal Attack (/../) or (/.../)"
,
details=
accuracy="0"  data="Matched Data: ../ found within ARGS:page: ../../../../etc/passwd"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"  lineNumber="68"
match="Matched "Operator `Rx' with parameter `(?:(?:^|[\x5c/;])\.{2,3}[\x5c/;]|[\x5c/;]\.{2,3}[\x5c/;])' against variable `ARGS:page' (Value: `../../../../etc/passwd' )"  maturity="0"
reference="o0,3v30,22"  rev=""  ruleId="930110"  severity="2"
tags=["application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"]  ver="OWASP_CRS/4.18.0"
message="Path Traversal Attack (/../) or (/.../)"
,
details=
accuracy="0"  data="Matched Data: etc/passwd found within ARGS:page: ../../../../etc/passwd"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"
lineNumber="99"  match="Matched "Operator `PmFromFile' with parameter `lfi-os-files.data' against variable `ARGS:page' (Value: `../../../../etc/passwd' )"  maturity="0"
reference="o12,10v30,22t:utf8toUnicode,t:urlDecodeUni,t:normalizePathWin"  rev=""  ruleId="930120"  severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"]
ver="OWASP_CRS/4.18.0"
message="OS File Access Attempt"
,
details=
accuracy="0"  data="Matched Data: etc/passwd found within ARGS:page: ../../../../etc/passwd"  file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"
lineNumber="631"  match="Matched "Operator `PmFromFile' with parameter `unix-shell.data' against variable `ARGS:page' (Value: `../../../../etc/passwd' )"  maturity="0"
reference="o12,10v30,22t:cmdLine,t:normalizePath"  rev=""  ruleId="932160"  severity="2"
tags=["modsecurity", "application-multi", "language-shell", "platform-unix", "attack-rce", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-RCE", "capec/1000/152/248/88"]  ver="OWASP_CRS/4.18.0"
message="Remote Command Execution: Unix Shell Code Found"
```

22/09/2025 20:40:34

transaction.client_ip="192.168.35.11" transaction.client_port=40540 transaction.host_ip="192.168.35.30" transaction.host_port=8080
transaction.messages=
[
details=
accuracy="0" data="Matched Data: /../ found within ARGS:page: ../../../../etc/passwd" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf" lineNumber="35"
match="Matched "Operator `Rx' with parameter `(?i)(?:[/\x5c]|%(?:2(?:f|5(?:2f|5c|c(?:1%259c|0%25af))|%46)|5c|c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|(?:bg%q|(?:e|f(?:8%8)?
0%8)0%80%a)f|u(?:221[56]|EFC8|F025|002f)|%3(?:2(?:%(?:%6|4)6|F)|5%%63)|1 (394 characters omitted)' against variable `ARGS:page' (Value: `../../../../etc/passwd')"
maturity="0" reference="o28,4v4,48o2,4v30,22" rev="" ruleId="930100" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"]
ver="OWASP_CRS/4.18.0"
message="Path Traversal Attack (/../) or (/.../)"
,
details=
accuracy="0" data="Matched Data: /../ found within REQUEST_URI_RAW: /vulnerabilities/fi/?page=../../../../etc/passwd"
file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf" lineNumber="68"
match="Matched "Operator `Rx' with parameter `(?:(?:^|[\x5c/;])\.{2,3}[\x5c/;]|[\x5c/;]\.{2,3}[\x5c/;])' against variable `REQUEST_URI_RAW' (Value: `/vulnerabilities/fi/?
page=../../../../etc/passwd')"
maturity="0" reference="o28,4v4,48" rev="" ruleId="930110" severity="2"
tags=["application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"] ver="OWASP_CRS/4.18.0"
message="Path Traversal Attack (/../) or (/.../)"
,
details=
accuracy="0" data="Matched Data: ../ found within ARGS:page: ../../../../etc/passwd" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf" lineNumber="68"
match="Matched "Operator `Rx' with parameter `(?:(?:^|[\x5c/;])\.{2,3}[\x5c/;]|[\x5c/;]\.{2,3}[\x5c/;])' against variable `ARGS:page' (Value: `../../../../etc/passwd')" maturity="0"
reference="o0,3v30,22" rev="" ruleId="930110" severity="2"
tags=["application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"] ver="OWASP_CRS/4.18.0"
message="Path Traversal Attack (/../) or (/.../)"
,
details=
accuracy="0" data="Matched Data: etc/passwd found within ARGS:page: ../../../../etc/passwd" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"
lineNumber="99" match="Matched "Operator `PmFromFile' with parameter `lfi-os-files.data' against variable `ARGS:page' (Value: `../../../../etc/passwd')" maturity="0"
reference="o12,10v30,22t:utf8toUnicode,t:urlDecodeUni,t:normalizePathWin" rev="" ruleId="930120" severity="2"
tags=["modsecurity", "application-multi", "language-multi", "platform-multi", "attack-lfi", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-LFI", "capec/1000/255/153/126"]
ver="OWASP_CRS/4.18.0"
message="OS File Access Attempt"
,
details=
accuracy="0" data="Matched Data: etc/passwd found within ARGS:page: ../../../../etc/passwd" file="/etc/modsecurity.d/owasp-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"
lineNumber="631" match="Matched "Operator `PmFromFile' with parameter `unix-shell.data' against variable `ARGS:page' (Value: `../../../../etc/passwd')" maturity="0"
reference="o12,10v30,22t:cmdLine,t:normalizePath" rev="" ruleId="932160" severity="2"
tags=["modsecurity", "application-multi", "language-shell", "platform-unix", "attack-rce", "paranoia-level/1", "OWASP_CRS", "OWASP_CRS/ATTACK-RCE", "capec/1000/152/248/88"] ver="OWASP_CRS/4.18.0"
message="Remote Command Execution: Unix Shell Code Found"
,
details=