**Sumário**

* **Introdução do Relatório**
* **Resumo Executivo**
* **Resultados da Varredura de Vulnerabilidades**
* **Associação com as Metodologias OWASP Top 10**
* **Plano de Ações de Mitigação**
* **Conclusão**
* **Anexos e Referencias**

**Introdução do Relatório**

Este relatório documenta as vulnerabilidades criticas identificadas no site <http://testphp.vulnweb.com>, realizada no dia **01 de março de 2025,** usando a ferramenta **OWASP Zap** no **Kali Linux**. O objetivo é fornecer informações detalhadas sobre as falhas encontradas, seus impactos e recomendações para mitigação.

Foram identificadas diversas falhas que necessitam ser gerenciadas e corrigidas para mitigar possíveis intrusões. Neste relatório, também são apresentadas melhores práticas para tratar as vulnerabilidades listadas, além da classificação das falhas com base no **OWASP Top 10**.

**Resultado da Varredura de Vulnerabilidades**

|  |  |  |
| --- | --- | --- |
| **Nome** | **Nível de Risco** | **Número de Instâncias** |
| Cross Site Scripting (Refletido) | Alto | 19 |
| Cross Site Scripting (baseado em DOM) | Alto | 11 |
| Injeção SQL - MySQL | Alto | 19 |
| Ausência de tokens Anti-CSRF | Médio | 4 |
| Content Security Policy (CSP) Header Not Set | Médio | 54 |
| Injeção XSLT | Médio | 2 |
| Missing Anti-clickjacking Header | Médio | 46 |
| O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By" | Baixo | 79 |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Baixo | 92 |
| X-Content-Type-Options Header Missing | Baixo | 82 |
| Authentication Request Identified | Informativo | 2 |
| Divulgação de Informações - Comentários Suspeitos | Informativo | 1 |
| GET for POST | Informativo | 3 |
| Modern Web Application | Informativo | 9 |
| Má Combinação de Charset (Cabeçalho versus Meta Content-Type Charset) | Informativo | 32 |
| User Agent Fuzzer | Informativo | 223 |
| User Controllable HTML Element Attribute (Potential XSS) | Informativo | 4 |

**Descrição das Principais Vulnerabilidades**

Foram encontradas 10 tipos de vulnerabilidades, sendo tres delas de alto risco, quatro de medio risco e três de baixo risco,

Dentre as principais temos:

**Cross Site Scripting (Refletido)**:

Impacto

**Cross Site Scripting (baseado em DOM)**:

Impacto

**Injeção SQL - MySQL**:

Impacto

**Associação com as Metodologias OWASP Top 10**

Nesse relatório foi identificado 3 grandes vulnerabilidades, que estão associados ao TOP 10 do OWASP de 2021, pode se perceber também que há semelhanças do tipo de ataque, na qual são ataques de INJECTIONs, na qual é feito a injeção de codigos maliosos.

