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.

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.