Relatório de vulnerabilidades

Pentest GreyBox

security@security.com.br

12-10-2024 | 12-11-2024

Sumário

1 Sumário Executivo

Durante a realização dos testes de segurança a equipe da **{SUA EMPRESA}** foi capaz de indentificar vulnerabilidades que puderam comprometer o ambiente de backoffice,assim como um acesso ao servidor XYZ de produção que permitiu a escalação de privilégios dentro da rede interna obtendo credenciais e planilhas com valores financeiros.

1.1 Objetivo

O objetivo desta avaliação foi realizar um teste de intrusão. Este teste simula uma tentativa de intrusão real e afim de identificar vulnerabilidades no ambiente. Permitindo que a **Empresa XYZ** possa agir proativamente na correção de vulnerabilidades do ambiente testado. Este relatório apresenta um parecer sobre os riscos existentes, assim como aponta ações necessárias para correção e/ou mitigação dos mesmos.

2 Especificações Técnicas

Para realizar um teste de intrusão bem feito é necessário seguir os padrões de mercado. Só assim é possível garantir excelência na execução do teste independente do ambiente avaliado.

OBS: Algumas nomenclaturas foram mantidas em inglês, afim de preservar os padrão internacionalmente utilizado.

2.1 Glossário

- **CVE** (Common Vulnerabilities and Exposures): Um identificador único para vulnerabilidades conhecidas, usado para rastrear e catalogar falhas de segurança publicamente divulgadas.
- **CWE** (Common Weakness Enumeration): Uma lista categorizada de falhas de design e desenvolvimento que podem levar a vulnerabilidades de segurança.
- **Exploit**: Um código ou técnica usado para explorar uma vulnerabilidade e obter acesso não autorizado ou controle de um sistema.
- **Payload**: Parte de um exploit que realiza a ação maliciosa após a exploração bem-sucedida de uma vulnerabilidade.
- **Zero-Day**: Uma vulnerabilidade previamente desconhecida pelos responsáveis pelo sistema, sem correção disponível.

2.2 Classificação de Risco

O risco é um evento que pode ocorrer no futuro e causar certos impactos, enquanto uma vulnerabilidade é uma fraqueza associada a um ativo, que pode vir a ser explorada por potenciais ameaças. O Risco é definido pela multiplicação entre o impacto e a probabilidade que uma vulnerabilidade tem de ser explorada.

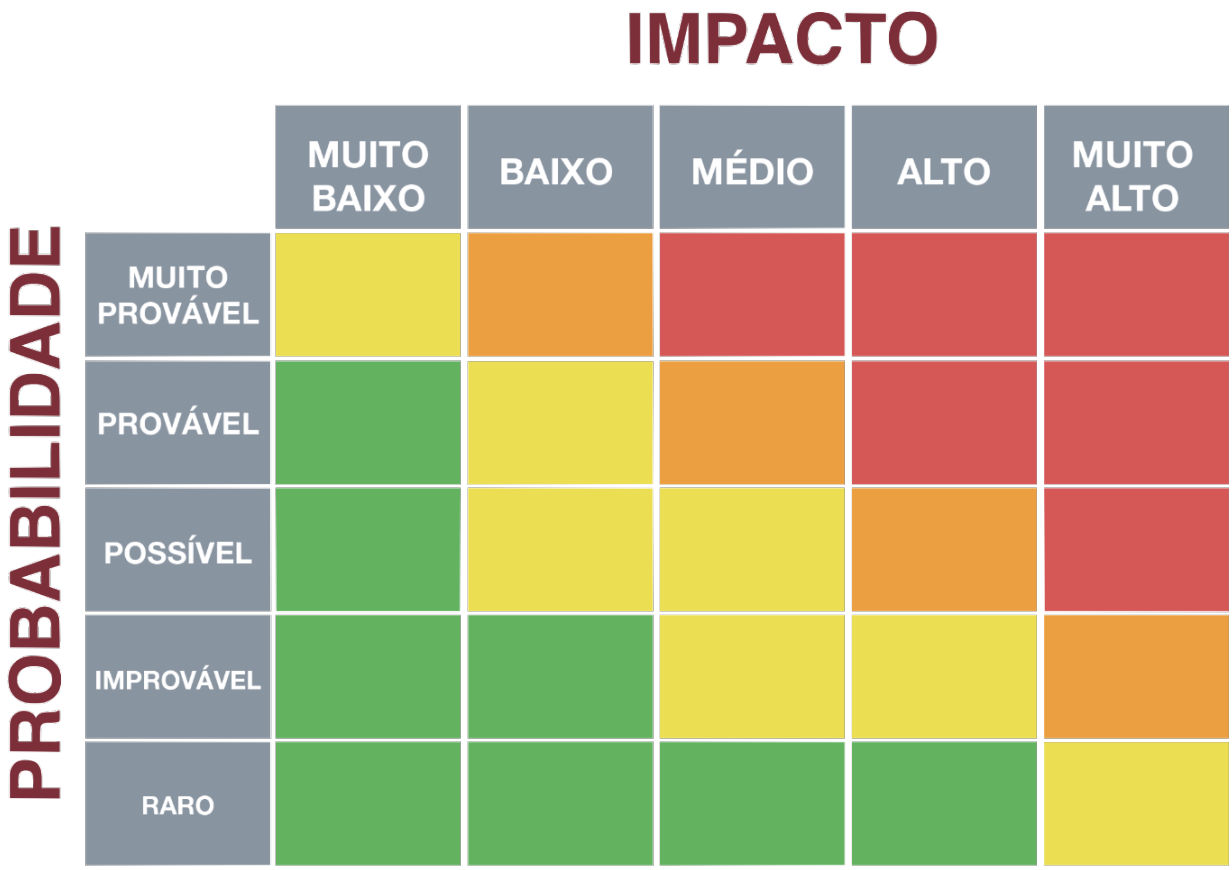

Figure 2.1: Impacto vs Probabilidade

2.3 Calculadora CVSS

O Common Vulnerability Scoring System (CVSS) é uma estrutura aberta para comunicar as características e a gravidade das vulnerabilidades de um software. O CVSS consiste em três grupos de métricas: Base, Temporal e Ambiental.

As métricas Base produzem uma pontuação que varia de **0 a 10**, que pode ser modificada pela pontuação das métricas Temporal e Ambiental. Assim, o CVSS funciona como um sistema de medição padrão para indústrias, organizações e governos que precisam de classificar a gravidade das vulnerabilidades de forma precisa e consistente.

Dois usos comuns do CVSS são:

- Cálculo da gravidade das vulnerabilidades;
- Fator de priorização de correção de vulnerabilidades.

Severidade	Pontuação CVSS 3.1	Descrição
Crítica	9.0 - 10.0	A exploração da vulnerabilidade permite a um atacante o acesso de nível administrativo a sistemas e/ou dados de alto nível que teriam um impacto catastrófico na organização. As vulnerabilidades marcadas como CRÍTICAS requerem atenção imediata e devem ser corrigidas sem demora, especialmente se ocorrerem num ambiente de produção.
Alta	7.0 - 8.9	A exploração da vulnerabilidade permite acessar a dados importantes. No entanto, há certos pré-requisitos que têm de ser cumpridos para que o ataque seja bem sucedido. Estas vulnerabilidades devem ser revistas e corrigidas sempre que possível.
Média	4.0 - 6.9	A exploração da vulnerabilidade pode depender de factores externos ou de outras condições difíceis de alcançar, como a necessidade de privilégios de utilizador para uma exploração bem sucedida. Estes são problemas de segurança moderados que exigem algum esforço para afetar com êxito o ambiente.
Baixa	0.1 - 3.9	As vulnerabilidades na gama baixa têm normalmente um impacto muito reduzido na atividade de uma organização. A exploração de tais vulnerabilidades requer normalmente o acesso local ou físico ao sistema e depende de condições que são muito difíceis de obter na prática.
Informativa	0	Estas vulnerabilidades representam um risco significativamente menor e são de natureza informativa. Estes itens podem ser corrigidos para aumentar a segurança.

Figure 2.2: Descrição - CVSS

Calculadora CVSS 3.0: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

2.4 Metodologias

Diversas organizações ao redor do mundo se dedicam a estudar e categorizar vulnerabilidades de segurança, fornecendo informações valiosas para profissionais que desejam compreender o cenário atual de ameaças. Essas organizações publicam documentos, classificações e ferramentas que ajudam a identificar as vulnerabilidades mais relevantes ao longo do tempo, guiando equipes de segurança na priorização de esforços.

2.4.1 OWASP

O OWASP – Open Web Application Security Project é uma comunidade global que promove a segurança no desenvolvimento de software. Seu objetivo é educar desenvolvedores e especialistas de segurança para que adotem boas práticas e desenvolvam sistemas mais seguros.

Através de iniciativas colaborativas, o OWASP disponibiliza gratuitamente:

- Artigos educativos;
- Metodologias de segurança;
- Documentação técnica;
- Ferramentas.

2.4.2 OWASP Top 10

O OWASP Top 10 é um documento de conscientização amplamente reconhecido, que apresenta os dez riscos mais críticos para a segurança de aplicações web. Atualizado periodicamente, o OWASP Top 10 serve como um guia essencial para desenvolvedores e equipes de segurança, destacando:

- As vulnerabilidades mais comuns e perigosas;
- Exemplos práticos para identificação;
- Recomendações de mitigação.

Além do Top 10 voltado para aplicações web, o OWASP ampliou seu escopo e atualmente também aborda segurança em outras áreas, como: **APIs**, **Apps mobile**, **blockchain** e **LLMs**. Adaptando as recomendações aos desafios particulares de cada área.

Figure 2.3: OWASP TOP 10

3 Vulnerabilidades Identificadas

> Todas as informações contidas aqui são confidenciais e não devem ser copiadas ou divulgadas antes do consentimento formal da empresa.

Identificador	Título da Vulnerabilidade	Risco
UID-01	Stored XSS	CRÍTICO
UID-02	IDOR	ALTO
UID-03	SQL Injection	MÉDIO
UID-04	Login Bypass	MÉDIO
UID-05	Exposed API Key	BAIXO

3.1 Stored XSS

3.1.1 Descrição

- **Endpoint Afetado:** www.example.com/api/v2/admin
- **Descrição Endpoint:** API responsável pelo acesos adminstrativo do sistema.

Durante os testes foi identificado uma possível injeção de javascript na página de admin do sistema **ABC** que permitiu o acesso a contas de clientes e funcionários.

3.1.2 Evidências

Figure 3.1: Shell

3.1.3 Impacto no ambiente

Além do acesso indevido a conta do cliente, foi possível extrair informações pessoais e alterar dados cadastrais.

3.1.4 Recomendação/Mitigação

- Aplicar uma regra de WAF para evitar esse tipo de ataque como forma de mitigação.
- Utilizar DOM Purify ou outra biblioteca que realize a sanitização dos campos da aplicacão.

3.1.5 Referências

1. DOM Purify

4 Considerações

As vulnerabilidades identificadas representam um alto risco financeiro reputacional para a **Empresa XYZ**. Uma vez que qualquer usuário logado no sistema **XPTO** é capaz de realizar um upload de um arquivo malicioso e obter acesso indevido ao sistema.

Recomenda-se corrigir as todas as vulnerabilidades reportadas durante o teste para garantir que um agente mal-intencionado não seja capaz de explorar esses sistemas no futuro, se utilizando das mesmas.

Vale lembrar que esses sistemas requerem avaliações frequentes e uma vez corrigidos, devem ser retestados afim de garantir que a correção aplicada é eficaz.