Relatório de Vulnerabilidades

João Pedro Duarte Nunes (12542460)
Henrico Lazuroz Moura de Almeida (12543502)
Pedro Rossi Silva Rodrigues (11871775)
Raphael David Philippe Leveque (12542522)
Victor Lucas de Almeida Fernandes (12675399)

Link para o Vídeo: https://youtu.be/Vpb0nWlkBNo

1. SQL Injection

- **Descrição:** A aplicação permite a inserção direta de dados do usuário na consulta SQL sem realizar o uso de parâmetros ou prepared statements.
- **Exploração:** Basta inserir um payload como `' OR '1'='1` no campo de login, e o sistema autenticará qualquer usuário.
- **Mitigação:** Utilizar prepared statements ou PDO (PHP Data Objects) para evitar a injeção de SQL.

2. Cross-Site Scripting (XSS)

- **Descrição:** O valor inserido pelo usuário é refletido diretamente na página HTML sem qualquer validação ou escape, possibilitando a execução de scripts maliciosos.
- **Exploração:** Um exemplo de payload seria `<script>alert('XSS')</script>` inserido no campo de username. Ao submeter, o JavaScript é executado no navegador da vítima.
- **Mitigação:** Usar a função `htmlspecialchars()` em PHP para escapar caracteres especiais no HTML.

3. Upload de Arquivo Malicioso

- **Descrição:** A aplicação permite o upload de arquivos sem verificar o tipo ou extensão do arquivo, possibilitando o upload de arquivos executáveis maliciosos, como scripts PHP.
- **Exploração:** Um invasor pode fazer upload de um arquivo PHP contendo código malicioso. Por exemplo, um arquivo PHP com `<?php system($_GET['cmd']); ?>` permite a execução de comandos.
- **Mitigação:** Verificar a extensão do arquivo e permitir apenas tipos seguros, como imagens (`.jpg`, `.png`), e renomear os arquivos no servidor.

4. Command Injection

- **Descrição:** A funcionalidade de ping aceita entradas do usuário que são diretamente utilizadas para a execução de comandos no servidor, sem qualquer validação ou sanitização. Isso permite que um atacante injete comandos adicionais usando operadores como `&`, `|` ou `;`.

- **Exploração:** Um atacante pode inserir um payload como `8.8.8.8 && ls` ou `127.0.0.1 | cat /etc/passwd` no campo de endereço IP. O servidor irá executar os comandos adicionais injetados.
- **Mitigação:** Utilizar funções como `escapeshellarg()` ou `escapeshellcmd()` para sanitizar as entradas ou validar estritamente que a entrada é um endereço IP válido, rejeitando qualquer outro tipo de entrada.