**RELATÓRIO DE SEGURANÇA DE SOFTWARE**

Data: 15/10/2024

* **Projeto: Teste de Segurança**
* Versão do software: 1.3
* **Introdução Geral sobre os Testes**

A segurança das aplicações é essencial no desenvolvimento de software moderno. Este relatório aborda três testes de segurança realizados em uma API de login e upload de imagens, focando em vulnerabilidades de SQL Injection, NoSQL Injection e Injeção de Comando.

* **Resumo das Falhas de Segurança**

**Falha 1:** Falhas no tratamento de entradas durante o login, que poderiam permitir acesso não autorizado a contas de usuário.

**Gravidade: Alta**

**Descrição:** Durante os testes, ao aplicar a senha "' or 1=1 --", esperava-se um erro 422, mas o site retornou um código 200, permitindo acesso às informações de login. Essa vulnerabilidade possibilita que um invasor obtenha acesso não autorizado a contas de usuários, expondo informações sensíveis e permitindo alterações de dados ou ações maliciosas em nome dos usuários.

**Falha 2:** NoSQL Injection permitindo acesso não autorizado.

**Gravidade: Alta**

**Descrição:** Durante os testes, ao utilizar a senha "$exists": true, esperava-se um erro 422, mas o site retornou um código 200, permitindo acesso às informações de login. Além disso, um ataque de NoSQL Injection foi realizado por meio de um POST. Essa vulnerabilidade possibilita que um invasor obtenha acesso não autorizado a contas de usuários, expondo informações sensíveis e permitindo atividades maliciosas.

**Falha 3:** Injeção de comando durante o upload de imagem.

**Gravidade: Alta**

**Descrição:** Durante os testes, foi realizado um código de teste no upload de imagem, que permitiu a injeção de comandos na página, revelando dados sensíveis e permitindo a inserção de códigos maliciosos no nome do arquivo. Essa vulnerabilidade possibilita que um invasor execute comandos arbitrários no sistema, comprometendo a segurança, expondo informações confidenciais e permitindo atividades maliciosas. A seção também detalha cada falha de segurança identificada, incluindo gravidade, cenários de exploração e recomendações para correção.

* **Descrição detalhada:** Durante os testes, foi possível injetar comandos maliciosos no sistema ao fazer upload de uma imagem, executando o comando "echo 'Meu Comando' & ls -la" e revelando dados sensíveis. A vulnerabilidade também permitiu a injeção de códigos maliciosos pelo nome do arquivo, representando um risco significativo para a segurança do sistema.
* **Cenários de exploração:** Um invasor pode explorar essa vulnerabilidade para executar comandos arbitrários no sistema, obtendo acesso não autorizado, comprometendo a segurança, expondo informações confidenciais e realizando atividades maliciosas.
* **Recomendações:** Recomenda-se implementar validação e sanitização adequadas para uploads de arquivos, permitindo apenas arquivos legítimos e tratando corretamente os nomes para evitar injeções de códigos maliciosos. Além disso, é fundamental manter o software atualizado, aplicar patches de segurança e realizar testes abrangentes para identificar e corrigir vulnerabilidades.
* **Conclusão Geral:** As vulnerabilidades identificadas, como SQL Injection, NoSQL Injection e Injeção de Comando, representam riscos significativos à segurança da aplicação e dos dados dos usuários. É crucial que as equipes de desenvolvimento adotem práticas rigorosas de validação e sanitização de entradas, utilizem consultas parametrizadas e bibliotecas seguras para uploads. A segurança deve ser uma prioridade contínua no ciclo de vida do desenvolvimento de software, garantindo a rápida identificação e correção de novas vulnerabilidades para proteger a integridade do sistema e a confiança dos usuários.