RELATÓRIO DE SEGURANÇA DE SOFTWARE

Data: 22/05/2023

Projeto: Teste de Segurança

Versão do software: 1.3

1.0 Introdução

O presente relatório tem como objetivo documentar e relatar as falhas de segurança identificadas no sistema [nome do sistema/software]. As falhas de segurança foram descobertas durante uma avaliação minuciosa e são apresentadas a seguir, juntamente com uma descrição das vulnerabilidades e suas possíveis consequências.

2.1 Resumo das Falhas de Segurança

Falha 1: Vazamento de informações de login através de injeção de SQL

Gravidade: Alta

Descrição: Durante os testes, foi possível acessar informações do login aplicando a seguinte informação na senha: "' or 1=1 --". Era esperado um retorno 422, indicando uma resposta inválida, porém o site retornou um código 200 e as informações do login.

Potenciais consequências: Essa vulnerabilidade permite que um invasor tenha acesso não autorizado a contas de usuário, podendo obter informações sensíveis, alterar dados ou realizar ações maliciosas em nome dos usuários.

Falha 2: NoSQL Injection permitindo acesso não autorizado

Gravidade: Alta

Descrição: Durante os testes, foi possível acessar informações de login aplicando a seguinte informação na senha: "$exists": true. Era esperado um retorno 422, indicando uma resposta inválida, porém o site retornou um código 200 e as informações do login. Além disso, foi realizado um ataque de NoSQL Injection através de um post.

Potenciais consequências: Essa vulnerabilidade permite que um invasor tenha acesso não autorizado a contas de usuário, expondo informações sensíveis e possibilitando atividades maliciosas.

Falha 3: Injeção de comando durante o upload de imagem

Gravidade: Alta

Descrição: Durante os testes, foi aplicado código de teste no upload de imagem:

O teste permitiu a injeção de comandos na página, retornando dados sensíveis que não deveriam ser exibidos. Além disso, o nome do arquivo também permitiu a injeção de códigos maliciosos.

Potenciais consequências: Essa vulnerabilidade permite que um invasor execute comandos arbitrários no sistema, podendo comprometer a segurança, expor informações confidenciais e realizar atividades maliciosas.

Detalhamento das Falhas de Segurança

Esta seção apresenta uma descrição detalhada de cada falha de segurança identificada, incluindo informações sobre sua gravidade, possíveis cenários de exploração e recomendações para correção.

3.1 Falha 1: Vazamento de informações de login através de injeção de SQL

Gravidade: Alta

3.2 Falha 2: NoSQL Injection permitindo acesso não autorizado

Gravidade: Alta

3.3 Falha 3: Injeção de comando durante o upload de imagem

Gravidade: Alta

Descrição detalhada: Durante os testes, foi possível injetar comandos maliciosos no sistema ao realizar o upload de imagem. O teste utilizado permitiu a execução do comando "echo 'Meu Comando' & ls -la", retornando dados sensíveis que não deveriam ser exibidos. Além disso, a vulnerabilidade permitiu a injeção de códigos maliciosos através do nome do arquivo, o que representa um risco significativo para a segurança do sistema.

Cenários de exploração: Um invasor mal-intencionado pode utilizar essa vulnerabilidade para executar comandos arbitrários no sistema, podendo obter acesso não autorizado, comprometer a segurança do sistema, expor informações confidenciais e realizar atividades maliciosas.

Recomendações: Recomenda-se implementar mecanismos de validação e sanitização adequados para o upload de arquivos. É importante garantir que apenas arquivos legítimos sejam permitidos e que os nomes dos arquivos sejam tratados corretamente para evitar a injeção de códigos maliciosos. Além disso, é essencial manter o software atualizado, aplicar patches de segurança e conduzir testes de segurança abrangentes para identificar e corrigir possíveis vulnerabilidades.

4.0 Conclusão

Este relatório destacou as falhas de segurança identificadas no sistema http://localhost:3000, relacionadas ao vazamento de informações de login através de injeção de SQL, NoSQL Injection permitindo acesso não autorizado e injeção de comando durante o upload de imagem. Essas vulnerabilidades apresentam um alto risco, permitindo acesso não autorizado a contas de usuário, exposição de informações sensíveis e execução de comandos arbitrários no sistema. Recomenda-se a implementação de medidas de segurança adequadas para corrigir essas falhas e garantir a integridade e confidencialidade do sistema.