Maylson de Paula Simoes - Matricula: 2023.02.45975-7

Polo Madureira - Rio de Janeiro - RJ

RPG00 – Software sem Segurança não Serve

GitHub: https://github.com/VascoMay/Software-sem-seguranca-nao-serve

RELATÓRIO DA MISSÃO PRÁTICA

1 INTRODUÇÃO

Este relatório tem como objetivo documentar a refatoração de uma aplicação web vulnerável, garantindo melhorias de segurança e a aplicação de boas práticas para prevenção de ataques. A atividade foca na implementação de mecanismos de proteção contra SQL Injection, CRLF Injection, uso inadequado de tokens e acessos não autorizados.

2 REFATORAÇÃO DA APLICAÇÃO

2.1 Substituição da geração do Session-ID

- O método de criptografia original foi substituído pela geração de tokens JWT.
- O JWT agora inclui um tempo de expiração e é armazenado com segurança.

2.2 Trafegando o token pelo header

- A URI não contém mais o session-id.
- O token JWT agora é enviado no header das requisições.

2.3 Validação do token em todas as requisições

- Implementação de middleware para verificação de autenticidade do token antes da execução de qualquer endpoint.

2.4 Controle de acesso por perfil

- Apenas usuários com perfil 'admin' podem acessar determinadas rotas.
- Criado endpoint para retorno de dados do usuário logado, acessível a qualquer usuário autenticado.

2.5 Proteção contra SQL Injection

- Implementação de consultas parametrizadas para evitar execução de código malicioso.
- Validação e sanitização de entradas para impedir manipulação de cabeçalhos HTTP.
- Restrição de redirecionamento para domínios autorizados.

3 TESTES REALIZADOS

- Testes unitários para verificação da segurança dos endpoints.
- Testes em ferramentas como Insomnia para validar a segurança das requisições.
- Simulação de ataques SQL Injection e CRLF Injection para garantir a eficácia das correções.

4 CONSIDERAÇÕES FINAIS

A refatoração da aplicação garantiu maior segurança e conformidade com boas práticas de desenvolvimento seguro. As medidas implementadas evitam acessos não autorizados e protegem os dados trafegados na API.