UNIVERSIDADE ESTÁCIO DE SÁ

RIO DE JANEIRO - POLO SANTA CRUZ

2024

DOCUMENTAÇÃO DE PROJETO

DESENVOLVIMENTO FULL STACK

MUNDO 5 – NÍVEL 5

RPG0035 – SOFTWARE SEM SEGURANÇA NÃO SERVE!

Aluna: Tamires de Souza Alves
Matrícula: 202203974271

Introdução

Este relatório tem como objetivo acompanhar o progresso da missão prática de refatoração de uma aplicação web com foco na segurança de dados e proteção contra vulnerabilidades. A aplicação em questão é uma API Rest com diversos pontos críticos que permitem a exploração de falhas de segurança, o que pode resultar no vazamento de dados sensíveis e no acesso não autorizado a informações confidenciais.

A missão do projeto foi identificar e corrigir as falhas de segurança em uma aplicação, garantindo que ela se torne mais segura e resistente a ataques comuns, como injeção de código, acesso não autorizado e falhas no controle de sessão.

Controle e Desafios Identificados

A aplicação possui vários pontos vulneráveis que poderiam ser explorados para obter acesso indevido a informações privadas. Entre as falhas identificadas, destacam-se:

- **Uso de "session-id" vulnerável:** O valor do parâmetro session-id utilizado para controlar a autenticação é gerado de forma insegura, permitindo ataques de força bruta para obter o ID do usuário e, com isso, acessar dados restritos.
- **Falta de proteção conta SQL Injection:** A aplicação não trata corretamente os parâmetros recebidos em requisições, tornando-a vulnerável a esses ataques, onde comandos maliciosos podem ser injetados em consultas ao banco de dados.
- **Falta de controle de acesso:** Não há um controle robusto de acesso, permitindo que usuários com perfis inadequados acessem informações restritas.
- **Exposição de dados sensíveis:** A aplicação trafega dados importantes como o session-id na URL, tornando-os acessíveis para quem interceptar a comunicação.

Metodologia e Ações Realizadas

Substituição do Mecanismo de Criptografia

O primeiro passo foi refatorar a geração do session-id, substituindo o mecanismo de criptografia atual por um método mais seguro: A utilização de tokens JWT (JSON Web Tokens).

Os tokens JWT oferecem várias vantagens, como:

- **Autenticação segura** sem expor dados sensíveis na URL;
- **Validação de expiração** dos tokens, garantindo que eles sejam inválidos após um determinado tempo.
- **Integração simples** com a API, onde o token é enviado através dos headers de requisição, e não mais na URL.

Essa mudança eliminou a vulnerabilidade associada ao método de criptografia fraco e ao uso de tokens na URL.

Implementação de Controle de Acesso

Refatoramos todos os endpoints para incluir controle de acesso baseado no perfil do usuário. Apenas usuários com perfil *admin* têm acesso a dados restritos, como informações dos usuários e contratos. Para usuários comuns, a resposta será “Forbidden” se tentarem acessar essas informações.

- **Endpoint de login:** Permite que o usuário obtenha um token JWT após uma autenticação bem-sucedida.
- **Endpoints protegidos:** Como `/api/users/:sessionid` e `/api/contracts/:empresa/:inicio/:sessionid`, agora exigem validação do token JWT e verificação do perfil do usuário.

Proteção contra SQL Injection

O código que manipulava as consultas no banco de dados foi refatorado para sanitizar os parâmetros de entrada, impedindo que os usuários mal-intencionados injetem comandos SQL através de parâmetros manipulados. Usamos prepared statements e ORM (Object-Relational Mapping) para evitar esse tipo de vulnerabilidade.

A consulta SQL foi modificada para que o parâmetro de entrada fosse devidamente tratado, prevenindo ataques.

Resultados Obtidos

A aplicação foi completamente renovada e agora oferece maior segurança, controle de acesso eficaz, melhoria no processo de autenticação e maior segurança no tráfego de dados.

Conclusão

Com a refatoração realizada, conseguimos resolver as falhas de segurança presentes na aplicação e implementar as melhores práticas de segurança recomendadas para APIs web. A aplicação agora está mais robusta, segura e pronta para ser utilizada em um ambiente de produção, sem expor dados sensíveis ou permitir o acesso não autorizado.

A missão realizada mostra a importância de se preocupar com a segurança desde o início do desenvolvimento de uma aplicação, e como pequenas falhas podem comprometer a integridade de todo o sistema. Ao corrigir essas vulnerabilidades, garantimos não apenas a proteção dos dados, mas também a confiança dos usuários no sistema.

A segurança é um processo contínuo, e as mudanças realizadas são um passo importante para manter a aplicação segura contra ameaças externas.