Curso :Desenvolvimento Full Stack
Turma : 9001
Matrícula: 202211381232
Aluno: Marco Sergio Albino Vittorio Barozzi
Disciplina : Software sem segurança não serve
Código :RPG0035

Missão Prática | Software sem segurança não serve

- Objetivos

Este projeto tem como objetivo os seguintes pontos :

- Descrever o controle básico de acesso a uma API Rest;

- Descrever o tratamento de dados sensíveis e log de erros com foco em segurança;

- Descrever a prevenção de ataques de acesso não autorizado com base em tokens desprotegidos/desatualizados;

- Descrever o tratamento de SQL Injection em códigos-fonte;

- Descrever a prevenção a ataques do tipo CSRF em sistemas web;

Curso :Desenvolvimento Full Stack
Turma : 9001
Matrícula: 202211381232
Aluno: Marco Sergio Albino Vittorio Barozzi
Disciplina : Software sem segurança não serve
Código :RPG0035

Missão Prática | Software sem segurança não serve

- Procedimentos

Os procedimentos das micro atividades assim como a missão pratica podem ser encontrados no link abaixo.

Link da missão
https://sway.cloud.microsoft/s/P89nF9yZ4YctBGSC/embed

O foco aqui será apenas nos itens principais do procedimento da missão pratica

Curso :Desenvolvimento Full Stack
Turma : 9001
Matrícula: 202211381232
Aluno: Marco Sergio Albino Vittorio Barozzi
Disciplina : Software sem segurança não serve
Código :RPG0035

Missão Prática | Software sem segurança não serve

- Relatório: Correção de Falhas de Segurança e Implementação

Contextualização

A atividade envolveu a análise de uma aplicação legada que apresentava falhas graves de segurança. As falhas identificadas incluíam:

1. **Vulnerabilidade no processo de geração de `session-id`**:
   - O `session-id` era gerado a partir do ID do usuário utilizando uma chave de criptografia simples (o nome da empresa).
   - Isso possibilitava ataques de força bruta para gerar valores válidos e acessar recursos protegidos.

2. Falta de validação de parâmetros:
   - Parâmetros não eram sanitizados, permitindo ataques de Injection em consultas SQL.

3. Ausência de separação de responsabilidades:
   - Todo o código estava em um único arquivo, dificultando a manutenção.

Curso :Desenvolvimento Full Stack
Turma : 9001
Matrícula: 202211381232
Aluno: Marco Sergio Albino Vittorio Barozzi
Disciplina : Software sem segurança não serve
Código :RPG0035

Missão Prática | Software sem segurança não serve

Ações Implementadas

Com base nos problemas identificados, as seguintes soluções foram aplicadas:

1. *Refatoração do Backend*

O backend foi reestruturado para separar responsabilidades e corrigir falhas de segurança.

Reestruturação do Código

A estrutura final do projeto inclui:

- **data/**: Contém dados fictícios de usuários e contratos.
- **middleware/**: Middlewares para autenticação (validar JWT) e controle de tentativas de login.
- **routes/:** Rotas separadas para autenticação, usuários e contratos.
- **utils/**: Configurações gerais, como chaves e parâmetros de segurança.
- **server.js**: Arquivo principal que inicia o servidor.

Melhorias nos Endpoints

- **Autenticação com JWT:**
  - Substitui o `session-id` por um token JWT seguro.
  - O JWT armazena informações do usuário e expira automaticamente após 5 minutos.

Curso :Desenvolvimento Full Stack
Turma : 9001
Matrícula: 202211381232
Aluno: Marco Sergio Albino Vittorio Barozzi
Disciplina : Software sem segurança não serve
Código :RPG0035

Missão Prática | Software sem segurança não serve

- **Sanitização de Parâmetros:**
  - Adicionamos validações nos parâmetros recebidos utilizando `express-validator`.

Controle de Perfis:

- Apenas usuários com perfil `admin` podem acessar certos recursos, como a listagem de usuários.

Endpoints Implementados

1. **/api/auth/login**:
   - Realiza login e retorna um token JWT para autenticação.

2. **/api/auth/profile:**
   - Retorna o perfil do usuário autenticado.

3. **/api/users:**
   - Disponível apenas para `admin`. Retorna a lista de usuários cadastrados.

4. **/api/contracts:**
   - Consulta contratos com filtros opcionais, disponível apenas para `admin`.

Curso :Desenvolvimento Full Stack
Turma : 9001
Matrícula: 202211381232
Aluno: Marco Sergio Albino Vittorio Barozzi
Disciplina : Software sem segurança não serve
Código :RPG0035

Missão Prática | Software sem segurança não serve

2. Refatoração do Frontend

No arquivo `auth.js`, implementamos:

- **Validação de Sessão :**
  - Funções para verificar se o token JWT está presente e válido.

- **Função de Login:**
  - Realiza login e armazena o token JWT no `localStorage`.

- **Recuperação de Perfil:**
  - Adicionada a função `getUserProfile` para consultar o perfil do usuário logado.

- **Melhorias Gerais:**
  - Integração com os novos endpoints do backend.

3. Correção de Falhas de Segurança

- **Criptografia do Session-ID :**
  - O uso do `session-id` foi substituído por JWT, que utiliza assinaturas seguras.

- **Sanitização de Inputs** :
  - Parâmetros de entrada são validados e sanitizados para evitar SQL Injection.

Curso :Desenvolvimento Full Stack
Turma : 9001
Matrícula: 202211381232
Aluno: Marco Sergio Albino Vittorio Barozzi
Disciplina : Software sem segurança não serve
Código :RPG0035

Missão Prática | Software sem segurança não serve

-**Controle de Acessos**:
- Middlewares como `isAdmin` garantem que apenas usuários autorizados podem acessar recursos protegidos.

Conclusão

As soluções implementadas corrigiram falhas críticas de segurança e organizaram o código em uma estrutura modular e segura. A reestruturação facilita futuras manutenções e escalabilidade, garantindo que a aplicação atenda aos padrões modernos de segurança e boas práticas de desenvolvimento.