Gabriel Henrique dos Santos – Matrícula 202208292411

Polo: Limeira Centro

Turma 2023.3

MUNDO 5 – SOFTWARE SEM SEGURANÇA NÃO SERVE!

Alterações realizadas:

Mecanismo de autenticação com JWT:

Cada usuário recebe um token JWT válido por uma hora ao realizar login.

O token inclui o id, username, perfil e data de expiração.

Validação de token no cabeçalho:

O token é enviado via cabeçalho Authorization no formato Bearer <token>, evitando exposição em URLs.

Controle de acesso por perfil:

Usuários com perfil diferente de admin são impedidos de acessar rotas sensíveis como /api/users.

Prevenção contra SQL Injection:

Parâmetros nos endpoints que interagem com o banco são sanitizados usando expressões regulares.

Criação de um endpoint /api/auth/me:

Permite que o usuário logado obtenha suas informações sem restrições de perfil.

Separação de responsabilidades e melhorias:

Código mais modular.

Dados sensíveis são tratados com segurança.

Tokens são gerenciados de maneira segura com data de expiração.

Testes esperados:

Login:

Enviar um POST para /api/auth/login com credenciais válidas. O token JWT será retornado.

Listar usuários (apenas admin):

Enviar um GET para /api/users com o token do admin no cabeçalho Authorization. Deve retornar a lista de usuários.

Acesso negado para usuários comuns

Enviar um GET para /api/users com o token de um usuário comum. Deve retornar 403 Forbidden.

Recuperar contratos com proteção:

Enviar um GET para /api/contracts?empresa=EmpresaA&inicio=2023-01-01 com o token válido. Parâmetros são tratados contra injeção.

Verificar dados do usuário logado:

Enviar um GET para /api/auth/me com o token válido. Retorna informações do usuário logado.

Essas mudanças eliminam os problemas identificados e fortalecem a segurança da API.