FACULDADE DE TECNOLOGIA SENAC PELOTAS

Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas

Desenvolvimento de Serviços e APIs – Edécio Fernando Iepsen

Trabalho #3: Adicionar Recursos de Segurança na API – Cadastro de Usuário / Login / Criptografia e Token.

Criar uma API para cadastrar usuários e dados em uma tabela relacionada aos usuários. Cada aluno deve escolher a sua tabela relacionada.

Criar, inicialmente, as models:

- Usuario (contendo: id, nome, email, senha, ...)

- Model associada a tabela principal do sistema (contendo: id, nome, ..., usuário_id). Implementar o recurso de exclusão lógica (*soft delete / paranoid*)

- Criar as rotas e as rotinas para realizar a inclusão e listagem dos dados dos usuários;

- Criar as rotas e as rotinas para realizar a inclusão, listagem, alteração, exclusão e pesquisa de dados na tabela principal do sistema (com os dados do usuário na listagem).

Escolher e implementar 5 dos recursos de segurança indicados a seguir:

1. Criptografia da senha do usuário.
2. Criação de Login com a geração de token. Definir middleware de verificação do token e adicioná-lo em 2 ou 3 rotas do sistema.
3. Criação da Model / tabela de Logs (relacionada com a tabela de usuários). Registrar 2 ou 3 ações (ou tentativas de ações) do sistema nos logs.
4. Implementar rotina de alteração de senha, validando a senha atual e criptografando a nova senha.
5. Implementar regras de composição na inclusão e alteração da senha (por exemplo, que a senha tenha, no mínimo 8 caracteres, tenha letras minúsculas, maiúsculas, números e símbolos), impedindo o cadastro de senhas fracas.
6. Implementar rotina de *reset* de senha, a partir do envio de mensagem para o e-mail do usuário ou do cadastro de pergunta/resposta de conhecimento exclusivo do usuário.
7. Definir níveis de acesso no cadastro do usuário, onde o usuário – a partir do seu nível, tenha privilégios diferentes no acesso aos recursos do sistema. Implementar o uso destes níveis no middleware de verificação de token / usuário logado.
8. Implementar um controle de tentativas de acesso inválidas para o usuário – no seu e-mail. Desta forma, ao atingir, por exemplo, 3 tentativas inválidas bloqueia o usuário (não permite acesso).
9. Implementar um controle de tentativas de acesso por tempo. Assim, ao atingir 3 tentativas inválidas, registra-se a data/hora da última tentativa. E, só verifica um novo login válido deste usuário, após 5 minutos da última tentativa – por exemplo.
10. Impedir o cadastro de 2 usuários com o mesmo e-mail. Exibir mensagem indicativa deste erro.

Data da Entrega/Apresentação: **04/07/2023**

Trabalho Individual

Conceitos:

- Rotas e funções dos cadastros em funcionamento e os 5 recursos de segurança implementados corretamente: A

- 1 dos recursos ausentes: B

- 2 dos recursos ausentes: C