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 / descrição, ..., 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).

Implementar os recursos de segurança já trabalhados em aula:

- Criptografia da senha do usuário;

- Validação da senha, a partir de regras de composição dos caracteres da senha (como, por exemplo, que a senha tenha, no mínimo 8 caracteres, tenha letras minúsculas, maiúsculas, números e símbolos). Impedir a inclusão e alteração das senhas sem que essa verificação seja realizada.

- Criação de Login com a geração de token. Definir middleware de verificação do token e adicioná-lo em 2 ou 3 rotas do sistema.

- 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.

- Recuperação de senha para usuários que esqueceram a senha, a partir da Implementação do recurso de envio de e-mail para o usuário que deseja recadastrar a senha e a rota/rotina de alteração da senha.

Escolher e implementar 3 novos recursos relacionados a controles de segurança, dos descritos a seguir:

1. Implementar rotina de alteração de senha, validando a senha atual e criptografando a nova senha. Impedir que a nova senha, seja igual a atual.
2. 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. Testar em rotas estes níveis.
3. Implementar um controle de tentativas de acesso inválidas para o usuário. Desta forma, ao atingir, por exemplo, 3 tentativas inválidas bloqueia o usuário (não permite novos acessos até ser retirado o bloqueio).
4. Impedir o cadastro de 2 usuários com o mesmo e-mail. Exibir mensagem indicativa deste erro.
5. Registrar data/hora do último login do usuário. Exibir essa data/hora no login (“Bem-vindo ... Seu último acesso ao sistema foi ...”)
6. Realizar backup das tabelas do sistema a partir do acionamento de uma determinada rota. Validar o acesso a essa rota pelo middleware de autenticação e salvar log da realização deste backup.
7. Definir um tempo limite para que o recurso de solicitação de nova senha tenha validade. Por exemplo: 1 hora – se o usuário não solicitar neste período, perde a validade.

Data da Entrega/Apresentação: **01/12/2023**

Trabalho Individual

Conceitos:

- Rotas e funções dos cadastros em funcionamento e os 3 recursos de segurança implementados corretamente: A
- 1 dos recursos ausentes: B
- 2 dos recursos ausentes: C