Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas
Prof. Edécio Fernando Iepsen

Desenvolvimento de Serviços e APIs

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/dupla deve escolher a sua tabela relacionada.

Criar as models do sistema:

- 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*)

- 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 e exclusão 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 de um usuário, com uma senha que não contemple essas regras.

- 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.

Escolher e implementar 2 novos recursos relacionados aos controles de segurança – como, por exemplo:

1. Implementar rotina de alteração de senha do usuário, validando a senha atual e criptografando a nova senha.
2. Implementar rotina para recuperação de senha para usuários que esqueceram a senha. O recurso deve ser implementado a partir de 2 rotas/rotinas. A primeira, é para o usuário solicitar a recuperação de senha. Neste processo validar o e-mail e gerar um código com 4 caracteres (por exemplo) e retornar para o usuário. A segunda, deve validar e-mail e o código (anteriormente enviado) e cadastrar a nova senha.
3. 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 nas rotas estes níveis (para realizar a exclusão de dados da tabela principal, o usuário tem que ser nível 3, por exemplo).
4. Implementar um controle de limite 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).
5. Impedir o cadastro de 2 usuários com o mesmo e-mail. Exibir mensagem indicativa deste erro.
6. Registrar data/hora do último login do usuário. Exibir essa data/hora no login (“Bem-vindo ... Seu último acesso ao sistema foi ...”)
7. Realizar backup das tabelas do sistema a partir do acionamento de uma determinada rota. Salvar log da realização deste backup.
8. Permitir a troca da senha (no caso do esquecimento) a partir de uma outra forma – como, por exemplo, o cadastro de uma pergunta e resposta do usuário no momento do seu cadastro. Na rota/rotina de solicitação de troca, verificar se a resposta está correta e realizar a alteração.

- Data da Entrega/Apresentação: **05/07/2024**
- Pode ser em duplas

Conceitos:

- Rotas e funções dos cadastros em funcionamento e os 2 recursos adicionais de segurança implementados corretamente: A

- 1 dos recursos ausentes: B

- 2 dos recursos ausentes: C