Engenharia de Segurança

Este documento descreve os requisitos de segurança do aplicativo do projeto A3 “My Health”, dividido por tópicos.

Validação de dados de entrada

Todas as entradas de dados de fontes externas (consumo de apis) ou de entrada de dados de pesquisa por parte do usuário precisam ser validadas, erros de formatação devem ser tratados automaticamente quando possível e caso contrário, o usuário deve ser informado sobre o erro de formatação.

Armazenamento de dados sensíveis

A arquitetura de banco de dados foi desenvolvida para armazenar o mínimo de informações do usuário possível, porém a senha de acesso a conta do usuário ainda é necessária, o armazenamento da senha de acesso deve ser feito exclusivamente em formato de hash1 sha-256 ao invés de texto simples, também será utilizado o uso de salt2 na senha para maior confidencialidade dos dados.

Limite de tentativa de acesso e recuperação

O sistema deve limitar a quantidade de tentativa de acesso, contabilizando as tentativas sem sucesso e bloqueando novas tentativas após um limite pré-definido ser atingido, a recuperação do acesso deve gerar um código de uso único no formato UUID3 v5, enviado para o e-mail cadastrado, ao acessar a url com o código, o mesmo deve ser automaticamente marcado como utilizado e o usuário deve atualizar a senha cadastrada. Não completar o processo de recuperação deve exigir a geração de um novo código de recuperação.

Confirmação de cadastro e aviso de alterações de configuração

Ao se cadastrar no aplicativo, o usuário só deve ter acesso completo às suas funcionalidades após confirmar o endereço de e-mail utilizado para criar o cadastro, alterações subsequentes de senha ou e-mail deve gerar uma nova confirmação a ser enviada no e-mail cadastrado, antes da alteração ser efetivada.

1. Hash é um algoritmo de criptografia que gera uma string alfanumérica de tamanho fixo a partir da leitura de dados, pode ser usado para identificar e validar de forma exclusiva esses dados.
2. Salt (sal) é uma técnica de gerar uma string de caracteres aleatórios para incluir na string de senha do usuário, antes do processo de geração da hash da senha, a fim de aumentar a segurança do usuário, mitigando ataques de tipos hash table ou força-bruta.
3. UUID significa Universally Unique Identifier (identificador único universal, em tradução livre).