Evil user stories

1. Como usuário malicioso, quero usar a força bruta para acessar contas não autorizadas no sistema usando credenciais comumente utilizadas;
Critérios de Aceitação:
- Limitar o número de tentativas erradas, num determinado intervalo de tempo. Notificar o usuário através de e-mail quando isso ocorrer.
- Bloquear o usuário após um determinado número de tentativas.
  Notificar o usuário através de e-mail quando isso ocorrer.
- Implementar captcha para realização do login.
- Implementar o cadastro de dispositivos confiáveis, exigindo uma autenticação de dois fatores quando o login for realizado de um novo dispositivo.
- Exigir criação de senhas fortes, utilizando os critérios da OWASP para validá-las.

2. Como usuário malicioso, pretendo executar SQL-Injection para poder acessar ou modificar dados do sistema de modo geral
Critérios de Aceitação:
- Fazer “limpeza” de caracteres em campos textuais de entrada
- Seguir recomendações da OWASP para prevenir SQL Injection
- Encriptar dados pessoais salvos na base de dados

3. Como usuário malicioso, pretendo injetar um código malicioso de modo a acessar ou modificar dados
Critérios de Aceitação:
- Fazer “limpeza” de caracteres em campos textuais de entrada
- Seguir recomendações da OWASP para prevenir Injeção de Código

4. Como usuário malicioso, pretendo utilizar credenciais roubadas para acessar as funcionalidades do sistema para as quais não tenho acesso.
Critérios de Aceitação:
- Implementar tempo de expiração de senha.
- Implementar o cadastro de dispositivos confiáveis, exigindo uma autenticação de dois fatores quando o login for realizado de um novo dispositivo.
- Exigir criação de senhas fortes, utilizando os critérios da OWASP para validá-las.

5. Como usuário malicioso, pretendo manipular dados para alterar os parâmetros de geração de relatórios, mostrando estoques inexistentes ou números incorretos.
Critérios de Aceitação:
- Realizar atualizações automáticas dos dados exibidos no dashboard, num curto intervalo de tempo
- Executar a exportação de relatórios através de códigos executados no lado servidor (*back-end*)
- Permitir a geração de relatórios assinados digitalmente, com possibilidade de validação posterior.