**Avaliação dos Riscos de Segurança e Privacidade**

1. Nome do consultor de segurança da equipe: **Milena Lara Reis Ferreira**

Levando em consideração os requisitos funcionais do sistema:

1. **(Segurança) Quais partes do projeto requerem modelos de ameaças antes da liberação?**

* RF001 - Cadastro de parceiros
* RF002 - Login de usuário
* RF008 - Envio de formulário para doação
* RF009 - Envio de formulário para recebimento de doação
* RF010 - Acompanhamento de doações registradas
* RF011 - Acompanhamento de solicitações registradas
* RF012 - Gerenciamento de entrada de doações
* RF013 - Gerenciamento de saída de doações
* RF015 - Geração de relatórios

1. **(Segurança) Quais partes do projeto requerem revisões do design de segurança antes da liberação?**

* Autenticação e autorização
  + RF002 - Login de usuário
* Formulários
  + RF001 – Cadastro de parceiros
  + RF008 – Formulário de doação
  + RF009 – Formulário de solicitação
* Gerenciamento de doações e solicitações
  + RF010 - Acompanhamento de doações registradas
  + RF011 - Acompanhamento de solicitações registradas
  + RF012 - Gerenciamento de entrada de doações
  + RF013 - Gerenciamento de saída de doações
* Visualização e exportação de dados
  + RF006 - Visualização de tabela de doações
  + RF015 - Geração de relatórios
* Notificações
  + RF014 – Notificações de campanhas

1. **(Segurança) Quais partes do projeto (se houver) exigirão um teste de penetração por um grupo de comum acordo que seja externo à equipe do projeto?**

* RF001 – Cadastro de parceiros
* RF002 - Login de usuário
* RF008 - Envio de formulário para doação
* RF009 - Envio de formulário para recebimento de doação
* RF012 - Gerenciamento de entrada de doações
* RF013 - Gerenciamento de saída de doações

1. **(Segurança) Existem outros requisitos de teste ou de análise considerados necessários pelo consultor de segurança para mitigar os riscos de segurança?**

Pensamos nestes testes adicionais, de acordo com as ameaças que devemos mitigar (Broken Access Control, Cryptographic Failures, Injection) e das práticas recomendadas no mercado:

* **Análise de Código Estático (Static Code Analysis / SAST):** análise automática do código-fonte para identificar falhas de segurança. Considerando que o nosso sistema será desenvolvido usando React.js no Front-ed e Spring Boot no Back-end, escolhemos a ferramenta **SonarQube**, que faz a análise de ambos. Além disso, vamos usar a ferramenta **npm audit** antes dos deploys.
* **Análise de Dependências e Bibliotecas (SCA – Software Composition Analysis)**: Iremos utilizar o **OWASP Dependency-Check** para verificar se as dependências instaladas no projeto possuem vulnerabilidades.
* **Testes de Autorização e Acesso (Access Control Tests)**: faremos um mapeamento das permissões de acordo com o Role dos usuários (parceiro, colaborador e ainda público geral - não autenticado) e as funcionalidades do sistema, criaremos casos de teste e executaremos testes manuais (no navegador ou no Swagger).
* **Verificação do armazenamento seguro de senhas**: Utilizar o site [bcrypt-generator.com](https://bcrypt-generator.com/) para verificar se a criptografia está sendo implementada corretamente - escolher alguns registros como amostra
* **Verificação de validade do JWT Token**: Utilizar a ferramenta de Debug do site [jwt.io](http://jwt.io) para verificar se o Token está sendo implementado corretamente, com assinatura válida e tempo de expiração) - escolher alguns registros como amostra
* **Testes de injeção SQL:** utilizaremos a ferramenta **OWASP ZAP**.

1. **(Segurança) Qual é o escopo específico dos requisitos de teste de fuzzing?**

identificar falhas de segurança, estouros, travamentos e comportamentos inesperados causados por entradas malformadas, aleatórias ou maliciosas.

* Formulários
  + RF001 – Cadastro de parceiros
  + RF008 – Formulário de doação
  + RF009 – Formulário de solicitação
* Endpoints de PUT, POST e PATCH da API REST
* Autenticação e sessão (RF002)
* Parâmetros em URLs

1. **(Privacidade) Qual é a Classificação de impacto de privacidade? A resposta para essa pergunta se baseia nas seguintes diretrizes:**
   * **P1 Risco de privacidade alto. O recurso, o produto ou o serviço armazena ou transfere PII (id), altera as configurações ou as associações de tipo de arquivo ou instala softwares.**
   * **P2 Risco de privacidade moderado. O único comportamento que afeta a privacidade no recurso, produto ou serviço é uma transferência de dados única, iniciada pelo usuário e anônima (por exemplo, o usuário clica em um link e o software vai para um site).**
   * **P3 Risco de privacidade baixo. Não há comportamento nesse recurso, produto ou serviço que afeta a privacidade. Nenhum dado anônimo ou pessoal é transferido, nenhum PII é armazenado na máquina, nenhuma configuração é alterada em nome do usuário e nenhum software é instalado.**

P1 – Risco de privacidade alto - O sistema armazena e manipula dados pessoais identificáveis (PII) de parceiros e usuários da ONG, como nome, e-mail, telefone, histórico de doações e solicitações.