Avaliação dos Riscos de Segurança e Privacidade

1. Nome do consultor de segurança da equipe:

Levando em consideração os requisitos funcionais do sistema:

1. (Segurança) Quais partes do projeto requerem modelos de ameaças antes da liberação?
2. (Segurança) Quais partes do projeto requerem revisões do design de segurança antes da liberação?
3. (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?
4. (Segurança) Existem outros requisitos de teste ou de análise considerados necessários pelo consultor de segurança para mitigar os riscos de segurança?
5. (Segurança) Qual é o escopo específico dos requisitos de teste de fuzzing?
6. (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.