Avaliação dos Riscos de Segurança e Privacidade

1. Nome do consultor de segurança da equipe:

Gabriel Ferreira Amaral

Levando em consideração os requisitos funcionais do sistema:

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

   Requerem modelos de ameaças (ex: STRIDE) antes da liberação:

   - **Módulo de autenticação (login/cadastro):** risco de spoofing, repudiation e information disclosure.
   - **Comunicação frontend ↔ backend:** risco de tampering e denial of service.
   - **Ações de solicitação de carona e autorização de motorista:** risco de elevation of privilege.
   - **Integração com o banco de dados:** risco de vazamento de dados sensíveis e manipulação não autorizada.

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

   Devem passar por revisão de design de segurança:

   - **Controle de acesso por tipo de usuário (motorista, passageiro, admin):** garantir que permissões não sejam burladas.
   - **Token de autenticação (JWT):** verificar se há expiração, assinatura e validação corretas.
   - **Criptografia de dados (senhas, dados pessoais):** uso adequado de hashing (ex: bcrypt para senhas).
   - **Rotas críticas (ex: solicitação/aceite de carona):** verificar se não é possível forjar ou interceptar chamadas.

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?

   Testes de penetração externos devem focar em:

   - **API REST do backend (Spring Boot):** endpoints públicos e protegidos.
   - **Módulo de login/autenticação:** tentativa de bypass, brute force e manipulação de JWT.
   - **Banco de dados:** injeções SQL, acesso não autorizado a informações.

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

   Sim:

   - **Testes automatizados de segurança (ex: OWASP ZAP, SonarQube Security):** avaliar código backend.
   - **Revisão de logs e auditoria:** para rastrear ações e evitar repúdio.
   - **Teste de HTTPS obrigatório:** garantir canal criptografado para todas as comunicações.
   - **Verificação de dependências (ex: mvn dependency-check):** evitar bibliotecas com CVEs conhecidas.

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

   Testes de fuzzing devem abranger:

   - **Endpoints da API:** envio de entradas malformadas, strings longas, dados inesperados.

- **Campos de formulário (cadastro, login, carona):** detectar crashes, exceções não tratadas, vazamentos.
- **Integração com o banco de dados:** simular entradas que possam causar comportamento anômalo.

6. (Privacidade) Qual é a Classificação de impacto de privacidade? A resposta para essa pergunta se baseia nas seguintes diretrizes:

   Classificação: P1 (Risco de privacidade alto)

   Justificativa:

- O sistema **armazena PII (Informações Pessoais Identificáveis)** como nome, e-mail, CPF e localização.
- Possui **autenticação com credenciais pessoais**.
- Registra e gerencia **rotas e pontos de encontro**, dados sensíveis de movimentação.
- Pode permitir que um usuário visualize o histórico de caronas de outro (dependendo do design).