**Avaliação dos Riscos de Segurança e Privacidade**

1. Nome do consultor de segurança da equipe: Vinicius Xavier Ramalho

Levando em consideração os requisitos funcionais do sistema:

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

O módulo de **autenticação e autorização**, pois lida diretamente com credenciais e controle de acesso a dados sensíveis.

O módulo de **gerenciamento de pacientes**, onde são armazenadas informações pessoais identificáveis, como nome, CPF, telefone, e histórico de consultas.

O módulo de **agendamento de consultas**, por envolver dados sensíveis e a possibilidade de conflitos ou manipulações indevidas.

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

O **controle de sessão** e gerenciamento de tokens JWT deve ser revisado para prevenir ataques como **session fixation** ou **token hijacking**.

A **API RESTful** exposta pelo backend deve ser revisada para evitar falhas como **exposição de dados sensíveis**, **injection attacks**, e **IDOR (Insecure Direct Object References)**.

O **sistema de permissões**, para garantir que usuários (pacientes, dentistas, recepcionistas) só tenham acesso aos dados e funcionalidades correspondentes ao seu perfil.

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?**

A aplicação como um todo deve passar por um **teste de penetração black-box**, com foco especial em, endpoints de autenticação, uploads e formulários e interfaces administrativas ou com maior privilégio.

O banco de dados também deve ser incluído no escopo do teste para identificar falhas como **SQL injection** ou **acesso indevido** por meio de configurações inseguras.

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

Sim. Recomendam-se os seguintes testes adicionais:

* **Teste de segurança automatizado com ferramentas como OWASP ZAP ou SonarQube**.
* **Verificação de dependências** usando ferramentas como **OWASP Dependency-Check** para identificar bibliotecas vulneráveis.
* **Revisões de código manuais** periódicas.
* Implementação de **logs seguros** e monitoramento para detectar padrões de comportamento suspeitos.

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

Os testes de fuzzing devem ser aplicados principalmente aos seguintes pontos:

* **Endpoints REST** que recebem entrada do usuário, como agendamento de consultas e cadastro de pacientes.
* **Campos de formulário** (nome, e-mail, data de nascimento, etc.), para detectar falhas de validação e tratamento inadequado de entrada.
* Áreas que lidam com **upload de arquivos**(por exemplo, envio de exames).

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

O sistema armazena dados sensíveis e PII, como nomes completos, contatos, CPF, e histórico de consultas médicas.

Também realiza autenticação de usuários e pode incluir integração com outros serviços (ex: envio de notificações por e-mail ou SMS), o que envolve transferência de dados.

Por isso, são necessárias políticas claras de **consentimento**, **armazenamento seguro**, **retenção e exclusão de dados**, e conformidade com a **LGPD**.