Avaliação dos Riscos de Segurança e Privacidade

1. Nome do consultor de segurança da equipe: Matheus Fernandes

Levando em consideração os requisitos funcionais do sistema:

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

- A geração e envio de pedidos via WhatsApp Business (RF-10), pois envolve integração externa e pode expor dados sensíveis.

- O cadastro e a manutenção de usuários internos (RF-02), pois trata de permissões e acessos administrativos.

- A visualização e filtragem de históricos de compras por dados pessoais (RF-11), que envolve PII.

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

- A autenticação e controle de acesso de administradores e supervisores (RF-02), para evitar acessos indevidos.

- A funcionalidade de exportação de catálogos (RF-05), que pode incluir dados sensíveis.

- A geração de relatórios e histórico de compras (RF-04 e RF-11), para evitar exposição indevida de dados pessoais.

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 interface pública da loja (catálogo online e carrinho – RF-08 a RF-10), para mitigar riscos de injeções, CSRF, e XSS.

- As APIs utilizadas para comunicação com o banco de dados e WhatsApp Business.

1. (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 validação de input de usuário devem ser implementados para prevenir injeções de código.

- Devem ser aplicadas políticas de senhas fortes e armazenamento seguro (hash/salt) das credenciais dos usuários.

- Monitoramento de logs de acesso e alteração de dados sensíveis.

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

O fuzzing deve ser aplicado principalmente nas entradas de formulários de cadastro, login e geração de pedidos (RF-02, RF-07, RF-10), para identificar vulnerabilidades de entrada maliciosa.

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 informações pessoais identificáveis (PII) como nome, CPF e telefone dos clientes (RF-07, RF-11), além de gerenciar permissões de usuários administrativos e enviar dados via integração externa (WhatsApp Business).