## PASTA planilha

|  |  |
| --- | --- |
| **Estágios** | **Empresa de tênis** |
| **I. Definir objetivos de negócios e segurança** | O aplicativo tem objetivos claros, que incluem:   * Facilitar a comunicação entre compradores e vendedores: Permitir mensagens diretas para incentivar o bom atendimento. * Avaliações de vendedores: Estimular a confiança no sistema e a qualidade do serviço prestado. * Opções de pagamento variadas: Proporcionar uma experiência de checkout tranquila e reduzir problemas legais associados ao manuseio de pagamentos. |
| **II. Definir o escopo técnico** | Lista de tecnologias usadas pelo aplicativo:  ● API (Interface de Programação de Aplicações)  ● PKI (Infraestrutura de Chaves Públicas)  ● AES (Sistema de Criptografia Avançada)  ● SHA-256  ● SQL  Essas tecnologias não só melhoram a experiência do usuário como oferecem uma base segura para o crescimento da aplicação. A priorização de APIs, por exemplo, é importante, mas deve-se garantir que as configurações estejam protegidas contra ataques comuns, como injeções de código. |
| **III.** **Decompor aplicação** | [Sample data flow diagram](https://docs.google.com/presentation/d/1ol7y79popTFfNHM-90ES-H-i1Lpd0YNvPShxBlXozjg/template/preview?resourcekey=0-DZAkf7Vzh2PXsP-j3oXV-g) |
| **IV. Análise de ameaças** | Duas ameaças importantes que podem impactar o aplicativo incluem:   * **Injeção de SQL:** Um atacante pode explorar campos de entrada (como formulários de login) para enviar comandos maliciosos ao banco de dados, obtendo acesso a informações sensíveis ou modificando dados. * ***Hijacking de Sessão:*** *Se tokens de sessão não forem protegidos, um invasor pode interceptar uma sessão ativa e agir como se fosse o usuário legítimo.* |
| **V. Análise de vulnerabilidade** | Duas vulnerabilidades que podem ser exploradas por essas ameaças:   * **Falta de declarações preparadas (Prepared Statements):** Torna o banco de dados suscetível a ataques de injeção de SQL, pois os comandos maliciosos não são filtrados corretamente. * ***Tokens de API mal configurados****: Tokens expostos ou sem validação adequada permitem que invasores acessem recursos protegidos.* |
| **VI. Modelagem de ataque** | [Sample attack tree diagram](https://docs.google.com/presentation/d/1FmWLyHgmq9XQoVuMxOym2PHO8IuedCkan4moYnI-EJ0/template/preview?usp=sharing&resourcekey=0-zYPY7AhPJdcClXamlAfOag) |
| **VII. Análise de risco e impacto** | 1. Hashing seguro com SHA-256 para senhas e dados sensíveis. 2. Uso de prepared statements para evitar injeções de SQL. 3. Política robusta de senhas para prevenir ataques de força bruta. 4. Princípio do menor privilégio para limitar acessos desnecessários. |