

Planilha PASTA

Cenário: Você faz parte da crescente equipe de segurança de uma empresa para entusiastas e colecionadores de tênis. A empresa está se preparando para lançar um app para dispositivos móveis que facilite a compra e a venda de calçados pelos clientes.

Você está executando um modelo de ameaças do aplicativo usando a estrutura PASTA. Você passará por cada um dos sete estágios da estrutura para identificar os requisitos de segurança do novo aplicativo da empresa de tênis.

Estágios	Empresa de tênis
I. Definir objetivos de negócios e segurança	<ul style="list-style-type: none">• Os usuários podem criar perfis de membros internamente ou conectando contas externas.• O aplicativo deve processar transações financeiras.• O aplicativo deve estar em conformidade com o PCI-DSS.
II. Definir o escopo técnico	<p>Lista de tecnologias utilizadas pelo aplicativo:</p> <ul style="list-style-type: none">• Interface de programação de aplicativos (API)• Infraestrutura de chave pública (PKI)• SHA-256• SQL <p>APIs facilitam a troca de dados entre clientes, parceiros e funcionários, portanto, devem ser priorizadas. Elas lidam com muitos dados sensíveis enquanto conectam vários usuários e sistemas entre si. No entanto, detalhes como quais APIs estão sendo utilizadas devem ser considerados antes de priorizar uma tecnologia em detrimento de outra. Portanto, elas podem ser mais propensas a vulnerabilidades de segurança porque há uma superfície de ataque maior.</p>
III. Decompor aplicação	Diagrama de fluxo de dados
IV. Análise de ameaças	<ul style="list-style-type: none">• <i>Injeção</i>• <i>Sequestro de sessão</i>

V. Análise de vulnerabilidade	<ul style="list-style-type: none"> • <i>Falta de instruções preparadas</i> • <i>Token de API quebrado</i>
VI. Modelagem de ataque	PASTA - Árvore de ameaça
VII. Análise de risco e impacto	SHA-256, procedimentos de resposta a incidentes, política de senhas, princípio do menor privilégio
