Criptografia Simétrica

A criptografia simétrica usa a mesma chave para criptografar e descriptografar os dados. É rápida e eficiente, mas apresenta o problema da distribuição segura da chave.

Exemplo: AES (Advanced Encryption Standard)
Um sistema de mensagens usa AES para criptografar os dados antes do envio. O destinatário precisa da mesma chave para descriptografá-los.

Criptografia Assimétrica

Utiliza um par de chaves: uma pública para criptografar e uma privada para descriptografar. É mais segura para comunicação, mas mais lenta que a simétrica.

Exemplo: RSA (Rivest-Shamir-Adleman)
Um site usa RSA para proteger a troca de chaves na comunicação HTTPS. O navegador criptografa dados com a chave pública do servidor, e só ele pode descriptografar com sua chave privada.

Vulnerabilidades em Aplicações Web

Erros no desenvolvimento podem expor aplicações a ataques.

Principais vulnerabilidades:

1. **SQL Injection** – Invasores inserem código SQL malicioso para acessar ou modificar um banco de dados.
    - **Exemplo***: `SELECT * FROM users WHERE username = 'admin' OR '1'='1';`*
2. **Cross-Site Scripting (XSS)** – Inserção de scripts maliciosos em páginas web para roubar dados do usuário.
    - **Exemplo:** *`<script>alert('Hackeado');</script>`*
3. **Cross-Site Request Forgery (CSRF)** – Induz um usuário autenticado a executar ações indesejadas em um site.
    - **Exemplo:** Link malicioso que força a transferência de dinheiro quando clicado.