Boas práticas de Segurança da Informação - *Injeção (XXE - XML External Entities, SQL Injection)*

- **Vulnerabilidade: SQL Injection**

- SQL Injection é uma vulnerabilidade comum em aplicativos da web, onde os invasores podem inserir comandos SQL maliciosos em campos de entrada, como formulários de login, campos de pesquisa ou parâmetros de URL. Se a aplicação não sanitizar corretamente esses dados, os atacantes podem manipular a consulta SQL original e obter acesso não autorizado a informações sensíveis, alterar, excluir ou manipular dados no banco de dados.

- **Boa prática para mitigar SQL Injection:**

- Usar Consultas Parametrizadas ou Prepared Statements: Em vez de construir consultas SQL dinamicamente concatenando strings, é recomendado o uso de **consultas parametrizadas** ou **prepared statements** fornecidos pela linguagem de programação ou framework utilizado. Isso separa os dados dos comandos SQL, tornando mais difícil para os invasores injetarem código malicioso.

- **Escapar e Validar Dados de Entrada:**

- Sempre escape e valide os dados de entrada antes de usá-los em consultas SQL. Isso garante que os caracteres especiais sejam tratados corretamente e evita que os invasores explorem a vulnerabilidade.

- **Princípio do Menor Privilégio:**

- Garantir que o usuário ou aplicativo tenha apenas os privilégios necessários no banco de dados. Isso limita o impacto de um ataque bem-sucedido.

- Banco de dados e servidor atualizados com as últimas correções de segurança. Isso reduz a exposição à vulnerabilidades conhecidas.

- Essas boas práticas ajudam a prevenir ataques de injeção SQL e proteger os aplicativos da web contra essa ameaça comum. No entanto, é importante lembrar que a segurança é um processo contínuo e deve ser abordada em todas as etapas do desenvolvimento de software.