Vulnerabilidades Web

Introduções a conceitos e bugs usados em ataques de web hacking.

- SQL Injection

SQL Injection

O SQL Injection é uma vulnerabilidade web que consiste em um payload malicioso que interfere com as *queries* que uma aplicação faz para sua base de dados. A exploração desta vulnerabilidade pode permitir que um atacante acesse informações de outros usuários, ou quaisquer outra presente na base de dados que esteja sendo usada pela aplicação afetada. Dependendo da aplicação, uma vulnerabilidade de SQL injection pode, inclusive, ser escalada para comprometer o servidor que hospeda a aplicação e outras partes da infraestrutura de back-end.
A vulnerabilidade possui longo histórico dentro da área de segurança web, atualmente estando em 1º na lista da OWASP Top Ten.

Exemplo de ocorrência

Quando estamos procurando por um conteúdo específico dentro de um site e usamos uma brra de busca, esta será responsável por enviar *queries* para o banco de dados do servidor, que por sua vez retornará as informações que são relevantes à nossa busca.