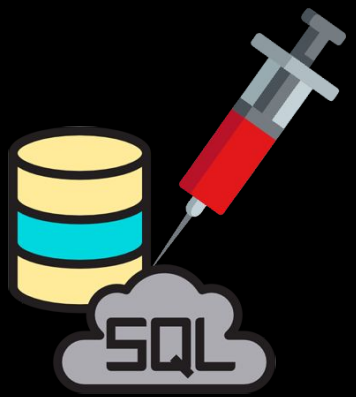
Out-Of-Band SQLi

OOB

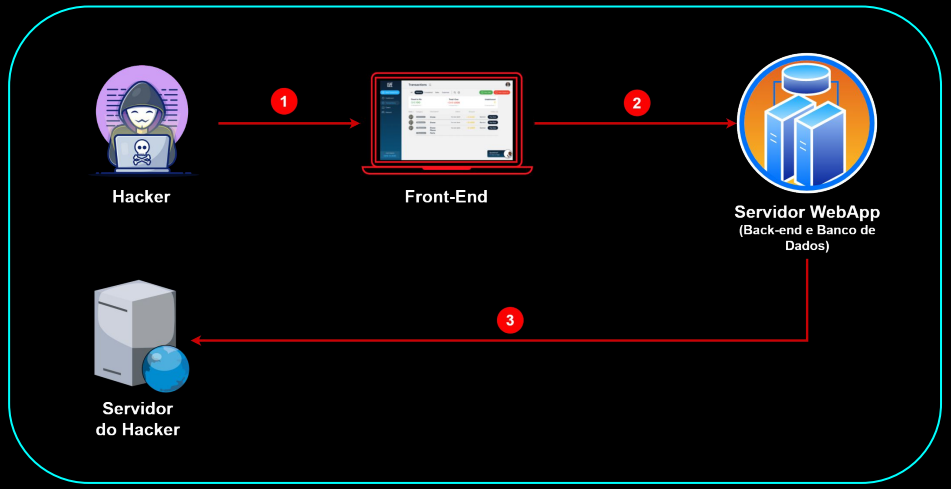
Out-Of-Band SQLi



Este tipo de SQL Injection não é muito comum, principalmente porque depende de funcionalidades ativas no servidor do banco de dados a ser utilizadas pela aplicação web. Out-Of-Band SQL Injection ocorre quando o atacante / hacker não é capaz de usar o mesmo canal para lançar os ataques e recolher os resultados.

Assim sendo, este tipo de SQLi depende da capacidade do servidor do banco de dados conseguir fazer requisições DNS e HTTP para enviar a informação do banco de dados para o atacante / hacker. Este é o caso do comando **xp_dirtree** do **Microsoft SQL Server**, que pode ser utilizado para fazer requisições DNS para um servidor controlado pelo atacante / hacker. O mesmo acontece com o pacote **UTL_HTTP** em **bases de dados ORACLE**, que pode ser utilizado para fazer requisições HTTP.

O que é SQL Injection - Exemplo



1 - O Hacker acede à aplicação web a partir do seu browser e injeta o payload SQL num dos inputs de usuário. Este payload consiste em fazer uma requisição DNS para o seu servidor.

2 - O Hacker submete a requisição Web com o respectivo payload como input de usuário. Esta requisição é enviado do browser do hacker para o servidor da aplicação Web.

3 - O servidor da aplicação web processa a requisição do hacker. Aqui, o payload do hacker é executado como sendo parte da query SQL do back-end o que gera uma interação Out-Of-Band, ou seja, o servidor da aplicação web comunica com o servidor controlado pelo hacker.