

Inyección SQL

Inyección SQL

- Consiste en inyectar una sentencia SQL en una entrada
- Previamente hay que escapar el comando
- Mediante este ataque se puede
 - Leer, insertar, eliminar o realizar un DROP

Inyección SQL - Ejemplo

Carlos

“SELECT * FROM usuarios WHERE nombre = ‘Carlos’ ”

Carlos’;DROP TABLE usuarios;SELECT * FROM usuarios WHERE
usuario=‘

“SELECT * FROM usuarios WHERE nombre = ‘Carlos’;DROP
TABLE usuarios;SELECT * FROM usuarios WHERE usuario=‘’ ”