

“ ‘; DROP TABLES -- ”

# Disclaimer

- SQL-injection vulnerability's still exist everywhere
- Don't do it on anything that you don't own or have permission to in writing
- Not my fault if you do 🙄

# What is SQL Injection

- `SELECT * FROM usersTable WHERE username = ?`
- *? Gets replaced with your input*

# What is SQL Injection

- `SELECT * FROM usersTable WHERE username = ?`
- *? Gets replaced with your input*
- `SELECT * FROM usersTable WHERE secret = "mydog1"`

# What is SQL Injection

- `SELECT * FROM usersTable WHERE username = ?`
- *? Gets replaced with your input*
- `SELECT * FROM usersTable WHERE secret = "mydog1"`
- `SELECT * FROM usersTable WHERE secret = " mydog1 " OR 1=1 -- "`

# What you can do with it

- Bypass authentication ( `"or 1=1 --` )
- View, Modify or Delete database records ( `' ; drop table [name] --` )
- A lot of websites are still vulnerable because a lot of tutorials online are outdated and teach people these flaws
- Never trust what a user inputs

# Activity

- 1. DVWA
  - Open Kali
  - Follow our instructions :-D
  - Try hack stuff (**<https://tinyurl.com/comsecsqlcheatsheet>**)
- 2. CTF
  - FBCTF – Product Manager
  - Have fun