2Mrt SQL injection

WORKSHop

SQL = Structured Query Lange

* Goal

Using Burp Suite   Works as Proxy and Intercepts

Get data From Tables

Demo 1 - Juice Shop

Typical Query

Use extra conditions

Also with comments

Start with quote '

Then find out what SQL it is

Place url: ' or 1=1

123 UNION SELECT SQL 1,2,3,4,5,6 From SQLite .....

Some sites are sanitised so use Burp Suite

BLIND SQL injection

Blind SQL injec is the same as SQL inj but without the Response

Use SQL map

Second level SQL inj

- Use comment on an existing user