

techtrick.in

Set up your own Lab for practicing SQL injection and XSS

Akash

5-7 minutos

I hope you learned about the Sql injection and XSS. But you may curious to practice the SQLi and XSS attacks. we know that doing the attack on third-party website is crime.

So how can we do the practice? Here is the solution for you friends. Why shouldnt set up your own web application ? Yes, you can setup your own Pen Testing lab for practicing the XSS and SQLi vulnerabilities. The lab we will be using for demonstration is SQLi Labs.

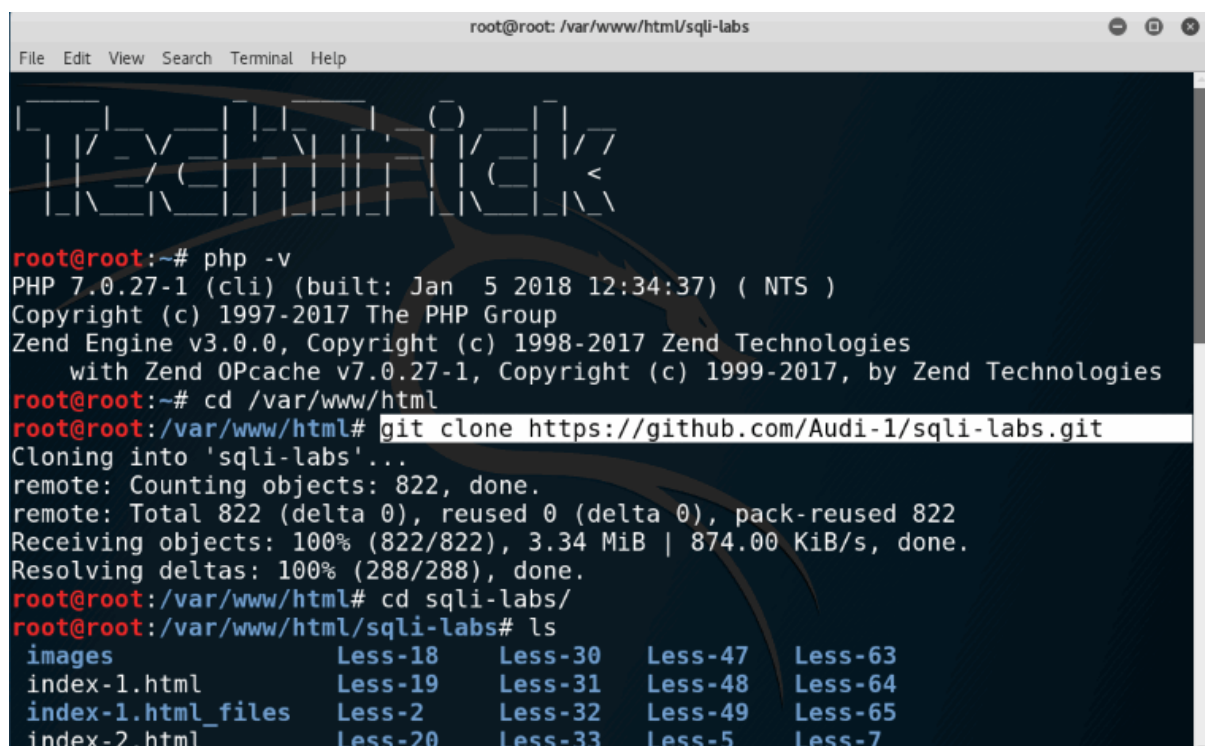
Lets Start with Set up your own Lab for practicing SQL injection

Step 1 :- In latest version of kali we are having PHP version 7.xxx which does not support MySQL functions because it support MySQLi functions.

So Start Kali Linux and open a terminal just type the following command :-

```
php-v  
cd /var/www/html
```

```
git clone https://github.com/Audi-1/sqli-labs.git
```



```

root@root: /var/www/html/sqli-labs
File Edit View Search Terminal Help

root@root:~# php -v
PHP 7.0.27-1 (cli) (built: Jan  5 2018 12:34:37) ( NTS )
Copyright (c) 1997-2017 The PHP Group
Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies
    with Zend OPcache v7.0.27-1, Copyright (c) 1999-2017, by Zend Technologies
root@root:~# cd /var/www/html
root@root:/var/www/html# git clone https://github.com/Audi-1/sqli-labs.git
Cloning into 'sqli-labs'...
remote: Counting objects: 822, done.
remote: Total 822 (delta 0), reused 0 (delta 0), pack-reused 822
Receiving objects: 100% (822/822), 3.34 MiB | 874.00 KiB/s, done.
Resolving deltas: 100% (288/288), done.
root@root:/var/www/html# cd sqli-labs/
root@root:/var/www/html/sqli-labs# ls
images                Less-18      Less-30      Less-47      Less-63
index-1.html          Less-19      Less-31      Less-48      Less-64
index-1.html_files    Less-2       Less-32      Less-49      Less-65
index-2.html          Less-20      Less-33      Less-5       Less-7

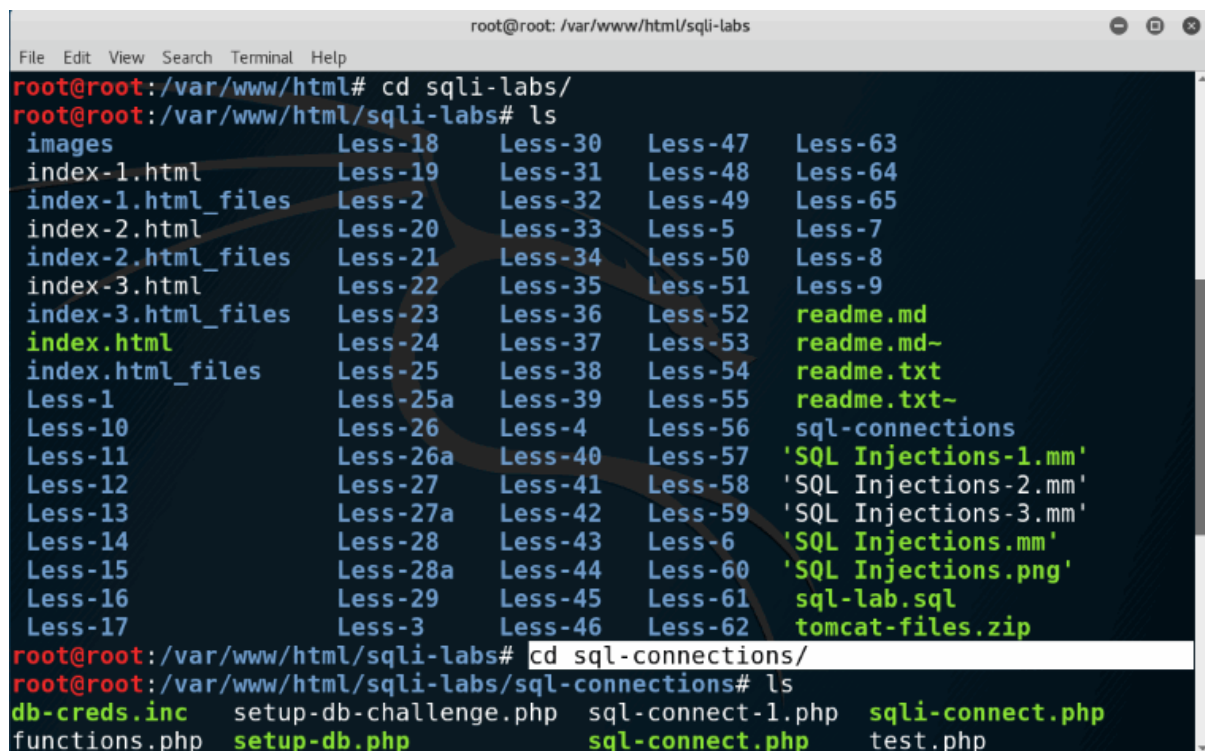
```

Step 2 :- this will install it, now type : **cd sqli-labs** to go to the directory, and type **ls** to see what is in there.

```
cd sqli-labs
```

```
cd sql-connections
```

```
ls
```



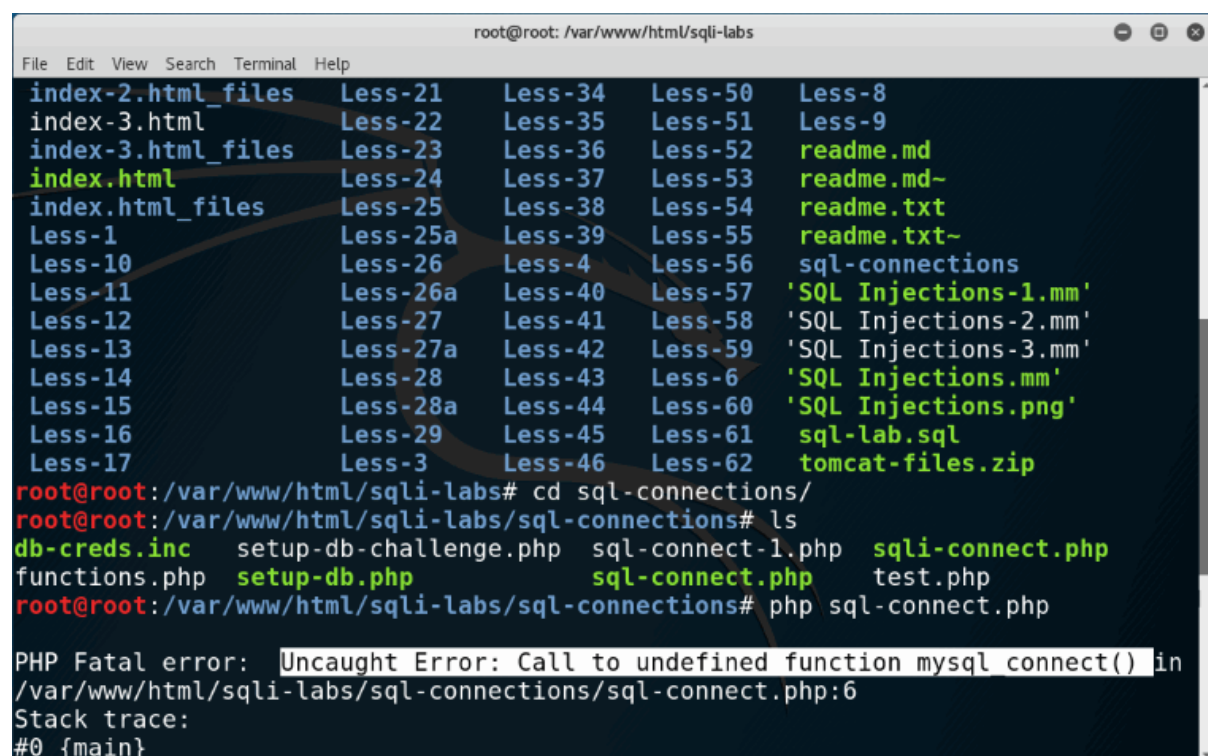
```

root@root:/var/www/html/sqli-labs# cd sqli-labs/
root@root:/var/www/html/sqli-labs# ls
images                Less-18      Less-30      Less-47      Less-63
index-1.html          Less-19      Less-31      Less-48      Less-64
index-1.html_files    Less-2       Less-32      Less-49      Less-65
index-2.html          Less-20      Less-33      Less-5       Less-7
index-2.html_files    Less-21      Less-34      Less-50      Less-8
index-3.html          Less-22      Less-35      Less-51      Less-9
index-3.html_files    Less-23      Less-36      Less-52      readme.md
index.html            Less-24      Less-37      Less-53      readme.md~
index.html_files      Less-25      Less-38      Less-54      readme.txt
Less-1                Less-25a     Less-39      Less-55      readme.txt~
Less-10               Less-26      Less-4       Less-56      sql-connections
Less-11               Less-26a     Less-40      Less-57      'SQL Injections-1.mm'
Less-12               Less-27      Less-41      Less-58      'SQL Injections-2.mm'
Less-13               Less-27a     Less-42      Less-59      'SQL Injections-3.mm'
Less-14               Less-28      Less-43      Less-6       'SQL Injections.mm'
Less-15               Less-28a     Less-44      Less-60      'SQL Injections.png'
Less-16               Less-29      Less-45      Less-61      sql-lab.sql
Less-17               Less-3       Less-46      Less-62      tomcat-files.zip
root@root:/var/www/html/sqli-labs# cd sql-connections/
root@root:/var/www/html/sqli-labs/sql-connections# ls
db-creds.inc  setup-db-challenge.php  sql-connect-1.php  sqli-connect.php
functions.php  setup-db.php            sql-connect.php    test.php

```

Step 3 :- when i tried to setup the sql-labs ,I know something is wrong in setup-db.php see below screenshot.

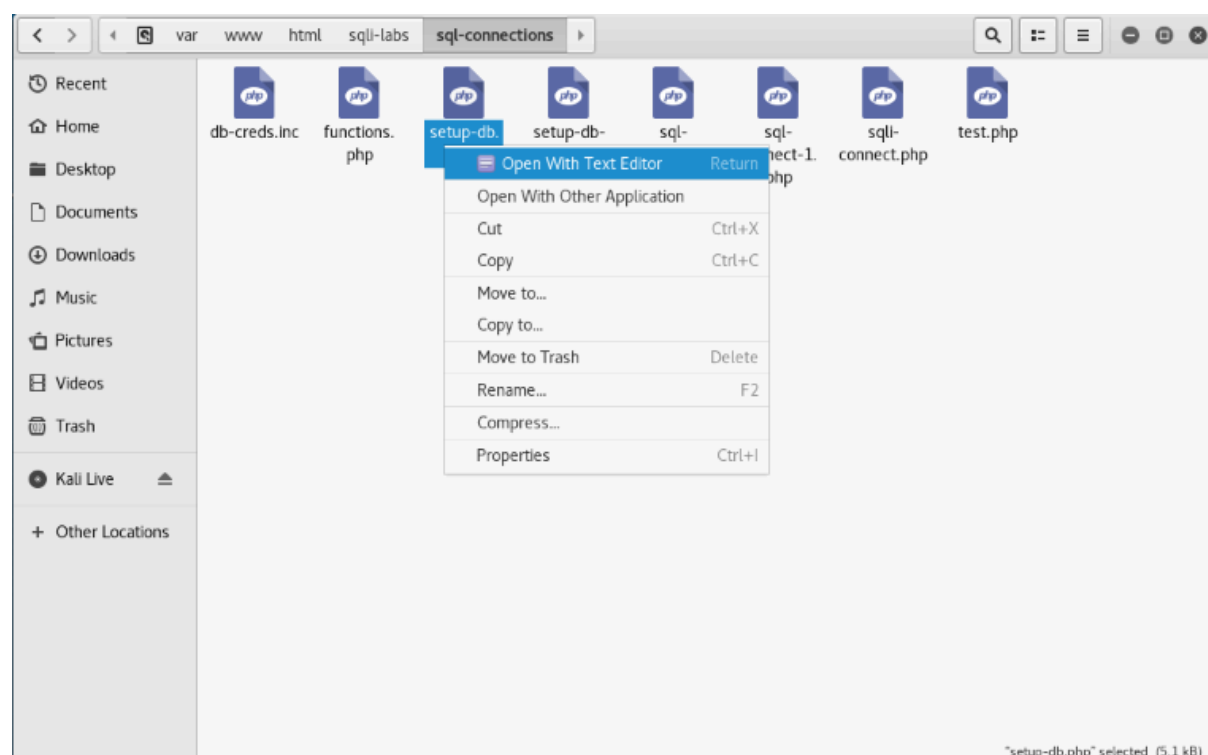
[php sql-connect.php



```
root@root: /var/www/html/sql-labs
File Edit View Search Terminal Help
index-2.html_files Less-21 Less-34 Less-50 Less-8
index-3.html Less-22 Less-35 Less-51 Less-9
index-3.html_files Less-23 Less-36 Less-52 readme.md
index.html Less-24 Less-37 Less-53 readme.md~
index.html_files Less-25 Less-38 Less-54 readme.txt
Less-1 Less-25a Less-39 Less-55 readme.txt~
Less-10 Less-26 Less-4 Less-56 sql-connections
Less-11 Less-26a Less-40 Less-57 'SQL Injections-1.mm'
Less-12 Less-27 Less-41 Less-58 'SQL Injections-2.mm'
Less-13 Less-27a Less-42 Less-59 'SQL Injections-3.mm'
Less-14 Less-28 Less-43 Less-6 'SQL Injections.mm'
Less-15 Less-28a Less-44 Less-60 'SQL Injections.png'
Less-16 Less-29 Less-45 Less-61 sql-lab.sql
Less-17 Less-3 Less-46 Less-62 tomcat-files.zip
root@root:/var/www/html/sql-labs# cd sql-connections/
root@root:/var/www/html/sql-labs/sql-connections# ls
db-creds.inc setup-db challenge.php sql-connect-1.php sql-connect.php
functions.php setup-db.php sql-connect.php test.php
root@root:/var/www/html/sql-labs/sql-connections# php sql-connect.php

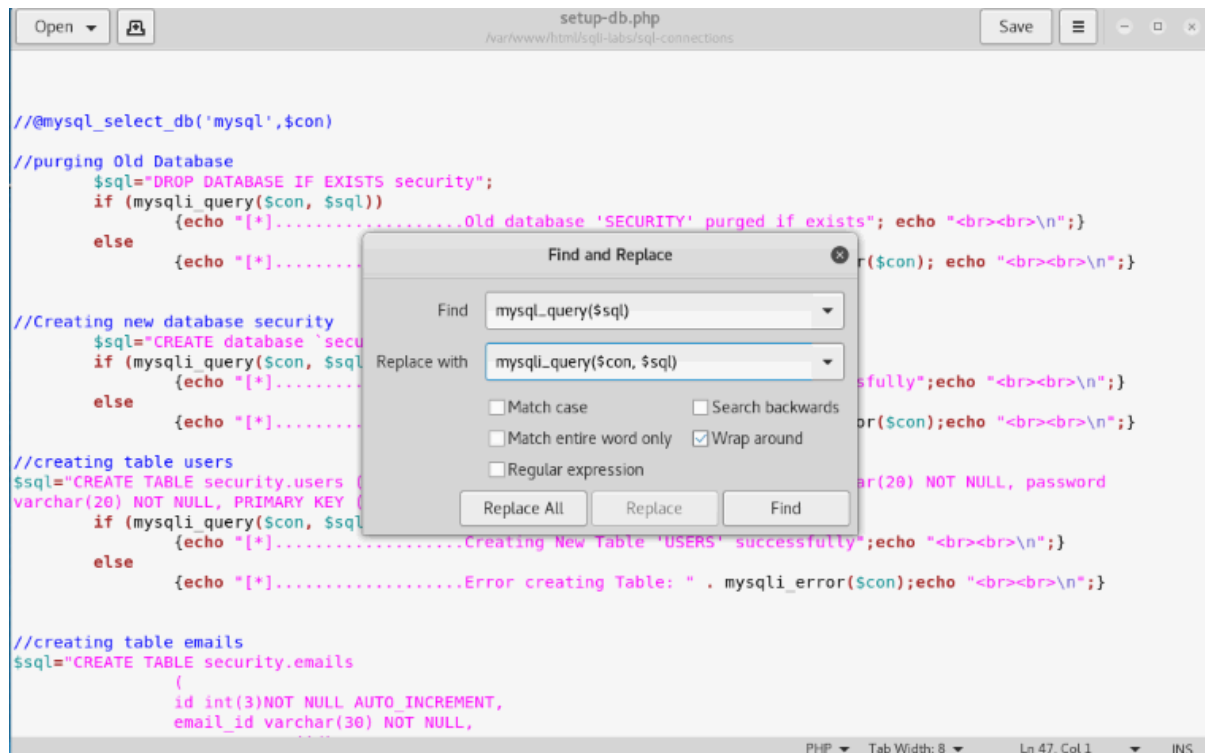
PHP Fatal error:  Uncaught Error: Call to undefined function mysql_connect() in
/var/www/html/sql-labs/sql-connections/sql-connect.php:6
Stack trace:
#0 {main}
```

Step 4 :- Lets solve this error to open setup-db.php file under root/var/www/html/sql-labs

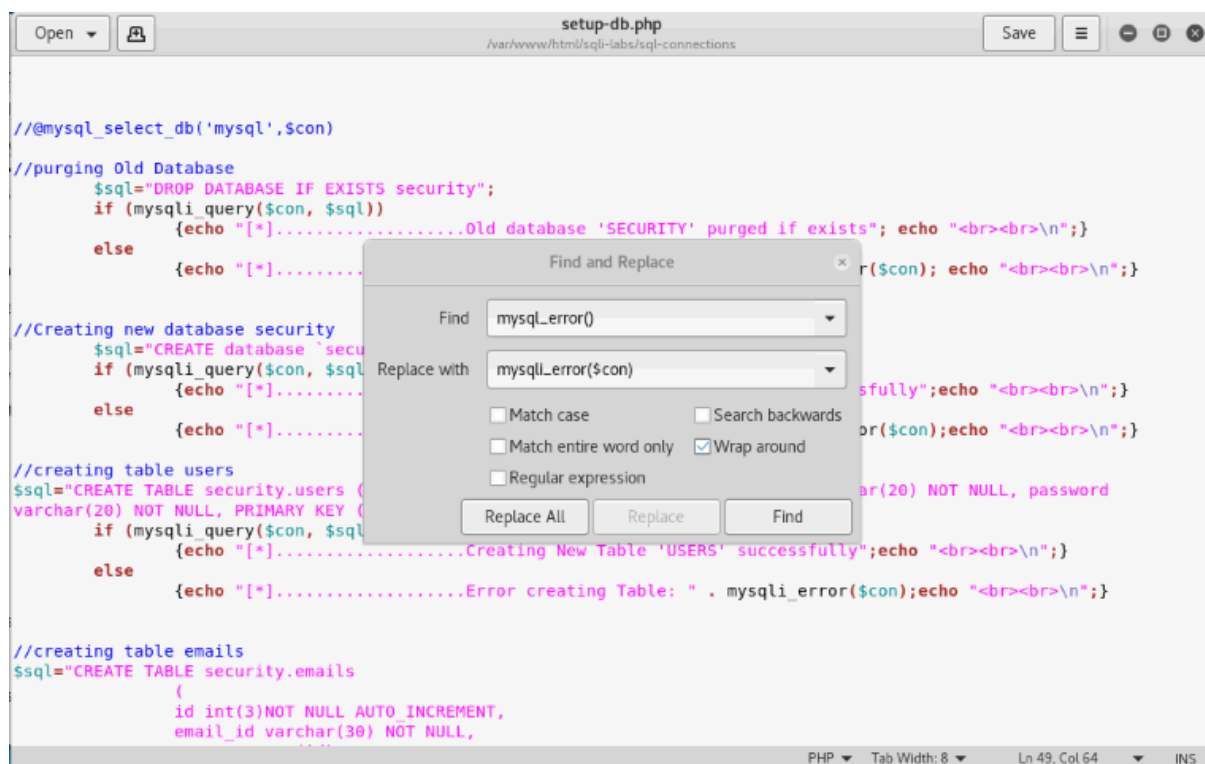


Step 5 :- To Solve this problem you have to replace

mysql_connect() with mysqli_connect() and mysql_query(\$sql) with mysqli_query(\$con, \$sql)

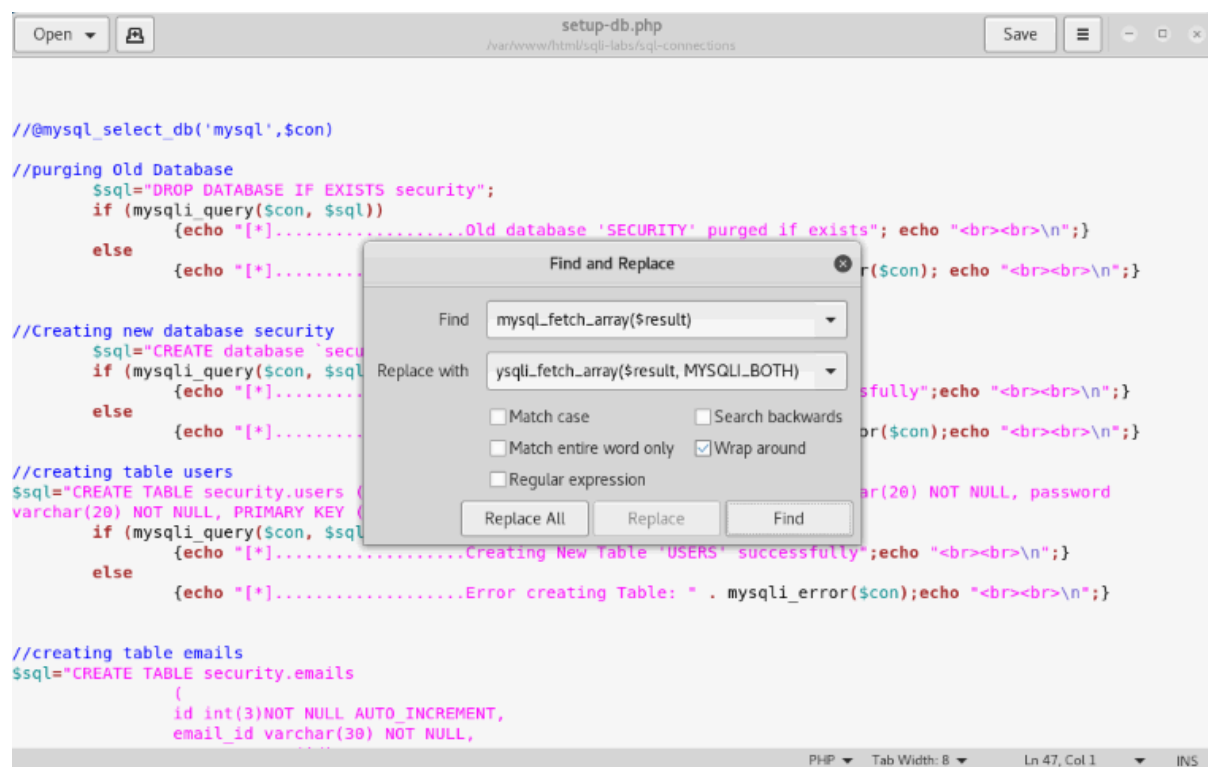


Step 6 :- If exists **mysql_error()** then replace with **mysqli_error(\$con)**

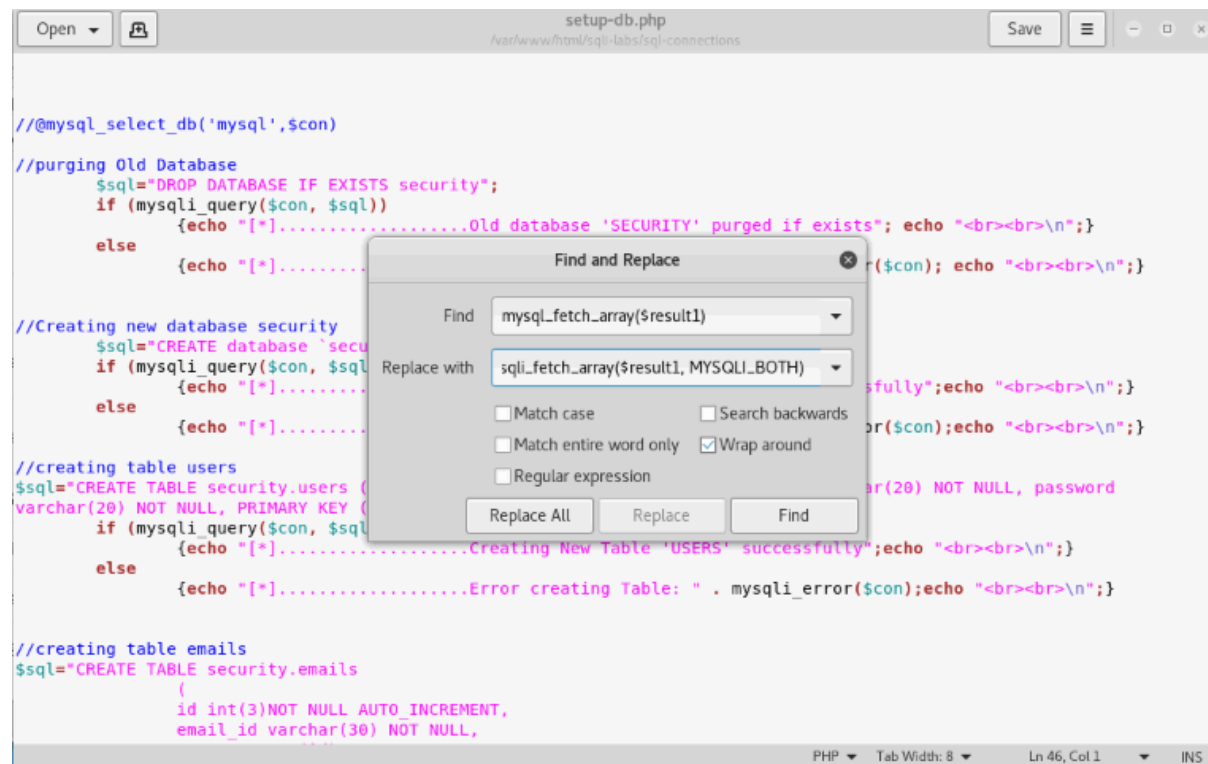


Step 7 :- If exists **mysql_fetch_array(\$result)** then replace with

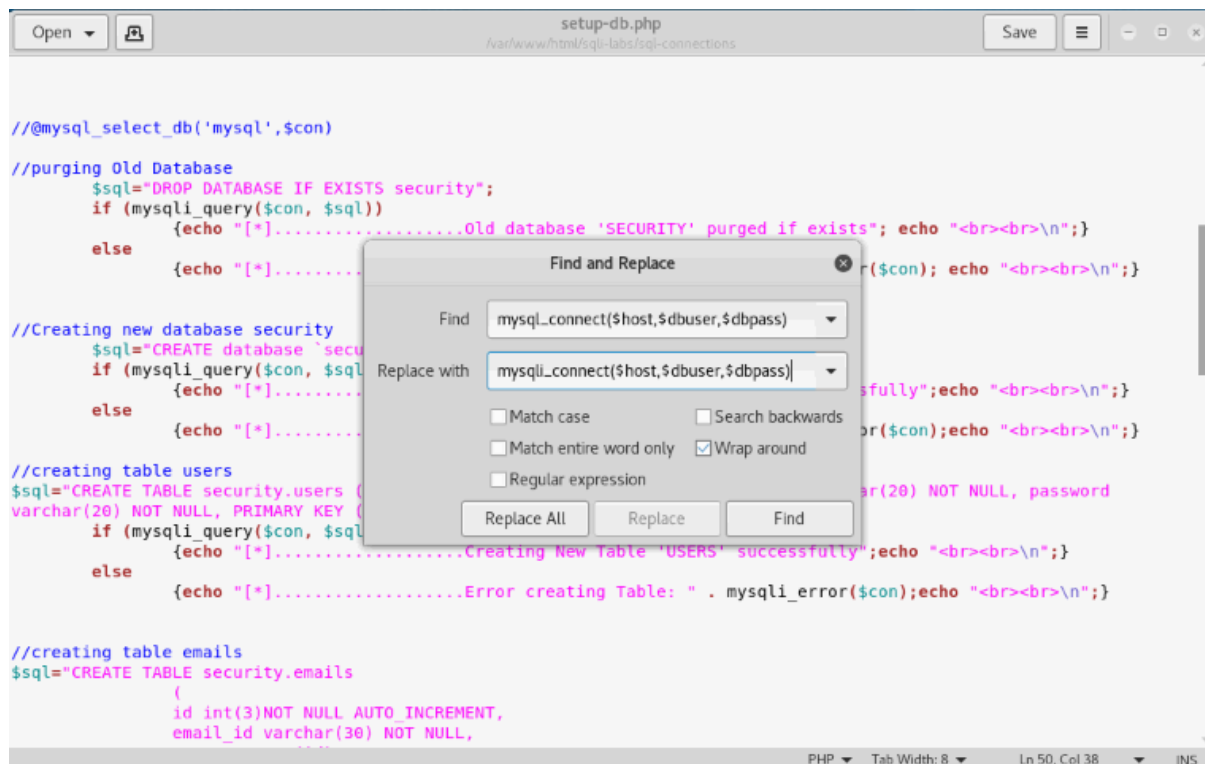
mysqli_fetch_array(\$result, MYSQLI_BOTH)



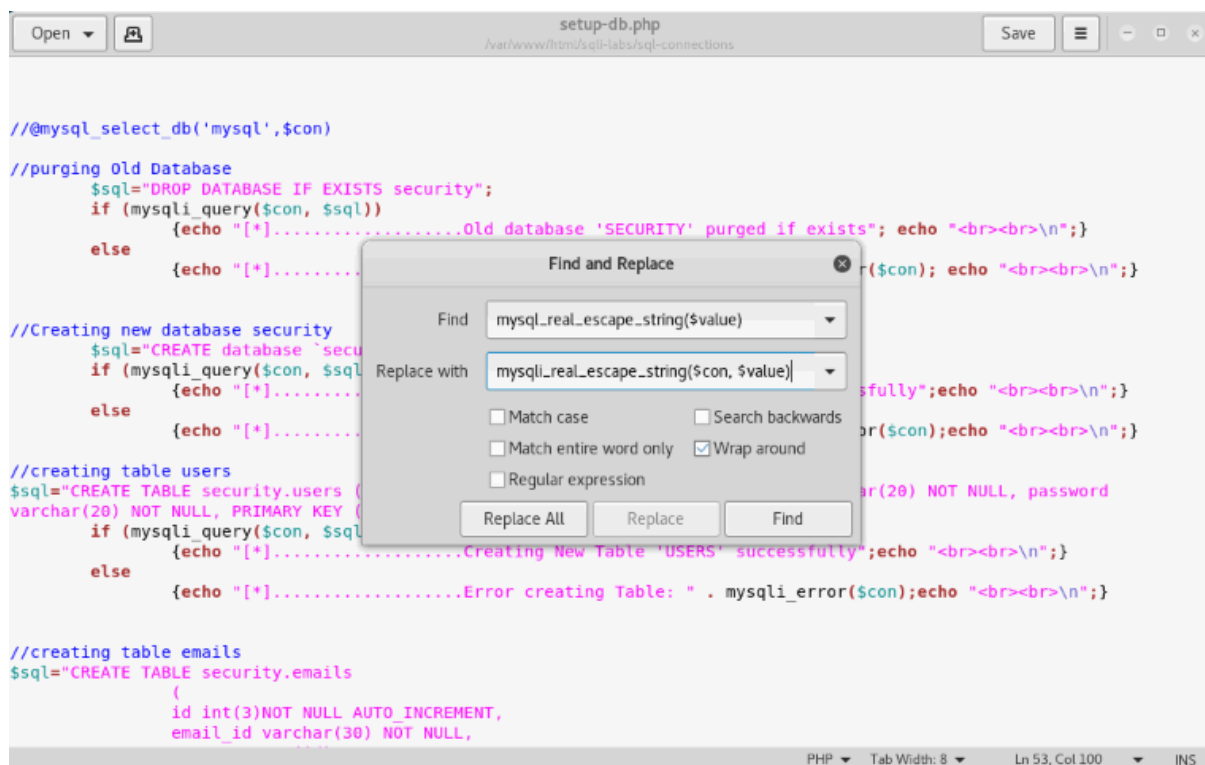
Step 8 :- If exists `mysqli_fetch_array($result1)` then replace with `mysqli_fetch_array($result1, MYSQLI_BOTH)`



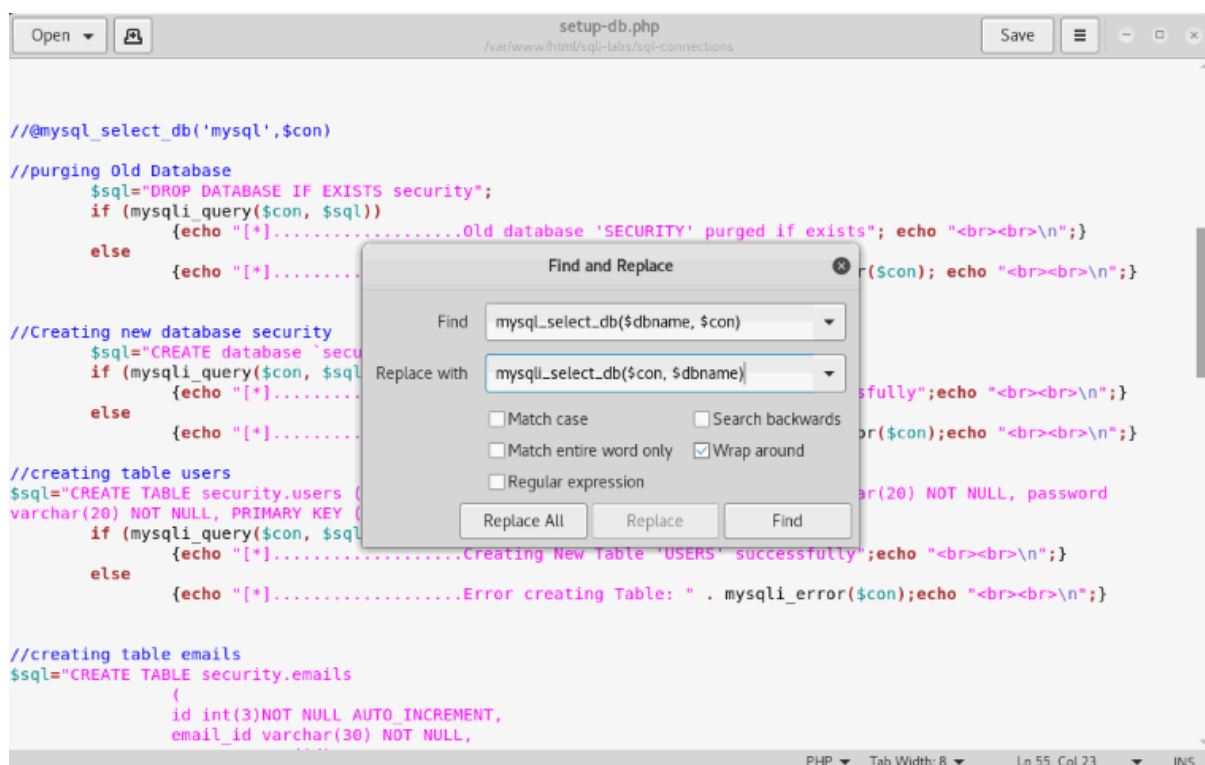
Step 9 :- If exists `mysqli_connect($host,$dbuser,$dbpass)` then replace with `mysqli_connect($host,$dbuser,$dbpass)`



Step 10 :- If exists `mysql_real_escape_string($value)` then replace with `mysql_real_escape_string($con, $value)`



Step 11 :- If exists `mysql_select_db($dbname, $con)` then replace with `mysqli_select_db($con, $dbname)`



Step 12 :- Now open kali terminal and move to this folder and give permissions to sqli-labs folder and give permissions to all files and folder using the following commands:-

```
cd ../  
chmod 777 sqli-labs  
cd sqli-labs  
chmod 777 *
```

```

root@root: /var/www/html/sqli-labs
File Edit View Search Terminal Help
Less-10 Less-26 Less-4 Less-56 sql-connections
Less-11 Less-26a Less-40 Less-57 'SQL Injections-1.mm'
Less-12 Less-27 Less-41 Less-58 'SQL Injections-2.mm'
Less-13 Less-27a Less-42 Less-59 'SQL Injections-3.mm'
Less-14 Less-28 Less-43 Less-6 'SQL Injections.mm'
Less-15 Less-28a Less-44 Less-60 'SQL Injections.png'
Less-16 Less-29 Less-45 Less-61 sql-lab.sql
Less-17 Less-3 Less-46 Less-62 tomcat-files.zip
root@root:/var/www/html/sqli-labs# cd sql-connections/
root@root:/var/www/html/sqli-labs/sql-connections# ls
db-creds.inc setup-db-challenge.php sql-connect-1.php sqli-connect.php
functions.php setup-db.php sql-connect.php test.php
root@root:/var/www/html/sqli-labs/sql-connections# php sql-connect.php

PHP Fatal error: Uncaught Error: Call to undefined function mysql_connect() in
/var/www/html/sqli-labs/sql-connections/sql-connect.php:6
Stack trace:
#0 {main}
  thrown in /var/www/html/sqli-labs/sql-connections/sql-connect.php on line 6
root@root:/var/www/html/sqli-labs/sql-connections# cd ../
root@root:/var/www/html/sqli-labs# cd ../
root@root:/var/www/html# chmod 777 sqli-labs/
root@root:/var/www/html# cd sqli-labs/
root@root:/var/www/html/sqli-labs# chmod 777 *

```

Step 13 :- Now start the apache server and stop mysql

```
service apache2 start
```

```
service mysql stop
```

```

root@root: /var/www/html/sqli-labs
File Edit View Search Terminal Help
Less-12 Less-27 Less-41 Less-58 'SQL Injections-2.mm'
Less-13 Less-27a Less-42 Less-59 'SQL Injections-3.mm'
Less-14 Less-28 Less-43 Less-6 'SQL Injections.mm'
Less-15 Less-28a Less-44 Less-60 'SQL Injections.png'
Less-16 Less-29 Less-45 Less-61 sql-lab.sql
Less-17 Less-3 Less-46 Less-62 tomcat-files.zip
root@root:/var/www/html/sqli-labs# cd sql-connections/
root@root:/var/www/html/sqli-labs/sql-connections# ls
db-creds.inc setup-db-challenge.php sql-connect-1.php sqli-connect.php
functions.php setup-db.php sql-connect.php test.php
root@root:/var/www/html/sqli-labs/sql-connections# php sql-connect.php

PHP Fatal error: Uncaught Error: Call to undefined function mysql_connect() in
/var/www/html/sqli-labs/sql-connections/sql-connect.php:6
Stack trace:
#0 {main}
  thrown in /var/www/html/sqli-labs/sql-connections/sql-connect.php on line 6
root@root:/var/www/html/sqli-labs/sql-connections# cd ../
root@root:/var/www/html/sqli-labs# cd ../
root@root:/var/www/html# chmod 777 sqli-labs/
root@root:/var/www/html# cd sqli-labs/
root@root:/var/www/html/sqli-labs# chmod 777 *
root@root:/var/www/html/sqli-labs# service apache2 start
root@root:/var/www/html/sqli-labs# service mysql stop

```

Step 14 :- Now type

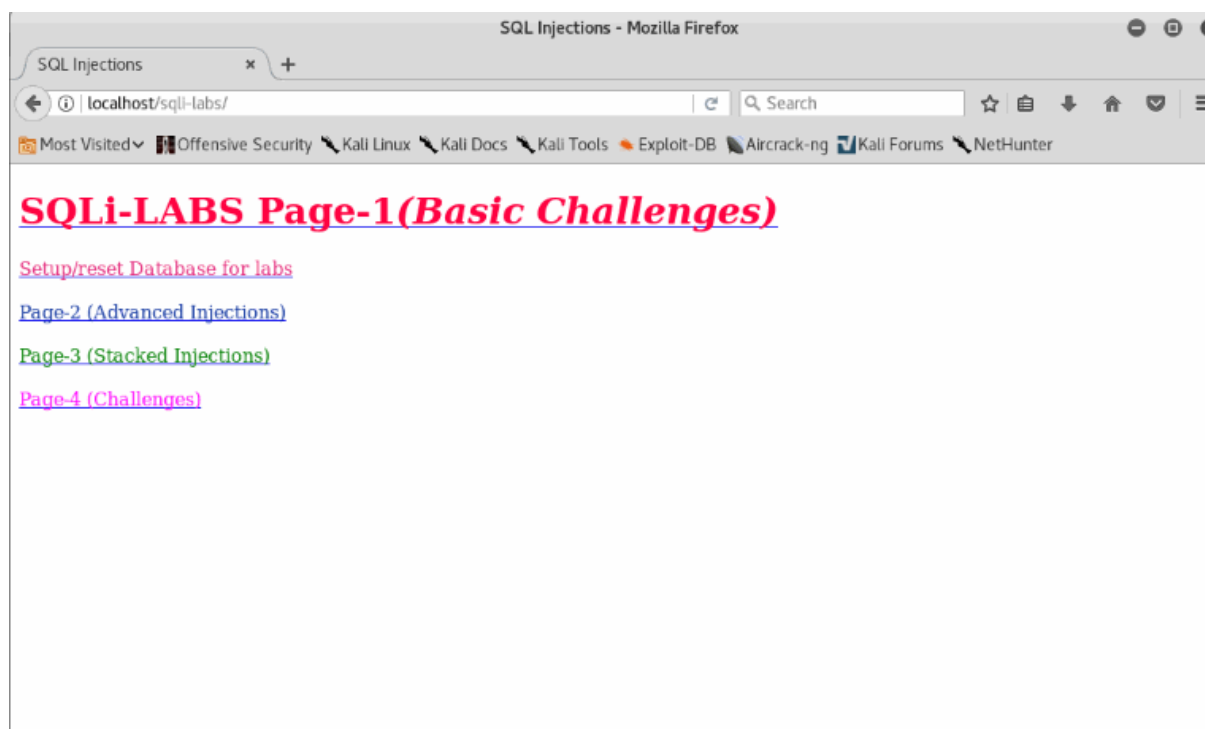
```
mysqld_safe --skip-grant-tables
```



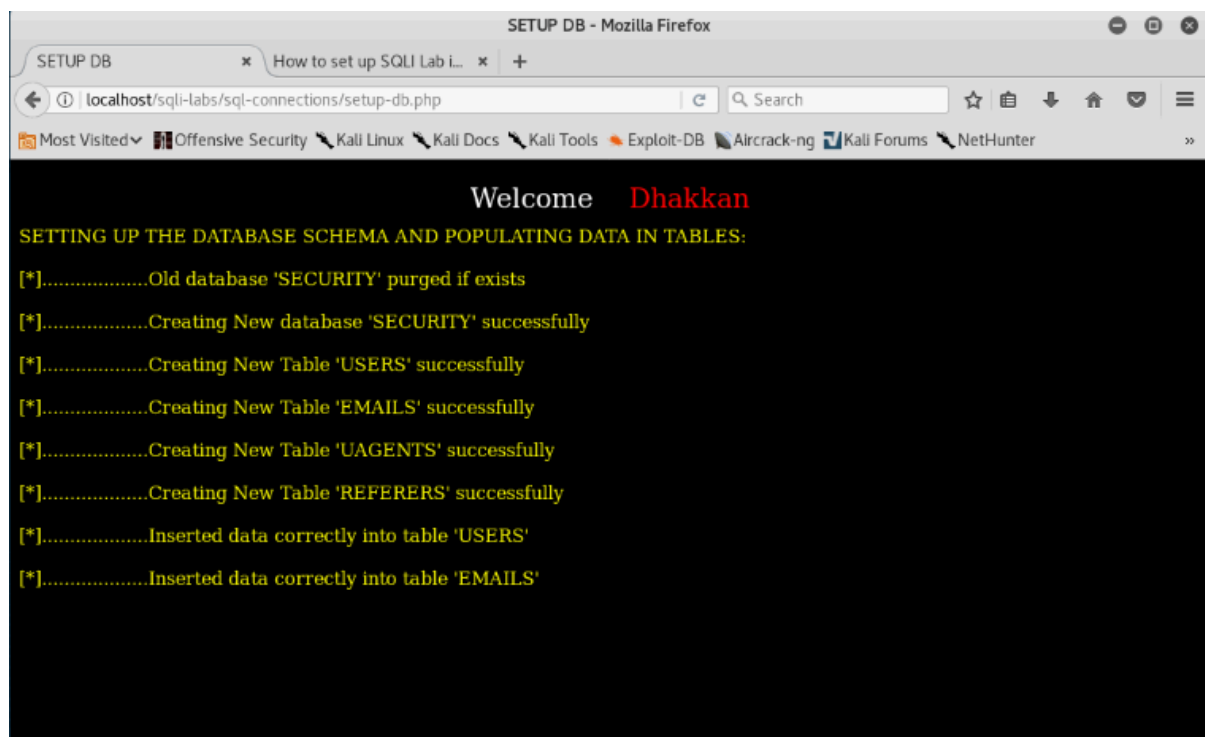
```
root@root: /var/www/html/sqli-labs
File Edit View Search Terminal Help
functions.php  setup-db.php  sql-connect.php  test.php
root@root:/var/www/html/sqli-labs/sql-connections# php sql-connect.php

PHP Fatal error:  Uncaught Error: Call to undefined function mysql_connect() in
/var/www/html/sqli-labs/sql-connections/sql-connect.php:6
Stack trace:
#0 {main}
  thrown in /var/www/html/sqli-labs/sql-connections/sql-connect.php on line 6
root@root:/var/www/html/sqli-labs/sql-connections# cd ../
root@root:/var/www/html/sqli-labs# cd ../
root@root:/var/www/html# chmod 777 sqli-labs/
root@root:/var/www/html# cd sqli-labs/
root@root:/var/www/html/sqli-labs# chmod 777 *
root@root:/var/www/html/sqli-labs# service apache2 start
root@root:/var/www/html/sqli-labs# service mysql stop
root@root:/var/www/html/sqli-labs# mysqld_safe --skip-grant-table
180121 08:14:50 mysqld_safe Logging to syslog.
180121 08:14:51 mysqld_safe Starting mysqld daemon with databases from /var/lib/
mysql
root@root:/var/www/html/sqli-labs# mysqld_safe --skip-grant-table
180121 08:27:54 mysqld_safe Logging to syslog.
180121 08:27:55 mysqld_safe Starting mysqld daemon with databases from /var/lib/
mysql
```

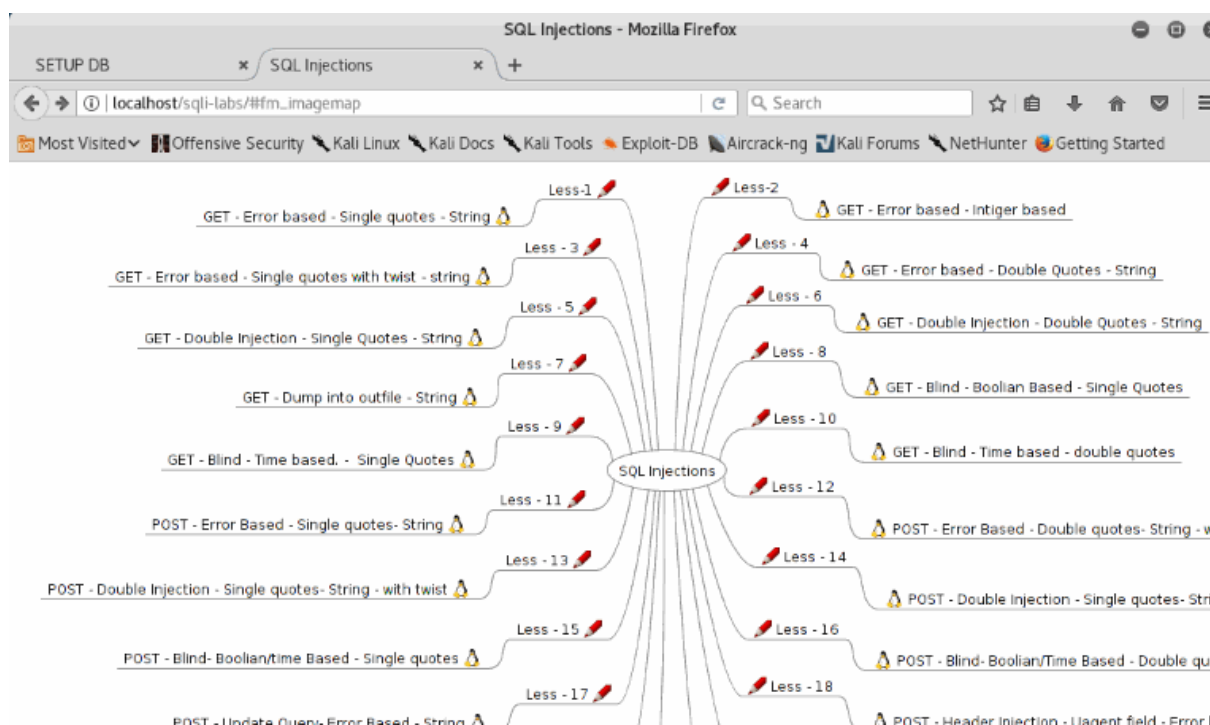
Step 15 :- Open the browser and type **localhost/sqli-labs/** to open the sqli-lab setup. And click on the setup/reset Database for labs.



Step 16 :-Now your database is setting up.



Step 17 :-After the database setup go back and **click on SQLi-LABS Page-1(Basic Challenges)** and here is your sql labs for practice SQL injection and XSS



For References :-

I hope you enjoyed this article.

