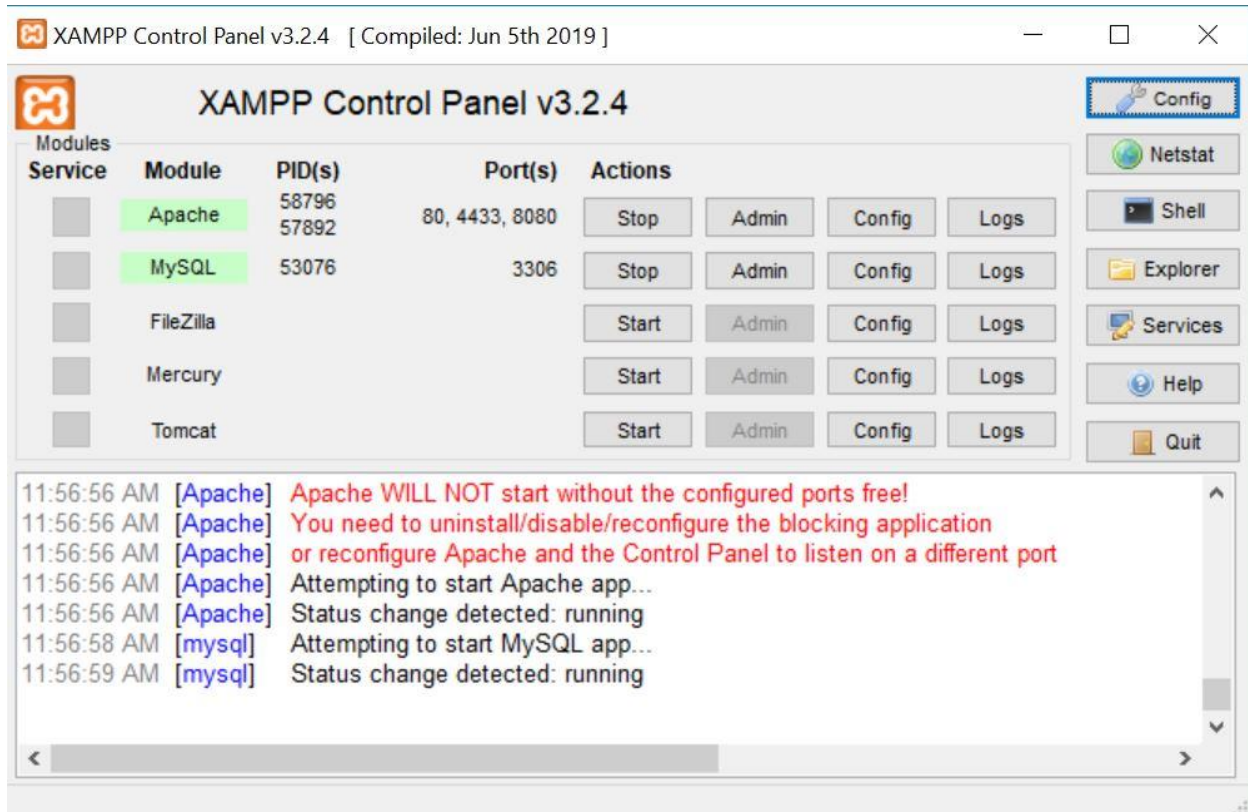


Instructions on how to setup:

Installation Xampp tools, the steps in below:

1- Run the Apache and Database.



2- Go to browser to check is a server running.

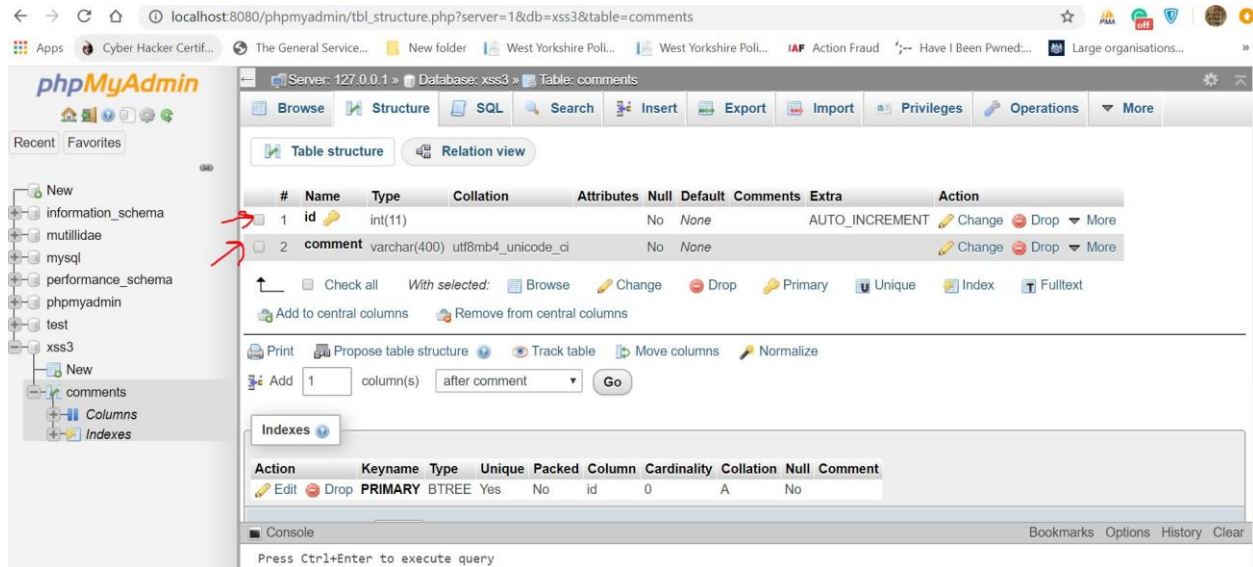


Welcome to XAMPP for Windows 7.4.2

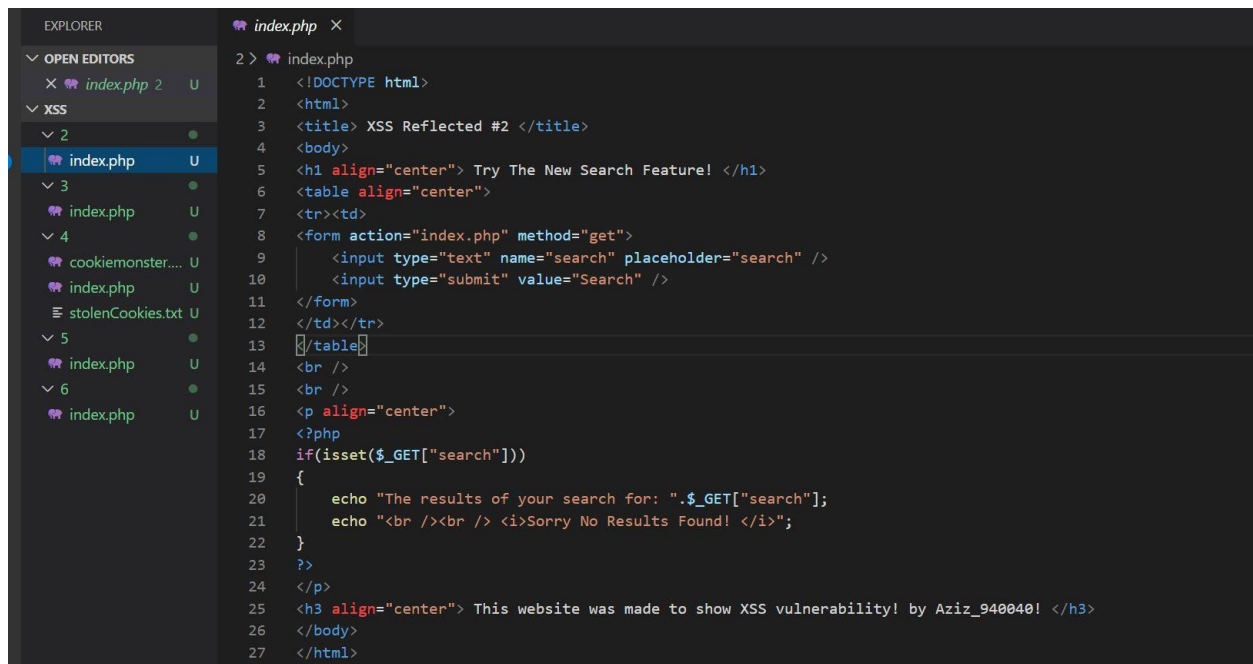
You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

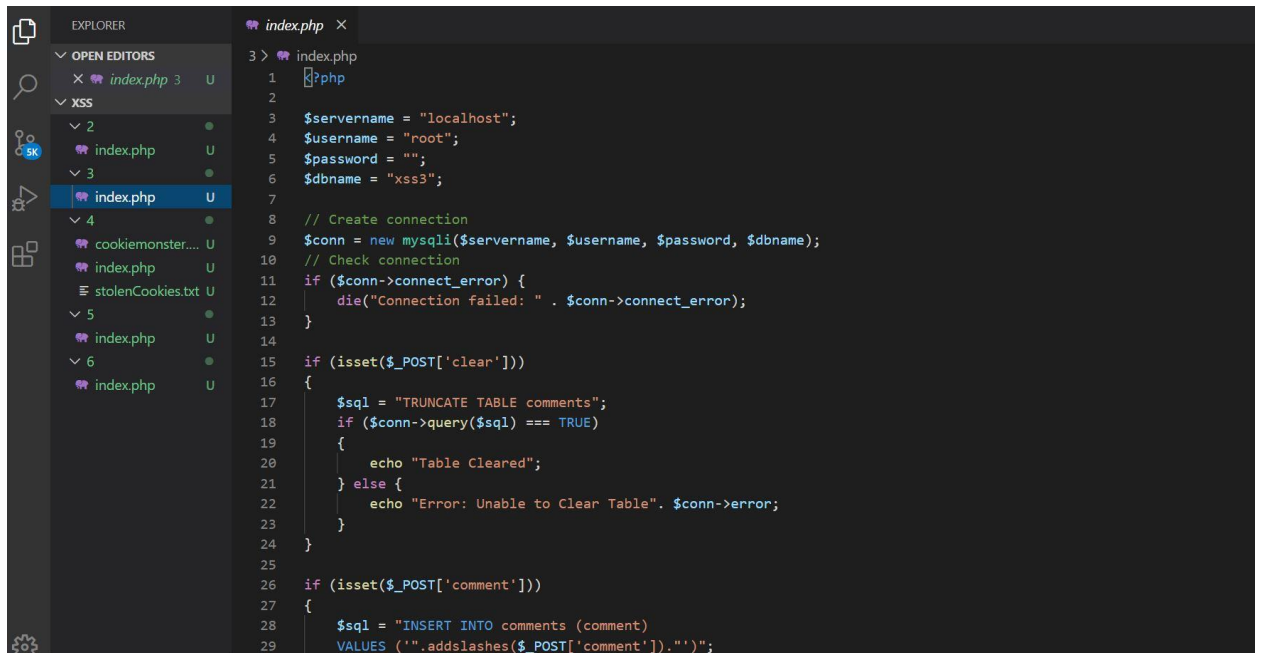
XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

3- Created id and comments in database



4- Create the index.php which is HTML pages (I had created five you will find it on folder xss).



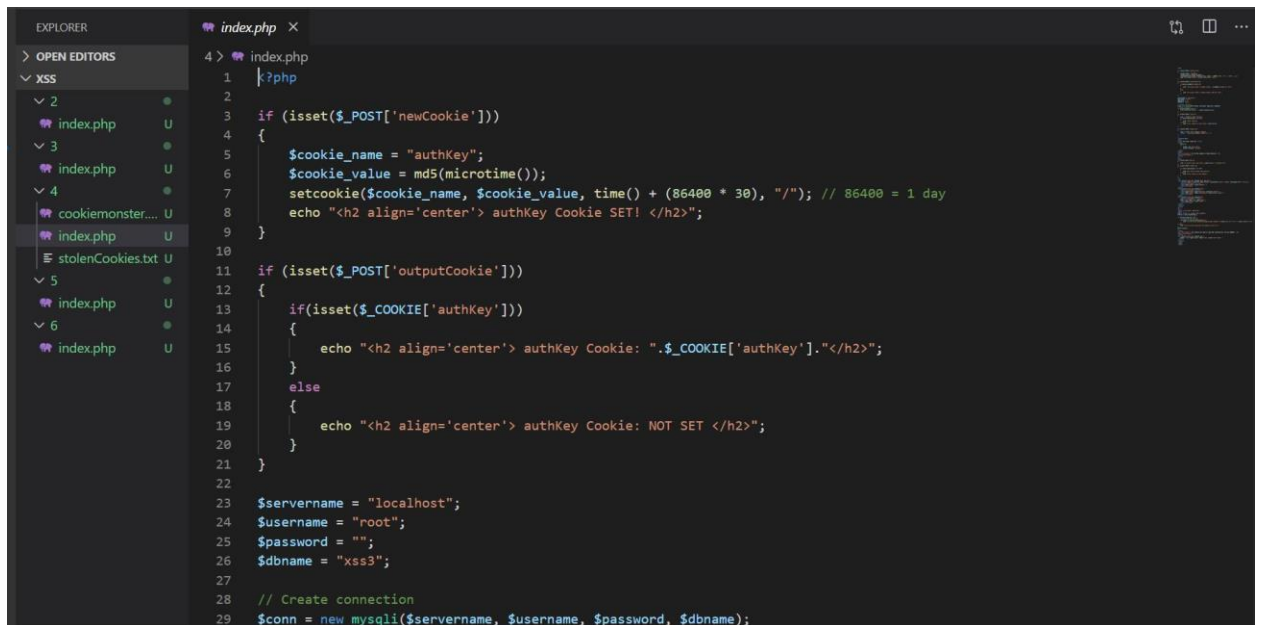


EXPLORER

- OPEN EDITORS
 - index.php 3 U
- XSS
 - 2
 - index.php U
 - 3
 - index.php U
 - 4
 - cookiemonster.... U
 - index.php U
 - stolenCookies.txt U
 - 5
 - index.php U
 - 6
 - index.php U

index.php X

```
3 > index.php
1  <?php
2
3  $servername = "localhost";
4  $username = "root";
5  $password = "";
6  $dbname = "xss3";
7
8  // Create connection
9  $conn = new mysqli($servername, $username, $password, $dbname);
10 // Check connection
11 if ($conn->connect_error) {
12     die("Connection failed: " . $conn->connect_error);
13 }
14
15 if (isset($_POST['clear']))
16 {
17     $sql = "TRUNCATE TABLE comments";
18     if ($conn->query($sql) === TRUE)
19     {
20         echo "Table Cleared";
21     } else {
22         echo "Error: Unable to Clear Table". $conn->error;
23     }
24 }
25
26 if (isset($_POST['comment']))
27 {
28     $sql = "INSERT INTO comments (comment)
29     VALUES ('".addslashes($_POST['comment'])."');";
```



EXPLORER

- OPEN EDITORS
 - index.php 4 U
- XSS
 - 2
 - index.php U
 - 3
 - index.php U
 - 4
 - cookiemonster.... U
 - index.php U
 - stolenCookies.txt U
 - 5
 - index.php U
 - 6
 - index.php U

index.php X

```
4 > index.php
1  <?php
2
3  if (isset($_POST['newCookie']))
4  {
5      $cookie_name = "authKey";
6      $cookie_value = md5(microtime());
7      setcookie($cookie_name, $cookie_value, time() + (86400 * 30), "/"); // 86400 = 1 day
8      echo "<h2 align='center'> authKey Cookie SET! </h2>";
9  }
10
11 if (isset($_POST['outputCookie']))
12 {
13     if(isset($_COOKIE['authKey']))
14     {
15         echo "<h2 align='center'> authKey Cookie: ".$_COOKIE['authKey']."</h2>";
16     }
17     else
18     {
19         echo "<h2 align='center'> authKey Cookie: NOT SET </h2>";
20     }
21 }
22
23 $servername = "localhost";
24 $username = "root";
25 $password = "";
26 $dbname = "xss3";
27
28 // Create connection
29 $conn = new mysqli($servername, $username, $password, $dbname);
```

```
5 > index.php
1 <?php
2
3 $servername = "localhost";
4 $username = "root";
5 $password = "";
6 $dbname = "xss3";
7
8 // Create connection
9 $conn = new mysqli($servername, $username, $password, $dbname);
10 // Check connection
11 if ($conn->connect_error) {
12     die("Connection failed: " . $conn->connect_error);
13 }
14
15 if (isset($_POST['clear']))
16 {
17     $sql = "TRUNCATE TABLE comments";
18     if ($conn->query($sql) === TRUE)
19     {
20         echo "Table Cleared";
21     } else {
22         echo "Error: Unable to Clear Table". $conn->error;
23     }
24 }
25
26 if (isset($_POST['comment']))
27 {
28     $sql = "INSERT INTO comments (comment)
29     VALUES ('".addslashes($_POST['comment'])."')";
```