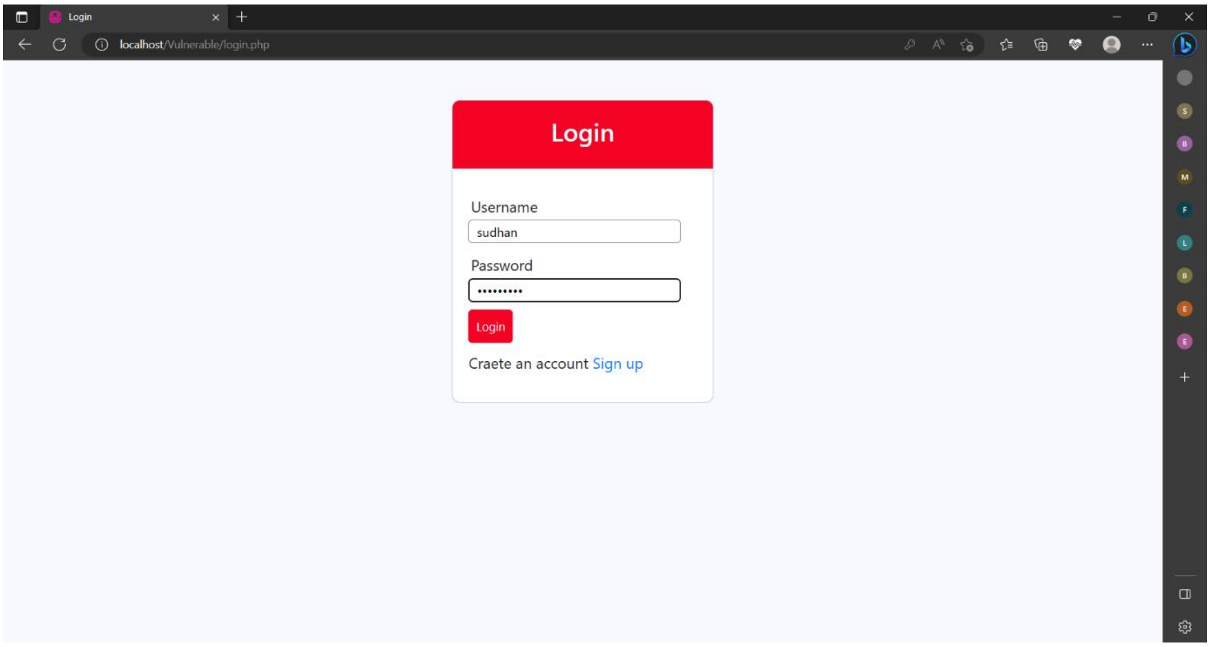
ADVANCED ETHICAL HACKING
AND
PENETRATION TESTING

ASSIGNMENT – 1

SUBMITED BY
SUDHAN S
22CSEH25
I.M.Sc.CYBER SECURITY

1.PHP Webpage :



localhost/Vulnerable/login.php

Login

Username

sudhan

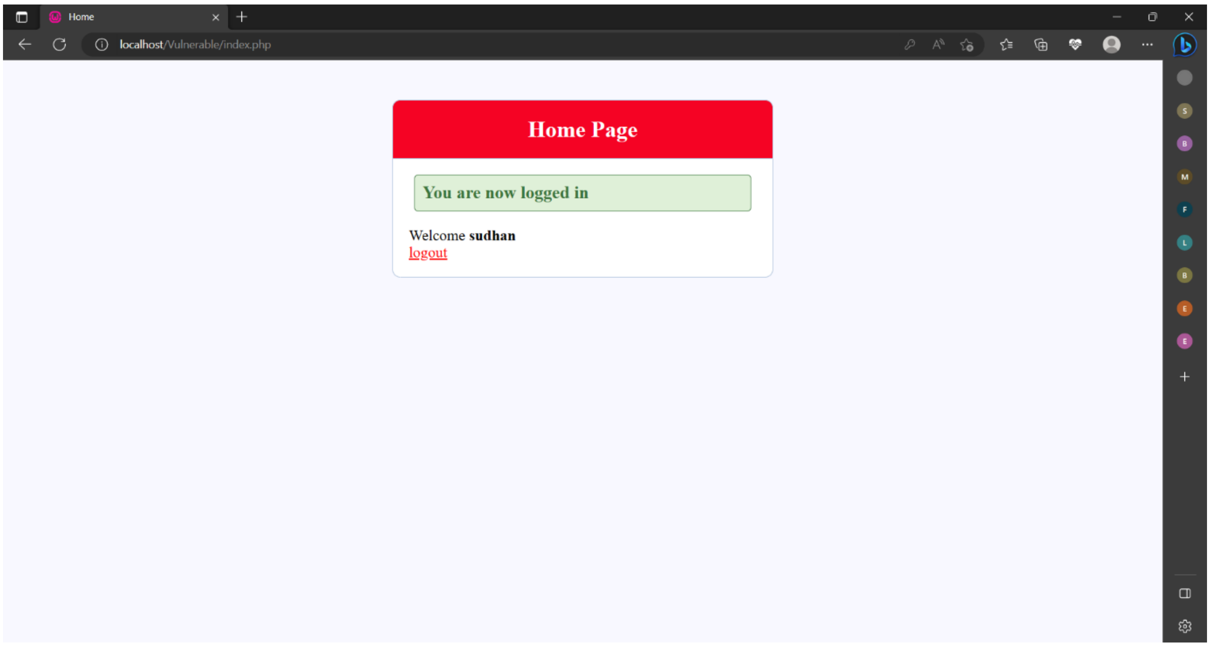
Password

•••••••••

Login

Craete an account Sign up

Login Page



localhost/Vulnerable/index.php

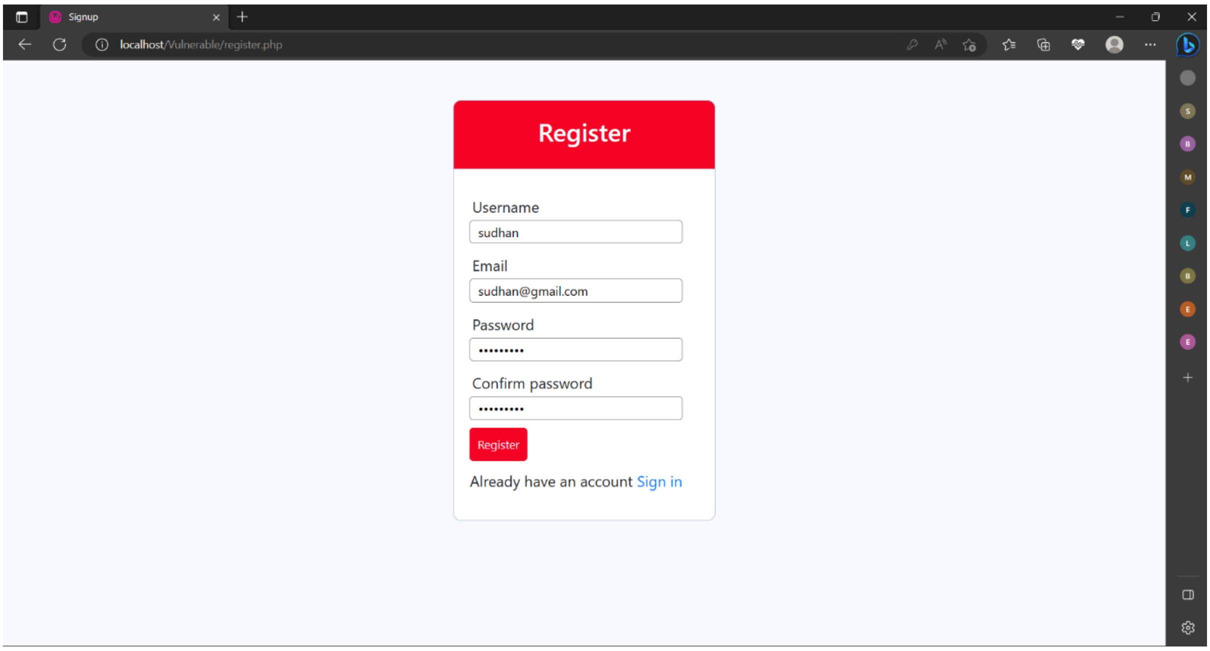
Home Page

You are now logged in

Welcome **sudhan**

logout

Login Display Page



Register

Username

sudhan

Email

sudhan@gmail.com

Password

•••••••••

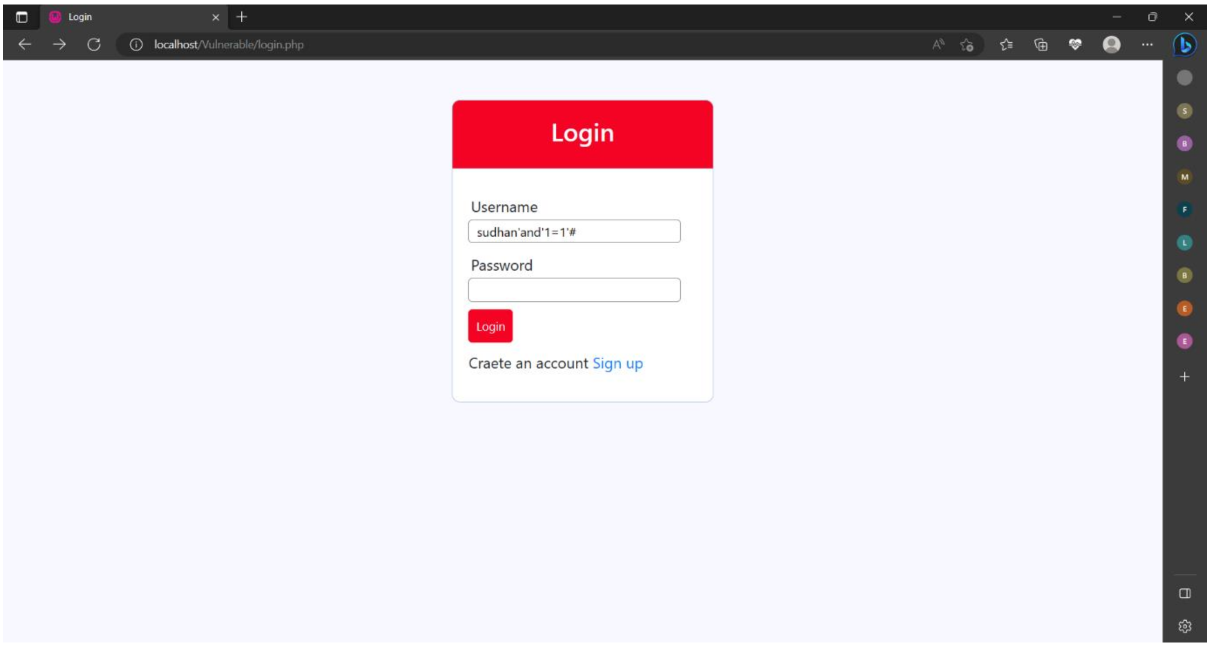
Confirm password

•••••••••

Already have an account Sign in

Sign up Page

2.SQL Injection :



Login

Username

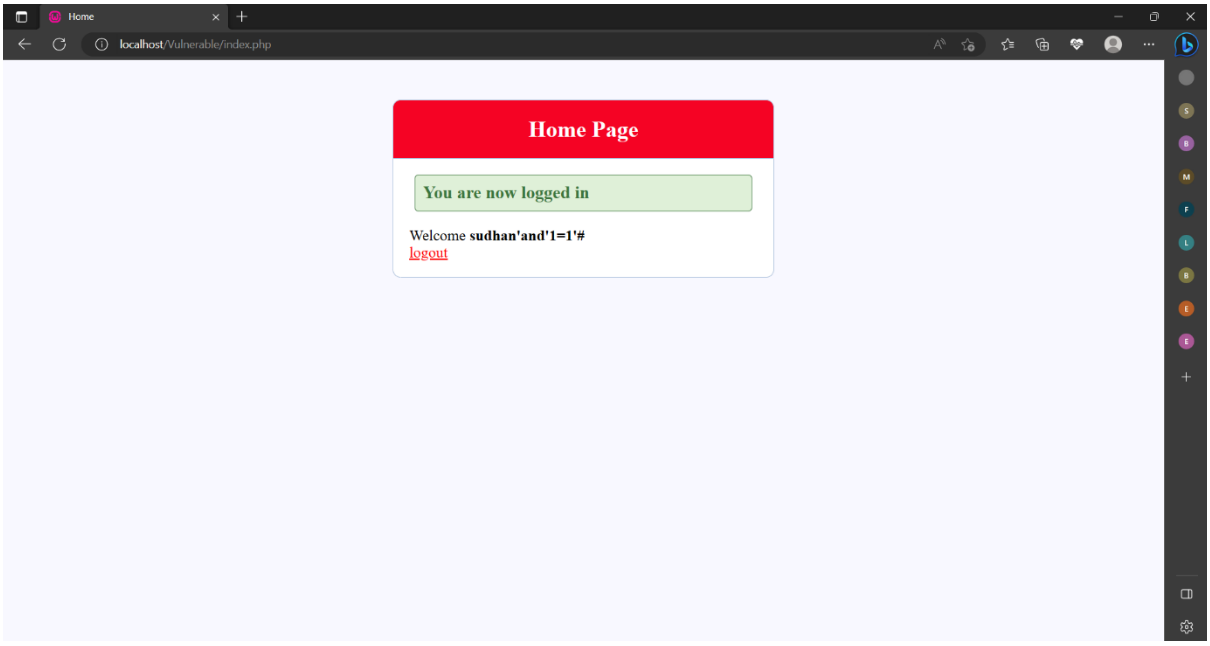
sudhan'and'1=1'#

Password

Craete an account Sign up

SQL Injection Using Bypassing Method in Login Page

Command : Sudhan’and’1=’#



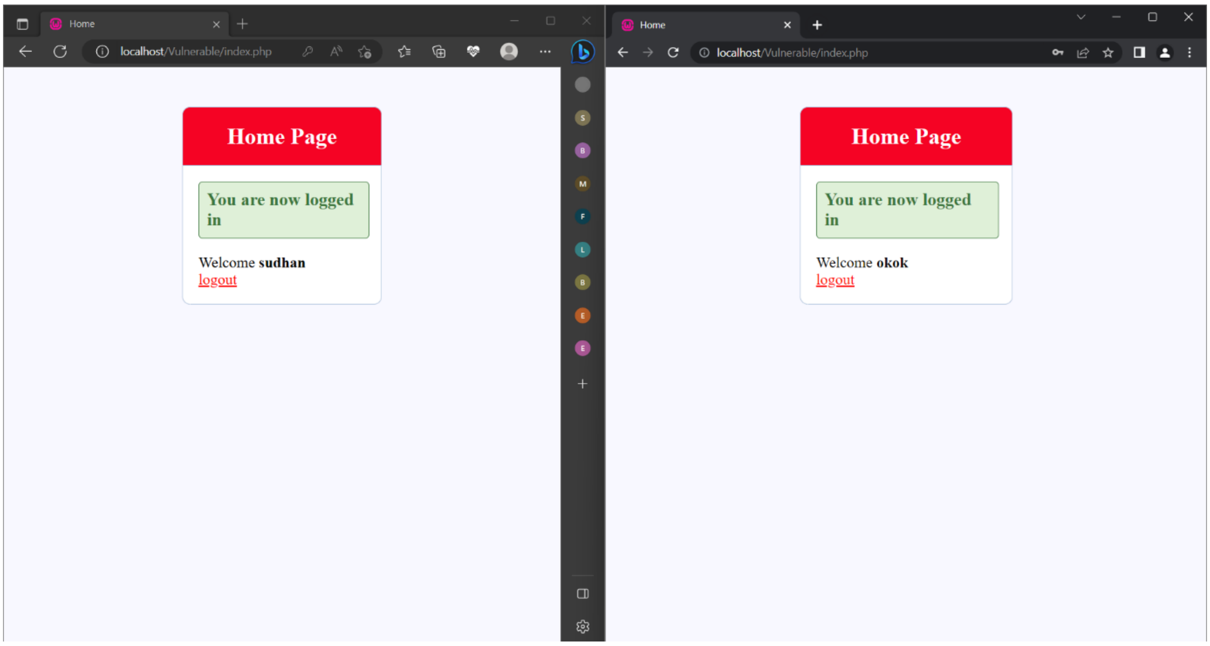
Home Page

You are now logged in

Welcome **sudhan'and'1=1'#**
logout

SQL Injection Using Bypassing Method is Successful logged

3.Session Hijacking Attack :



Home
localhost/Vulnerable/index.php
Home
localhost/Vulnerable/index.php

Home Page

You are now logged in

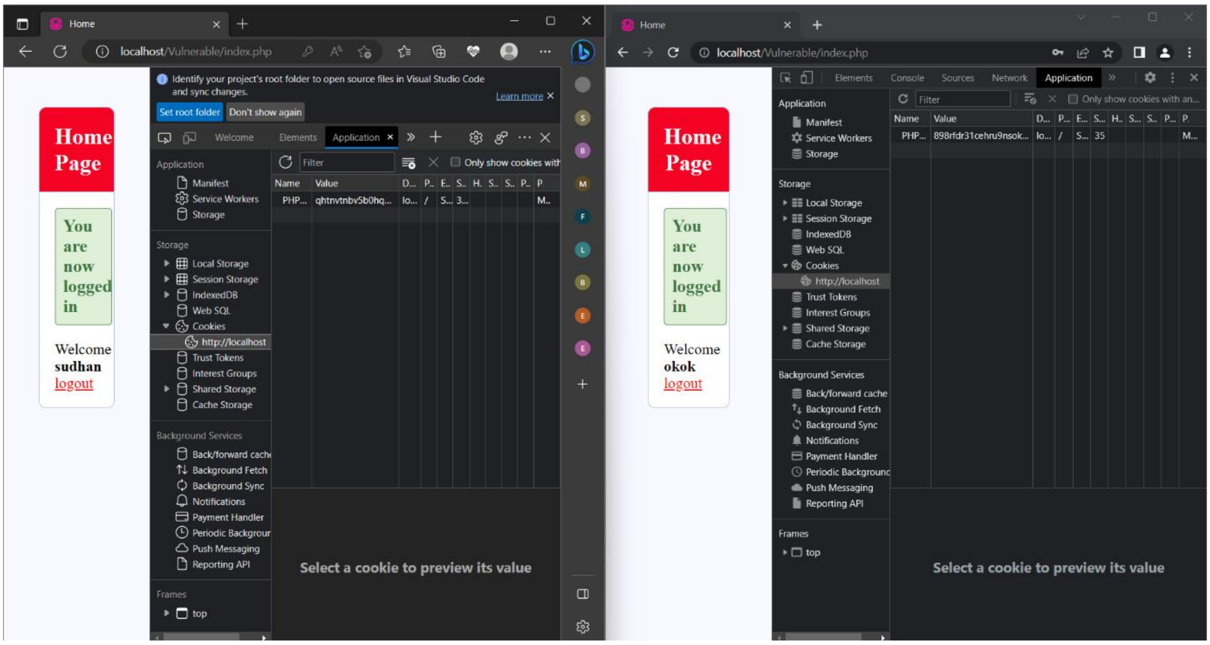
Welcome **sudhan**
logout

Home Page

You are now logged in

Welcome **okok**
logout

Session Hijacking Using This Two User ID



localhost/Vulnerable/index.php

Home Page

You are now logged in

Welcome sudhan logout

Name	Value	D...	P...	E...	S...	H...	S...	S...	P...	P
PHP...	qhtnvtnbv5b0hq...	lo...	/	S...	3...					M...

Select a cookie to preview its value

localhost/Vulnerable/index.php

Home Page

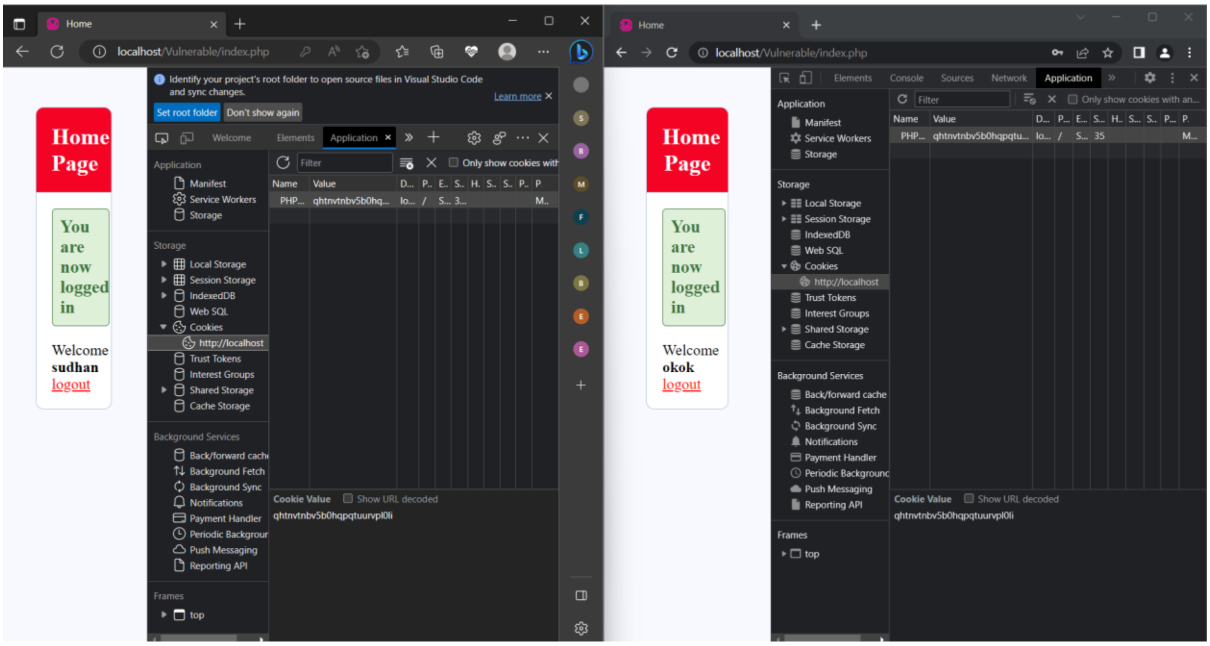
You are now logged in

Welcome okok logout

Name	Value	D...	P...	E...	S...	H...	S...	S...	P...	P.
PHP...	898rfdr31cehru9nsok...	lo...	/	S...	35					M...

Select a cookie to preview its value

Different Session ID’s



localhost/Vulnerable/index.php

Home Page

You are now logged in

Welcome sudhan logout

Name	Value	D...	P...	E...	S...	H...	S...	S...	P...	P
PHP...	qhtnvtnbv5b0hq...	lo...	/	S...	3...					M...

Cookie Value ☐ Show URL decoded

qhtnvtnbv5b0hqpqtuurvpl0li

localhost/Vulnerable/index.php

Home Page

You are now logged in

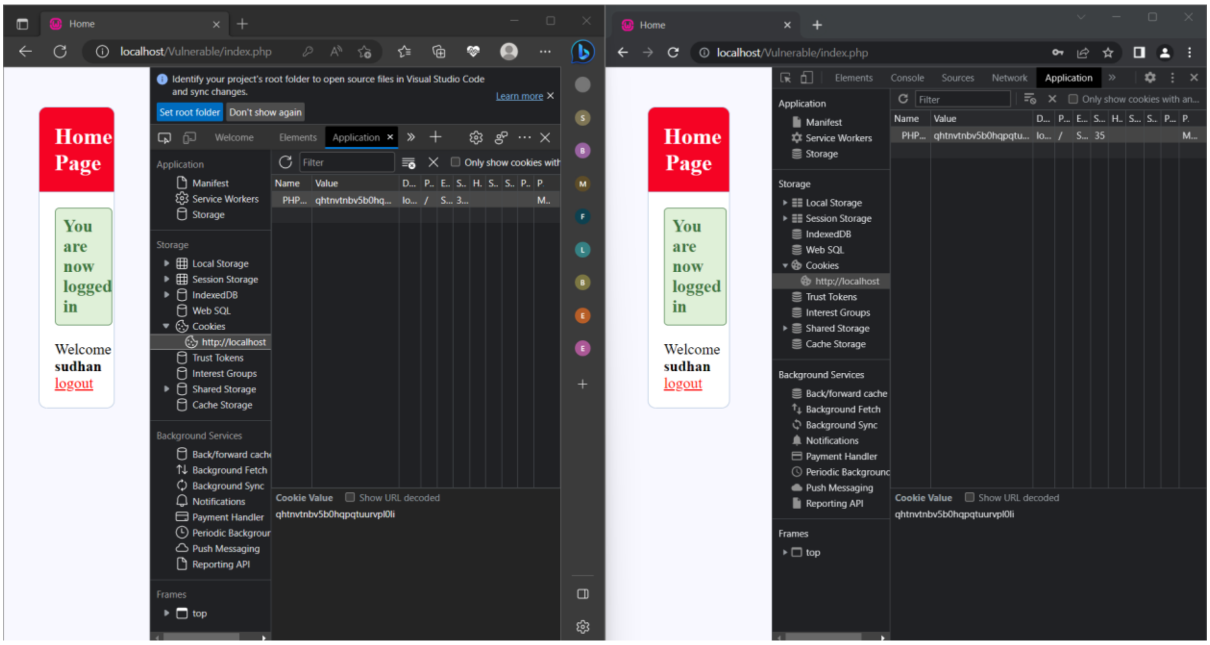
Welcome okok logout

Name	Value	D...	P...	E...	S...	H...	S...	S...	P...	P.
PHP...	qhtnvtnbv5b0hqpqtu...	lo...	/	S...	35					M...

Cookie Value ☐ Show URL decoded

qhtnvtnbv5b0hqpqtuurvpl0li

Replacing The Session ID One User To Another User



Home Page

You are now logged in

Welcome sudhan

logout

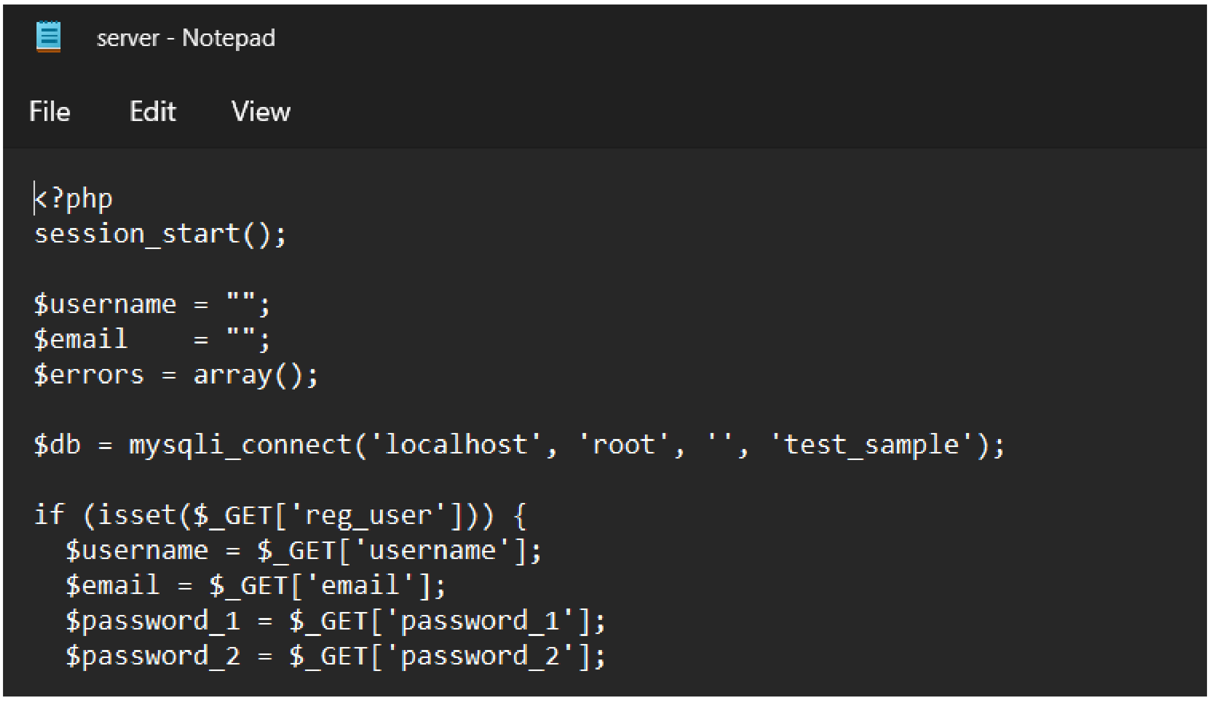
Cookie Value

qhtnvtnbv5b0hqpqtuurvpl0li

Session Hijacking is Successfully Performed

4.The Mitigation For SQL Injection :

Vulnerable Code :



server - Notepad

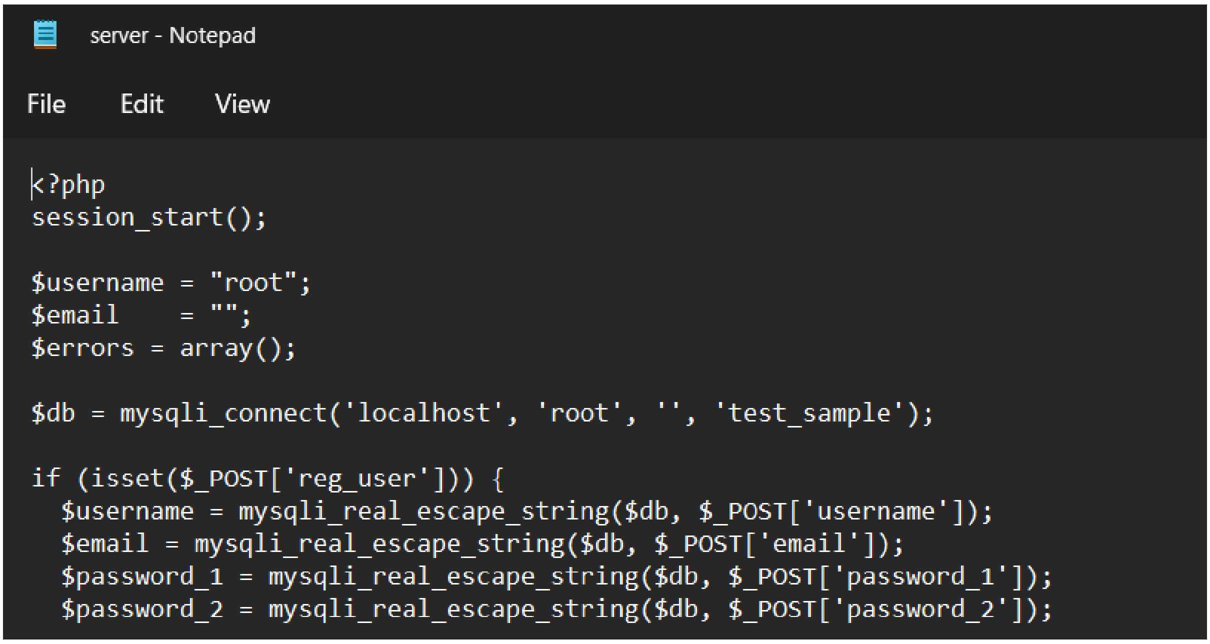
```
<?php
session_start();

$username = "";
$email    = "";
$errors = array();

$db = mysqli_connect('localhost', 'root', '', 'test_sample');

if (isset($_GET['reg_user'])) {
  $username = $_GET['username'];
  $email = $_GET['email'];
  $password_1 = $_GET['password_1'];
  $password_2 = $_GET['password_2'];
```

Non Vulnerable Code :



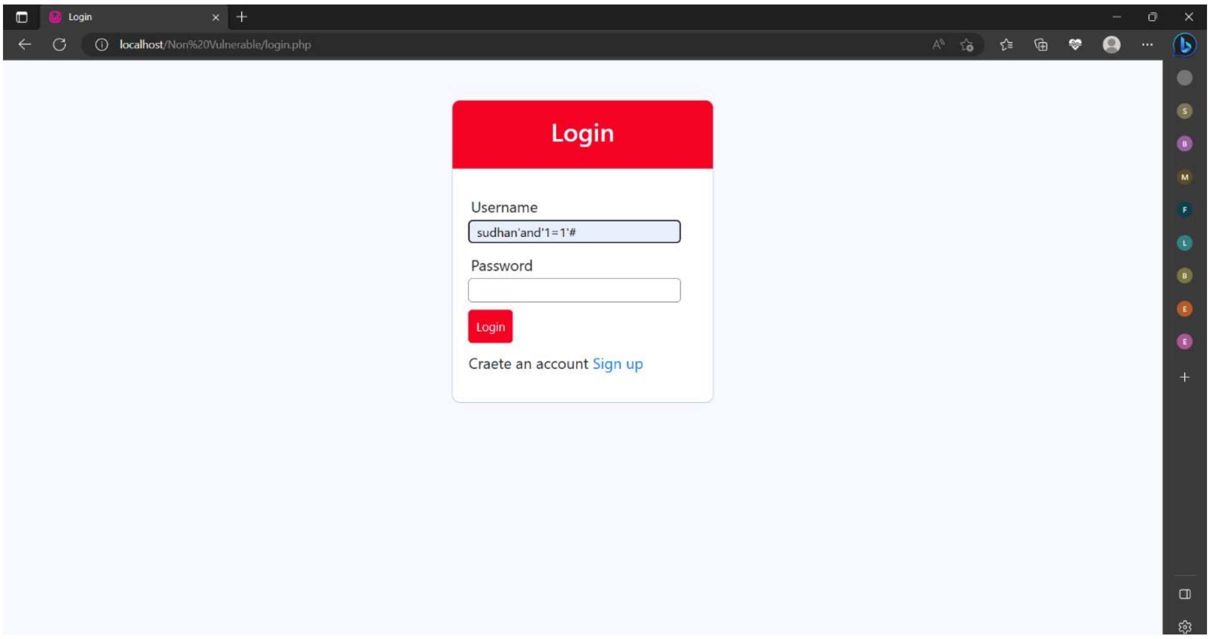
```
<?php
session_start();

$username = "root";
$email    = "";
$errors = array();

$db = mysqli_connect('localhost', 'root', '', 'test_sample');

if (isset($_POST['reg_user'])) {
  $username = mysqli_real_escape_string($db, $_POST['username']);
  $email = mysqli_real_escape_string($db, $_POST['email']);
  $password_1 = mysqli_real_escape_string($db, $_POST['password_1']);
  $password_2 = mysqli_real_escape_string($db, $_POST['password_2']);
```

After fixing :



Login

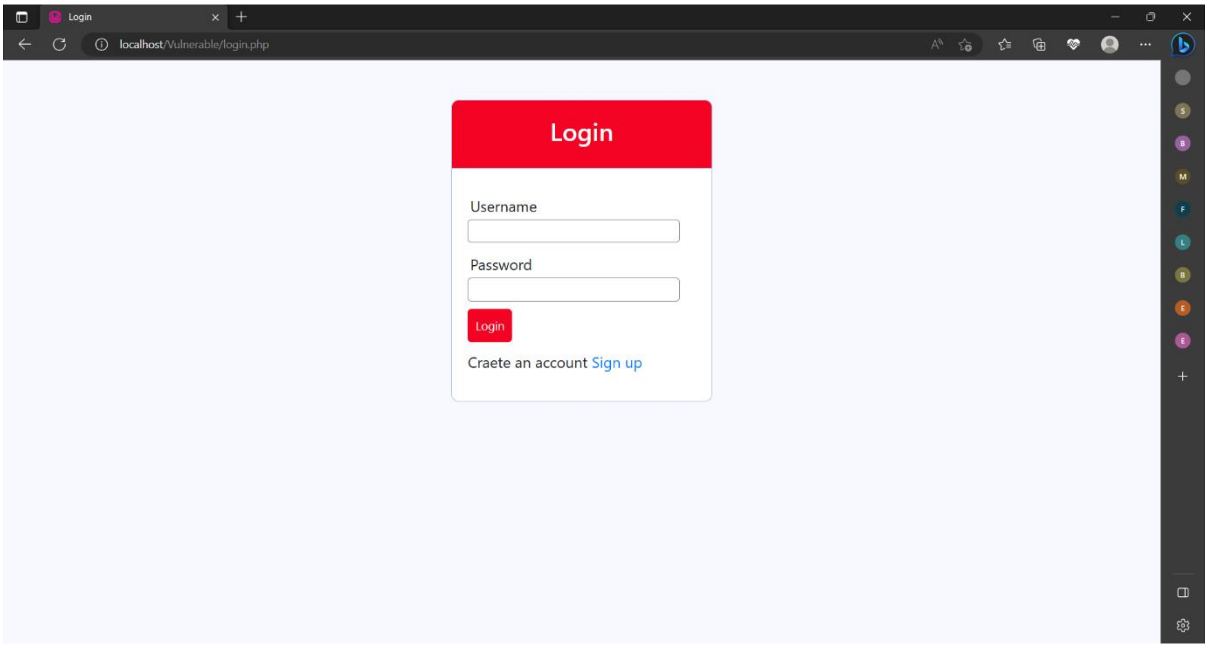
Username

sudhan'and'1=1'#

Password

Login

Create an account Sign up



SQL Injection is Not Working