

## VI Module: SQL Injection and Session Hijacking

### A. SQL Injection for website hacking

Softwares:

In XAMPP

Create database named studusers



Create a table login\_user and insert data:

Options			
id	name	user_name	password
1	Ashwini	admin	admin
2	Kajal	vv	vv
3	Uttkarsha	system	system
4	Sailee	system	md5(' Ethical@\$%Hacking')
5	Robert	sys	pass

**PHP code:**

**login.php**

```
<?php
session_start();
$message="";
if(count($_POST)>0)
{
$con = mysqli_connect('127.0.0.1:3306','root','','studusers') or die('Unable To connect');
$result = mysqli_query($con,"SELECT * FROM login_user WHERE user_name='".$_POST["user_name"]."' and password = '".$_POST["password"]."");
$row = mysqli_fetch_array($result);
if(is_array($row))
{
$_SESSION["id"] = $row['id'];
$_SESSION["name"] = $row['name'];
}
else
{
$message = "Invalid Username or Password!";
}
}
if(isset($_SESSION["id"]))
{
}
```

```

header("Location:index.php");
}

?>
<html>
<head>
<title>User Login</title>
</head>
<body>

<form name="frmUser" method="post" action="" align="center">
  <div class="message"><?php if($message!="") { echo $message; } ?></div>
  <h3 align="center">Enter Login Details</h3>
  Username:<br>
  <input type="text" name="user_name">
  <br>
  Password:<br>
  <input type="password" name="password">
  <br><br>
  <input type="submit" name="submit" value="Submit">
  <input type="reset">
</form>
</body>
</html>

```

### **index.php**

```

<?php
session_start();
?>
<html>
<head>
<title>User Login</title>
</head>
<body bgcolor=green>
<?php
if($_SESSION["name"]) {
?>
<center>
<h1>
Welcome <?php echo $_SESSION["name"]; ?>. Click here to <a href="logout.php"
tite="Logout">Logout.
</h1>

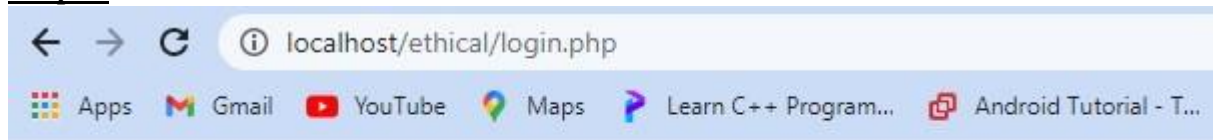
</center>
<?php
} else echo "<h1>Please login first .</h1>";
?>
</body>
</html>

```

### Logout.php

```
<?php
session_start();
unset($_SESSION["id"]);
unset($_SESSION["name"]);
header("Location:login.php");
?>
```

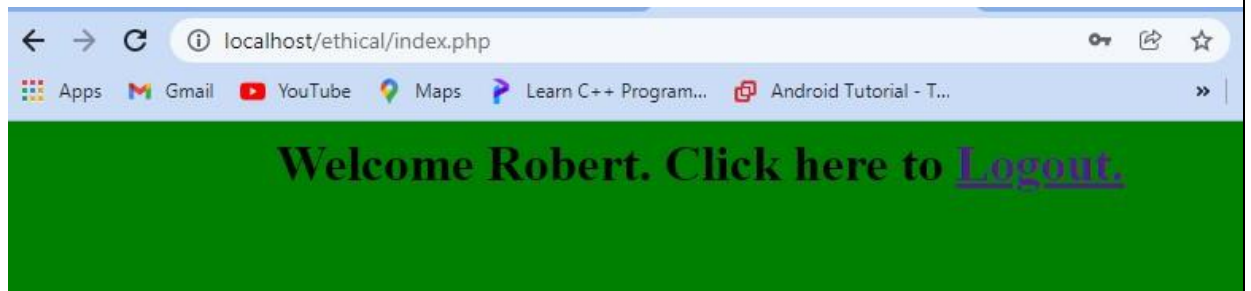
### Output:



### Enter Login Details

Username:

Password:



**Result:** You are logged into the index.php webpage inspite of giving a wrong username.

## B. Session Hijacking

Perform session hijacking for the above login php program.

What are the ways to prevent your data hacked by packet sniffers?

Solution:

- Using HTTPS, the secure version of HTTP will prevent packet sniffers from seeing the traffic on the websites you are visiting.
- To make sure you are using HTTPS, check the upper left corner of your browser.
- Tunnel your connectivity to a virtual private network, or a VPN. A VPN encrypts the traffic being sent between your computer and the destination. This includes

<https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgfbg?hl=en>

Login as username=sys and password =pass

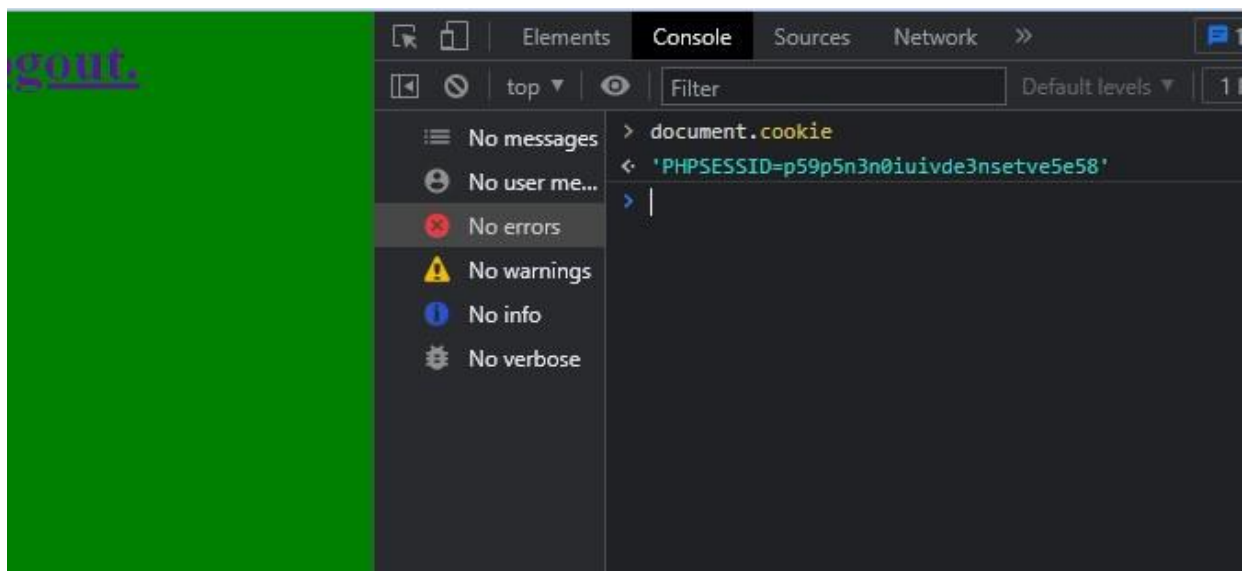
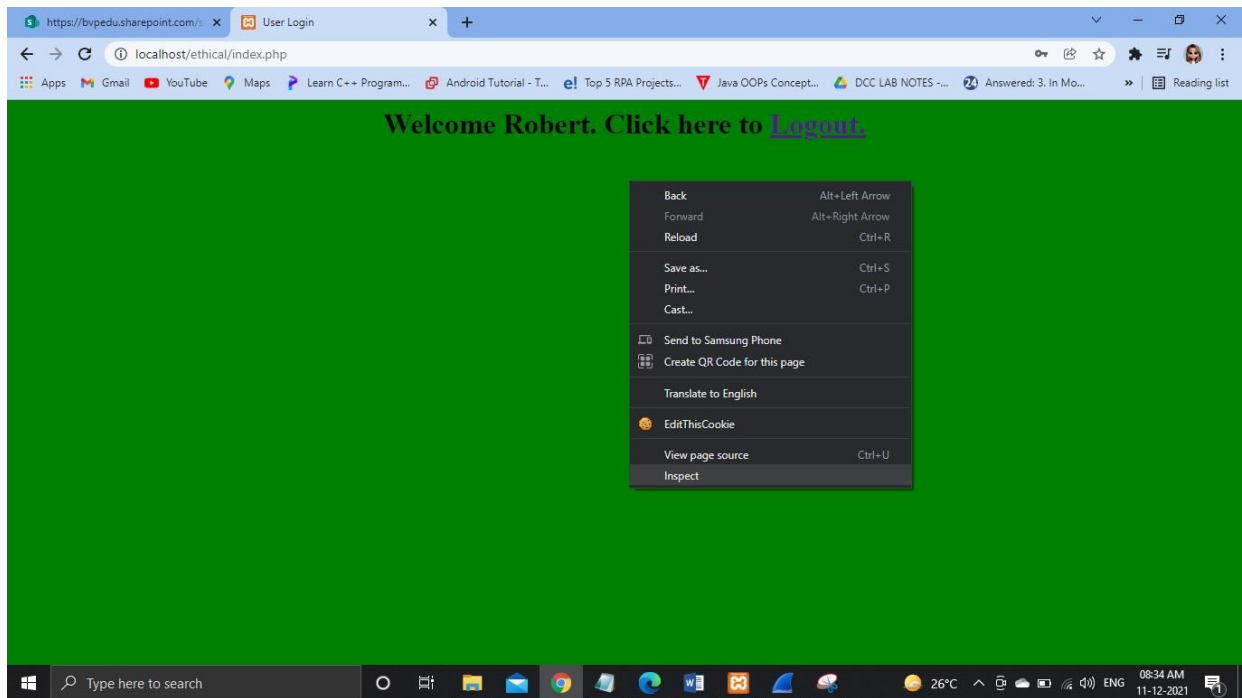
# Enter Login Details

Username:

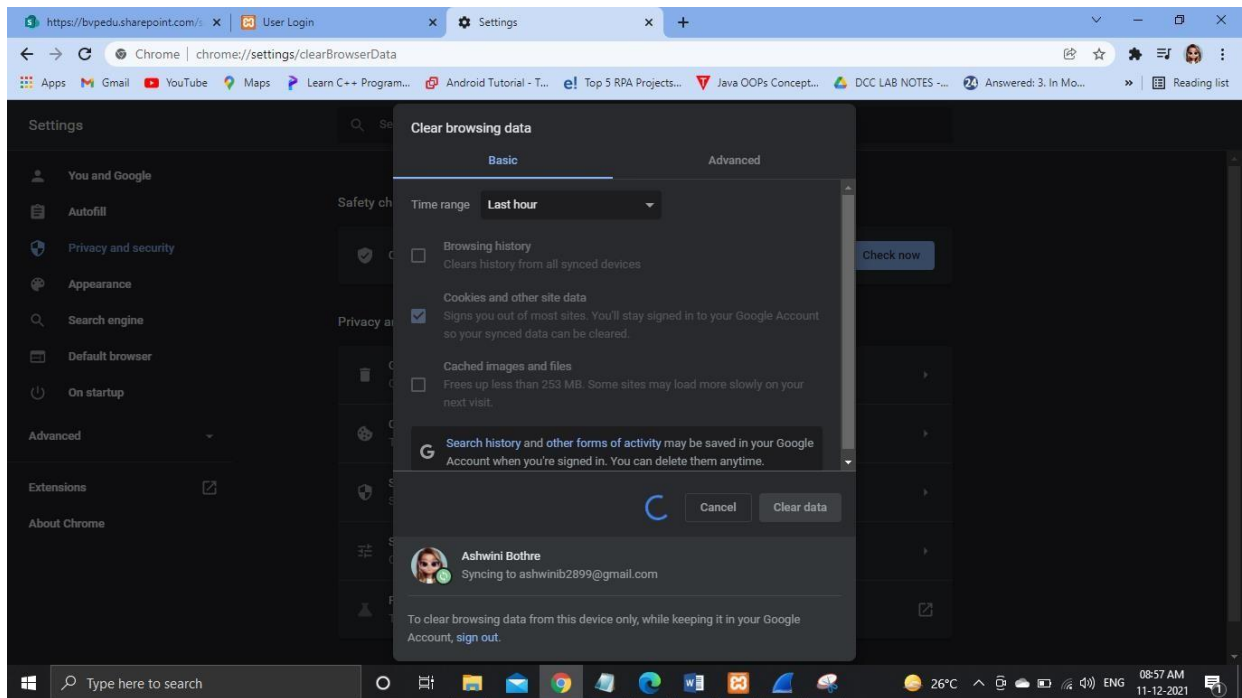
Password:



Right click->inspect->document.cookie



Now PHPSESSID for sys = PHPSESSID=p59p5n3n0iuijde3nsetve5e58  
Next, delete the above session after it is recorded above.



Login as username=admin and password =admin

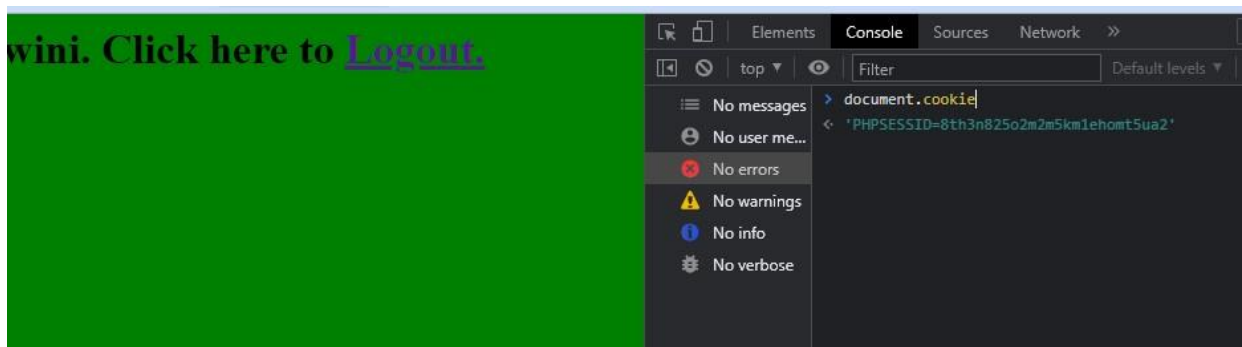
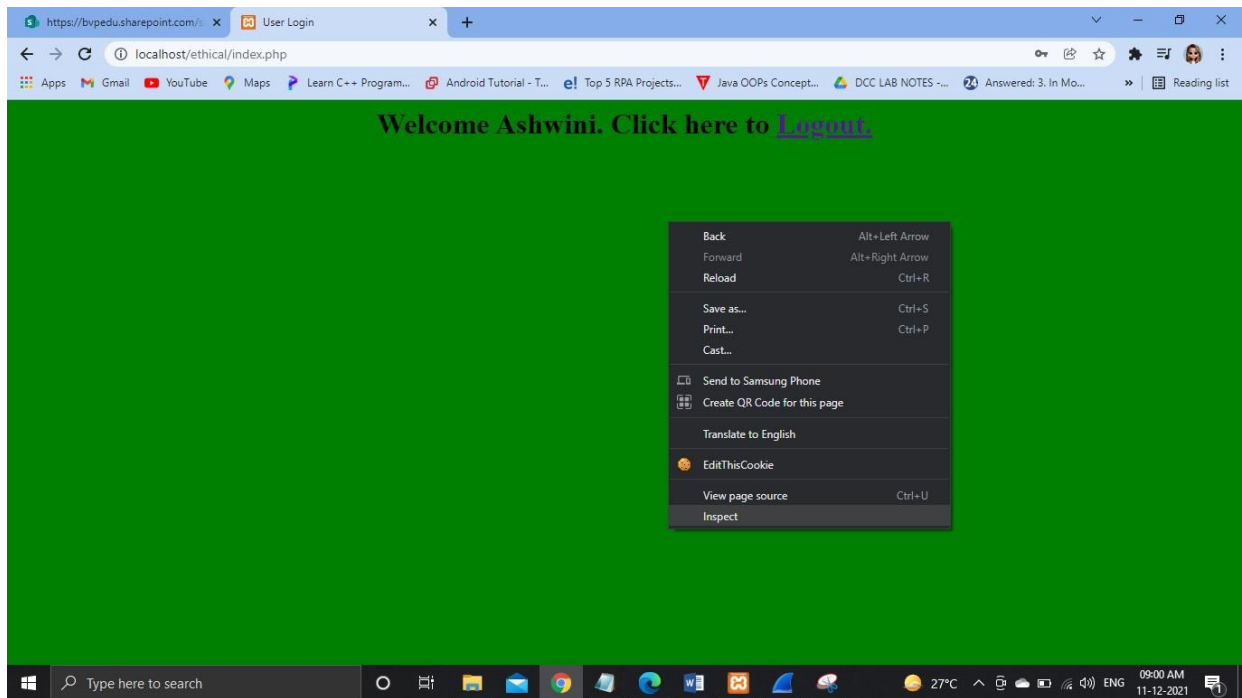
**Enter Login Details**

Username:

Password:

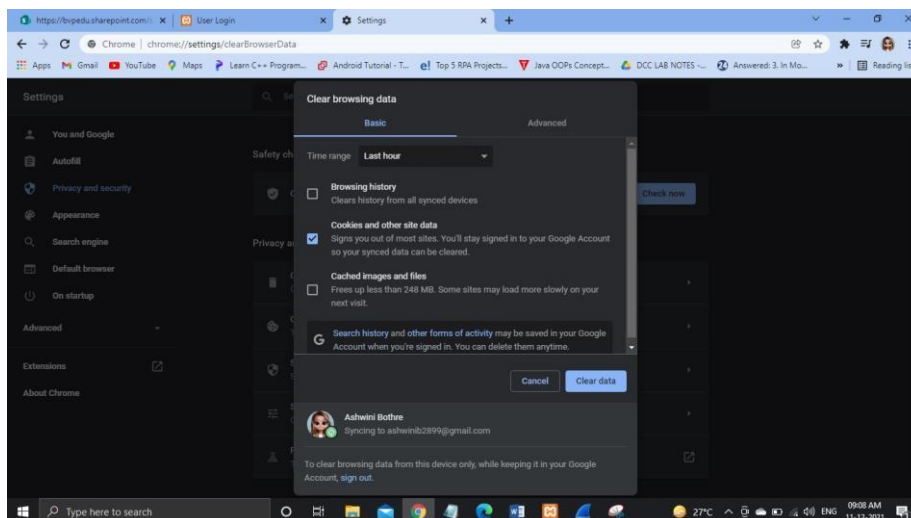


Right click->inspect->document.cookie



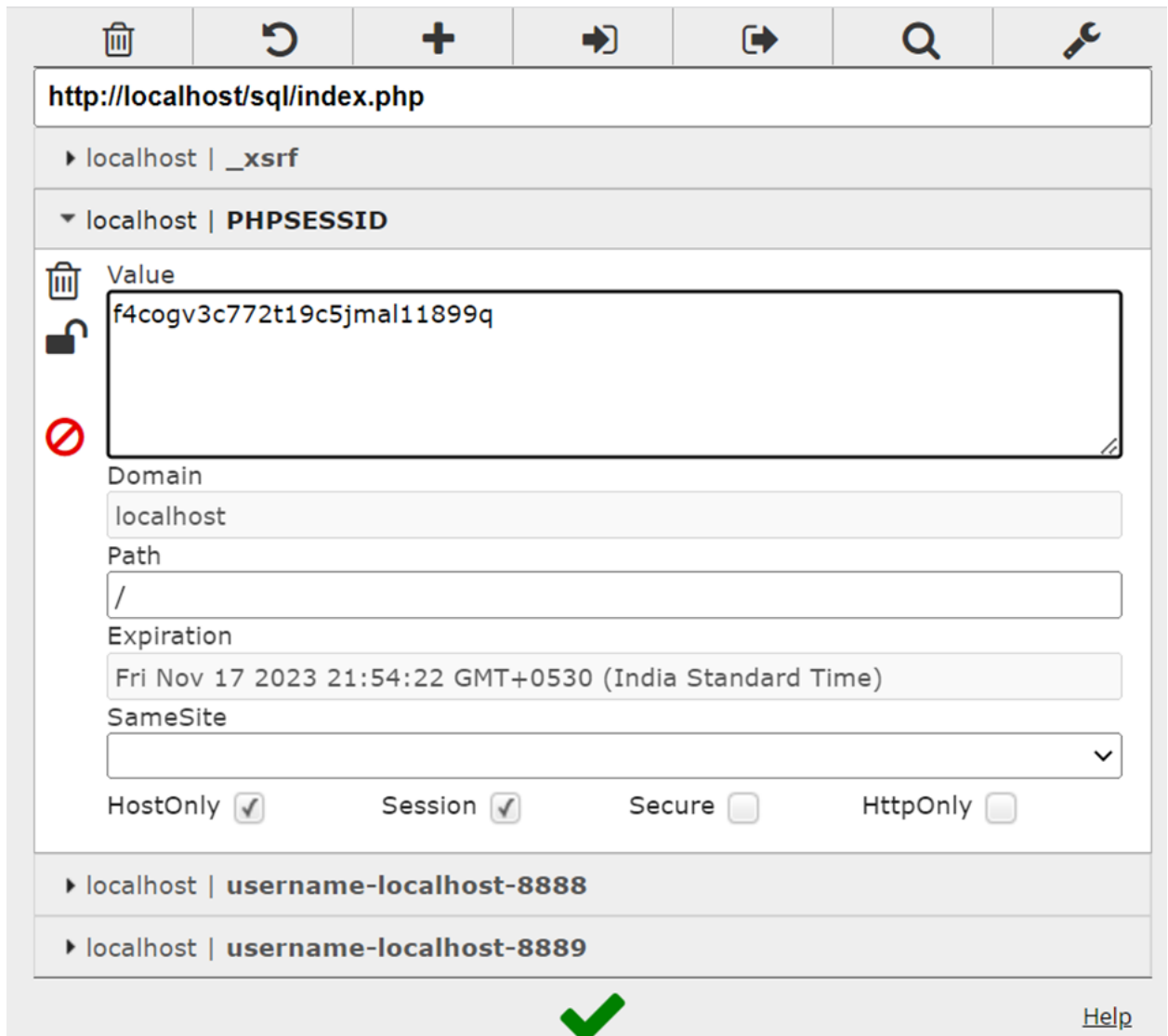
Now PHPSESSID for admin = PHPSESSID=**8th3n825o2m2m5km1ehomt5ua2**

Again clear cookie



Now the sys is trying to hijack the session of username admin  
Click EditThisCookie

In the PHPSESSID replace admin's PHPSESSID=**8th3n825o2m2m5km1ehomt5ua2** With sys  
sessionid PHPSESSID= p59p5n3n0iuiivde3nsetve5e58



The screenshot shows a web browser's developer tools interface. The address bar displays `http://localhost/sql/index.php`. The left sidebar shows the 'Cookies' tab selected, with a tree view showing `localhost | _xsrf` and `localhost | PHPSESSID`. The main pane shows the details for the `PHPSESSID` cookie. The 'Value' field contains `f4cogv3c772t19c5jmal11899q`. Other fields include 'Domain' (localhost), 'Path' (/), 'Expiration' (Fri Nov 17 2023 21:54:22 GMT+0530 (India Standard Time)), and 'SameSite' (dropdown menu). At the bottom, there are checkboxes for 'HostOnly' (checked), 'Session' (checked), 'Secure' (unchecked), and 'HttpOnly' (unchecked). A green checkmark is visible at the bottom center of the interface, and a 'Help' link is at the bottom right.

Click the green tick symbol and refresh the page

Welcome IT. Click here to [Logout.](#)