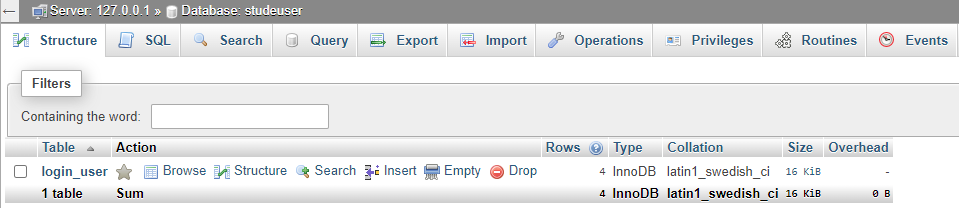
**Practical 6**

1. **SQL injection for website hacking**

**XAMPP**

**Create database named studusers**

****

**CREATE TABLE `login\_user` (**

**`id` int(11) NOT NULL,**

**`name` varchar(60) NOT NULL,**

**`user\_name` varchar(50) NOT NULL,**

**`password` varchar(300) NOT NULL**

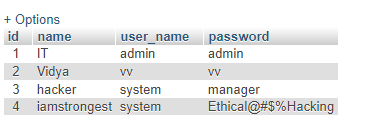
**Insert into login\_user values(1,’IT’,’admin’,’admin’);**

**Insert into login\_user values(2,’Vidya’,’vv’,’vv’);**

**Insert into login\_user values(3,’hacker’,’system’,’manager’);**

**Insert into login\_user values(4,’iamstrongest’,’system’,**

**‘ Ethical@#$%Hacking’);**

****

**Login.php**

**<?php**

**session\_start();**

**$message="";**

**if(count($\_POST)>0)**

**{**

**$con = mysqli\_connect('127.0.0.1:3306','root','','studeuser') 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");**

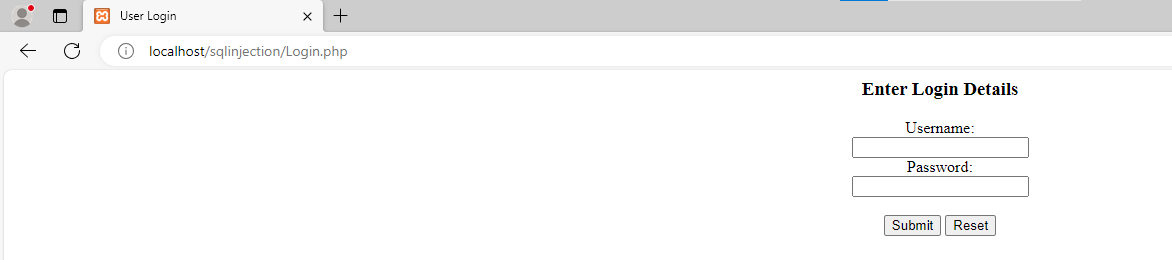
**?>**

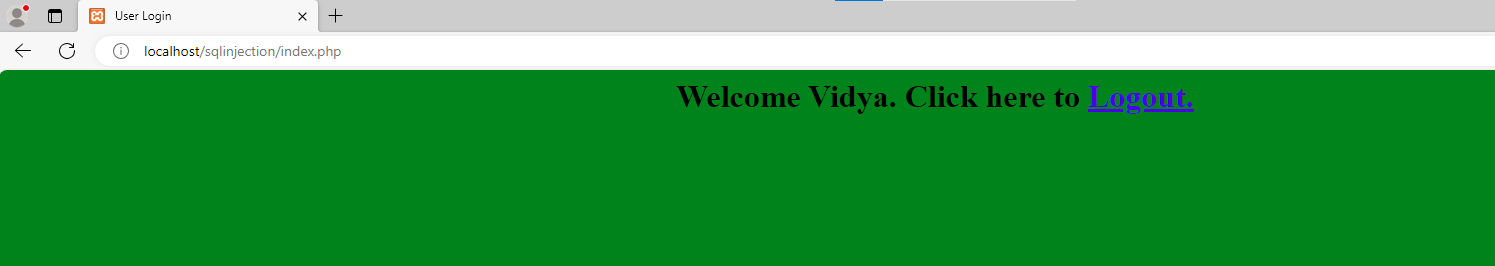
**Enter :**

**Username = ' OR 1=1--'**

**Password = 12345 or vv (the one in the studentusers table)**

**Result :**





Conclusion : we are logged into the index.php webpage inspite of giving a wrong username. The username = ' OR 1=1--' is a sql injection malicious code.

**How to prevent SQL injection attack?**

To prevent SQL injection attack, we use the prepared statement concept – ie parameterized query to avoid SQL injection attack.

LoginPrevent.php

<?php

session\_start();

$message="";

if(count($\_POST)>0)

{

$uname = $\_POST["user\_name"];

$pass =$\_POST["password"];

**$con = mysqli\_connect('127.0.0.1:3306','root','','studusers') or die('Unable To**

**connect');**

**$sql="SELECT \* FROM login\_user WHERE user\_name=? and password =?";**

**//echo $sql;**

**$stmt =$con->prepare($sql);**

**$stmt->bind\_param('ss',$uname,$pass);**

**$stmt->execute();**

**$result = $stmt->get\_result();**

$row = mysqli\_fetch\_array($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>

