Jurusan Teknologi Informasi Politeknik Negeri Malang

Jobsheet- 9: PHP (Login, Cookies, Session)

Mata Kuliah Desain dan Pemrograman Web

Pengampu: Tim Ajar Desain dan Pemrograman Web

Agustus 2020

Ketentuan;

Simpanlah file lembar jawaban ini dengan format; **Kelas_Nama Lengkap**

Contoh; **TI 2A_Elok Nur Hamdana**

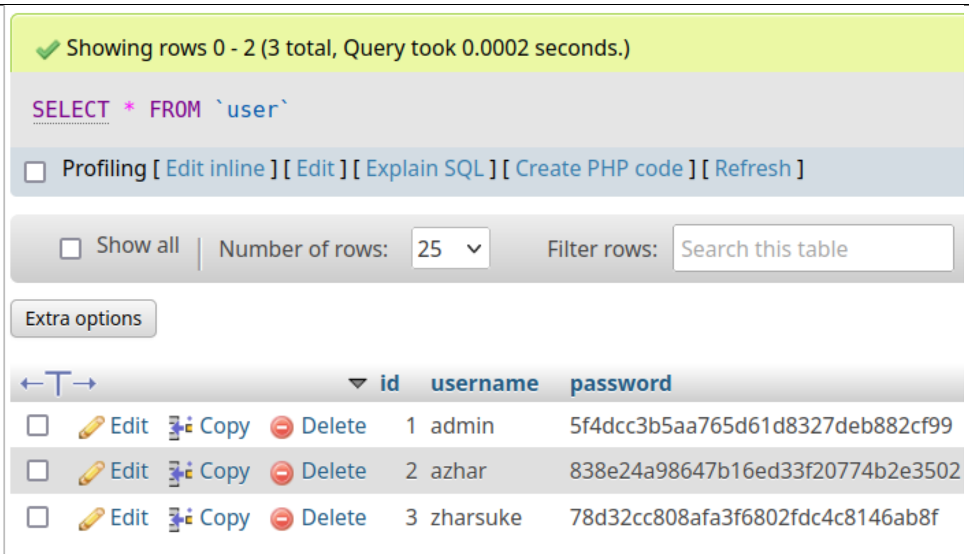
Upload tugas jobsheet ini dengan batas maksimum sesuai jadwal perkuliahan masing masing kelas

Upload file tugas jobsheet di website **lms.polinema**

Nama	:	AL AZHAR RIZQI RIFA'I FIRDAUS
Nim	:	2241720263
Kelas	:	TI 2I

Tulislah Jawaban Pada Kolom Yang tersedia di bawah ini;

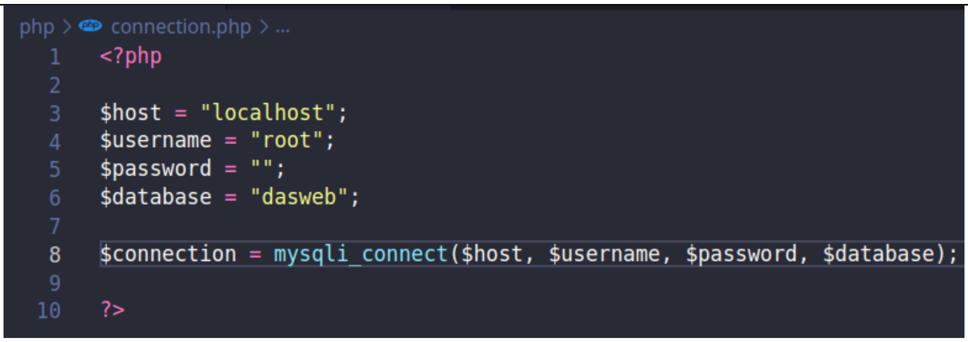
LEMBAR JAWABAN JOBSHEET- 9: PHP (Login, Cookies, Session)

<table>
<tr><th>Soal No</th><th>Jawaban</th></tr>
<tr><td>1</td><td>

✓ Showing rows 0 - 2 (3 total, Query took 0.0002 seconds.)

SELECT * FROM `user`

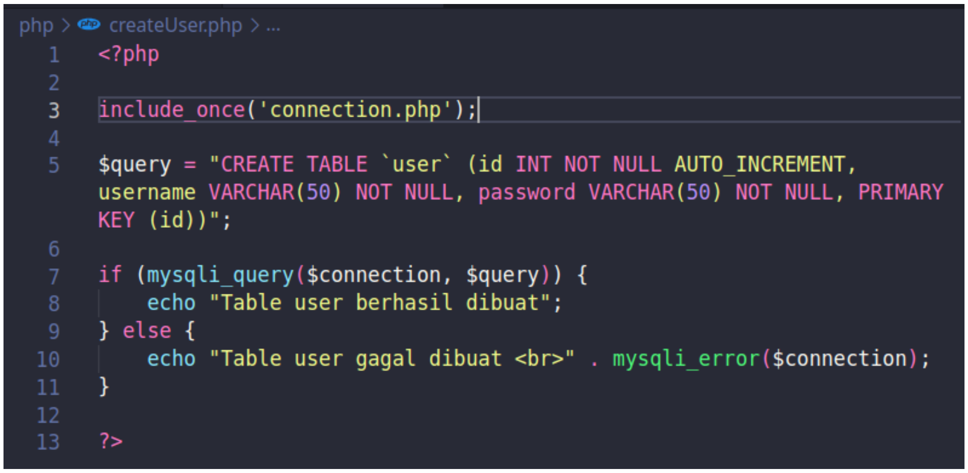
□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
□ Show all
Number of rows: 25
Filter rows: Search this table
Extra options
←T→

<table>
<tr><th></th><th></th><th></th><th></th><th>id</th><th>username</th><th>password</th></tr>
<tr><td>□</td><td>Edit</td><td>Copy</td><td>Delete</td><td>1</td><td>admin</td><td>5f4dcc3b5aa765d61d8327deb882cf99</td></tr>
<tr><td>□</td><td>Edit</td><td>Copy</td><td>Delete</td><td>2</td><td>azhar</td><td>838e24a98647b16ed33f20774b2e3502</td></tr>
<tr><td>□</td><td>Edit</td><td>Copy</td><td>Delete</td><td>3</td><td>zharsuke</td><td>78d32cc808afa3f6802fdc4c8146ab8f</td></tr>
</table>
</td></tr>
<tr><td>2</td><td>Connection.php</td></tr>
</table>



php > connection.php > ...

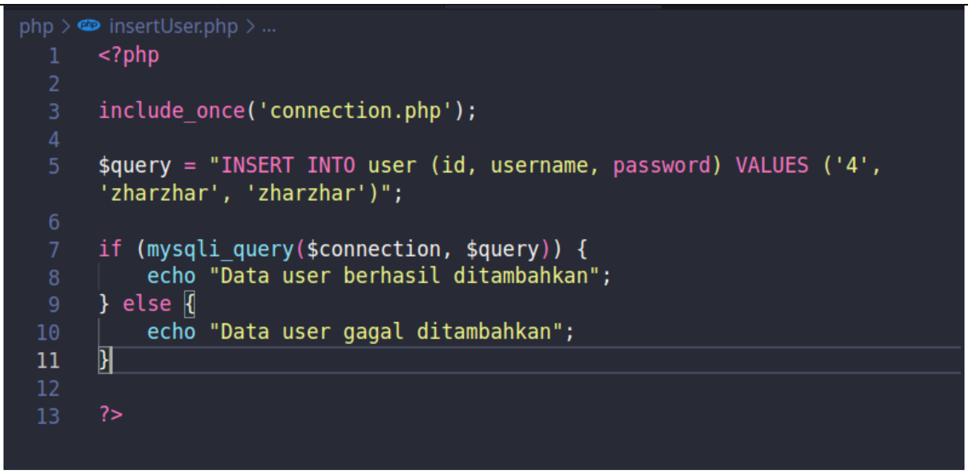
```php
<?php

$host = "localhost";
$username = "root";
$password = "";
$database = "dasweb";

$connection = mysqli_connect($host, $username, $password, $database);

?>
```



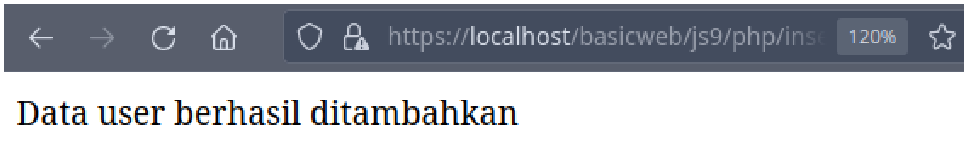
php > createUser.php > ...

```php
<?php

include_once('connection.php');

$query = "CREATE TABLE `user` (id INT NOT NULL AUTO_INCREMENT, username VARCHAR(50) NOT NULL, password VARCHAR(50) NOT NULL, PRIMARY KEY (id))";

if (mysqli_query($connection, $query)) {
    echo "Table user berhasil dibuat";
} else {
    echo "Table user gagal dibuat <br>" . mysqli_error($connection);
}

?>
```

3

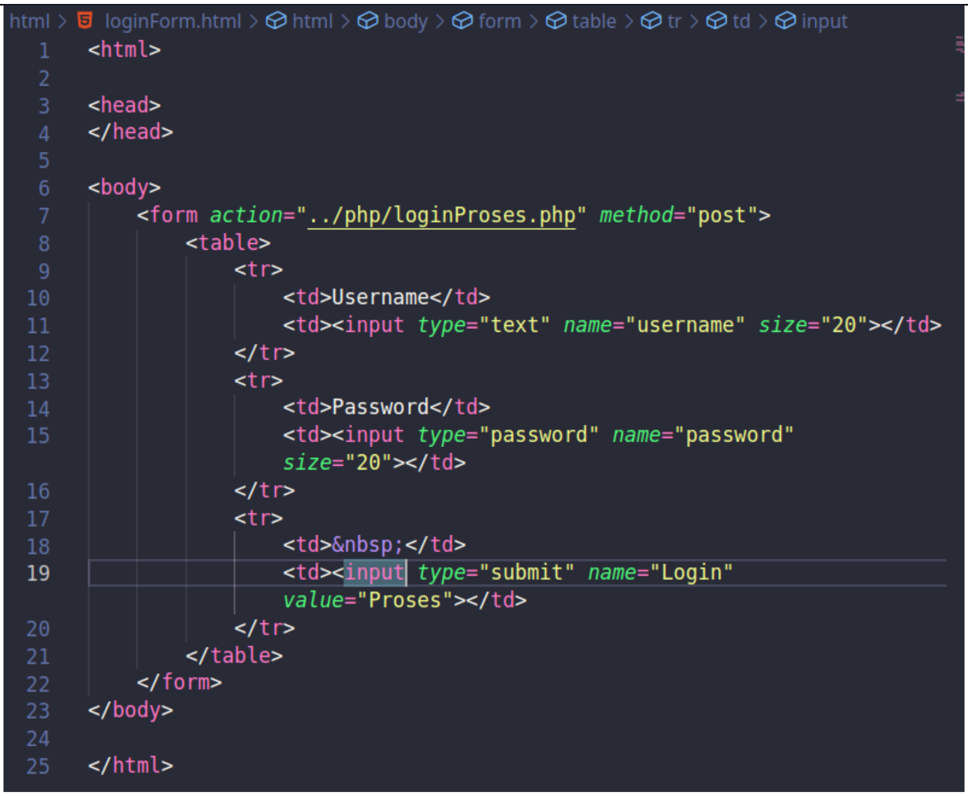


```php
<?php

include_once('connection.php');

$query = "INSERT INTO user (id, username, password) VALUES ('4',
'zharzhar', 'zharzhar')";

if (mysqli_query($connection, $query)) {
    echo "Data user berhasil ditambahkan";
} else {
    echo "Data user gagal ditambahkan";
}

?>
```

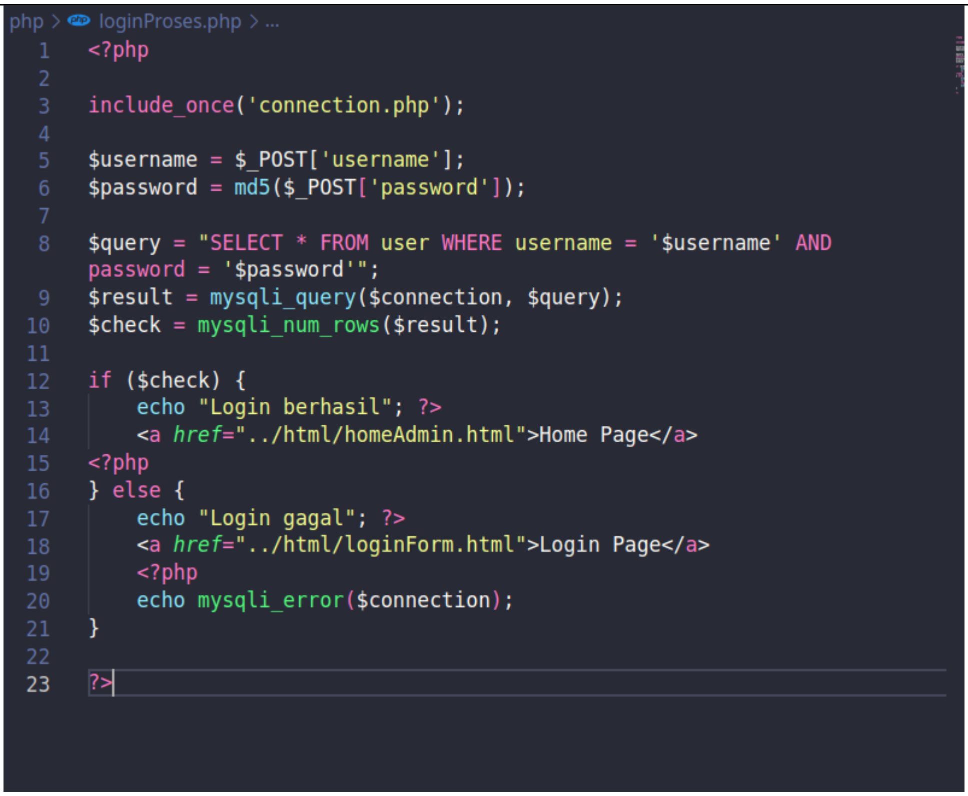


Data user berhasil ditambahkan

4

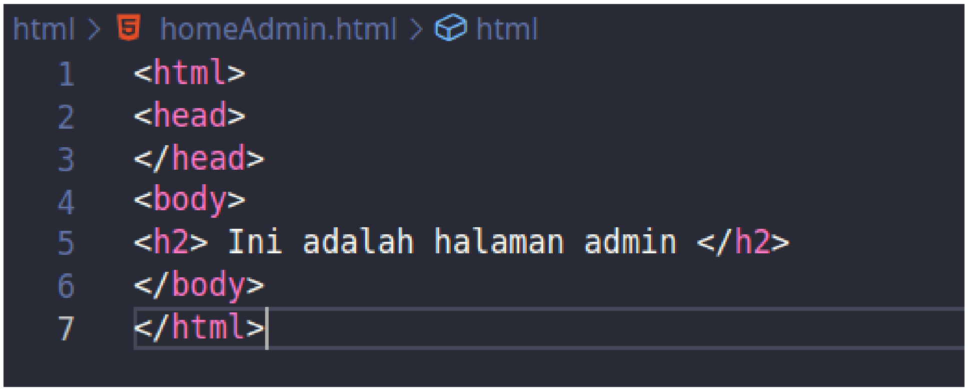

html > loginForm.html > html > body > form > table > tr > td > input

```html
<html>

<head>
</head>

<body>
    <form action="../php/loginProses.php" method="post">
        <table>
            <tr>
                <td>Username</td>
                <td><input type="text" name="username" size="20"></td>
            </tr>
            <tr>
                <td>Password</td>
                <td><input type="password" name="password" size="20"></td>
            </tr>
            <tr>
                <td>&nbsp;</td>
                <td><input type="submit" name="Login" value="Proses"></td>
            </tr>
        </table>
    </form>
</body>

</html>
```



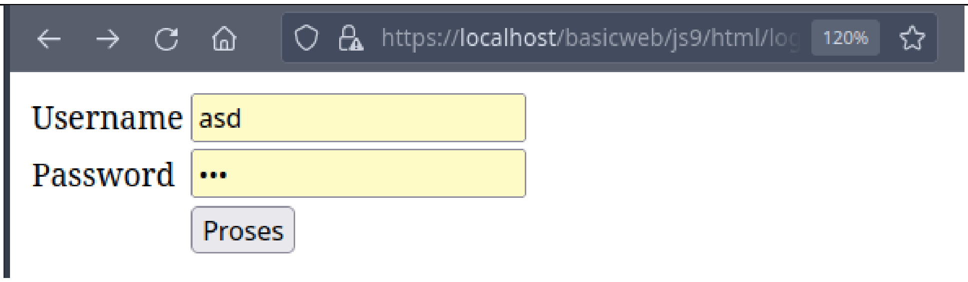
php > loginProses.php > ...

```php
<?php

include_once('connection.php');

$username = $_POST['username'];
$password = md5($_POST['password']);

$query = "SELECT * FROM user WHERE username = '$username' AND password = '$password'";
$result = mysqli_query($connection, $query);
$check = mysqli_num_rows($result);

if ($check) {
    echo "Login berhasil"; ?>
    <a href="../html/homeAdmin.html">Home Page</a>
<?php
} else {
    echo "Login gagal"; ?>
    <a href="../html/loginForm.html">Login Page</a>
    <?php
    echo mysqli_error($connection);
}

?>
```



html > homeAdmin.html > html

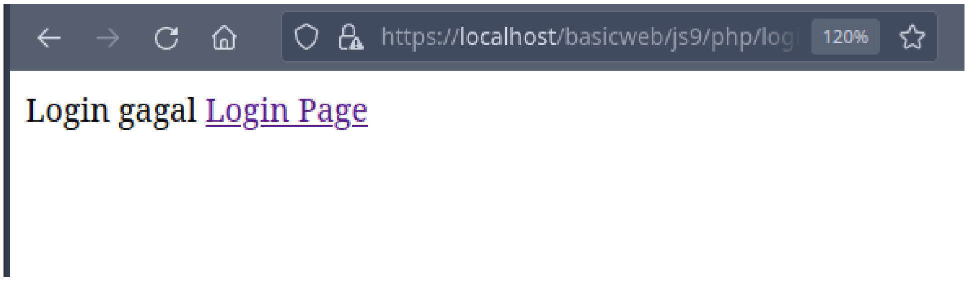
```html
<html>
<head>
</head>
<body>
<h2> Ini adalah halaman admin </h2>
</body>
</html>
```



https://localhost/basicweb/js9/html/log

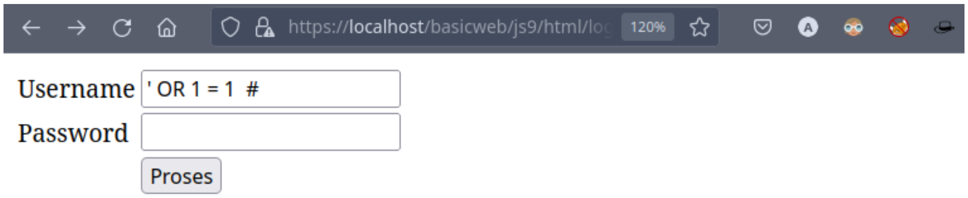
Username: asd

Password: •••



https://localhost/basicweb/js9/php/log

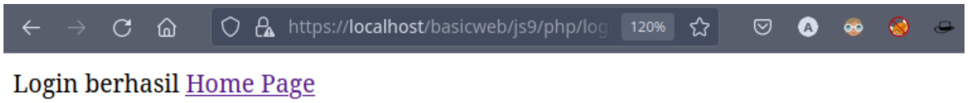
Login gagal Login Page



https://localhost/basicweb/js9/html/lo

Username: ' OR 1 = 1 #

Password:

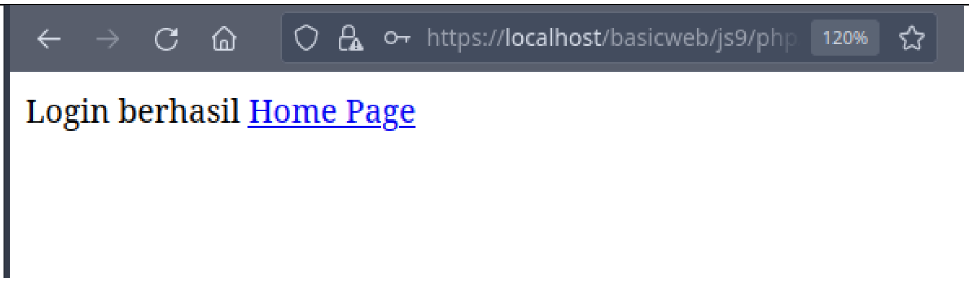


https://localhost/basicweb/js9/php/log

Login berhasil Home Page

- The result will display "you failed to log in" because in loginProcess.php there is a query that selects the username and password that matches the database. But it can be exploit with sql injection with insert payload “‘ OR 1 = 1#”. It happened because there is no sanitize filter to check the query.

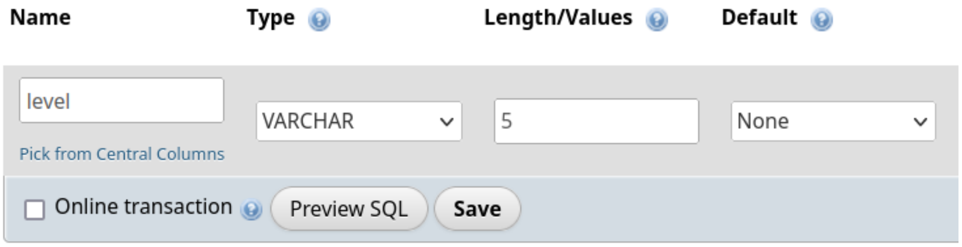
5



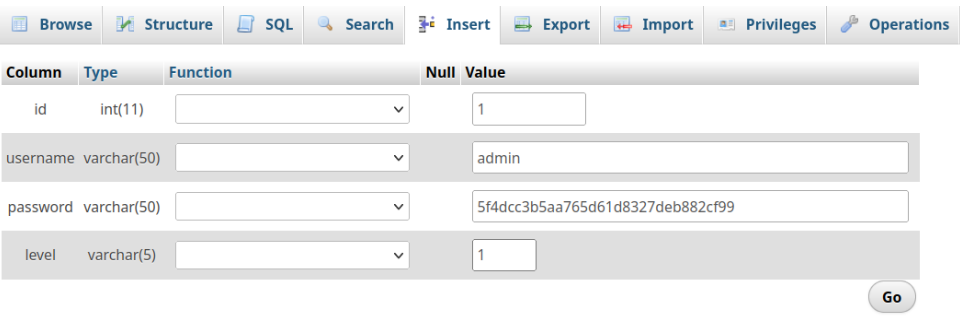
Login berhasil Home Page

- The result is successful login because the username and password data matches the one in the database.

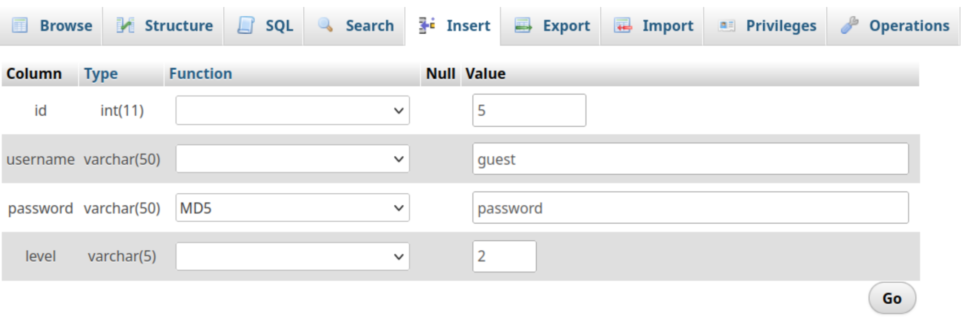
6



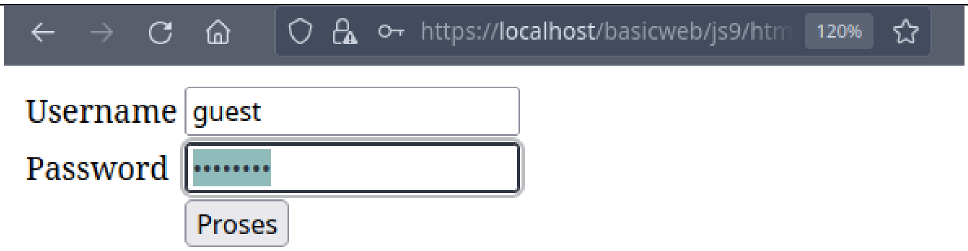
Name	Type	Length/Values	Default
level	VARCHAR	5	None



Column	Type	Function	Null	Value
id	int(11)			1
username	varchar(50)			admin
password	varchar(50)			5f4dcc3b5aa765d61d8327deb882cf99
level	varchar(5)			1



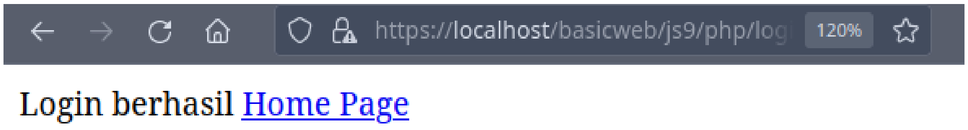
Column	Type	Function	Null	Value
id	int(11)			5
username	varchar(50)			guest
password	varchar(50)	MD5		password
level	varchar(5)			2



https://localhost/basicweb/js9/htm

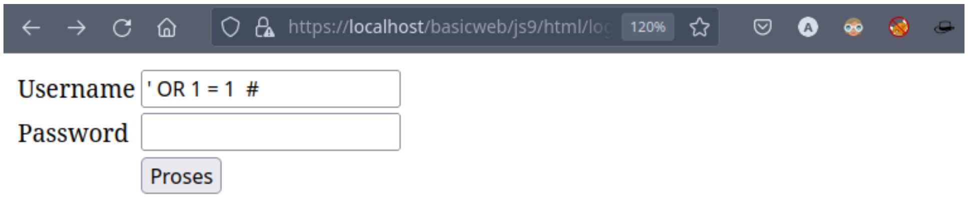
Username: guest

Password: •••••••••



https://localhost/basicweb/js9/php/log

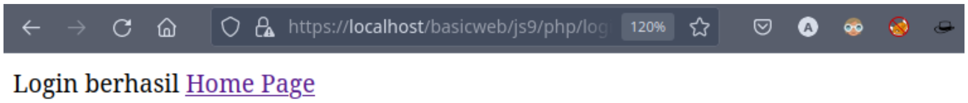
Login berhasil Home Page



https://localhost/basicweb/js9/html/lo

Username: ' OR 1 = 1 #

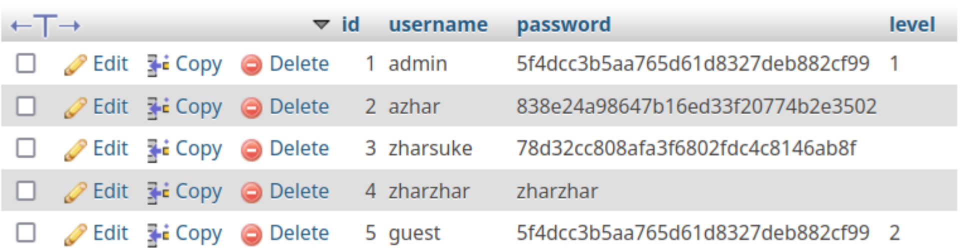
Password:



https://localhost/basicweb/js9/php/log

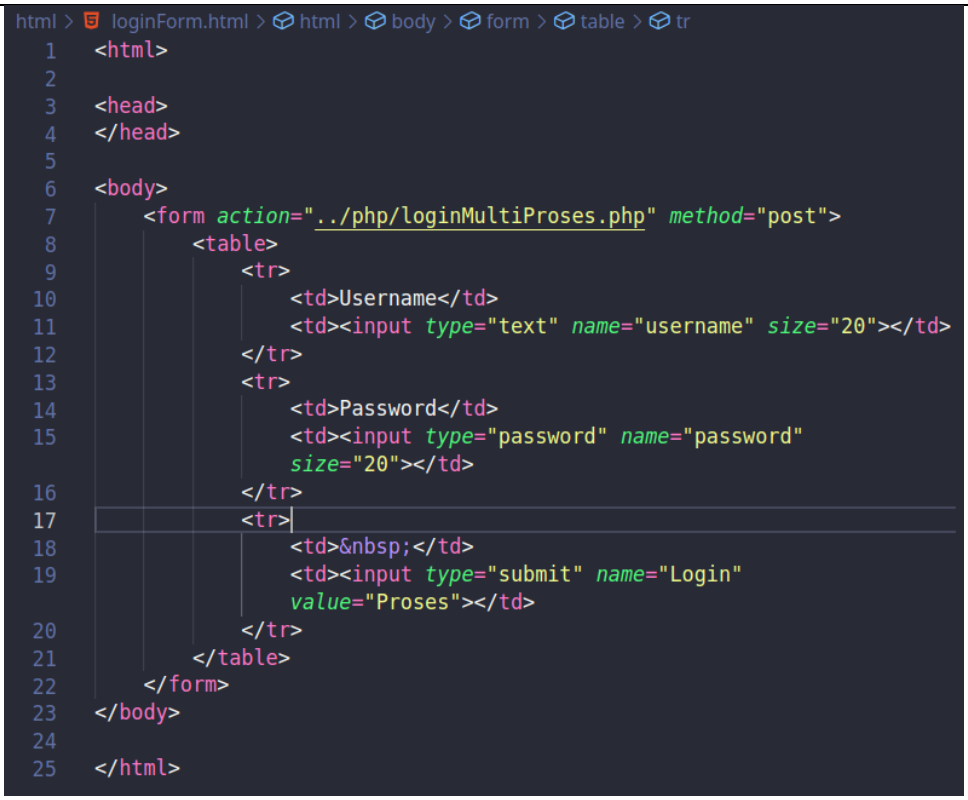
Login berhasil Home Page

- Guest data or all of users that registered is successfully logged in. But it can be exploit with sql injection with insert payload "' OR 1 = 1#". It happened because there is no sanitize filter to check the query.

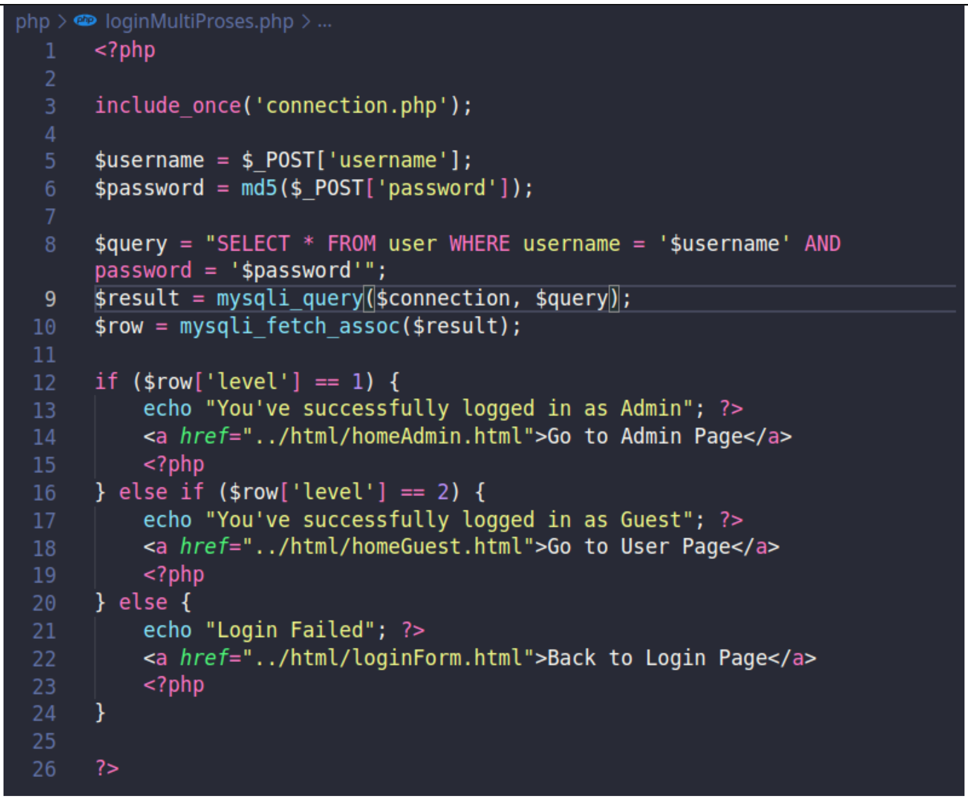
7	

←T→				▼ id	username	password	level
☐	Edit	Copy	Delete	1	admin	5f4dcc3b5aa765d61d8327deb882cf99	1
☐	Edit	Copy	Delete	2	azhar	838e24a98647b16ed33f20774b2e3502	
☐	Edit	Copy	Delete	3	zharsuke	78d32cc808afa3f6802fdc4c8146ab8f	
☐	Edit	Copy	Delete	4	zharzhar	zharzhar	
☐	Edit	Copy	Delete	5	guest	5f4dcc3b5aa765d61d8327deb882cf99	2

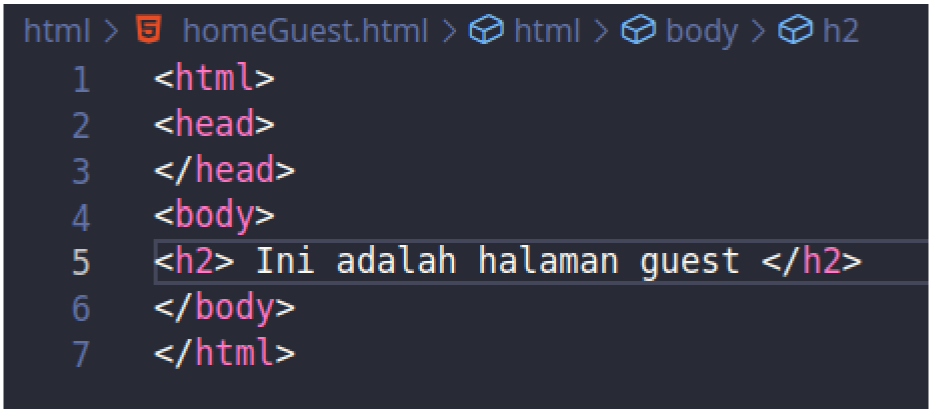
8



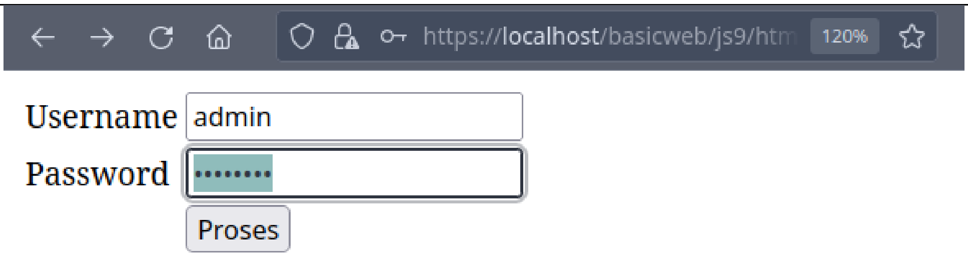
```html
<html>

<head>
</head>

<body>
    <form action="../php/loginMultiProses.php" method="post">
        <table>
            <tr>
                <td>Username</td>
                <td><input type="text" name="username" size="20"></td>
            </tr>
            <tr>
                <td>Password</td>
                <td><input type="password" name="password" size="20"></td>
            </tr>
            <tr>
                <td>&nbsp;</td>
                <td><input type="submit" name="Login" value="Proses"></td>
            </tr>
        </table>
    </form>
</body>

</html>
```



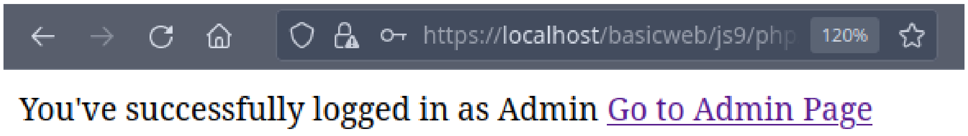
```php
<?php

include_once('connection.php');

$username = $_POST['username'];
$password = md5($_POST['password']);

$query = "SELECT * FROM user WHERE username = '$username' AND password = '$password'";
$result = mysqli_query($connection, $query);
$row = mysqli_fetch_assoc($result);

if ($row['level'] == 1) {
    echo "You've successfully logged in as Admin"; ?>
    <a href="../html/homeAdmin.html">Go to Admin Page</a>
    <?php
} else if ($row['level'] == 2) {
    echo "You've successfully logged in as Guest"; ?>
    <a href="../html/homeGuest.html">Go to User Page</a>
    <?php
} else {
    echo "Login Failed"; ?>
    <a href="../html/loginForm.html">Back to Login Page</a>
    <?php
}

?>
```



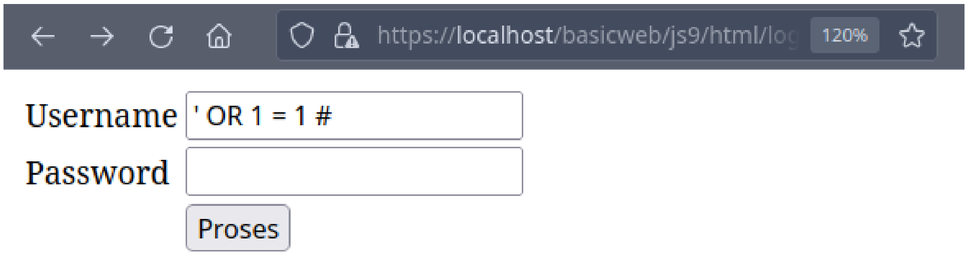
```html
<html>
<head>
</head>
<body>
<h2> Ini adalah halaman guest </h2>
</body>
</html>
```



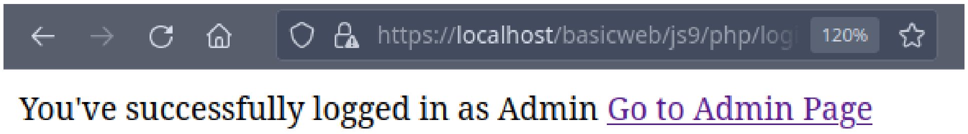
Username admin
Password ••••••••



You've successfully logged in as Admin Go to Admin Page

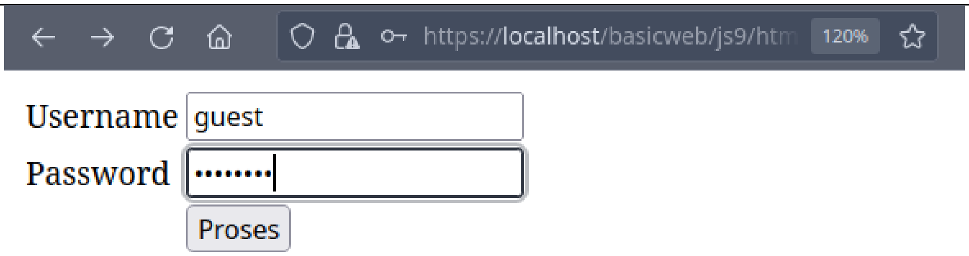
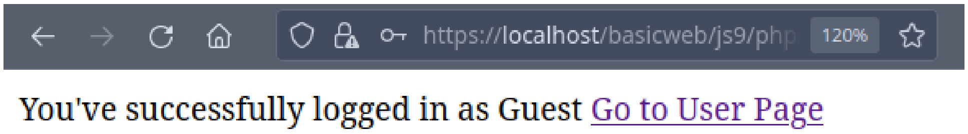
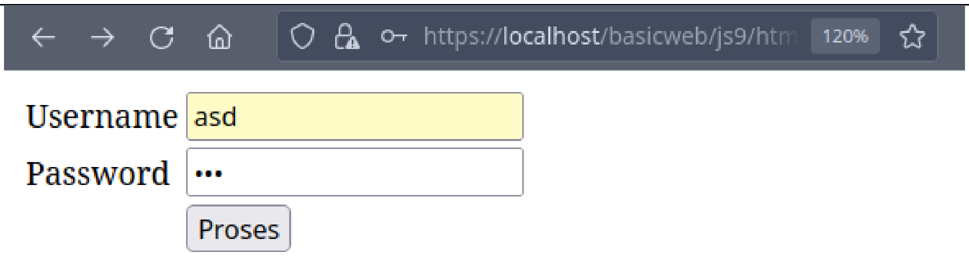
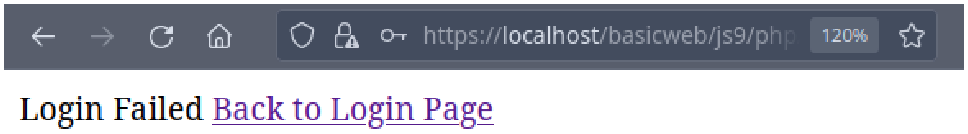


Username ' OR 1 = 1 #
Password

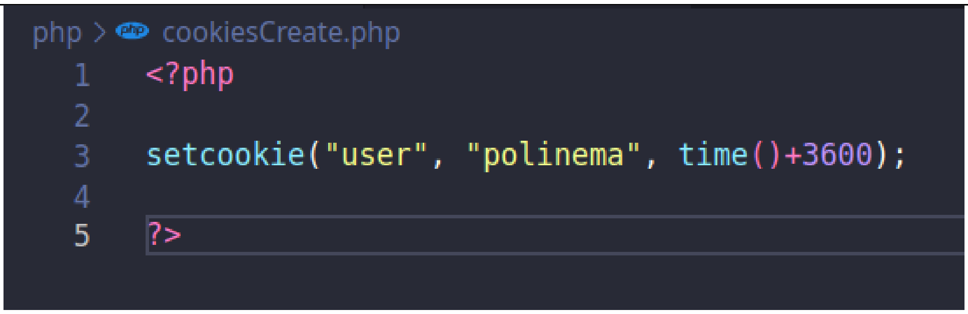


You've successfully logged in as Admin Go to Admin Page

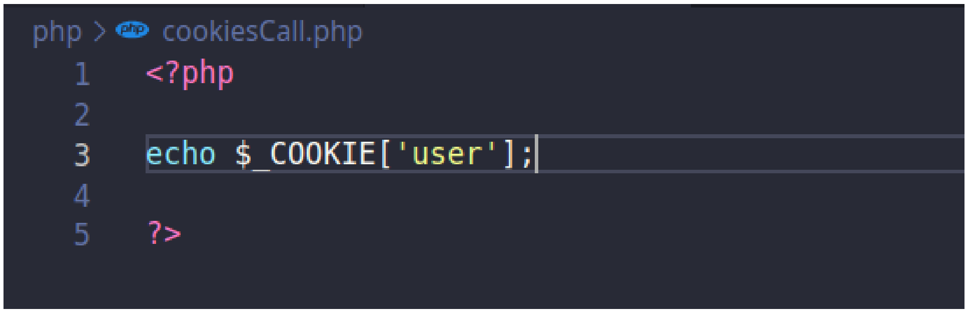
- It redirect to admin page output because the admin is at level 1. But when I attempt to exploit with sql injection, it login as admin.

9	 https://localhost/basicweb/js9/htm Username guest Password •••••••• Proses  https://localhost/basicweb/js9/php You've successfully logged in as Guest Go to User Page - It redirect to Guest page output because the admin is at level 2.
10	 https://localhost/basicweb/js9/htm Username asd Password ••• Proses  https://localhost/basicweb/js9/php Login Failed Back to Login Page - Output has return login failed because there is no asd user on user table.

11



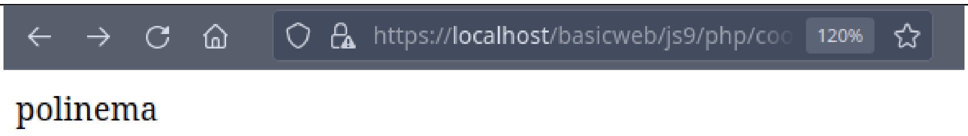
```php
<?php

setcookie("user", "polinema", time()+3600);

?>
```



```php
<?php

echo $_COOKIE['user'];

?>
```

- The program will blank because the cookie has not been created yet but has been called.

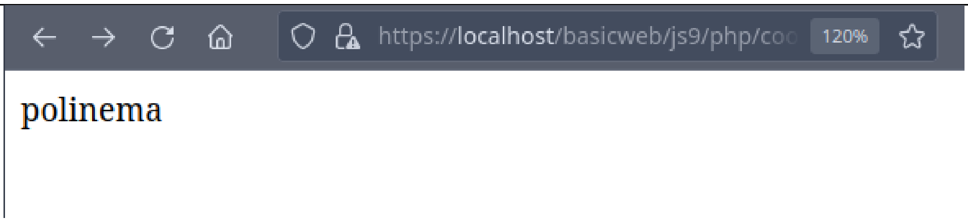
12



polinema

- The cookie displayed is polynema because the cookie created is polinema.

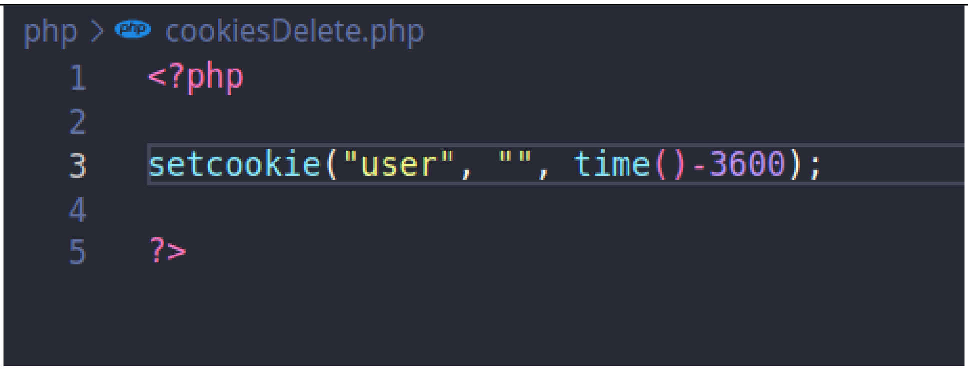
<table>
<tr>
<td>13</td>
<td>



polinema

- After restart my computer, the cookie still appear. It happen because cookie has not expired. Cookie will be deleted after expired.

</td>
</tr>
<tr>
<td>14</td>
<td>

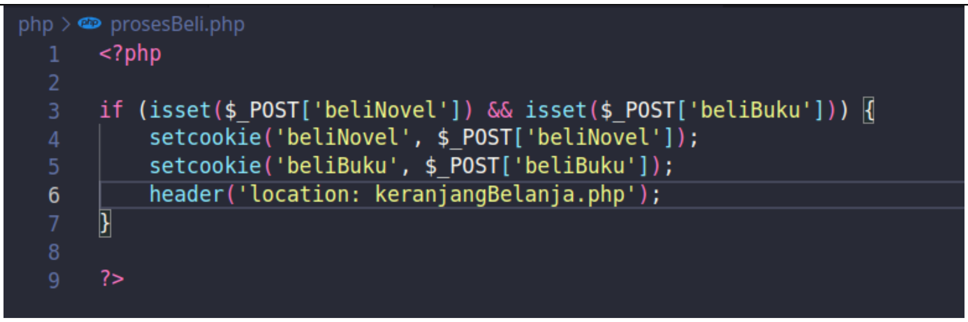


```php
<?php

setcookie("user", "", time()-3600);

?>
```

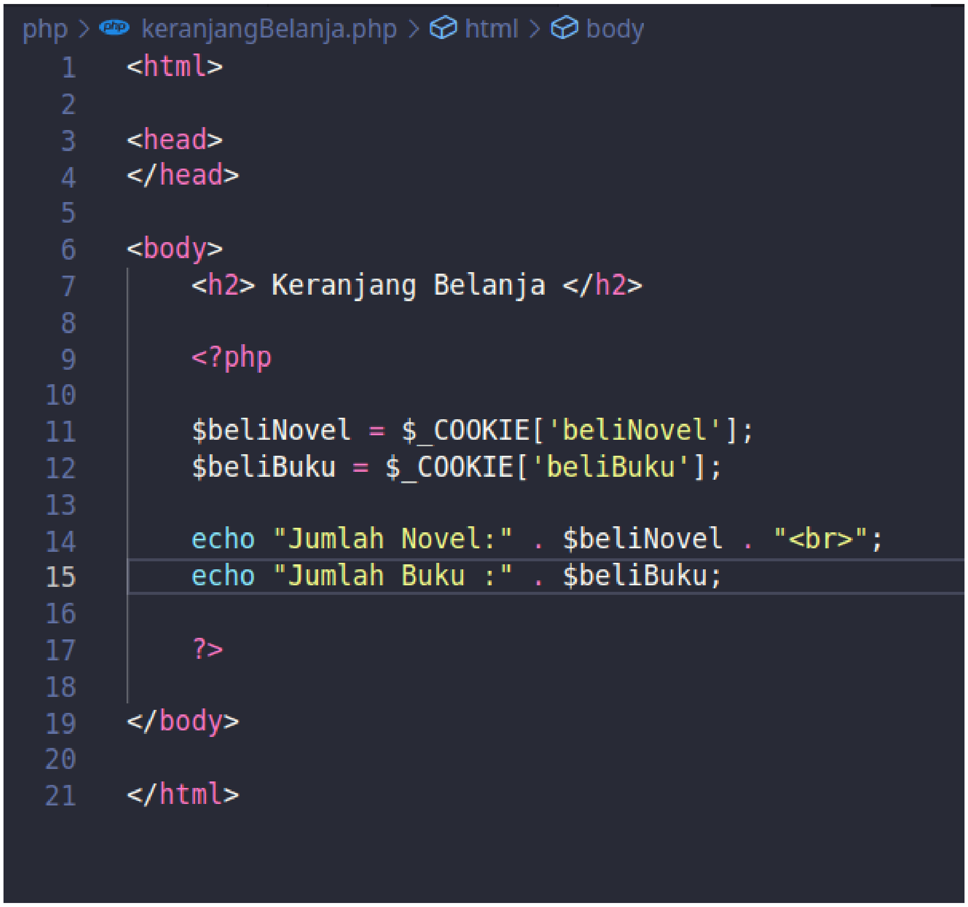
- The result is blank because cookie has already deleted.

</td>
</tr>
</table>

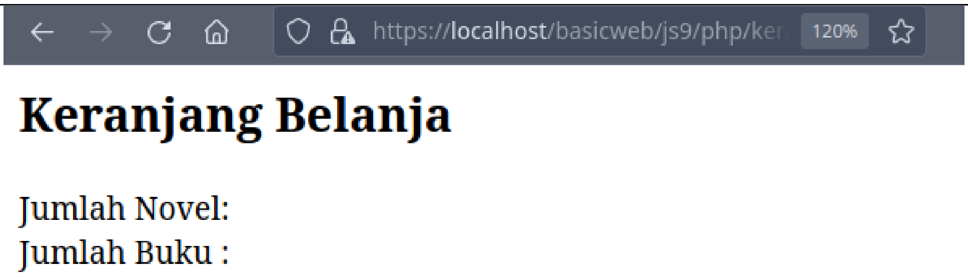
15



```php
<?php

if (isset($_POST['beliNovel']) && isset($_POST['beliBuku'])) {
    setcookie('beliNovel', $_POST['beliNovel']);
    setcookie('beliBuku', $_POST['beliBuku']);
    header('location: keranjangBelanja.php');
}

?>
```

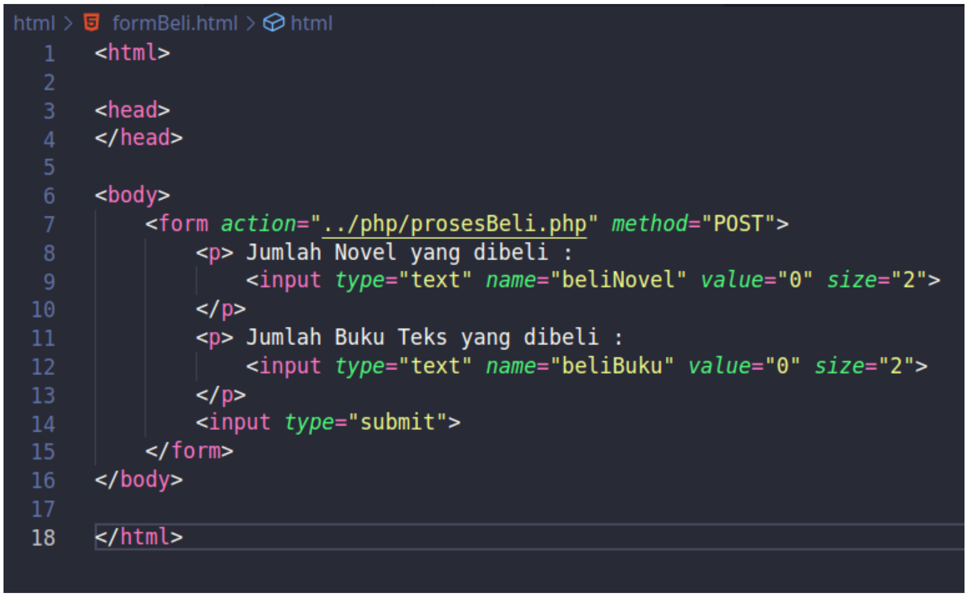


```php
<html>

<head>
</head>

<body>
    <h2> Keranjang Belanja </h2>

    <?php

    $beliNovel = $_COOKIE['beliNovel'];
    $beliBuku = $_COOKIE['beliBuku'];

    echo "Jumlah Novel:" . $beliNovel . "<br>";
    echo "Jumlah Buku :" . $beliBuku;

    ?>

</body>

</html>
```



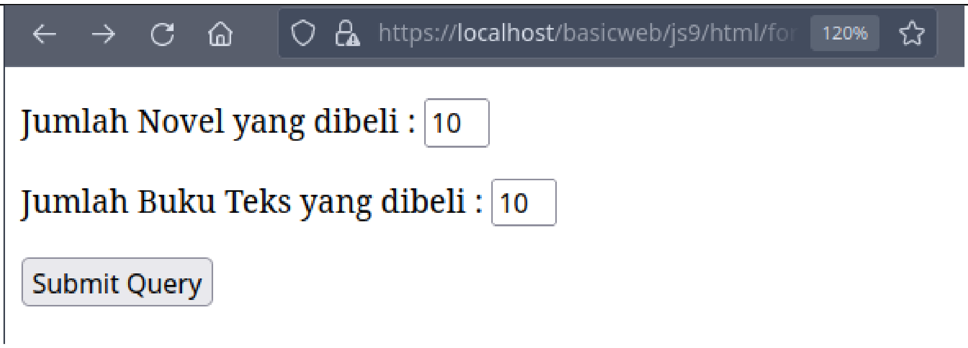
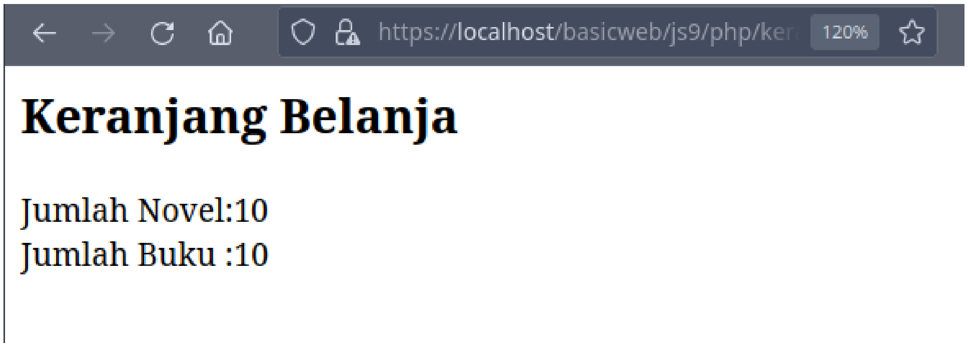
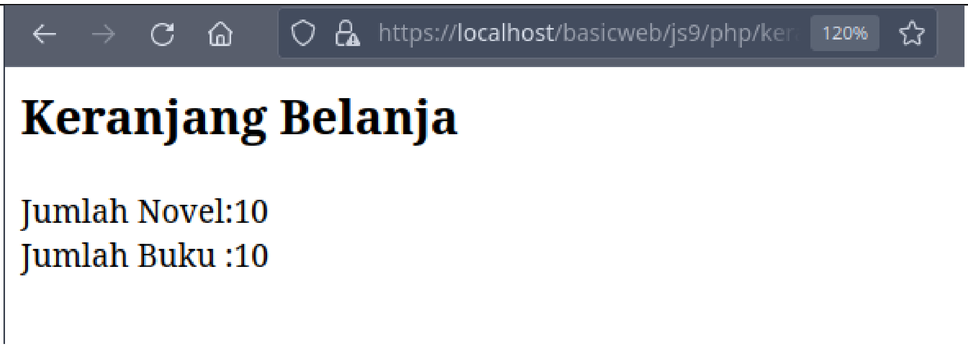
Keranjang Belanja

Jumlah Novel:
Jumlah Buku :

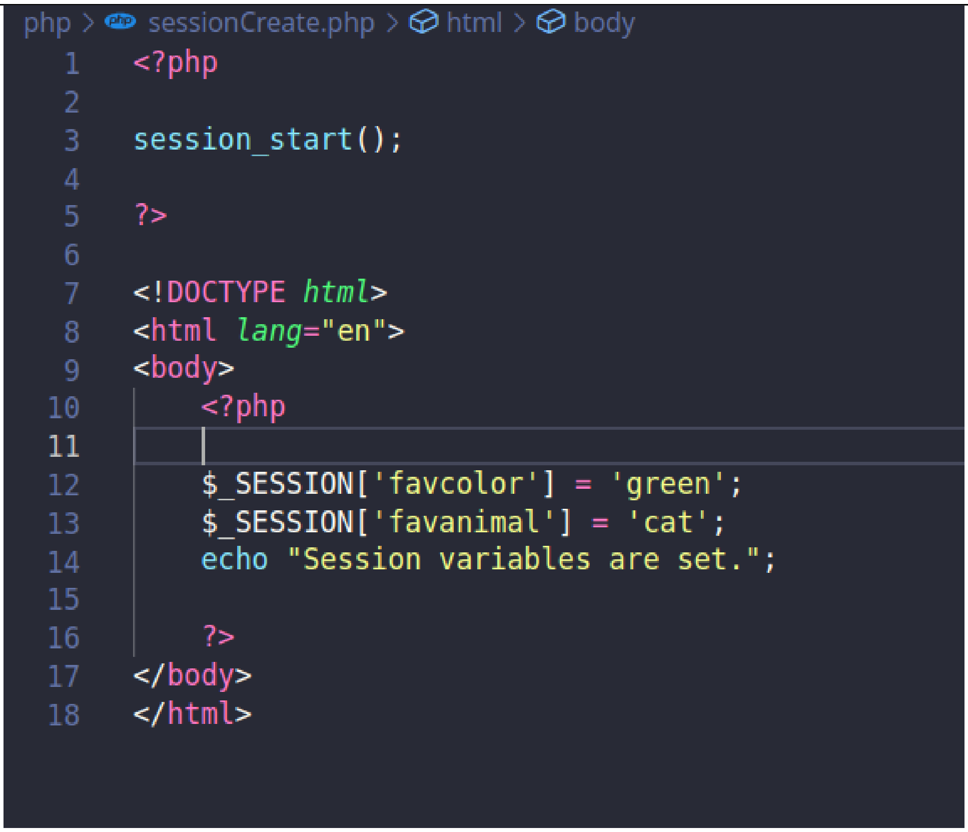


```
<html>

<head>
</head>

<body>
    <form action="../php/prosesBeli.php" method="POST">
        <p> Jumlah Novel yang dibeli :
            <input type="text" name="beliNovel" value="0" size="2">
        </p>
        <p> Jumlah Buku Teks yang dibeli :
            <input type="text" name="beliBuku" value="0" size="2">
        </p>
        <input type="submit">
    </form>
</body>

</html>
```

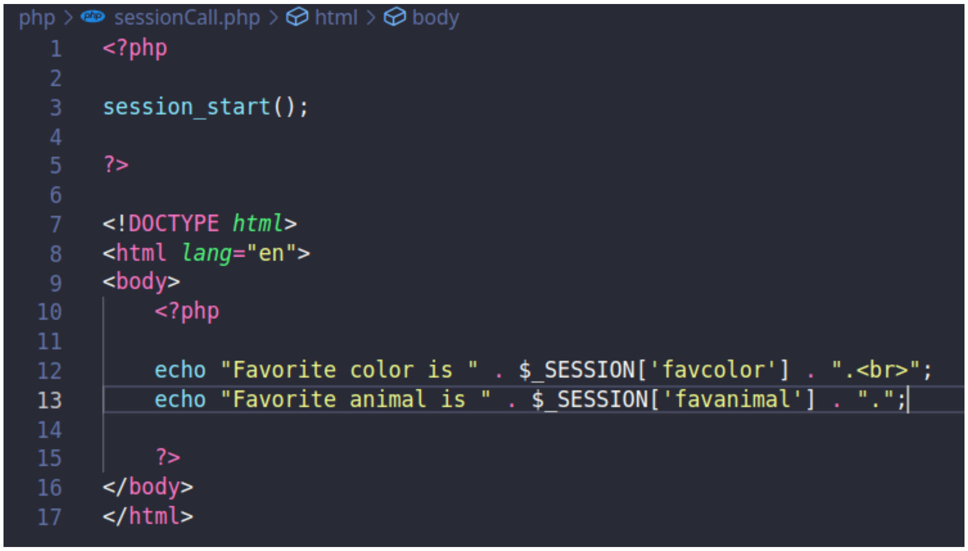
- The result is blank because novel and book still empty.

16	 Jumlah Novel yang dibeli : 10 Jumlah Buku Teks yang dibeli : 10  Keranjang Belanja Jumlah Novel:10 Jumlah Buku :10 - We successfully to insert value at amount novel and book.
17	 Keranjang Belanja Jumlah Novel:10 Jumlah Buku :10 - The amount novel and book appear. It means cookie still stored.

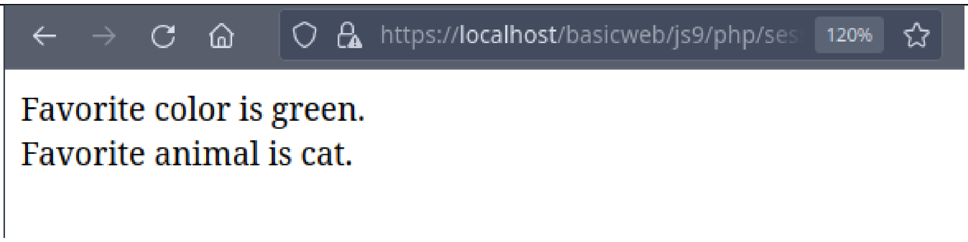
18



```
<?php

session_start();

?>

<!DOCTYPE html>
<html lang="en">
<body>
    <?php
    
    $_SESSION['favcolor'] = 'green';
    $_SESSION['favanimal'] = 'cat';
    echo "Session variables are set.";

    ?>
</body>
</html>
```



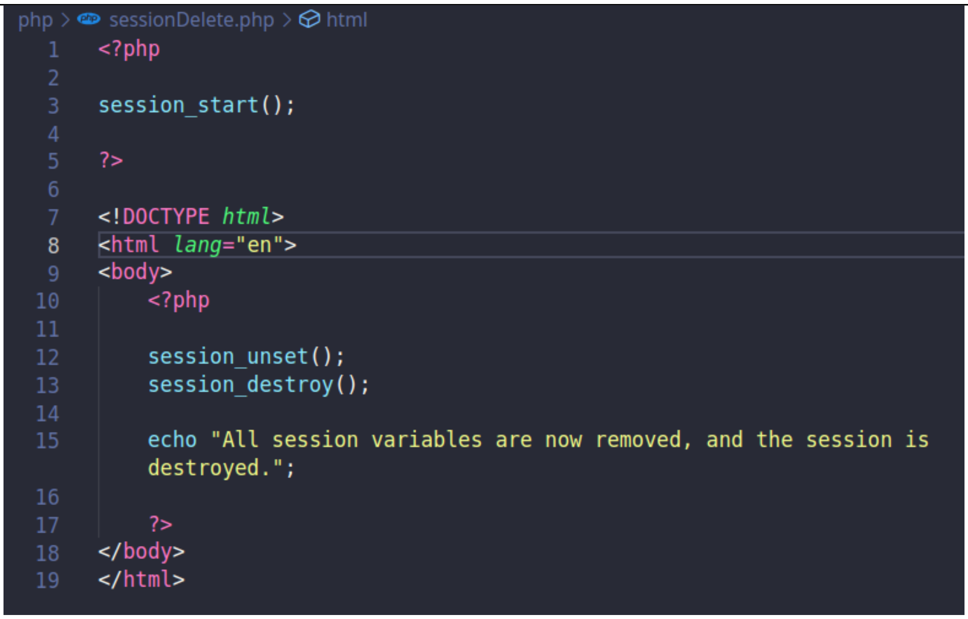
```
<?php

session_start();

?>

<!DOCTYPE html>
<html lang="en">
<body>
    <?php

    echo "Favorite color is " . $_SESSION['favcolor'] . ".<br>";
    echo "Favorite animal is " . $_SESSION['favanimal'] . ".";

    ?>
</body>
</html>
```



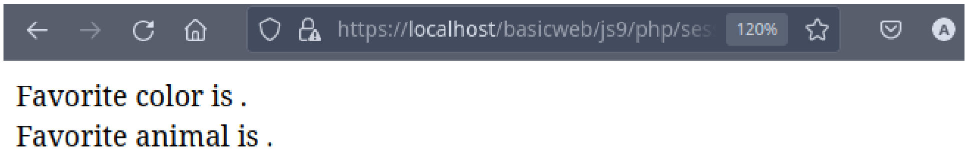
Favorite color is green.
Favorite animal is cat.

- Successfully display fav color and animal.

19



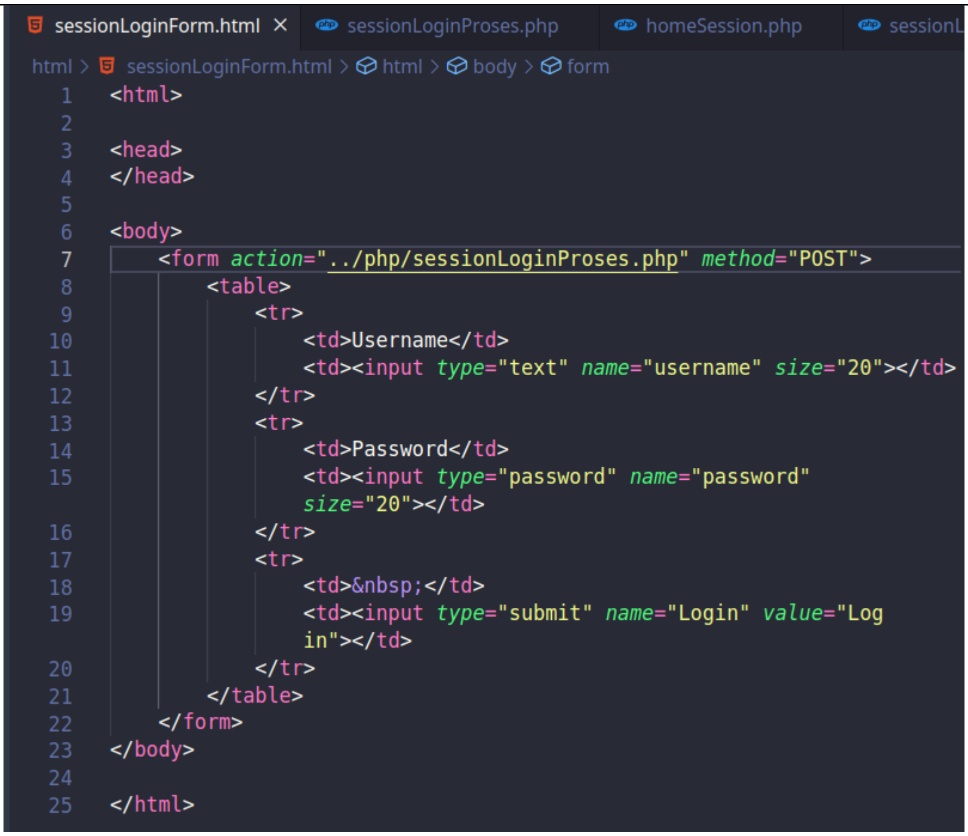
```php
<?php

session_start();

?>

<!DOCTYPE html>
<html lang="en">
<body>
    <?php

    session_unset();
    session_destroy();

    echo "All session variables are now removed, and the session is destroyed.";

    ?>
</body>
</html>
```



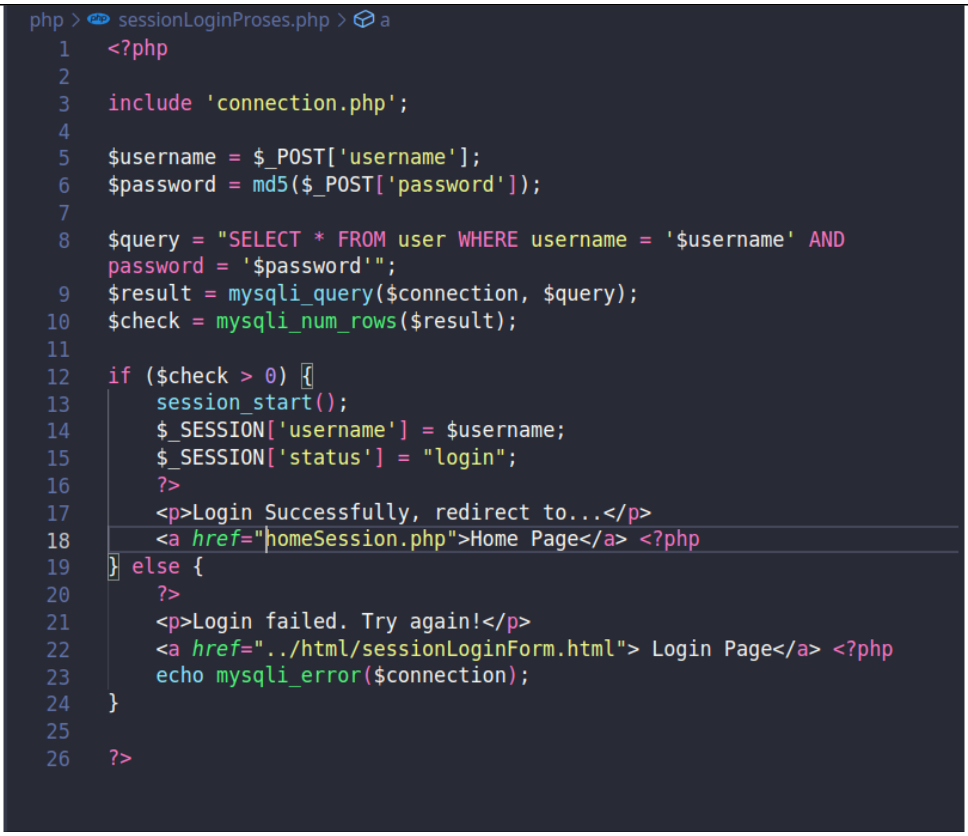
Favorite color is .
Favorite animal is .

- favcolor and favanimal session doesn’t appear because has already deleted.

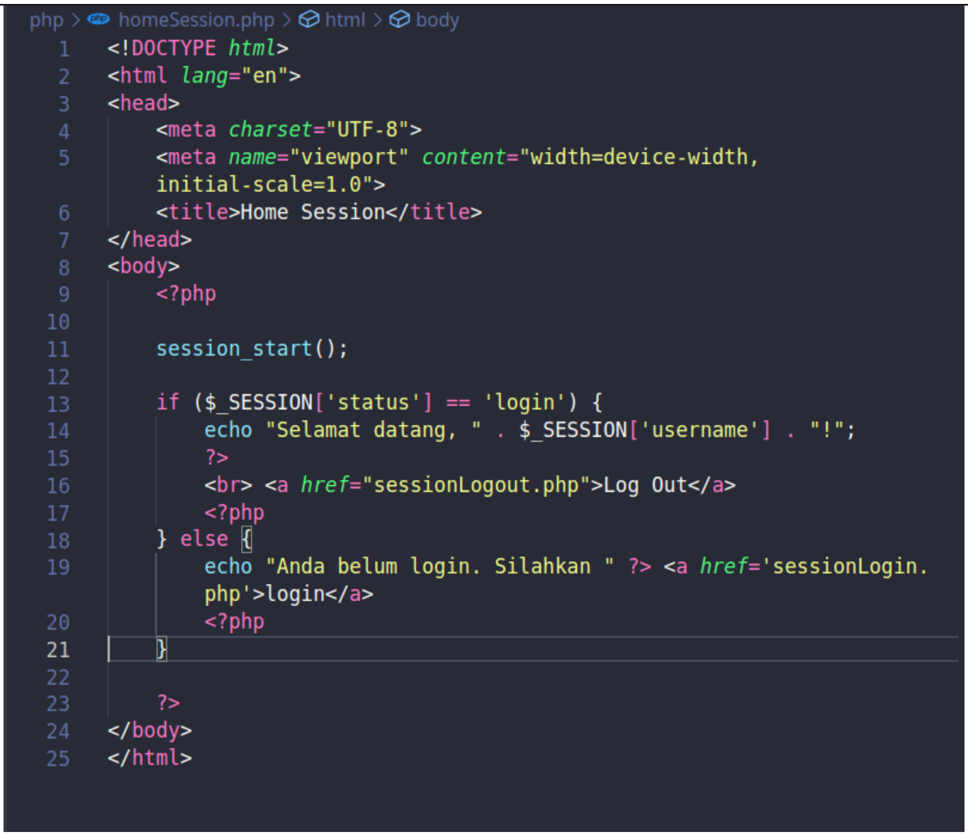
20



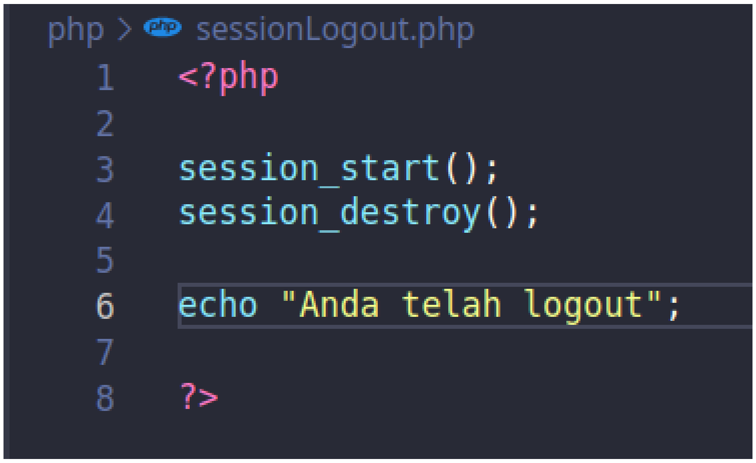
```
<html>

<head>
</head>

<body>
    <form action="../php/sessionLoginProses.php" method="POST">
        <table>
            <tr>
                <td>Username</td>
                <td><input type="text" name="username" size="20"></td>
            </tr>
            <tr>
                <td>Password</td>
                <td><input type="password" name="password" size="20"></td>
            </tr>
            <tr>
                <td>&nbsp;</td>
                <td><input type="submit" name="Login" value="Login"></td>
            </tr>
        </table>
    </form>
</body>

</html>
```



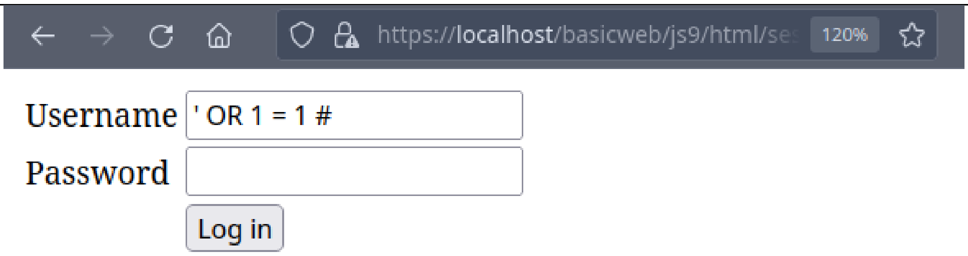
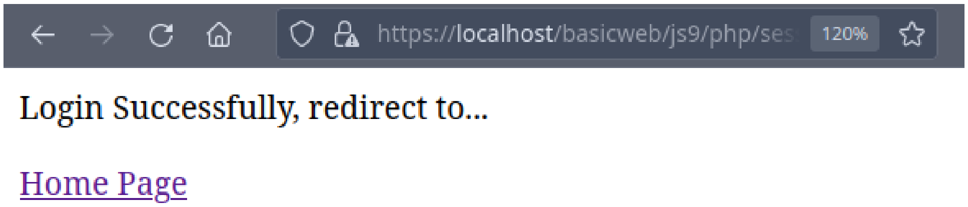
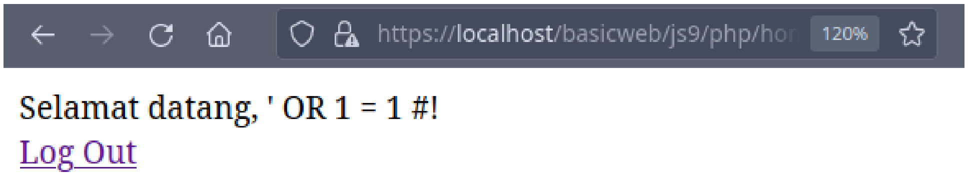
```php
<?php

include 'connection.php';

$username = $_POST['username'];
$password = md5($_POST['password']);

$query = "SELECT * FROM user WHERE username = '$username' AND password = '$password'";
$result = mysqli_query($connection, $query);
$check = mysqli_num_rows($result);

if ($check > 0) {
    session_start();
    $_SESSION['username'] = $username;
    $_SESSION['status'] = "login";
    ?>
    <p>Login Successfully, redirect to...</p>
    <a href="homeSession.php">Home Page</a> <?php
} else {
    ?>
    <p>Login failed. Try again!</p>
    <a href="../html/sessionLoginForm.html"> Login Page</a> <?php
    echo mysqli_error($connection);
}

?>
```



```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Home Session</title>
</head>
<body>
    <?php

    session_start();

    if ($_SESSION['status'] == 'login') {
        echo "Selamat datang, " . $_SESSION['username'] . "!";
        ?>
        <br> <a href="sessionLogout.php">Log Out</a>
        <?php
    } else {
        echo "Anda belum login. Silahkan " ?> <a href='sessionLogin.php'>login</a>
        <?php
    }

    ?>
</body>
</html>
```



```
<?php

session_start();
session_destroy();

echo "Anda telah logout";

?>
```

	 https://localhost/basicweb/js9/html/se Username ' OR 1 = 1 # Password Log in  https://localhost/basicweb/js9/php/ses Login Successfully, redirect to... Home Page  https://localhost/basicweb/js9/php/hor Selamat datang, ' OR 1 = 1 #! Log Out - Successful bypass login with sql injection.
21	- First enter the sessionLoginForm.html file to log in by inputting your username and password then click login, then it will enter the sessionLogin.php file in accordance with the action entered on the form, in the file is checked whether the data entered is correct or not, if appropriate, a successful login will appear and there is a home page link that will go to the file. there is a home page link that will go to the homeSession.php file, then there will be a link to log out which will go to the homeSession.php file. to log out which will go to the sessionLogout.php file which will perform the session deletion. session deletion,

	if the input data does not match, it will display a failed login and there will be a link to re-login to the session. there will be a link to re-login to the sessionLoginForm.html file,
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	