**3 Lab Tasks**

**3.1**

* Task 1.1
  + Yes it is, if we are aware of a user’s name we can simply type in **username’); #** (the variable username is used only for demonstration purposes) and have full access to that particular account without the need of a password. With the use of **#**  we can comment out the rest of the query. If we are not aware of the username we can still access an account by typing in **‘ OR LIKE name ‘X%’); #** (X can be any letter or number).
* Task 1.2
  + We can type in **username’); X; #** (X is an UPDATE or DELETE operation), however mysql\_query() does not support multiple queries, different versions might be able to though.

**3.2**

* Task 2
  + After opening the class.user.php and finding the edit() function we noticed that the company field was commented out, which clearly indicated that this was the vulnerability we needed to exploit. Connected to alice’s account we could change ted’s password and personal information if we wanted to. We simply entered **ted** into the user field and **‘, pass = ‘522B276A356BDF39013DFABEA2CD43E141ECC9E8’ WHERE ID = 4; #** into the company field. After submitting this we were able to access ted’s account with the password **alice** .The above sha1 value was generated by a website we found online for the word alice. We found ted’s id after a few tries.

**3.3**

* Task 3.1
  + After setting magic\_quotes\_gpc = On, we were not able to access any accounts as we did in Task 1.1 and we could not modify another account from an already accessed account like we did in Task 2.
* Task 3.2
  + After opening the class.user.php file and adding the mysql\_real\_escape\_string() function for the company field in the edit() function and in the login() function for the username and password we were able to close all vulnerabilities like we did in Task 3.1 .
* Task 3.3

function edit($id, $name, $realname, $email, $tel1, $tel2, $company, $zip, $gender, $url, $address1, $address2, $state, $country, $tags, $locale, $avatar = "", $rate = 0.0)

{

$rate = (double) $rate;

$id = (int) $id;

if ($avatar != "")

{

$stmt = $db->prepare("UPDATE user SET name=?,email=?,tel1=?, tel2=?,company?,zip=?,gender=?,url=?,adress=?,adress2=?,state=?,country=?,tags=?,locale=?,avatar=?,rate=? WHERE ID = ?");

$stmt-> bind\_param("sssssssssssssssdi", $name, $email, $tel1, $tel2, $company, $zip, $gender, $url, $address1, $address2, $state, $country, $tags, $locale, $avatar, $rate, $id);

$upd = $stmt-> execute();

}

else

{

$stmt = $db-> prepare("UPDATE user SET name=?,email=?, tel1=?, tel2=?, company=?,zip=?,gender=?,url=?,adress=?,adress2=?,state=?,country=?,tags=?,locale=?,rate=? WHERE ID = ?");

$stmt-> bind\_param("ssssssssssssssdi", $name, $email, $tel1, $tel2, $company, $zip, $gender, $url, $address1, $address2, $state, $country, $tags, $locale, $rate, $id);

$upd = $stmt-> execute();

}

if ($upd)

{

$this->mylog->add($name, 'user', 2, 0);

return true;

}

else

{

return false;

}

}

function login($user, $pass)

{

if (!$user)

{

return false;

}

$db\_host = 'localhost';

$db\_name = 'sql\_collabtive\_db';

$db\_user = 'root';

$db\_pass = 'seedubuntu';

$db = new mysqli($db\_host, $db\_user, $db\_pass, $db\_name);

$stmt = $db->prepare("SELECT ID,name,locale,lastlogin,gender FROM user WHERE (name = ? OR email = ?) AND pass = ?");

$stmt-> bind\_param("sss", $user, $user, sha1($pass));

$stmt-> execute();

$stmt-> bind\_result($bind\_id, $bind\_name, $bind\_locale, $bind\_lastlogin, $bind\_gender);

$chk = $stmt->fetch();

if($bind\_id != ""){

return true;

}

else{

return false;

}

}

### 