

# Project 5 SQL Injection Attack

Yang Guo [yguo3@clemson.edu](mailto:yguo3@clemson.edu)

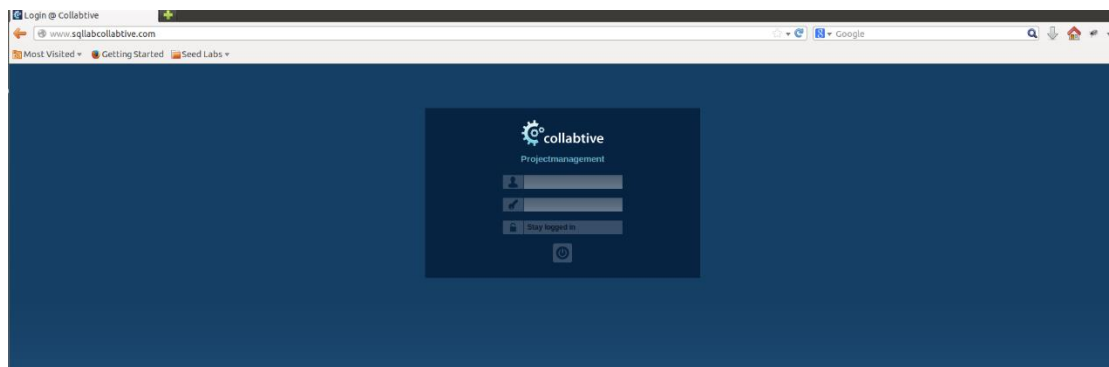
## Task 1 SQL Injection Attack on SELECT Statements

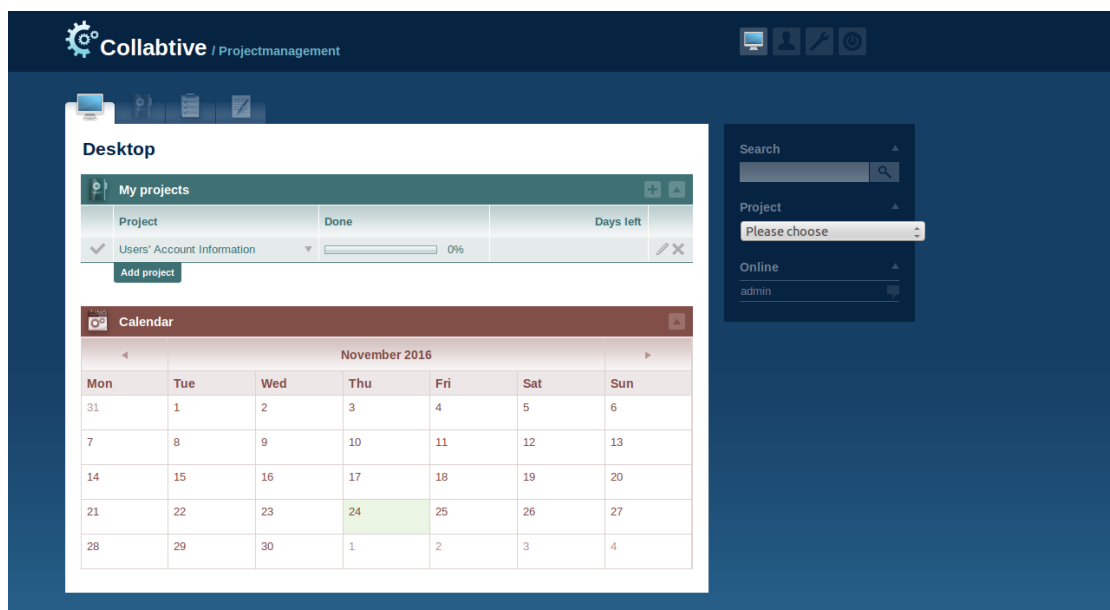
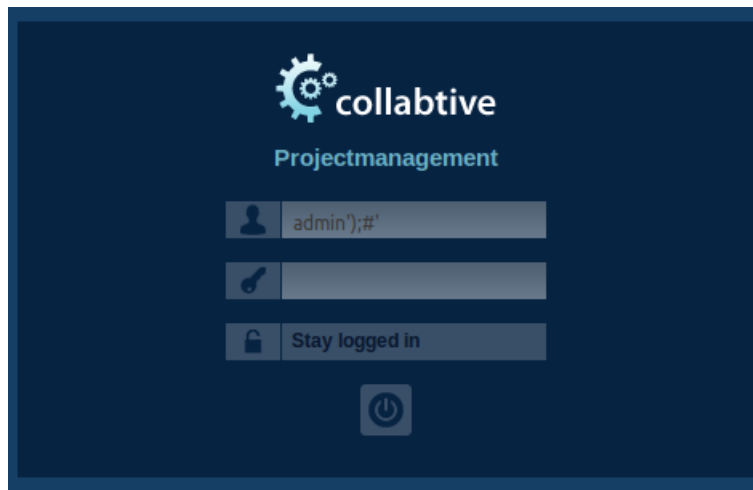
Before task1, we should first turn off the countermeasure. Then restart Apache server.

```
; Magic quotes are a preprocessing feature of PHP where PHP will attempt to  
; escape any character sequences in GET, POST, COOKIE and ENV data which might  
; otherwise corrupt data being placed in resources such as databases before  
; making that data available to you. Because of character encoding issues and  
; non-standard SQL implementations across many databases, it's not currently  
; possible for this feature to be 100% accurate. PHP's default behavior is to  
; enable the feature. We strongly recommend you use the escaping mechanisms  
; designed specifically for the database your using instead of relying on this  
; feature. Also note, this feature has been deprecated as of PHP 5.3.0 and is  
; scheduled for removal in PHP 6.  
; Default Value: On  
; Development Value: Off  
; Production Value: Off  
; http://php.net/magic-quotes-gpc  
magic_quotes_gpc = Off
```

*Task 1.1: Can you log into another person's account without knowing the correct password?*

Yes, we can.





From above we can see that we have logged in without knowing the correct password. This is because the query statement in the class.user.php file is:

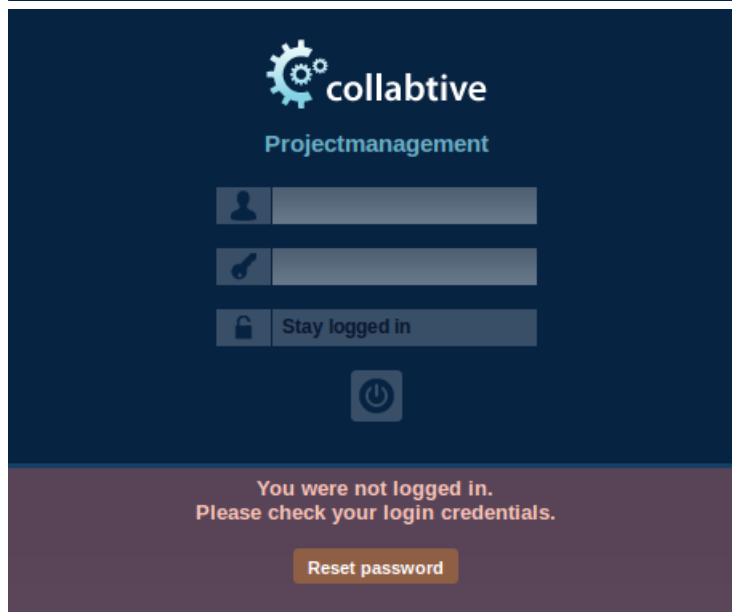
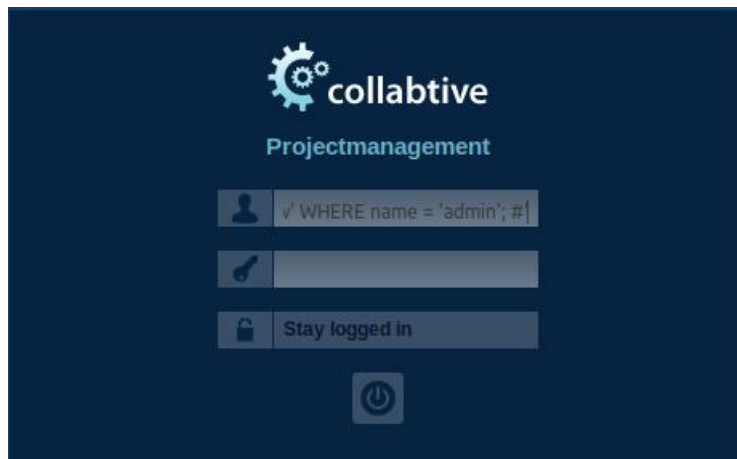
```
$sel1 = mysql_query("SELECT ID,name,locale,lastlogin,gender FROM user WHERE (name = '$user' OR email = '$user') AND pass = '$pass'");
$chk = mysql_fetch_array($sel1);
```

This statement is susceptible to injection attack.

*Task 1.2: Can you find a way to modify the database (still using the above SQL query)?*

No, we can't. I tried but failed to modify the database.

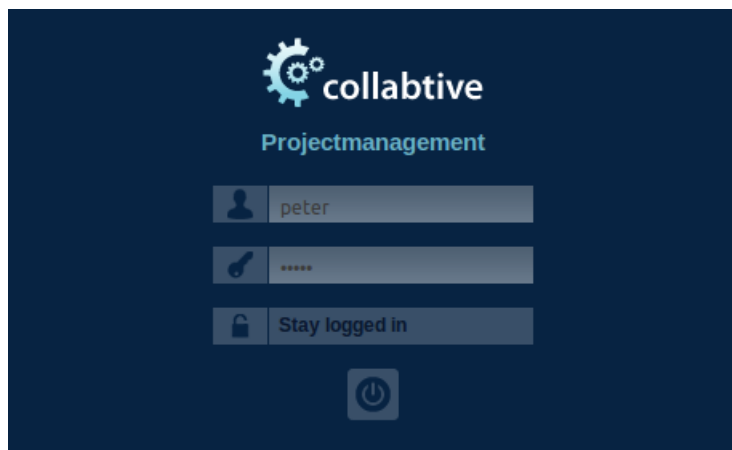
Write "admin'); UPDATE user SET pass='new' WHERE name='admin'; # '" in the user input field.



We can see that we can't execute two separate SQL statements. Because in php function `mysql_query()` it's not allowed to execute two separate SQL statements.

## Task 2: SQL Injection on UPDATE Statements

Log in as user peter.



```

*/
function edit($id, $sname, $realname, $email, $tel1, $tel2, $company, $zip, $gender, $url, $address1, $address2, $state, $country, $tags, $locale, $avatar = "", $rate = 0.0)
{
    $sname = mysql_real_escape_string($sname);
    $realname = mysql_real_escape_string($realname);

    //modified for SQL Lab
    // $company = mysql_real_escape_string($company);
    $email = mysql_real_escape_string($email);
    $tel1 = mysql_real_escape_string($tel1);
    $tel2 = mysql_real_escape_string($tel2);
    $zip = mysql_real_escape_string($zip);
    $gender = mysql_real_escape_string($gender);
    $url = mysql_real_escape_string($url);
    $address1 = mysql_real_escape_string($address1);
    $address2 = mysql_real_escape_string($address2);
    $state = mysql_real_escape_string($state);
    $country = mysql_real_escape_string($country);
    $tags = mysql_real_escape_string($tags);
    $locale = mysql_real_escape_string($locale);
    $avatar = mysql_real_escape_string($avatar);

    $rate = (float) $rate;
    $id = (int) $id;

    if ($avatar != "")
    {
        $upd = mysql_query("UPDATE user SET name='$sname',email='$email',tel1='$tel1',
tel2='$tel2',company='$company',zip='$zip',gender='$gender',url='$url',address='$address1',address2='$address2',state='$state',country='$country',tags='$tags',locale='$locale',avatar='$avatar',rate='$rate'
WHERE ID = $id");
    }
    else
    {
        $upd = mysql_query("UPDATE user SET name='$sname',email='$email', tel1='$tel1', tel2='$tel2',
company='$company',zip='$zip',gender='$gender',url='$url',address='$address1',address2='$address2',state='$state',country='$country',tags='$tags',locale='$locale',rate='$rate' WHERE ID = $id");
    }
    if ($upd)
    {
        $this->mylog->add($sname, 'user', 2, 0);
        return true;
    }
}

```

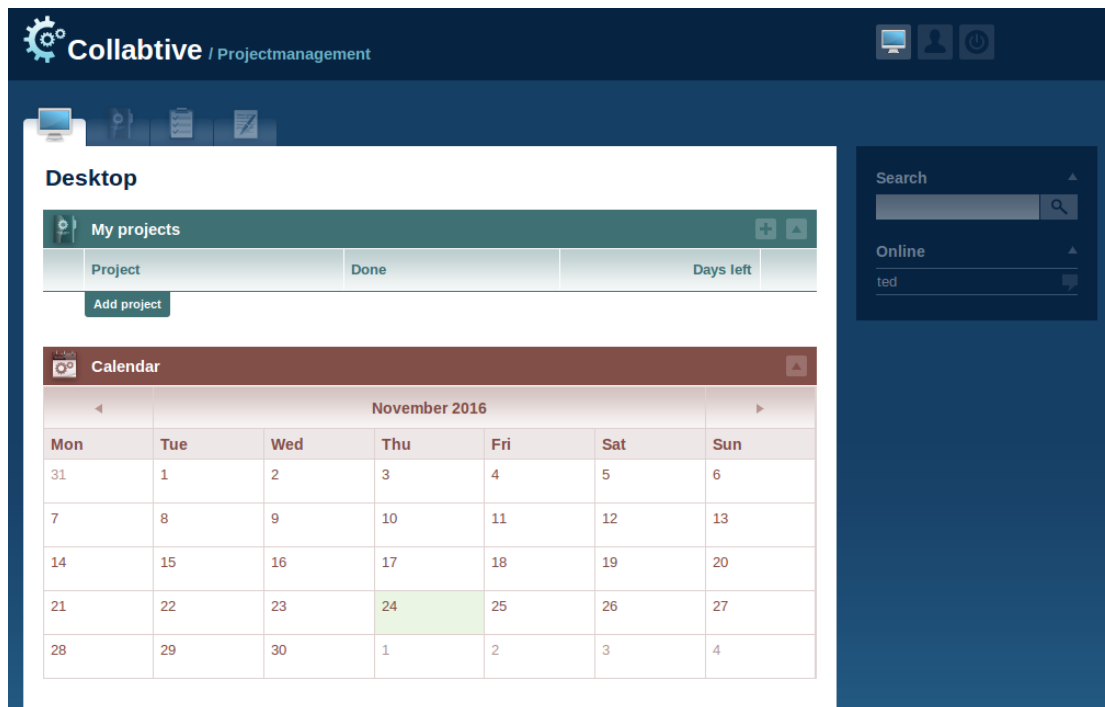
As we can see in class.user.php, the variable \$company can be used for injection because the escape statement has been modified by the author.

In the edit page, edit peter's profile like below:( we find that the id of ted is 4 and we can calculate the sha1() value of "newted" is 430821196724429165bdb03d7358141cef0b20de.

The screenshot shows the 'Edit user / peter' form. The 'Company' field is populated with the SQL injection payload: '724429165bdb03d7358141cef0b20de' WHERE ID = 4 #'. The form also includes a 'Send' button at the bottom right.

After click send button. We log out from peter's account and log in as ted using new password.

The screenshot shows the login page for 'collabtive Projectmanagement'. The login form has a username field containing 'ted' and a password field with masked characters '\*\*\*\*\*'. There is a 'Stay logged in' checkbox and a power button icon at the bottom.

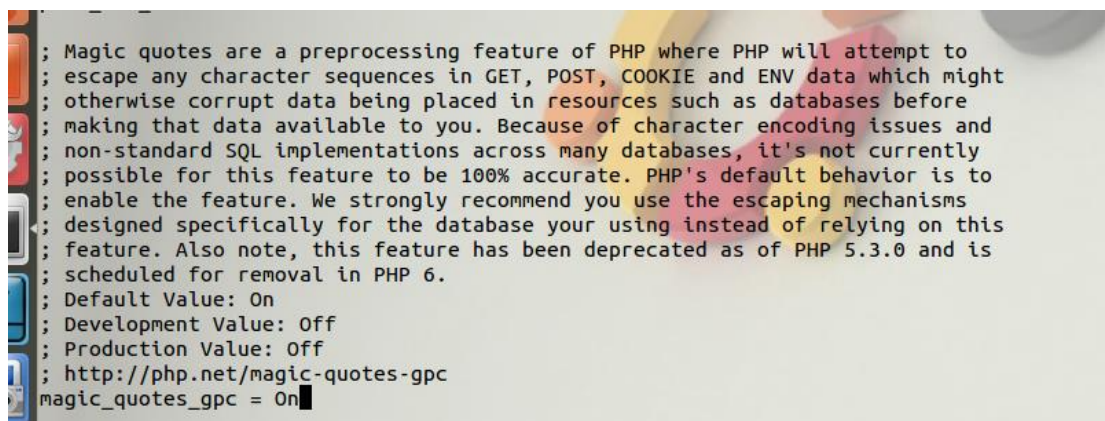


From above we can see that we can log in using ted's new password "newted". And it illustrates we successfully accomplish SQL injection on UPDATE statement.

## Task 3: Countermeasures

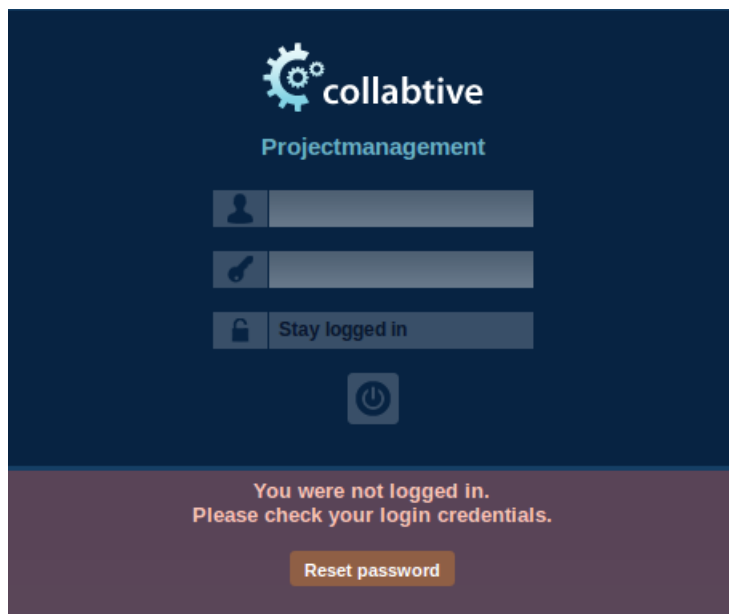
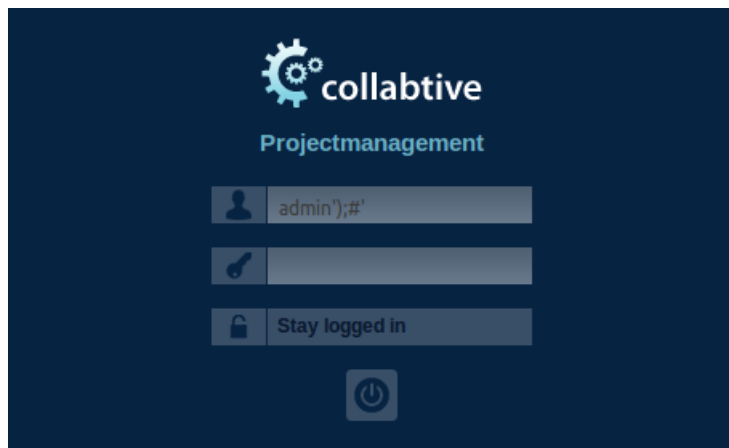
### Task 3.1: Escaping Special Characters using magic quotes gpc.

Turn on magic\_quotes\_gpc



Save the change and restart apache server.

Log in using the method of Task1.



We can see the result is different. We can't log in without the correct password any more. Because with `magic_quotes_gpc` turned on, it will automatically escape any ' or " or \ or other null characters.

### *Task 3.2: Escaping Special Characters using mysql real escape string.*

MySQL provides an escaping mechanism, called `mysql_real_escape_string()`, which prepends backslashes to a few special characters, including `\x00`, `\n`, `\r`, `\`, `'`, `"` and `\x1A`.

We can edit the `class.user.php` using this method.

```
function login($user, $pass)
{
    if (!$user)
    {
        return false;
    }
}

//modified for SQL Lab
$user = mysql_real_escape_string($user);
$pass = mysql_real_escape_string($pass);
$pass = sha1($pass);

$select = mysql_query("SELECT ID,name,locale,lastlogin,gender FROM user WHERE (name = '$user' OR email = '$user') AND pass = '$pass'");
$chk = mysql_fetch_array($select);
```

```

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

    //modified for SQL Lab
    $company = mysql_real_escape_string($company);
    $email = mysql_real_escape_string($email);
    $tel1 = mysql_real_escape_string($tel1);
    $tel2 = mysql_real_escape_string($tel2);
    $zip = mysql_real_escape_string($zip);
    $gender = mysql_real_escape_string($gender);
    $url = mysql_real_escape_string($url);
    $address1 = mysql_real_escape_string($address1);
    $address2 = mysql_real_escape_string($address2);
    $state = mysql_real_escape_string($state);
    $country = mysql_real_escape_string($country);
    $tags = mysql_real_escape_string($tags);
    $locale = mysql_real_escape_string($locale);
    $avatar = mysql_real_escape_string($avatar);

```

### Task 3.3: Prepare Statement.

We can edit the class.user.php using this method.

```

function login($user, $pass)
{
    if (!$user)
    {
        return false;
    }

    //modified for SQL Lab
    *
    $user = mysql_real_escape_string($user);
    $pass = mysql_real_escape_string($pass);
    $pass = sha1($pass);

    $sel1 = mysql_query("SELECT ID,name,locale,lastlogin,gender FROM user WHERE (name = '$user' OR email = '$user') AND pass = '$pass'");
    $chk = mysql_fetch_array($sel1);

    /
    $stmt = $conn->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();

```

In the edit() function, we can edit it as below:

```

    $country = mysql_real_escape_string($country);
    $tags = mysql_real_escape_string($tags);
    $locale = mysql_real_escape_string($locale);
    $avatar = mysql_real_escape_string($avatar);
*/
    $rate = (float) $rate;
    $id = (int) $id;

    if ($avatar != "")
    {
        $stmt = $conn->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("ssssssssssss", $name, $email, $tel1, $tel2,
            $company, $zip, $gender, $url, $address1,
            $address2, $state, $country, $tags, $locale,
            $avatar, $rate, $id);
        $supd = $stmt->execute();
    }
    else
    {
        $stmt = $conn->prepare("UPDATE user SET name=?, email=?, tel1=?,
            tel2=?, company=?, zip=?, gender=?, url=?,
            adress=?, adress2=?, state=?, country=?,
            tags=?, locale=?, rate=? WHERE ID = ?");
        $stmt->bind_param("ssssssssssssdi", $name, $email, $tel1, $tel2,
            $company, $zip, $gender, $url, $address1,
            $address2, $state, $country, $tags, $locale,
            $rate, $id);
        $supd = $stmt->execute();
    }
    if ($supd)
    {
        $this->mylog->add($name, 'user', 2, 0);
        return true;
    }
    else
    {
        return false;
    }
}

```