

**CLASS 8****SQL Injection Lab****吴瑞欣-E41614059****1、 SQL 危害:**

- 1、非法读取、篡改、添加、删除数据库中的数据。
- 2、盗取用户的各类敏感信息，获取利益。
- 3、通过修改数据库来修改网页上的内容。
- 4、私自添加或删除账号。
- 5、注入木马等等。

**2、 Environment Configuration**

```
sudo service apache2 start
```

```
/var/www/SQL/SQLLabMysqlPhpbb/
```

```
Go to /etc/php5/apache2/php.ini.
```

```
Find the line: magic_quotes_gpc = On.
```

```
Change it to this: magic_quotes_gpc = Off.
```

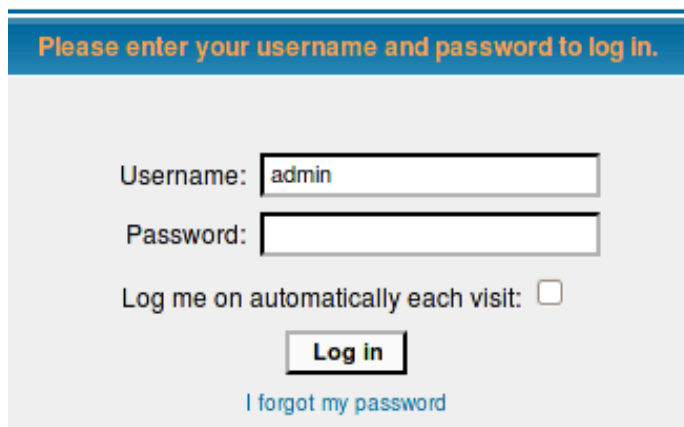
```
Restart the apache server by running "sudo service apache2  
restart"
```

**3、 Task 1(30 Points):SQL Injection Attack on SELECT  
Statements****源代码为:**

```
SELECT user_id, username, user_password, user_active,  
user_level,  
  
user_login_tries, user_last_login_try  
  
FROM USERS_TABLE  
  
WHERE username = ' $username' AND user_password  
= ' md5($password)' ;  
  
if (found one record)  
  
then {allow the user to login}
```

### 改为:

```
$sql_checkpasswd = "SELECT user_id, username, user_password,  
user_active, user_level, user_login_tries, user_last_login_try  
  
FROM " . USERS_TABLE . "WHERE username = '" . $username .  
"'#'" . " AND user_password = '" . md5($password) . "'";
```




Please enter your username and password to log in.

Username:

Password:

Log me on automatically each visit: ☐

[I forgot my password](#)




## phpBB on MySQL4

This is the phpBB2 forum with SQL Injection vulnerability

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#)  
[Profile](#) [You have no new messages](#) [Log out \[ admin \]](#)

You last visited on 12 Nov 2018 11:40 am  
The time now is 12 Nov 2018 11:41 am  
[phpBB on MySQL4 Forum Index](#)

[View posts since last visit](#)  
[View your posts](#)  
[View unanswered posts](#)

Forum	Topics	Posts	Last Post
<b>Test category 1</b>			
 <b>Test Forum 1</b> This is just a test forum.	3	3	27 Mar 2009 08:37 pm <a href="#">admin</a> ➡

[Mark all forums read](#) All times are GMT

### Who is Online

Our users have posted a total of 3 articles  
We have 5 registered users  
The newest registered user is [ted](#)

In total there is 1 user online :: 1 Registered, 0 Hidden and 0 Guests [ [Administrator](#) ] [ [Moderator](#) ]  
Most users ever online was 2 on 17 Aug 2010 01:53 am  
Registered Users: [admin](#)

This data is based on users active over the past five minutes

#### 4、Task 2 (30 Points): SQL Injection on UPDATE Statements

该系统中存在 update 造成的注入点：

phpBB on MySQL4 Forum Index

### Viewing profile :: ted

Avatar	All about ted
	Joined: 14 Mar 2009
	Total posts: 0 [0.00% of total / 0.00 posts per day] <a href="#">Find all posts by ted</a>
	Location: 11
	Website:
	Occupation: 11
	Interests:

### Contact ted

E-mail address: [email](#)  
Private Message: [pm](#)  
MSN Messenger:  
Yahoo Messenger:  
AIM Address:  
ICQ Number: [ICQ](#)

Jump to:

#### 5、Task 3 (40 Points): Countermeasures

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

gpc

通过开启 magic quotes gpc = On 防止 SQL 注入

`get_magic_quotes_gpc()`；值为 1，表示开启。那么 php 会自动为 POST、GET、COOKIE 传过来的参数值自动增加转义字符“\”，来确保这些数据的安全性。尤其是防止 SQL 注入。

`get_magic_quotes_gpc()`；值为 0，表示关闭。php 解析器不会自动为 POST、GET、COOKIE 传过来的参数值加转义字符“\”，那么这时就用 `addslashes` 函数来转义参数。

### Task3.2: Escaping Special Characters using addslashes()

MySQL 提供一个函数 `mysql_real_escape_string()`，这个函数可以用来过滤一些特殊字符；如 `\x00`, `\n`, `\r`, `\`, `'`, `"` and `\x1a`;

[illegible]

```
        email = '$user') AND pass = '$pass');

$chk = mysql_fetch_array($sell);

if ($chk["ID"] != "")

    {

        // New user session object and cookie creation
code

        // removed for brevity

        return true;

    }

else

    {

        return false;

    }

}
```

### 3、防御策略 3—数据与 sql 语句的分离

通过 SQL 逻辑分离来告诉数据库到底是哪部分是数据部分，哪一部分是 SQL 语句部分；

```
function login($user, $pass)

{

    if (!$user)

    {

        return false;
```

```
    }

    // using prepared statements

    // note that $conn is instantiated in the datenbank
    class found in

    // ./class.datenbank.php. this may need to be passed in,
    but we

    // will assume we have access to it for the sake of
    brevity

    $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();

    if ($bind_ID != "")
    {

        // New user session object and cookie creation
code

        // removed for brevity

        return true;
    }
}
```

```
    }  
    else  
    {  
        return false;  
    }  
}
```