New issue

Jump to bottom

SQL Injection in ForgotPassUserName #192

Closed **H4niz** opened this issue on Sep 1, 2021 · 3 comments

H4niz commented on Sep 1, 2021 • edited

Hi **@openSISAdmin**, **@ArnabOs4ed** , I found a sql injection vulnerability in `ForgotPassUserName` function. I can inject special character in URL to escape SQL query in backend because of lacking of sanitize user input.
PoC:
`http://172.16.0.12:2222/ForgotPassUserName.php?used_for=username&u=admin%27%20or%20%271%27=%271`

Bug:

```
        if($used_for=='username')
        {
            $username = $_GET['u']; // <--- Lacking of sanitize input here!!!
            $usr_type = $_GET['user_type'];
            $found= false;
            if($usr_type=='student')
            {
                $check_uname=  DBGet(DBQuery('SELECT * FROM login_authentication WHERE USERNAME = \''.$username.'\'  AND PROFILE_ID IN (SELECT ID FROM user_profiles WHERE 
PROFILE=\'student\')'));
            }
            elseif($usr_type=='staff')
            {
                $check_uname=  DBGet(DBQuery('SELECT * FROM login_authentication WHERE USERNAME = \''.$username.'\'  AND PROFILE_ID IN (SELECT ID FROM user_profiles WHERE ID NOT IN 
(0,3,4))'));
            }
            else
            {
                $check_uname=  DBGet(DBQuery('SELECT * FROM login_authentication WHERE USERNAME = \''.$username.'\'  AND PROFILE_ID IN (SELECT ID FROM user_profiles WHERE 
PROFILE=\'parent\')'));
            }
            if($check_uname[1]['USERNAME']!='')
            {
                echo '1';
            }
            else
                echo '0';
        }
```

In line 278, the code does not sanitize param `u` , in order that, I can escape the SQL query easily.

Solution:

Use function `sqlSecurityFilter()` before assign `$_GET['u'];` to `username` param.
The code should look like:

```
$username = sqlSecurityFilter($_GET['u']);
```

openSISAdmin commented on Sep 3, 2021 Member

Fixed

👍 1

openSISAdmin closed this as completed on Sep 3, 2021

H4niz commented on Sep 4, 2021 • edited Author

Dear openSIS Administrator,
After auditing your source-code, I found many vulnerabilities, most of them
are SQL Injection. The reason causes many bugs because you missed to filter
user input parameters before assigning to php parameters. So, to secure your
solution, please recheck and fix all mistake in your code, please!

If you need a support to secure your code, feel free to contact me! I
always willing to help you! And obviously, It's free!
...

openSISAdmin commented on Sep 4, 2021 Member

@H4niz

Thanks for your note. We will sincerely appreciate it if you can chip in and fix the vulnerabilities that you have found. Please make sure you do not regress any system functionalities as it is largely undocumented.

Please do PR for the fixes.

👍 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants