**DedeCMS-V5.7-UTF8-SP版前台鸡助getshell漏洞（二）**

0x00 介绍

**织梦**内容管理系统([DedeCms](https://baike.baidu.com/item/DedeCms)) 以简单、实用、开源而闻名，是国内最知名的[PHP](https://baike.baidu.com/item/PHP/9337)开源网站管理系统，也是使用用户最多的PHP类[CMS系统](https://baike.baidu.com/item/CMS%E7%B3%BB%E7%BB%9F)，在经历多年的发展，目前的版本无论在功能，还是在易用性方面，都有了长足的发展和进步，DedeCms免费版的主要目标用户锁定在[个人站长](https://baike.baidu.com/item/%E4%B8%AA%E4%BA%BA%E7%AB%99%E9%95%BF)，功能更专注于[个人网站](https://baike.baidu.com/item/%E4%B8%AA%E4%BA%BA%E7%BD%91%E7%AB%99)或中小型门户的构建，当然也不乏有企业用户和学校等在使用本系统。

织梦5.7会员中心，由于为了安全性问题，限制了注册会员在会员中心发布信息的时候上传图片，但是管理员登录会员中心发布信息的时候上传图片却不受影响。那该如何解决呢？下面我们来说明一下具体的解决方案。

首先，具体的问题为，注册会员点击图片上传，预览选择好本地图后点击上传到服务器上，会出现如下所示结果：

图片上传失败，并无像正常上传图片后提交按钮跳转到相应的图像属性界面上，仅在当前窗口上弹出一个滚动条，上面的滚动条里面提示为“提示：需输入后台管理目录才能登陆”，但因滚动条高度受限制了所以我们看不到提示。想要查看具体的提升信息的话，请点击向下的滚动条一直往下，即可出现文字提示。如图：

现在知道具体原因后就容易解决问题了，直接搜索织梦网站程序文件夹下的全部包含“提示：需输入后台管理目录才能登陆“的文件，找到includedialogconfig.php文件。其中有段代码

//检验用户登录状态  $cuserLogin = new userLogin();    if($cuserLogin->getUserID() <=0 )  {  if(emptyempty($adminDirHand))  {  ShowMsg( 提示：需输入后台管理目录才能登录请输入后台管理目录名： width:120px;  /> ,  javascript:; );  exit();  }  $gurl =  ../../{$adminDirHand}/login.php?gotopage= .urlencode($dedeNowurl);  echo  location= $gurl ; ;  exit();  }

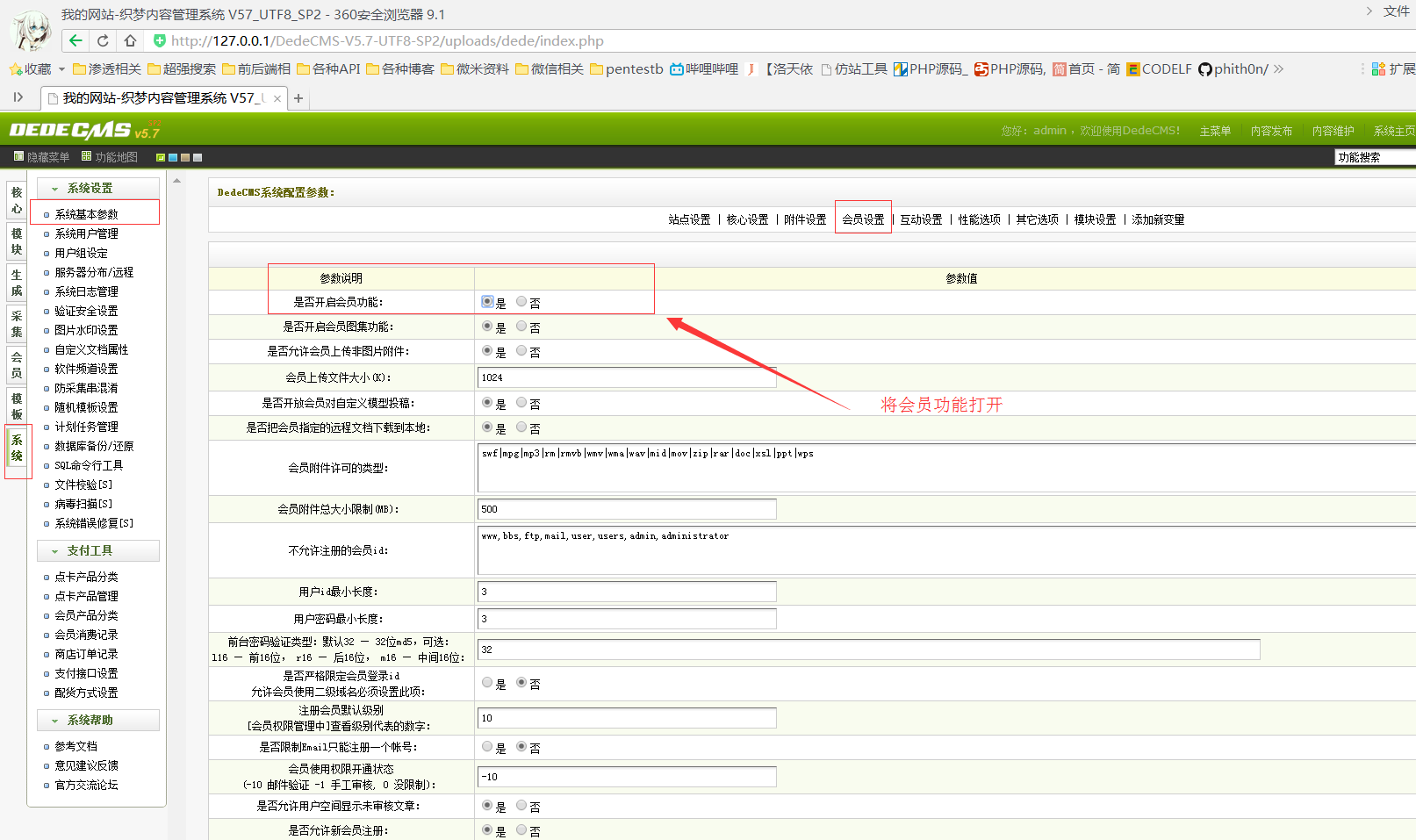
所以说dedecms5.7要上传图片的话，必须按照上面做，我们这里是按照这个规则，认为管理员开启了会员上传图片的权限，低于5.7的只要开启会员中心即可日传

扎心哦~~~~

0x01 准备工作

1,安装最新版cms

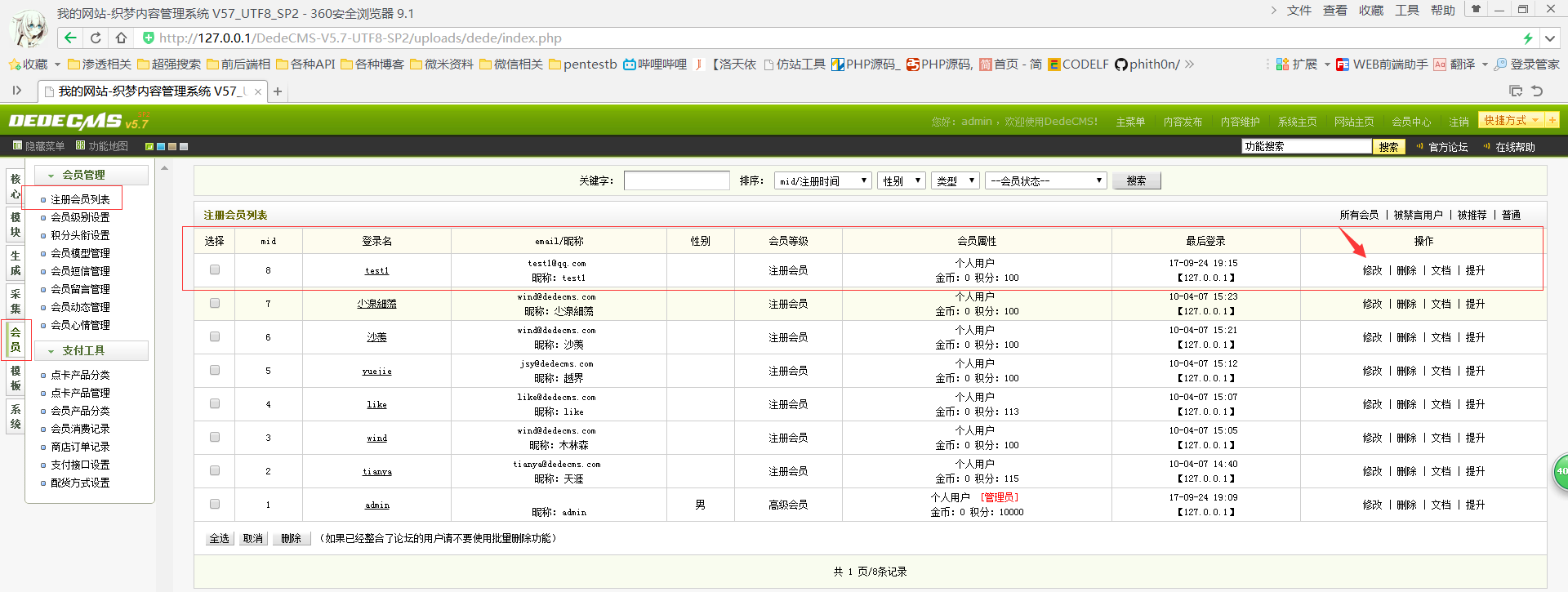
地址：<http://updatenew.dedecms.com/base-v57/package/DedeCMS-V5.7-UTF8-SP2.tar.gz>

2, 打开dede会员功能

3,注册一个新用户



4,审核一下此用户



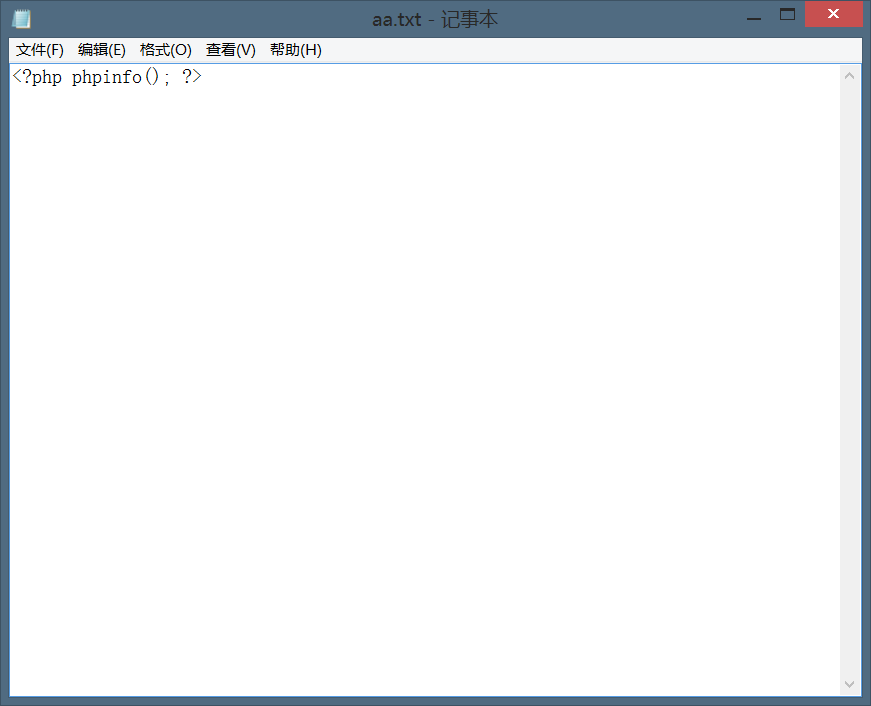


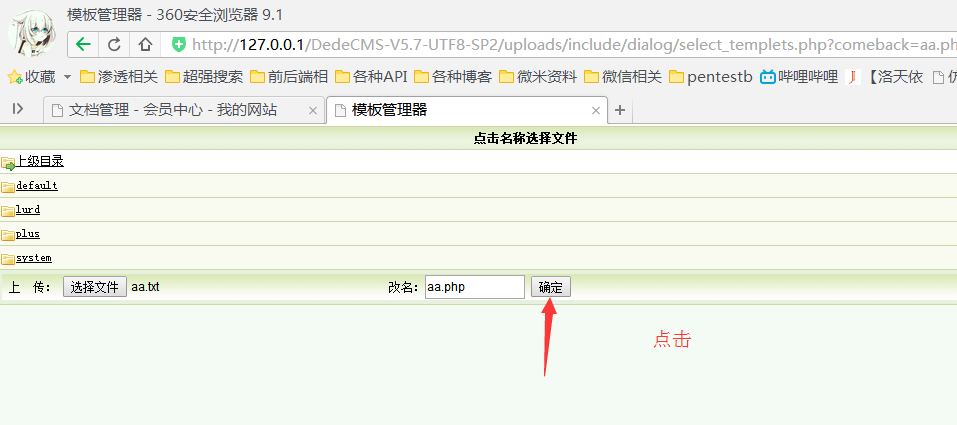
嗯~~~~这样一个基本的站点就完成了。我们也可以进行测试了

0x01 利用过程

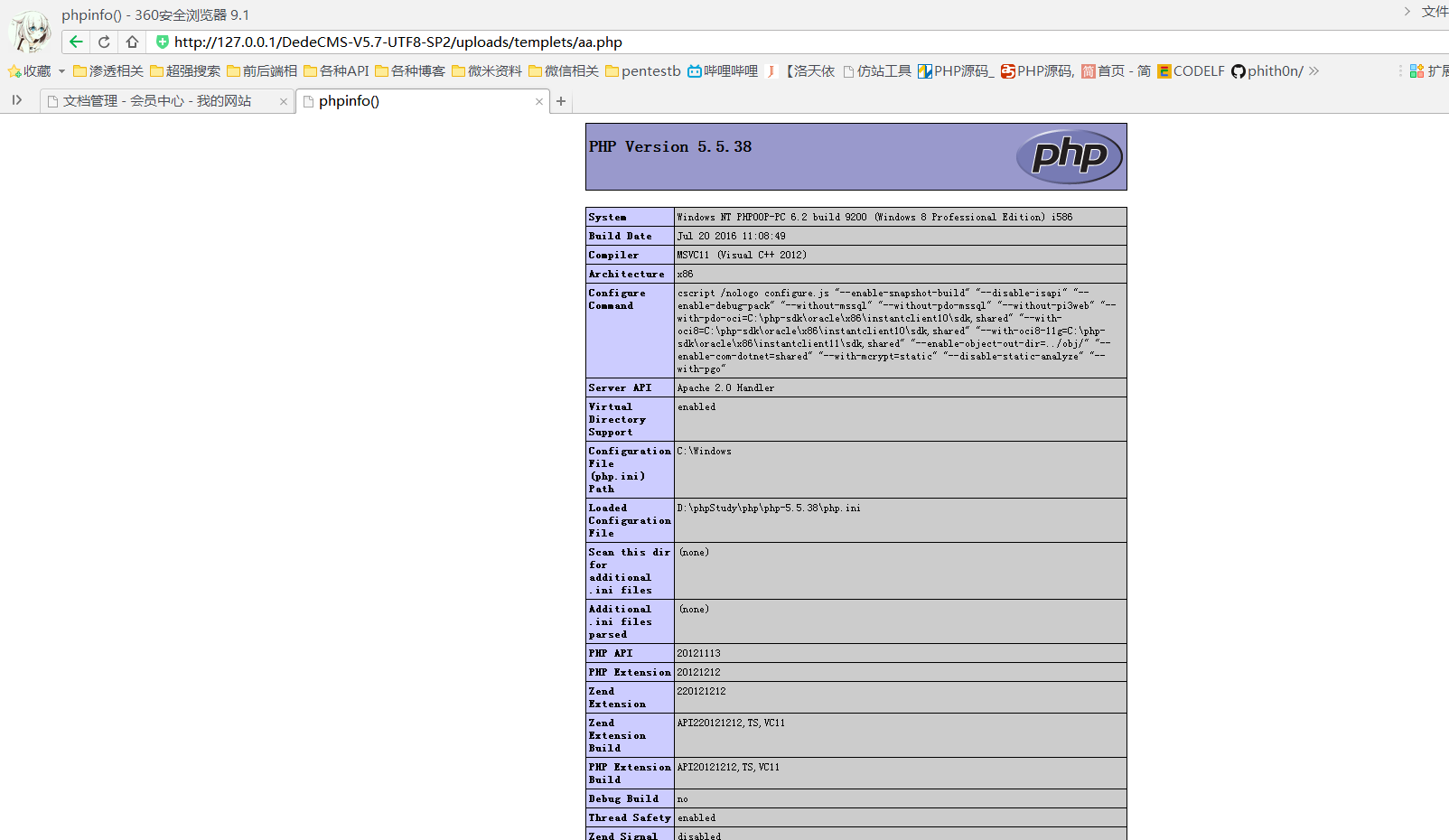
地址：http://127.0.0.1/DedeCMS-V5.7-UTF8-SP2/uploads/include/dialog/select\_templets.php

写一个txt txt中写恶意代码





漏洞生成地址：<http://127.0.0.1/DedeCMS-V5.7-UTF8-SP2/uploads/templets/aa.php>



0x02 漏洞原理

