**DedeCMS-V5.7-UTF8-SP版前台鸡助getshell漏洞（一）**

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();  }

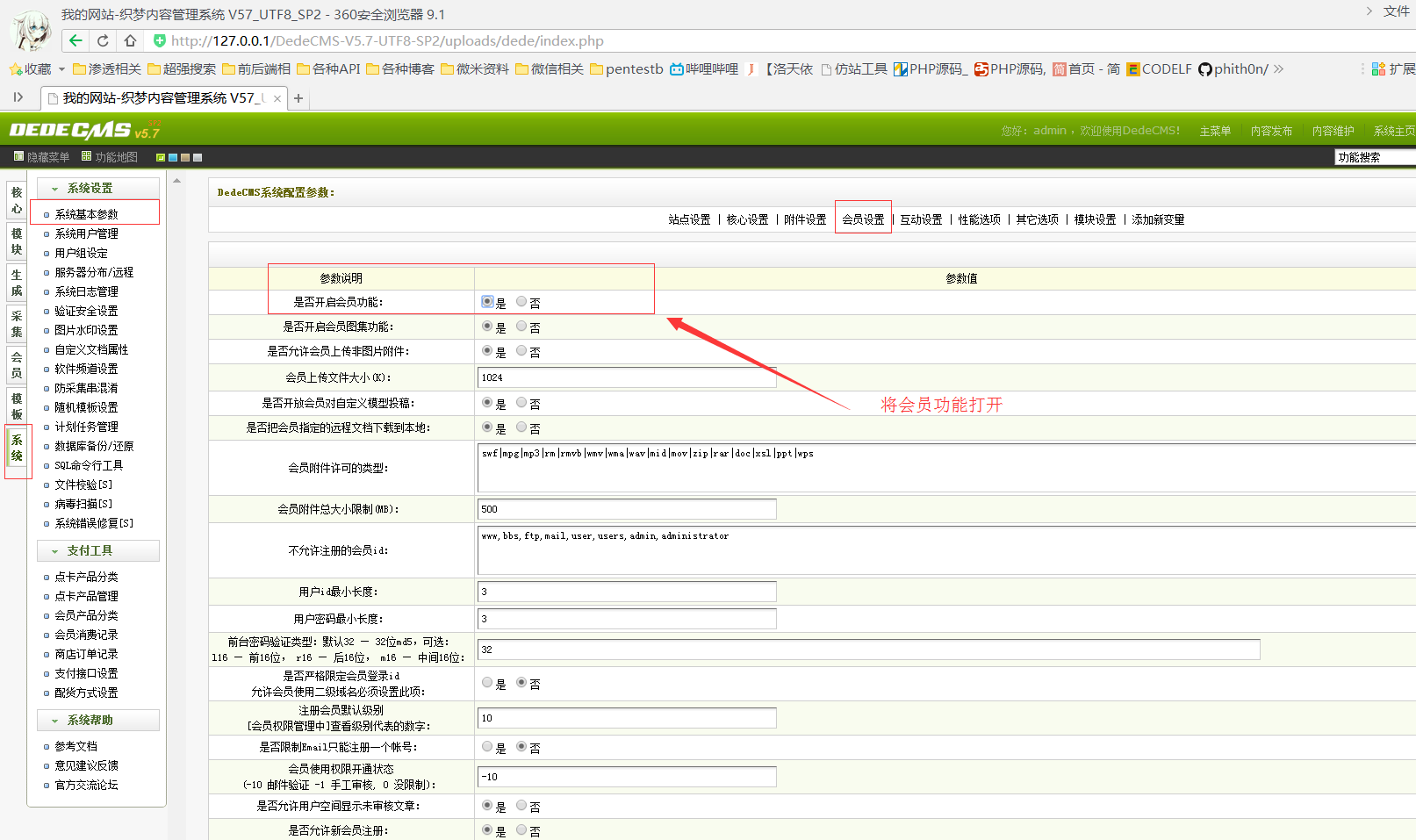
所以说dedecms5.7要上传图片的话，必须按照上面做，我们这里是按照这个规则，认为管理员开启了会员上传图片的权限，低于5.7的只要开启会员中心即可日传

扎心哦~~~~

0x01 准备工作

1,安装最新版cms

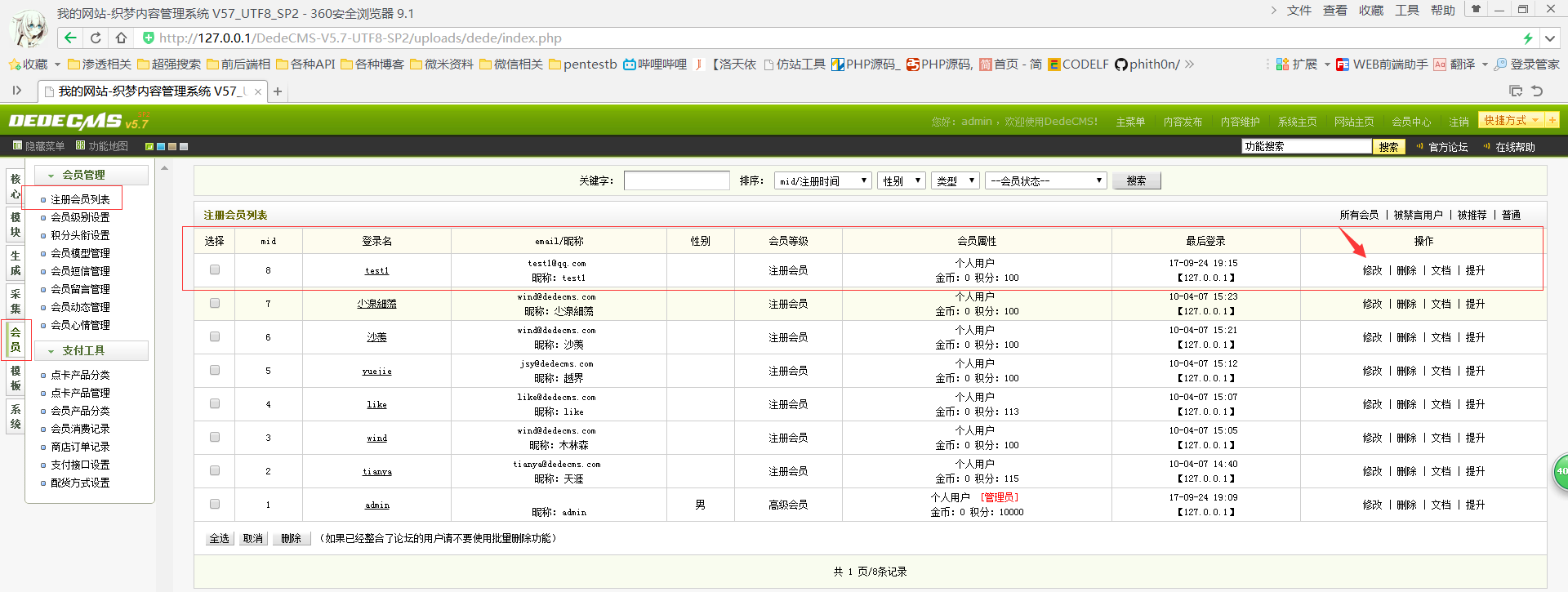
地址：<http://updatenew.dedecms.com/base-v57/package/DedeCMS-V5.7-UTF8-SP2.tar.gz>

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

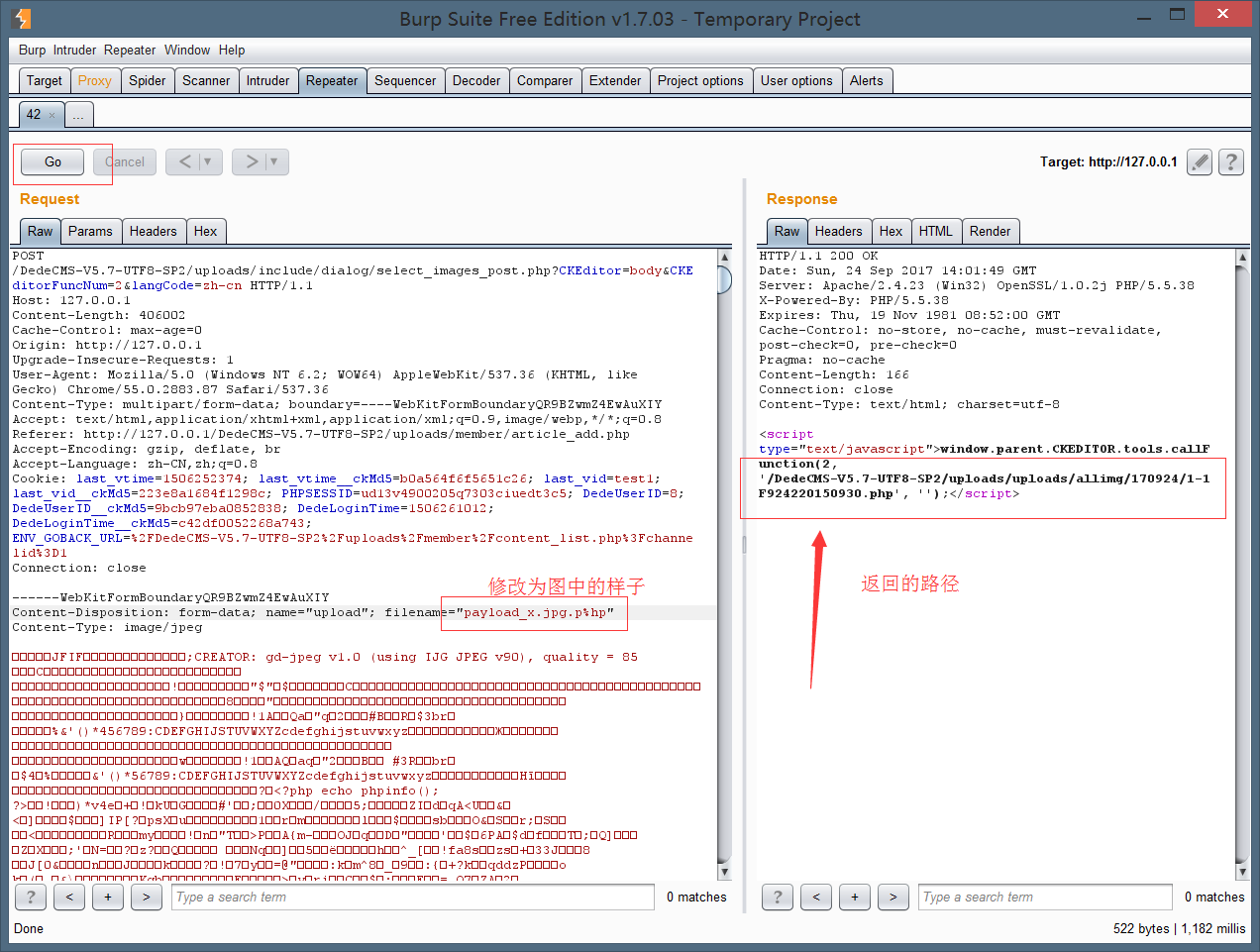
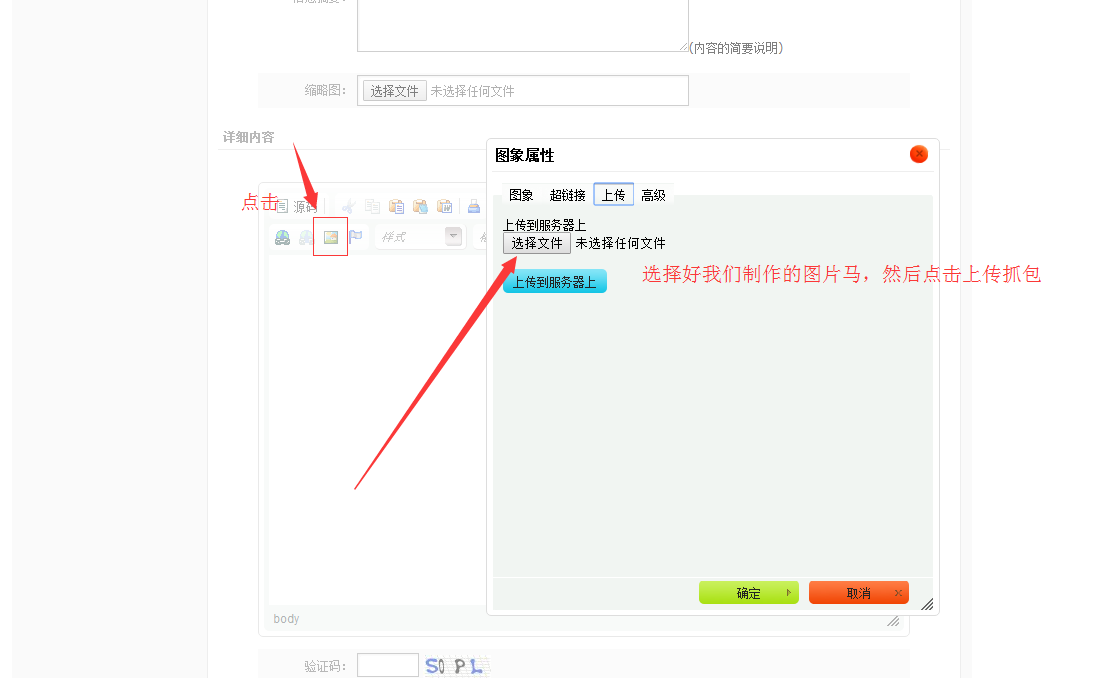
0x01 利用过程

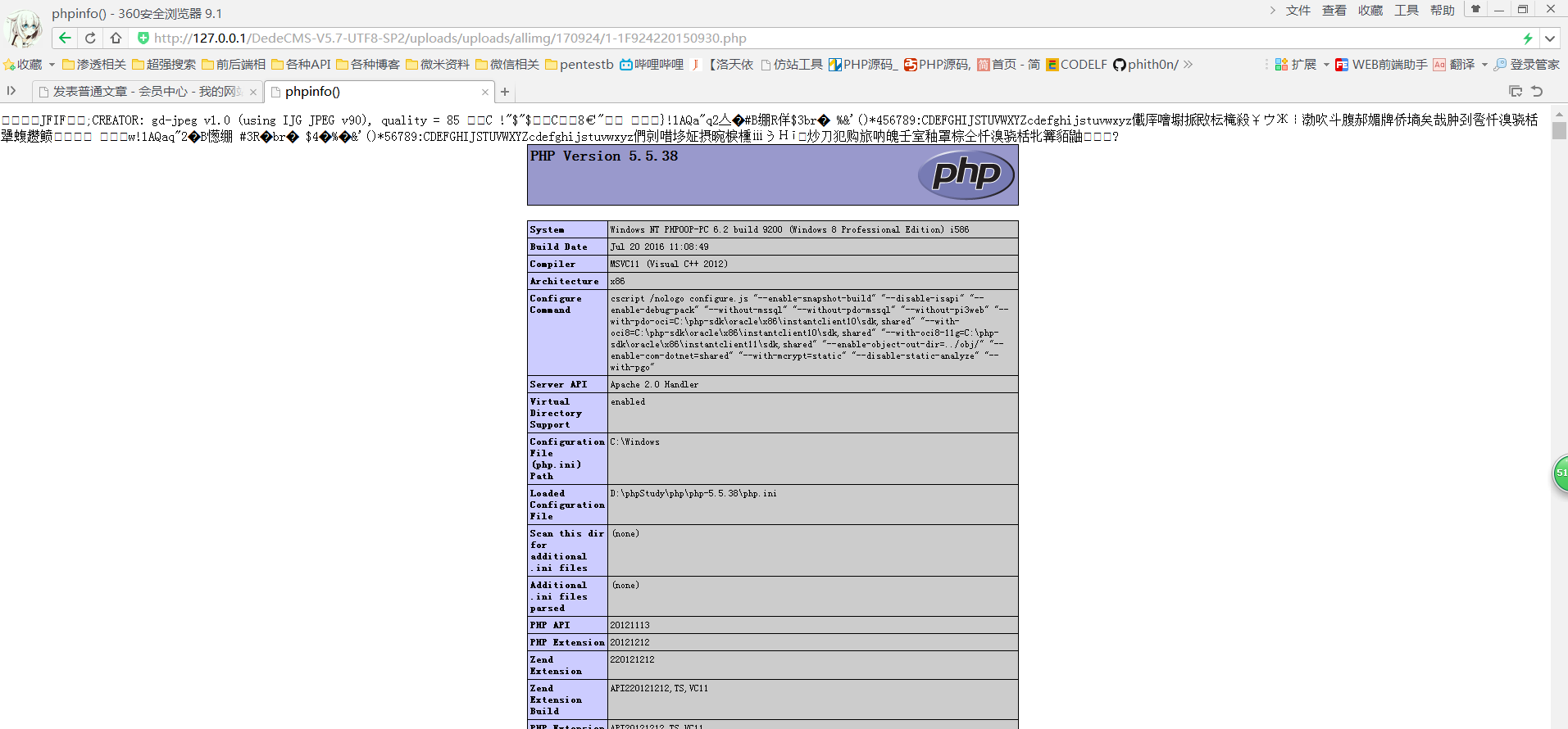
1,先添加一个图片马



上图这个是经过处理的图片马，需要处理的图片马是因为（绕过文件后缀名检测以后，php-GD对图片的渲染和处理会导致webshell代码错位失效，所以需要特殊的图片马进行绕过,图片马的制作）

2, 





0x02 图片马制作

首先感谢先知安全的文章，没有先知的文章还真的绕不过去。。。

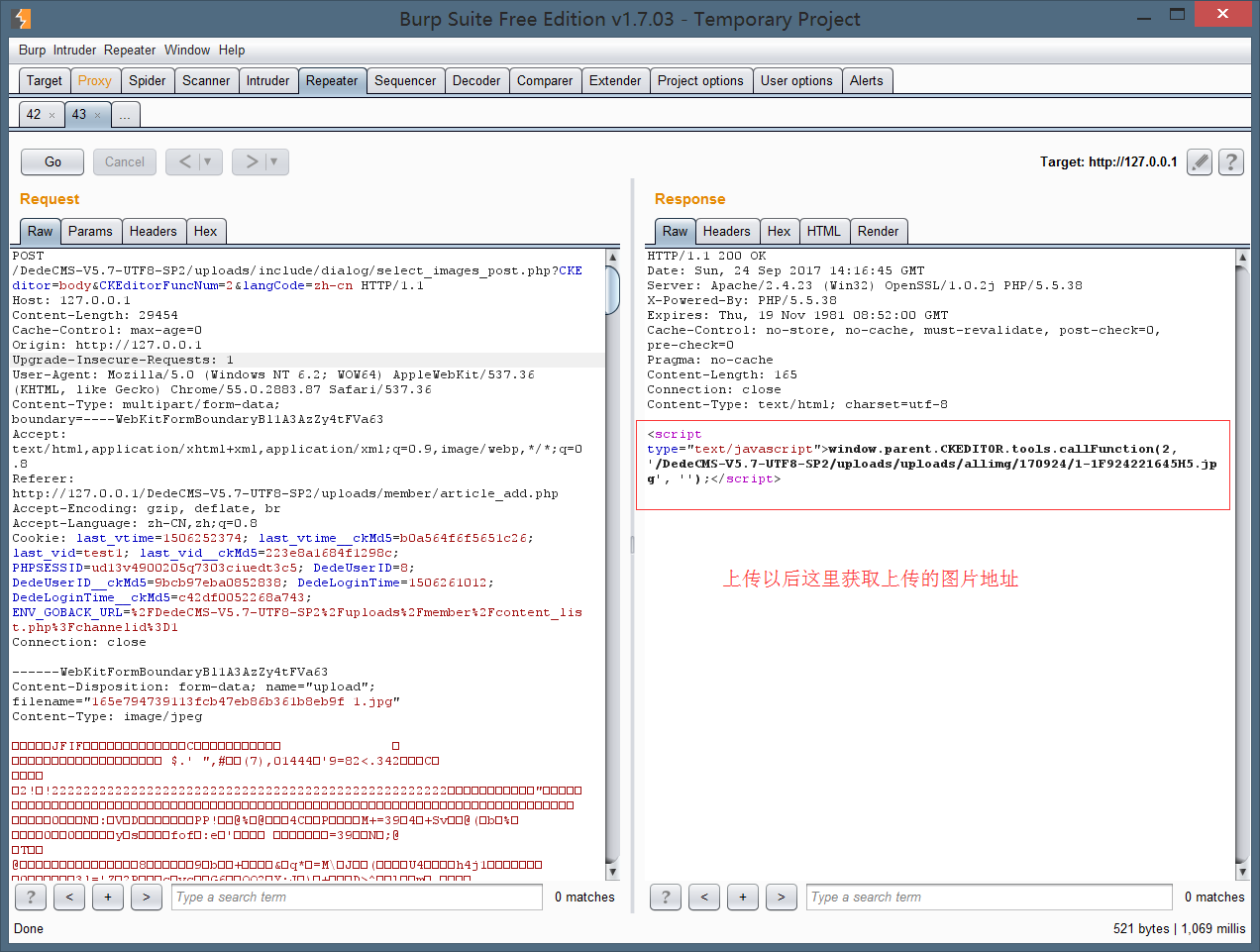
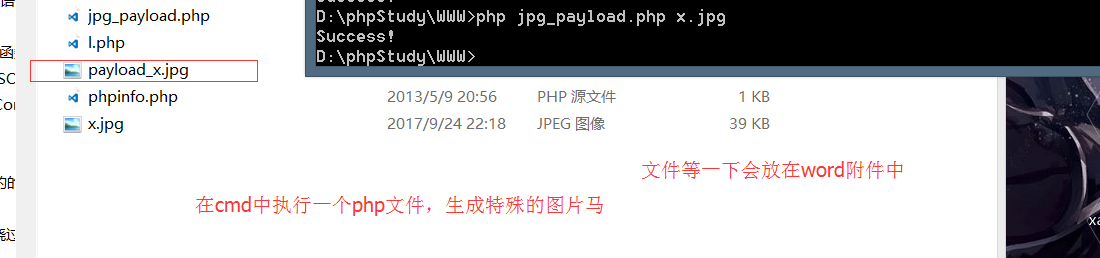
这里确实不要多说什么，因为绕过文件后缀名检测以后，php-GD对图片的渲染和处理会导致webshell代码错位失效，所以我们需要进行绕过。

**绕过php-GD对图片的渲染和处理导致webshell代码错位失效(此处参考索马里海盗方法)**

图片会经过php-GD处理，会导致webshell语句错位失效，如何在处理后仍然保留shell语句呢？

在正常图片中插入shell并无视GD图像库的处理，常规方法有两种  
1.对比两张经过php-gd库转换过的gif图片，如果其中存在相同之处，这就证明这部分图片数据不会经过转换。然后我可以注入代码到这部分图片文件中，最终实现远程代码执行  
2.利用php-gd算法上的问题进行绕过

这里我们选择第二种，使用脚本进行处理图片并绕过  
1、上传一张jpg图片，然后把网站处理完的图片再下回来 比如x.jpg  
2、执行图片处理脚本脚本进行处理   php jpg\_payload.php x.jpg  
3、如果没出错的话，新生成的文件再次经过gd库处理后，仍然能保留webshell代码语句

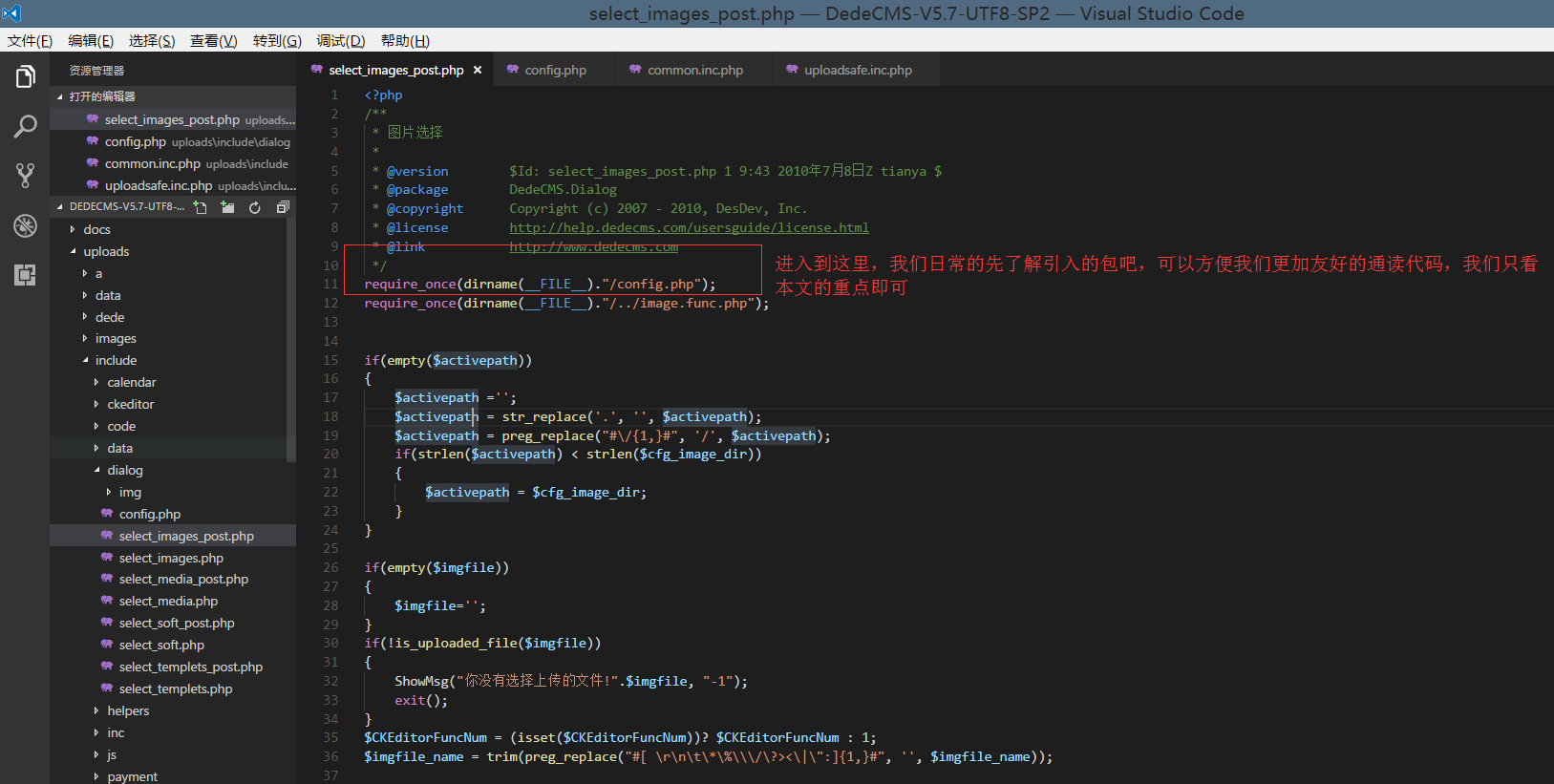
提示：  
1、图片找的稍微大一点 成功率更高  
2、shell语句越短成功率越高  
3、一张图片不行就换一张 不要死磕  
注：上面的字全部是抄的，先说明一下不然给人按在地上骂就不好了  
  
制作过程：  
  
  
 

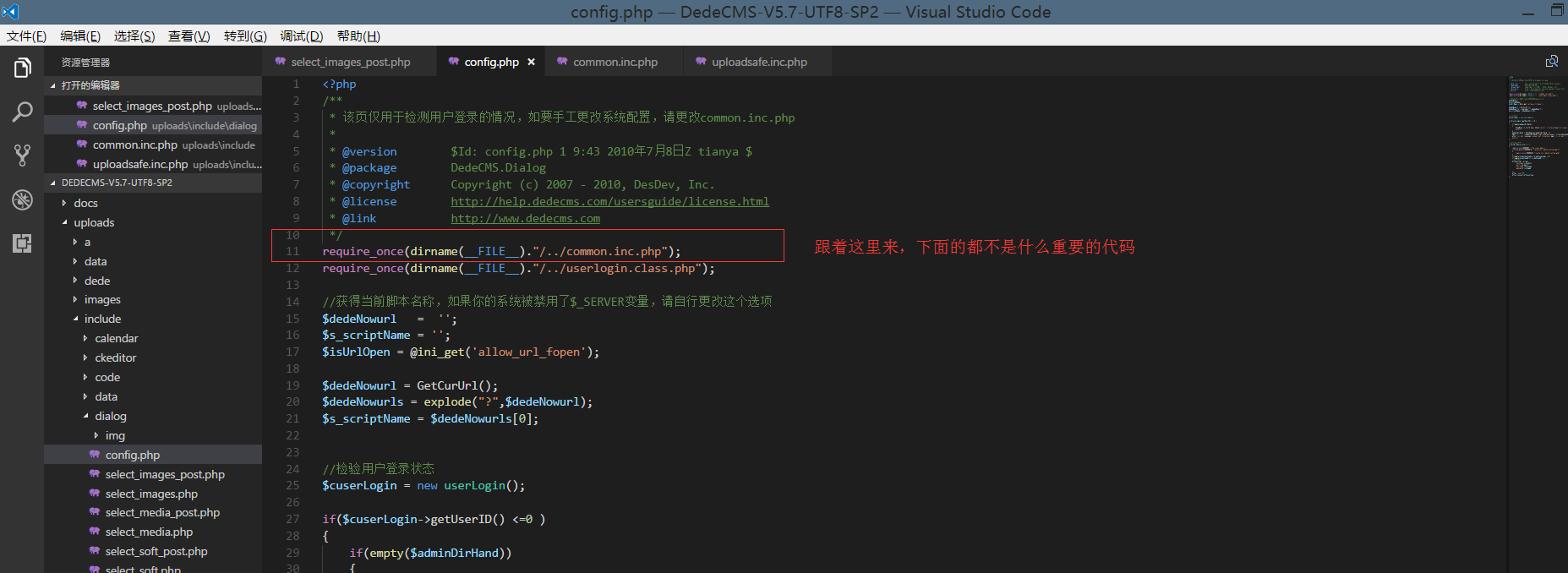


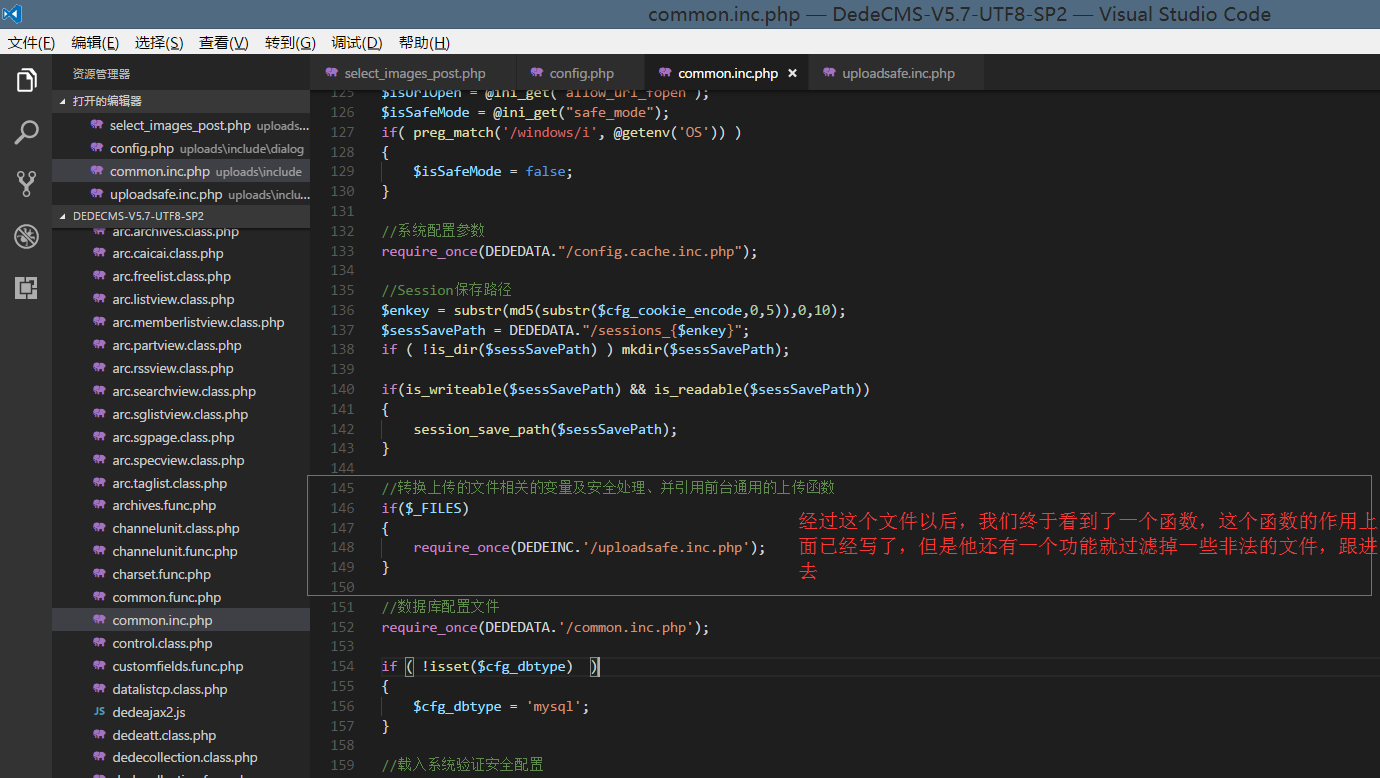
0x03 漏洞原理

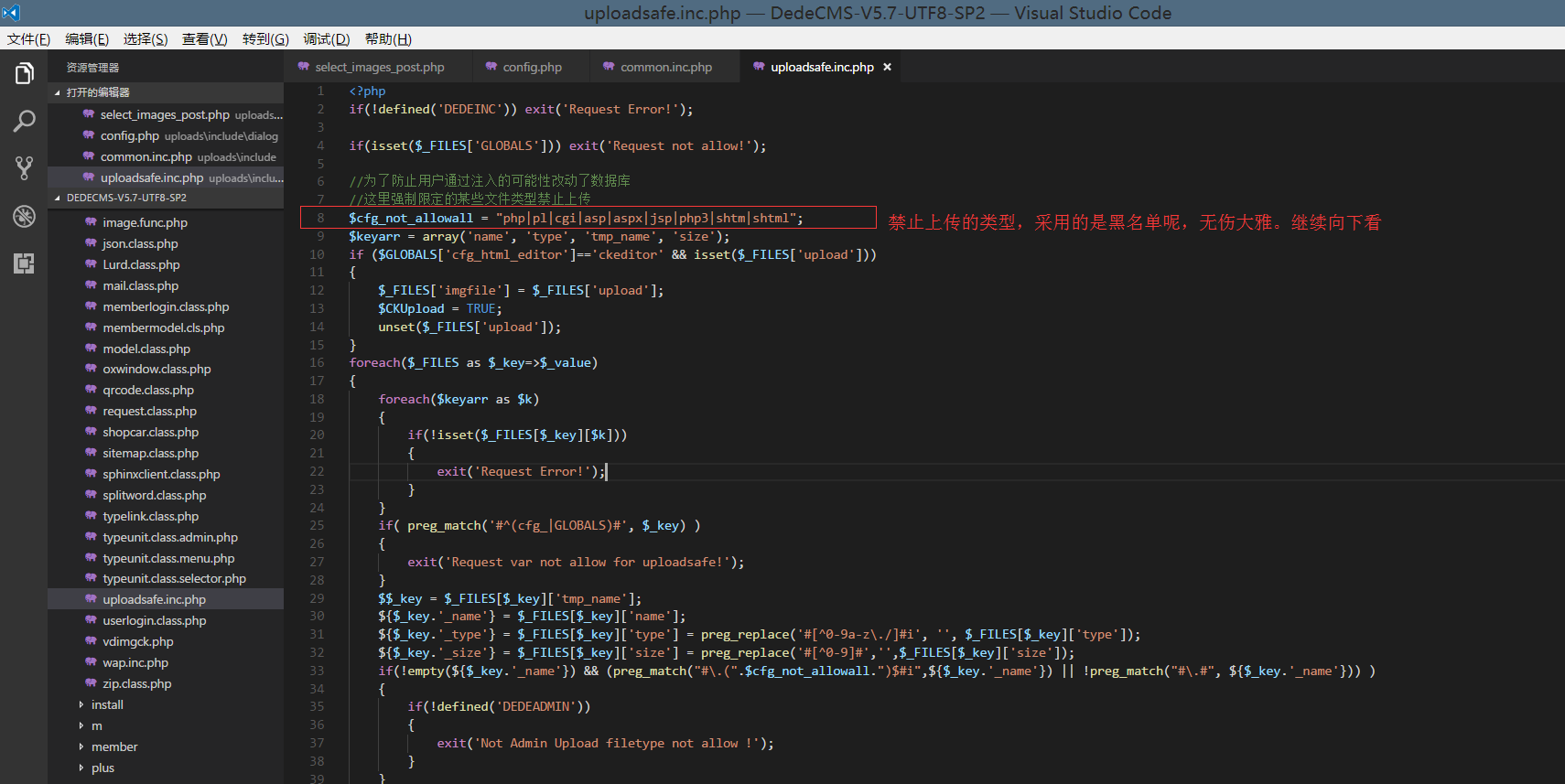
漏洞地址：<http://127.0.0.1/DedeCMS-V5.7-UTF8-SP2/uploads/include/dialog/select_images_post.php>

漏洞文件：select\_images\_post.php

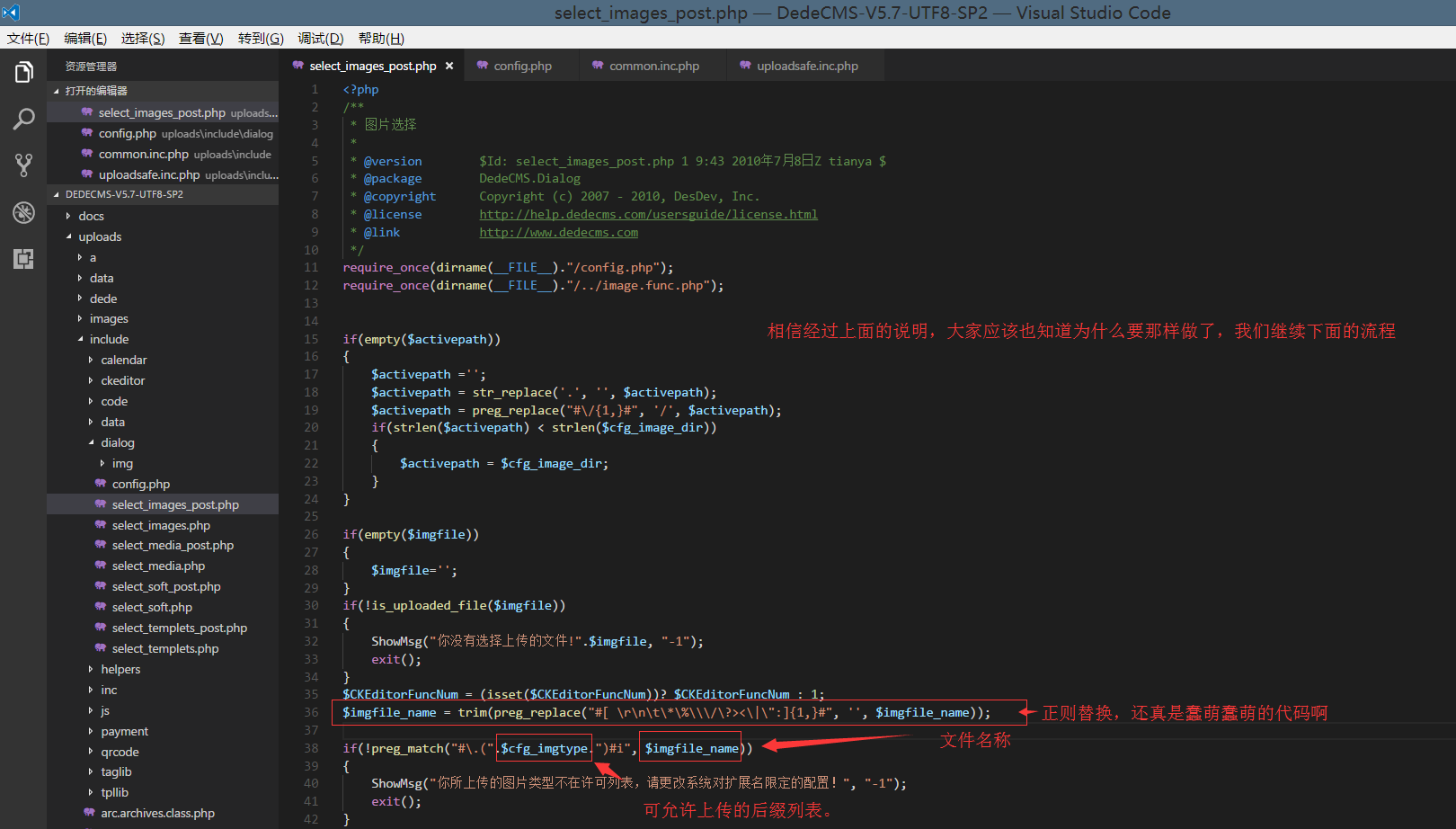




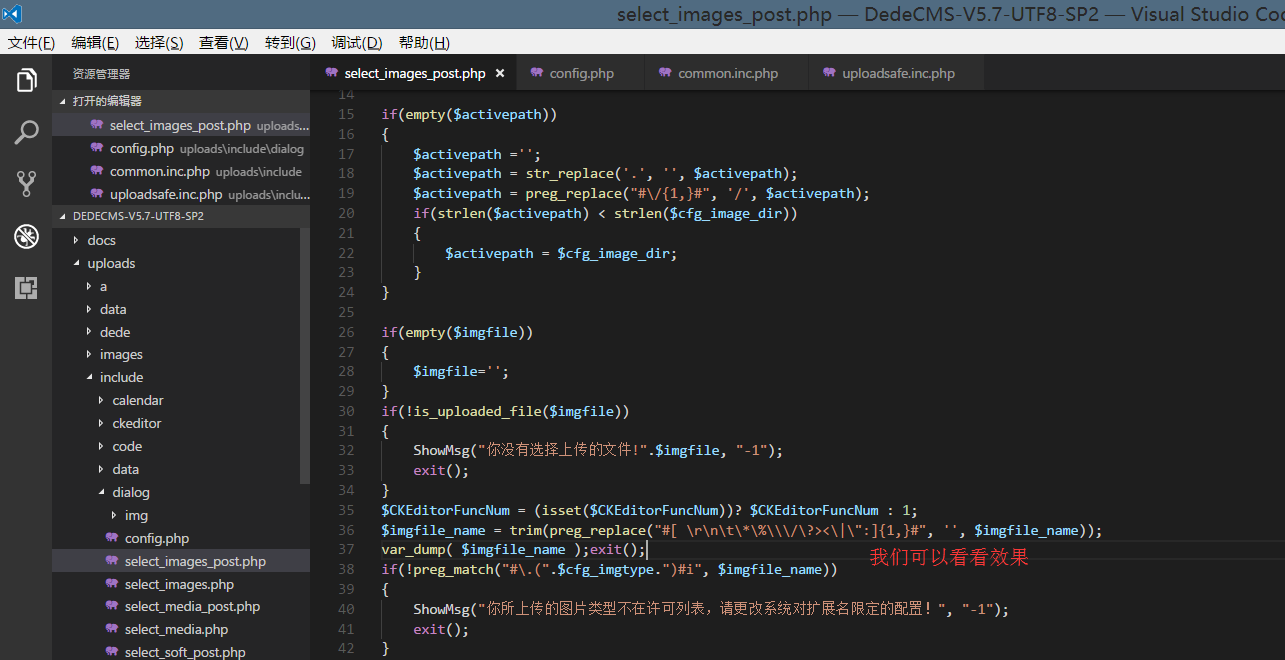


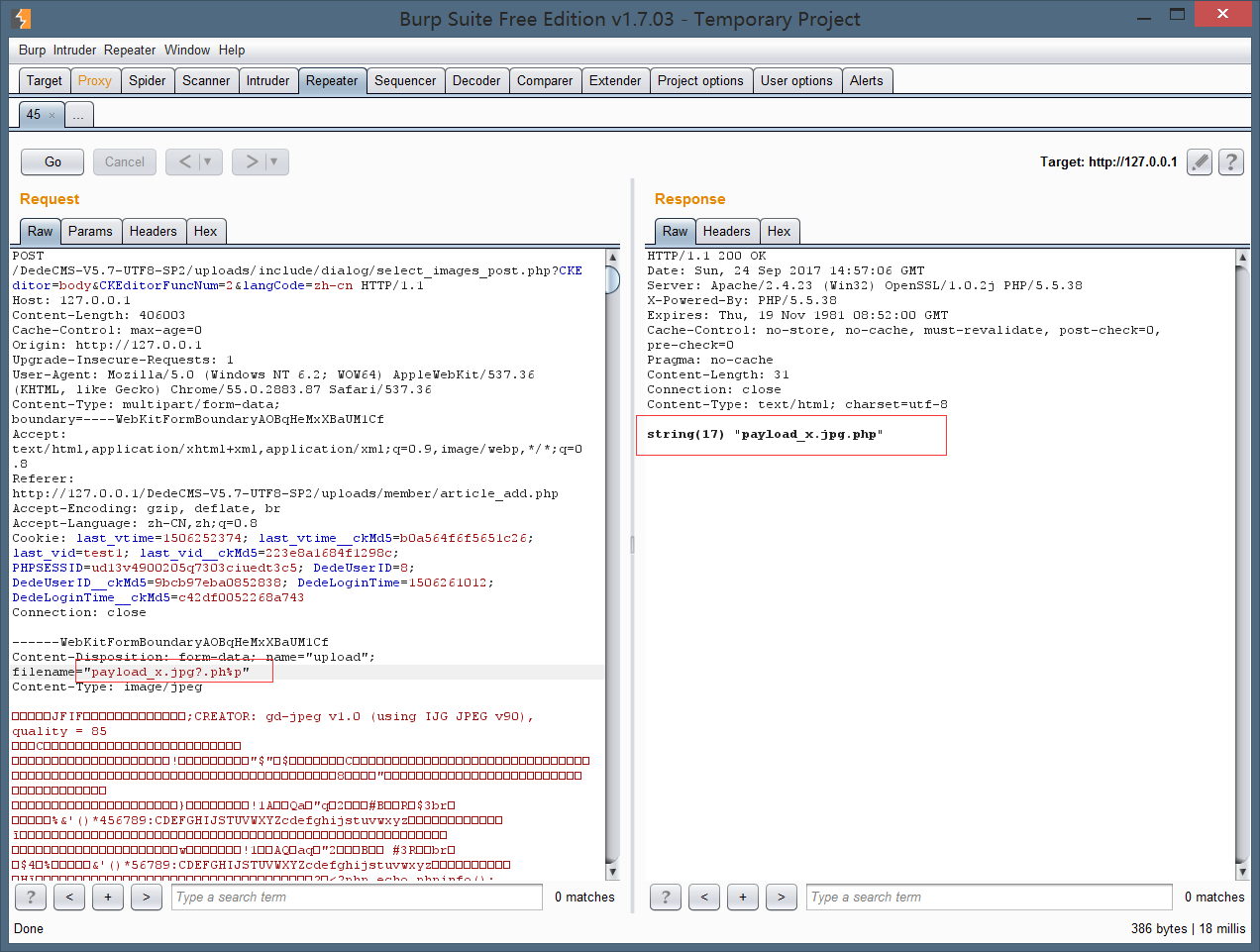


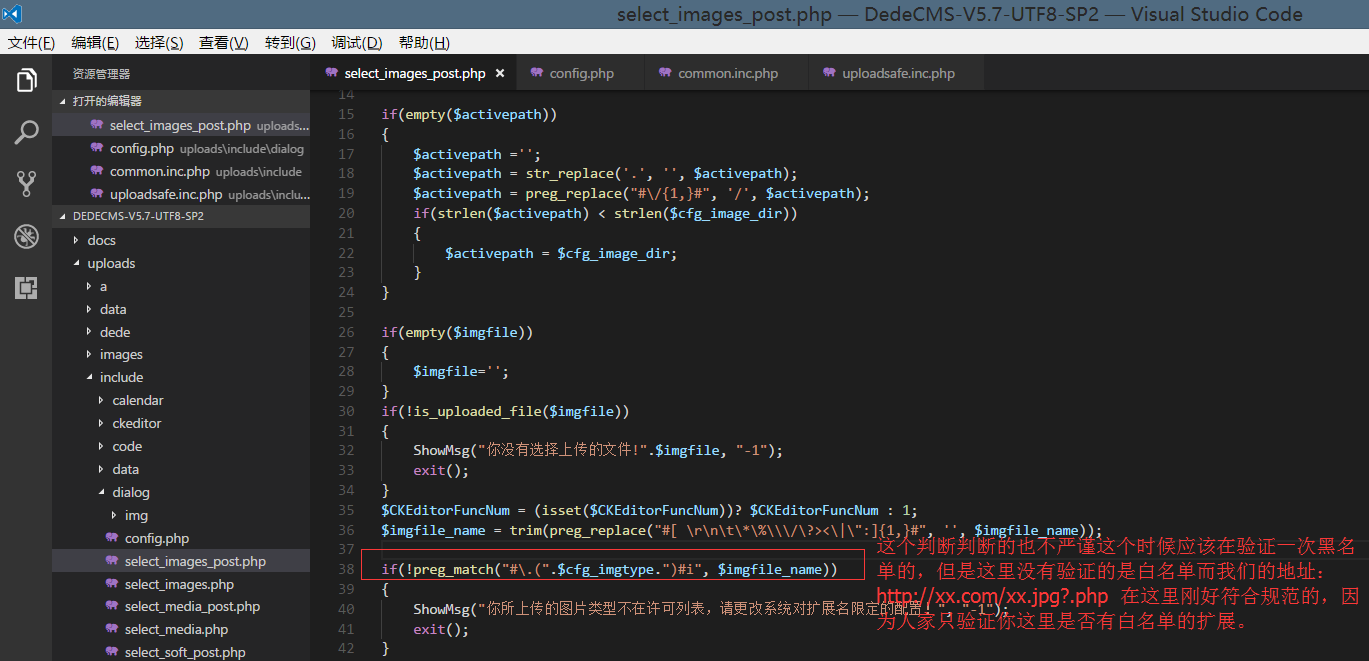


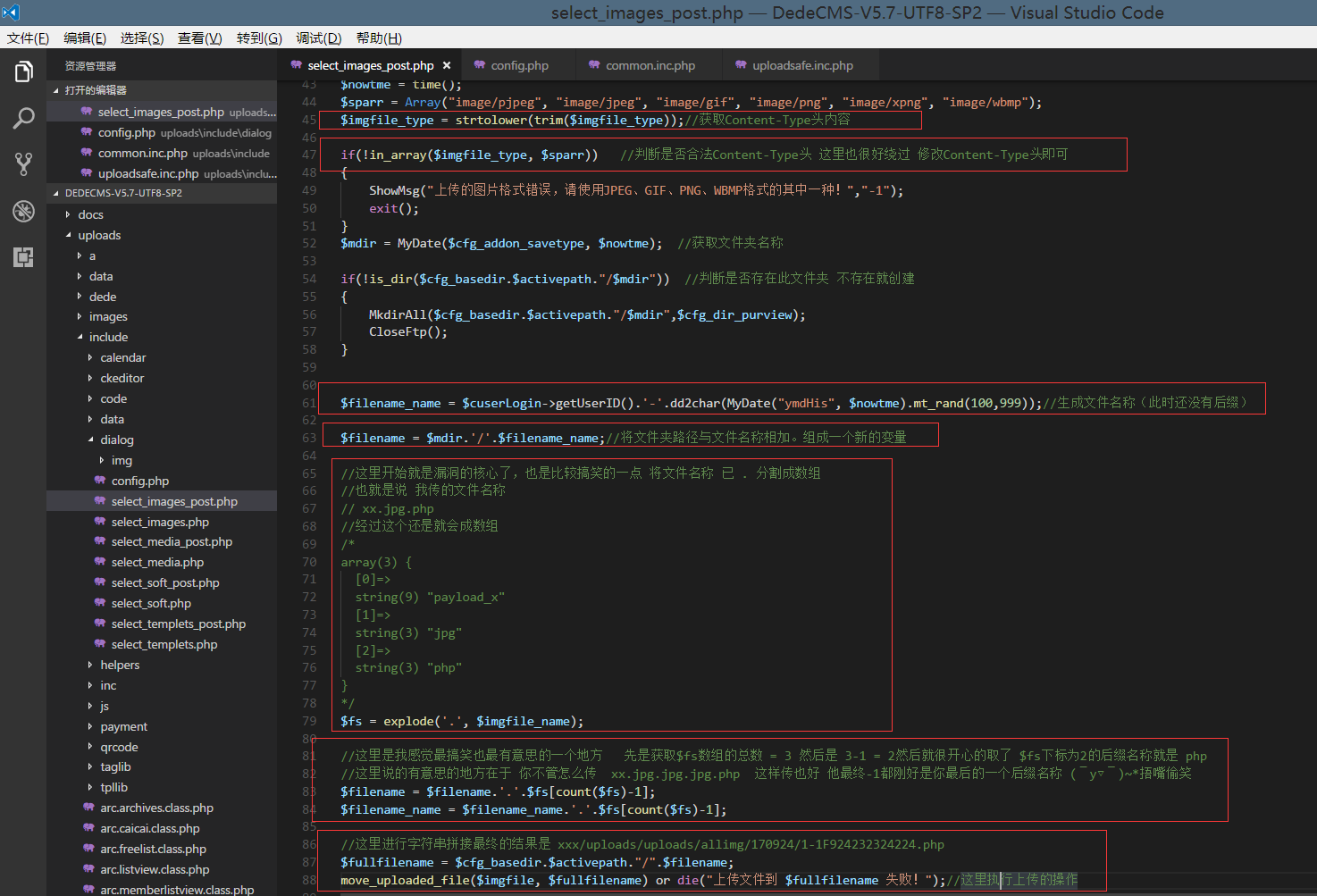


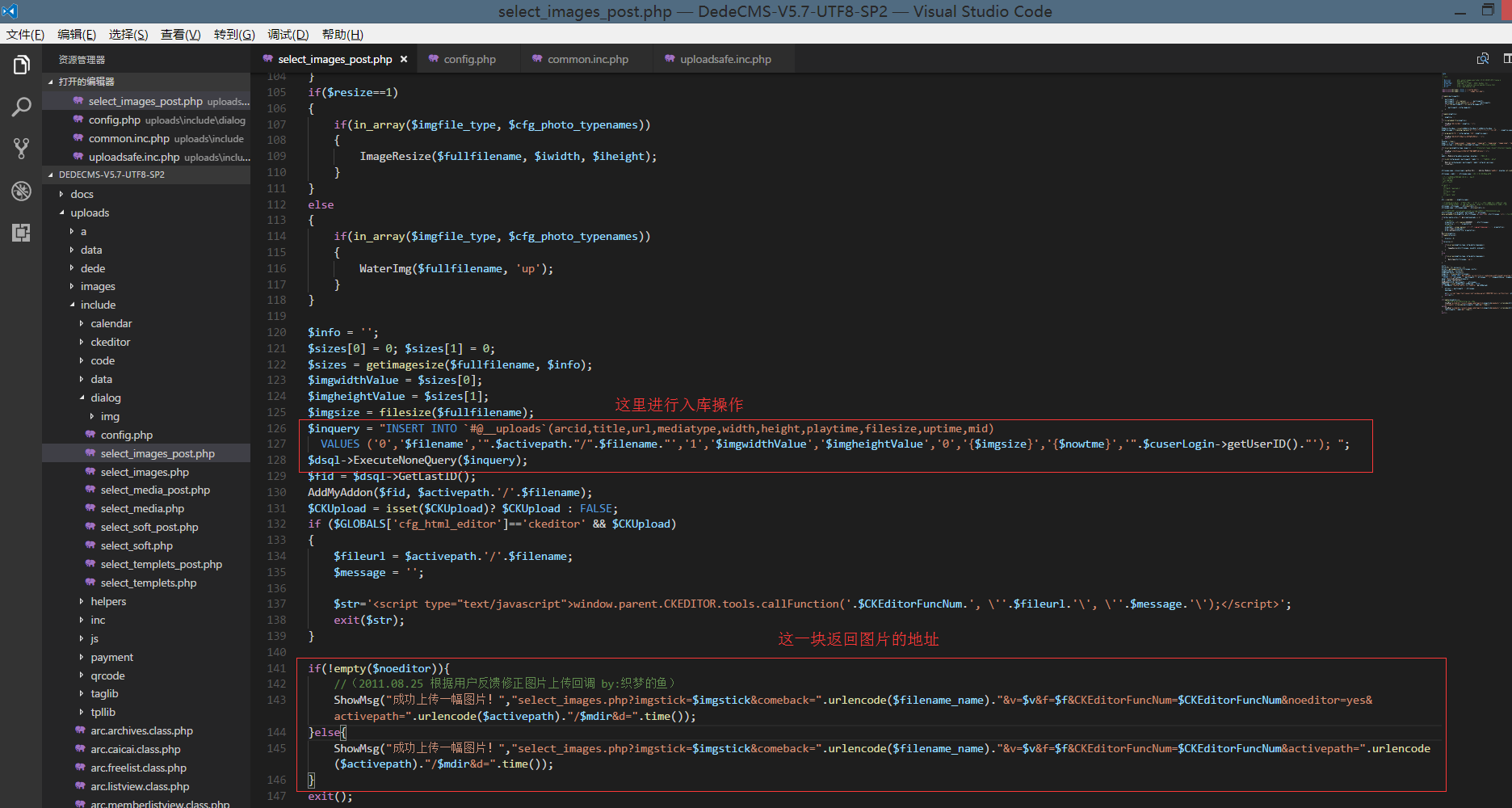












0x04 漏洞修复

前面有提到过，没有？没看到？说的不清不楚？等官方更新版本咯。