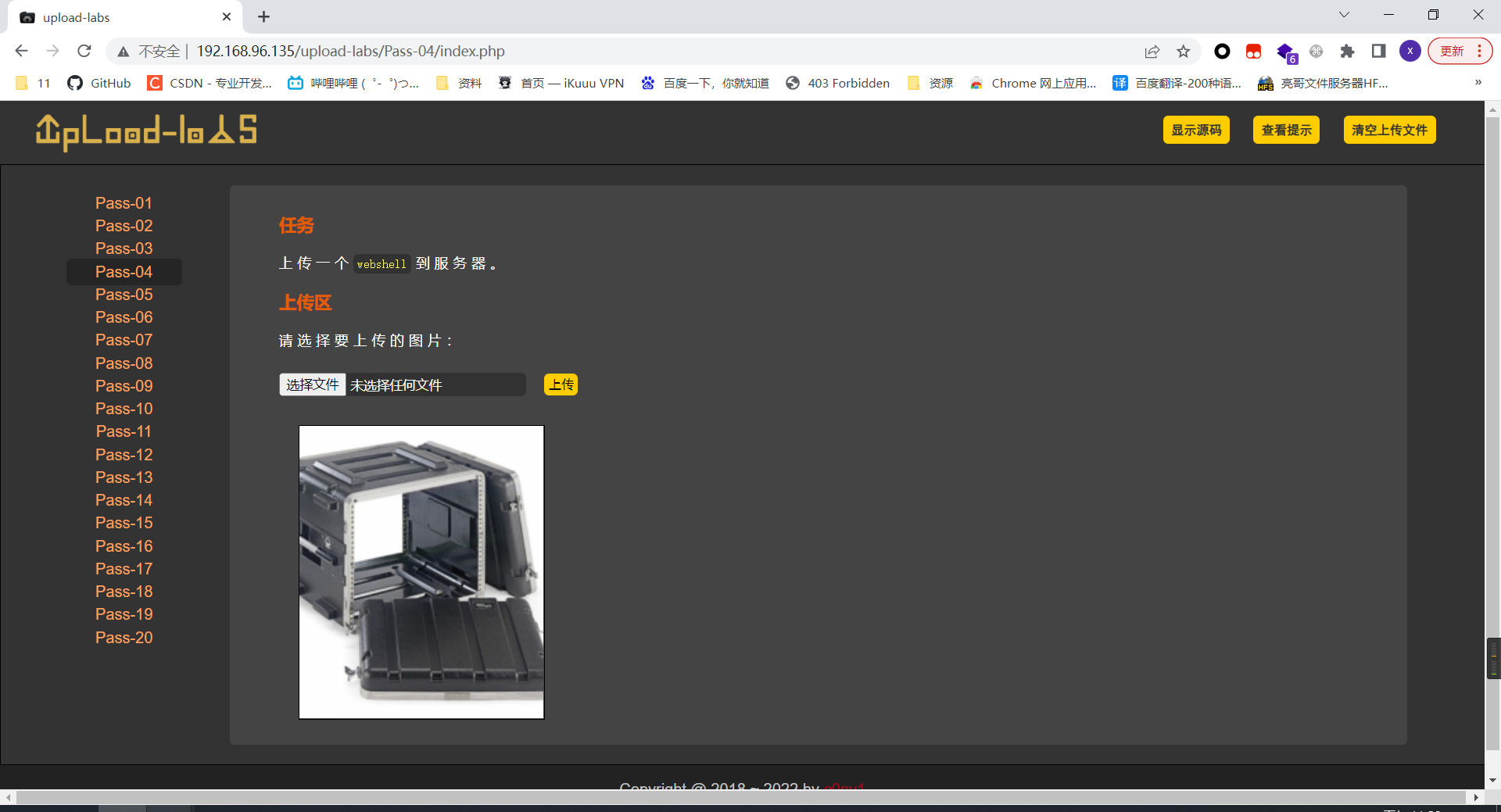
upload-labs第4、5关解题笔记

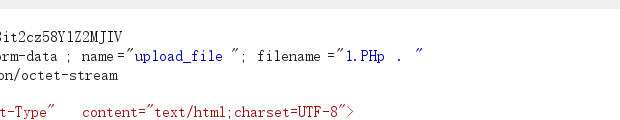
第4关

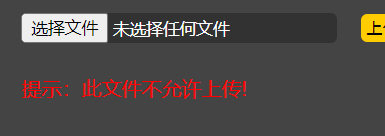
1. 上传正常文件验证功能点是否完好



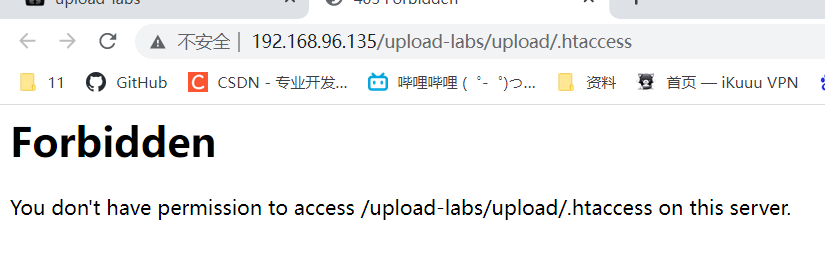
上传后确认上传功能完好

2.尝试后缀名大小写,空格,点号绕过



发现都被过滤

3.尝试上传.htaccess格式的文件,. htaccess文件是Apache 服务器配置相关的一些指令文件,只作用于当前目录



可以看到已经上传成功,

这个文件中包含了以下代码:

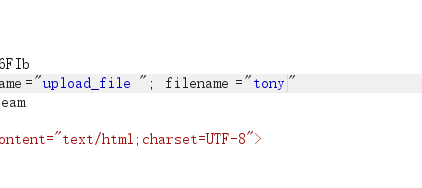
<FilesMatch "tony">

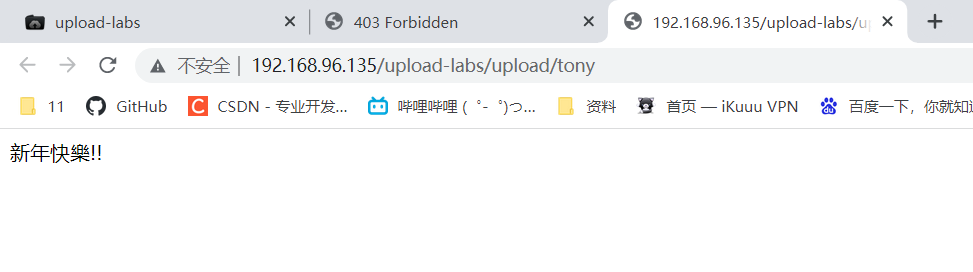
    SetHandler application/x-httpd-php

</FilesMatch>

此代码的作用是将名为tony的文件当做php文件解析,

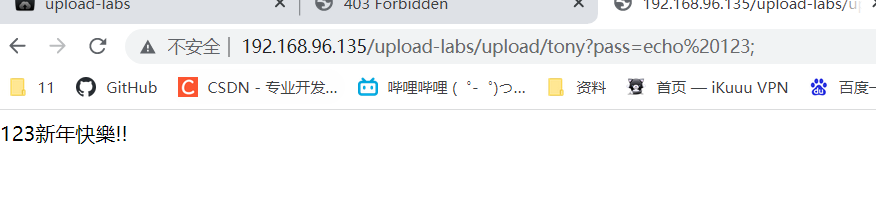
4. 此时我们就可以上传一个一句话文件,并且抓包将文件名改成tony



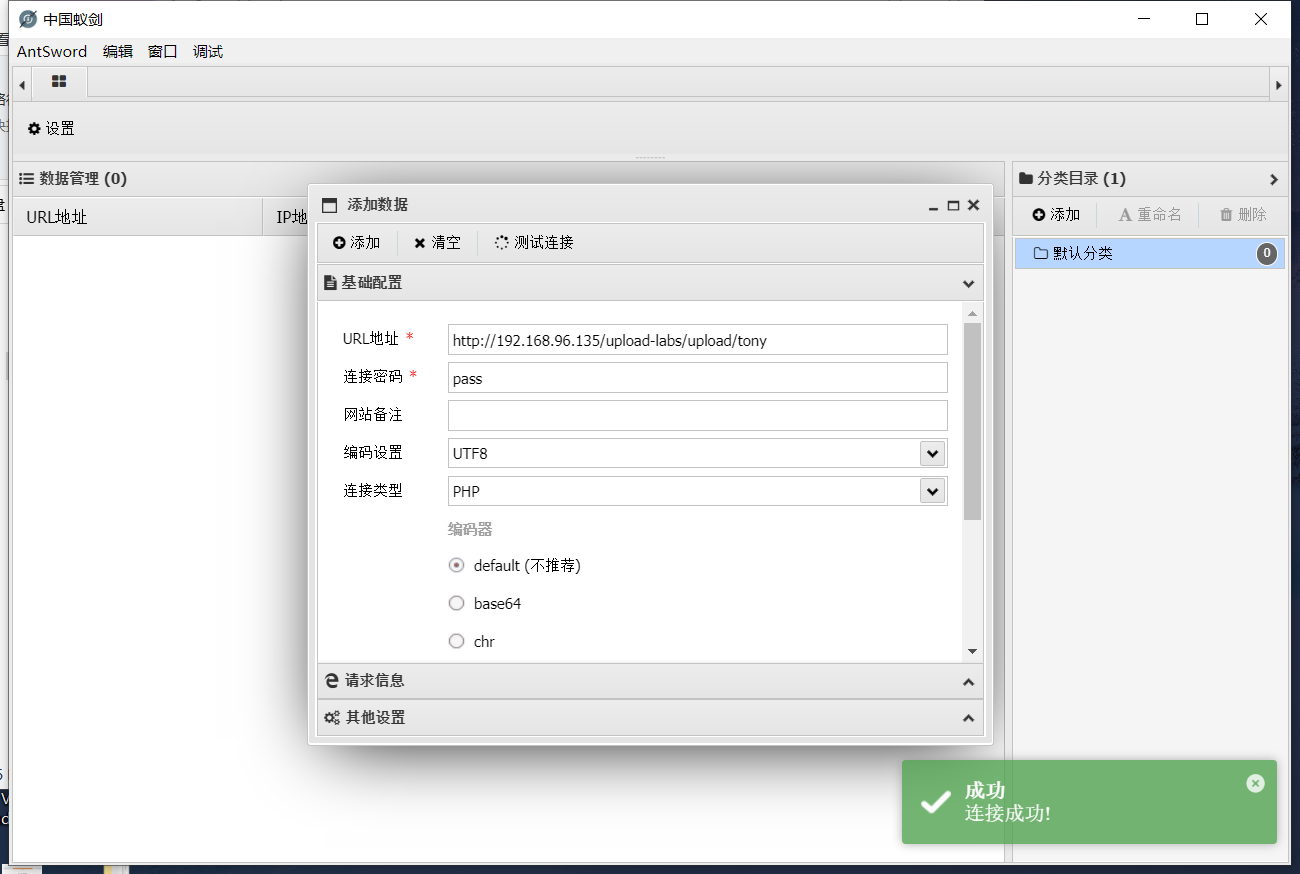


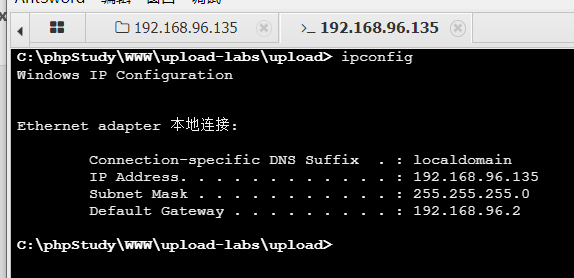
上传成功!

尝试执行命令



尝试蚁剑连接

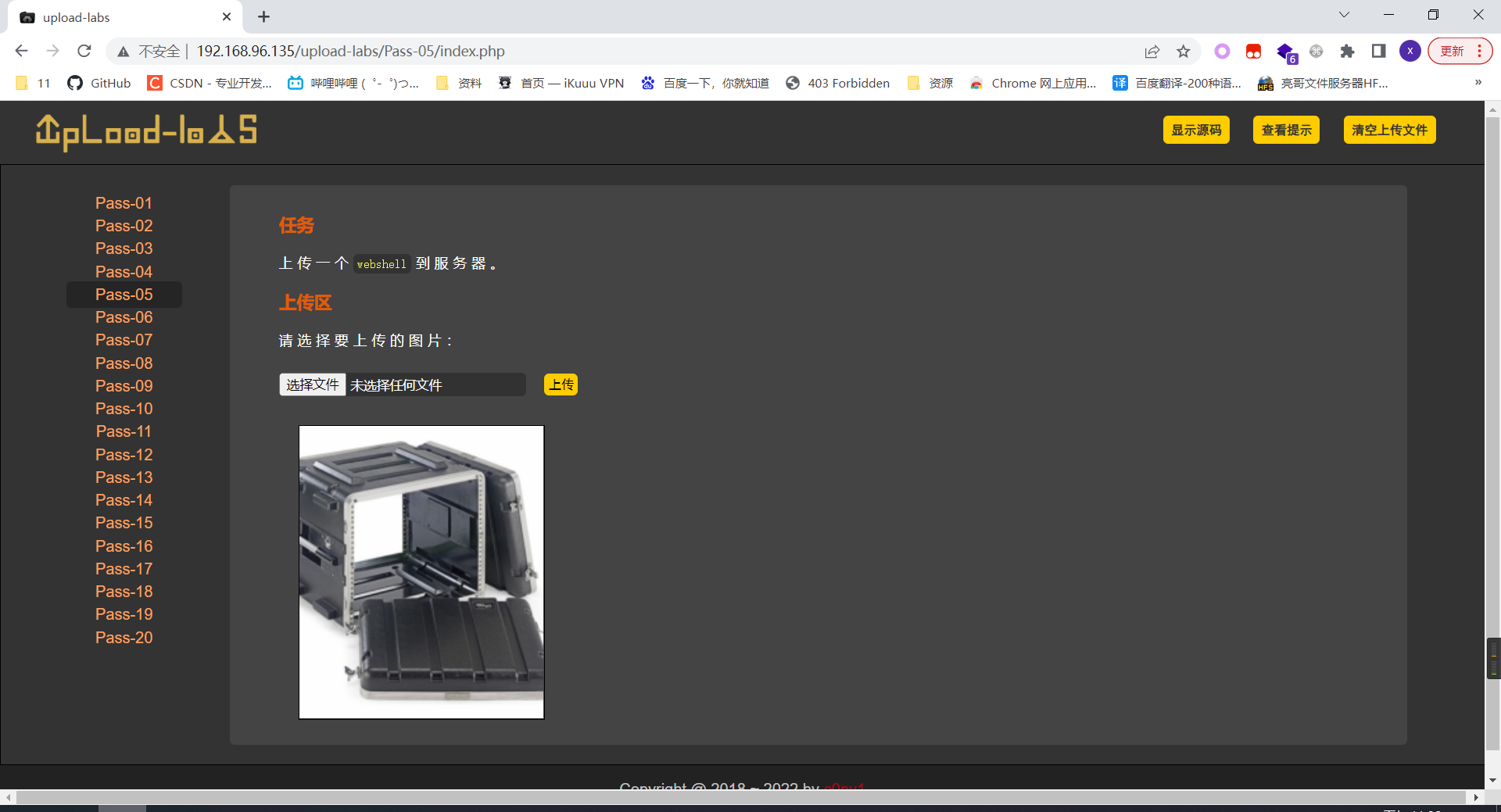




成功get shell

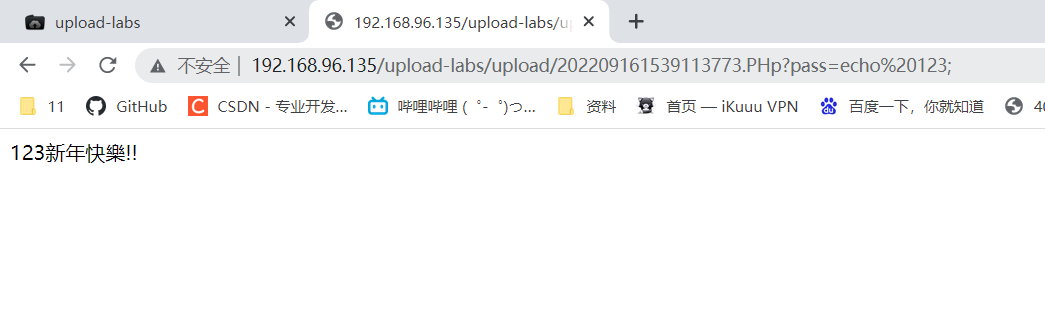
第五关

1. 验证上传点功能



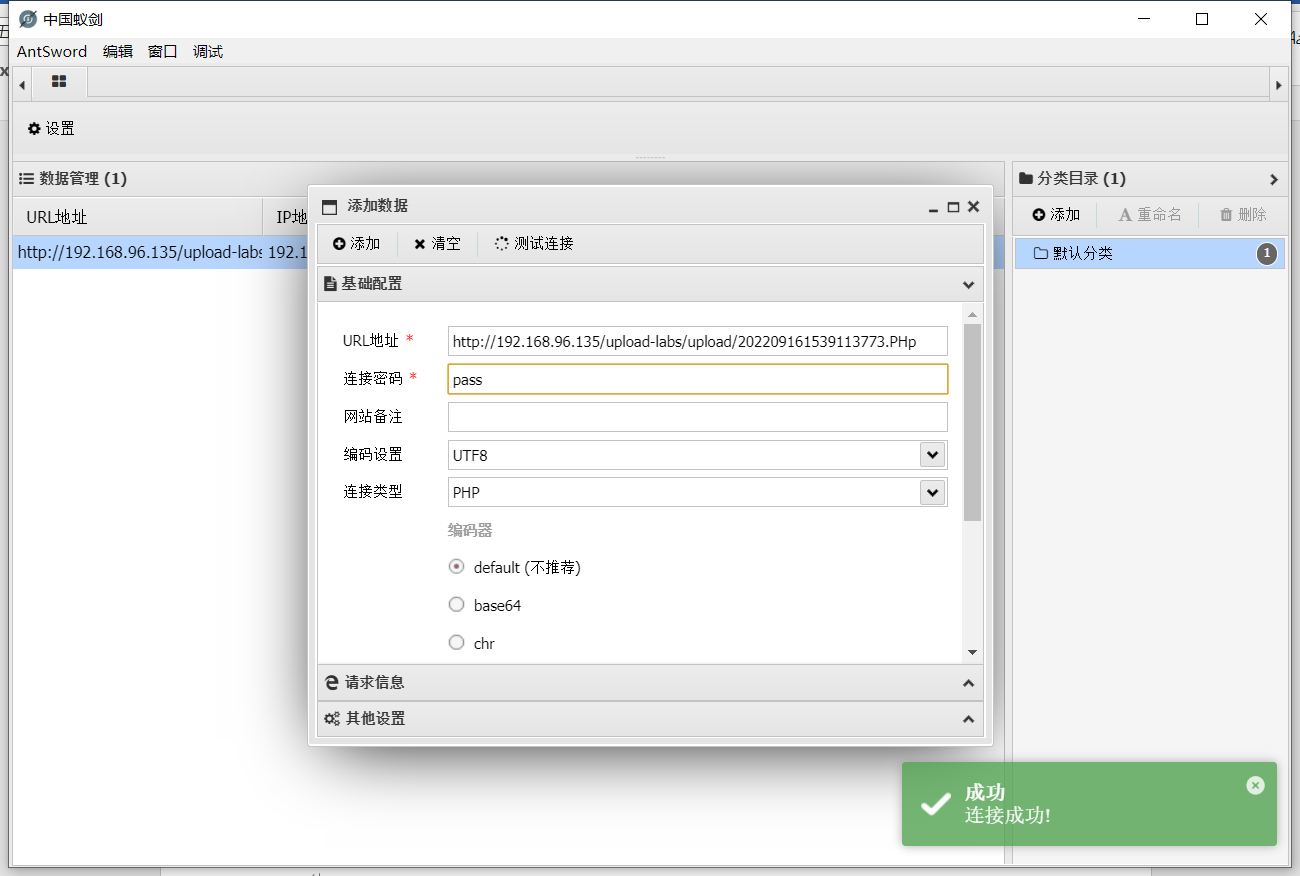
2.尝试后缀名大小写,空格,点号绕过





上传成功

3.连接蚁剑



成功get shell