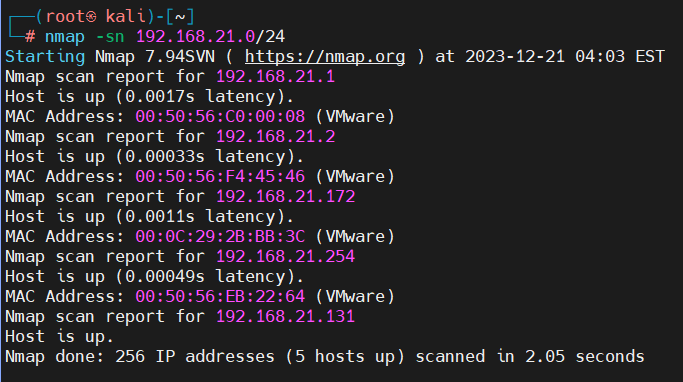
ki

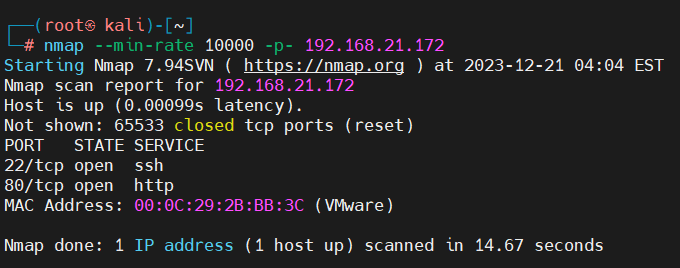
下载地址：<https://www.vulnhub.com/entry/ki-1,641/>

主机发现

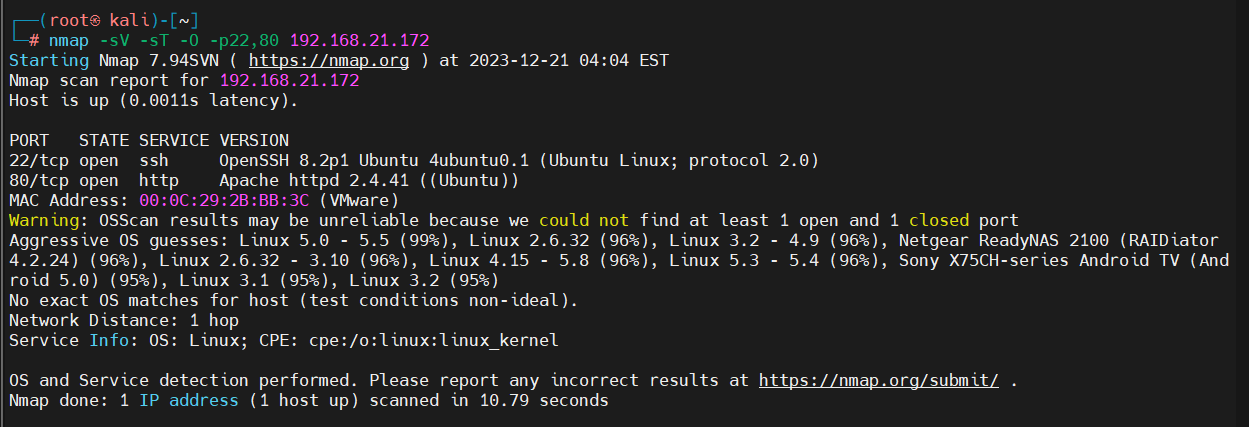


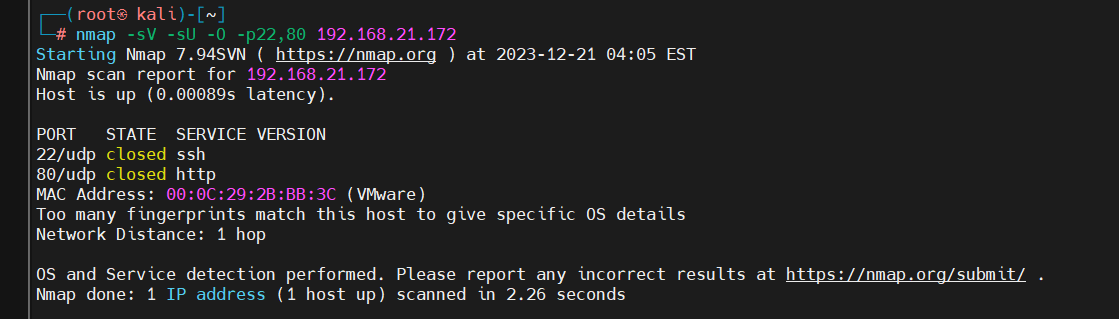
目标172

端口扫描

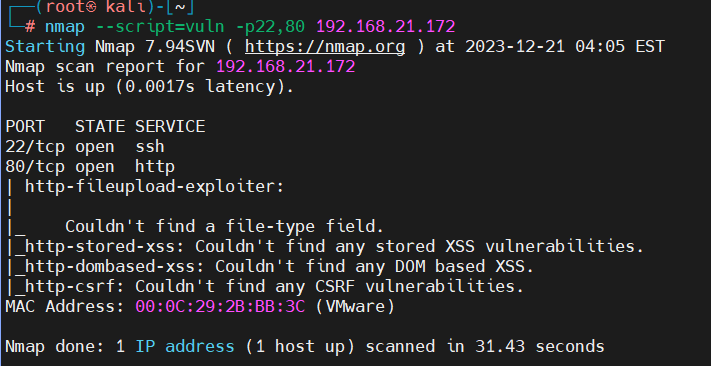


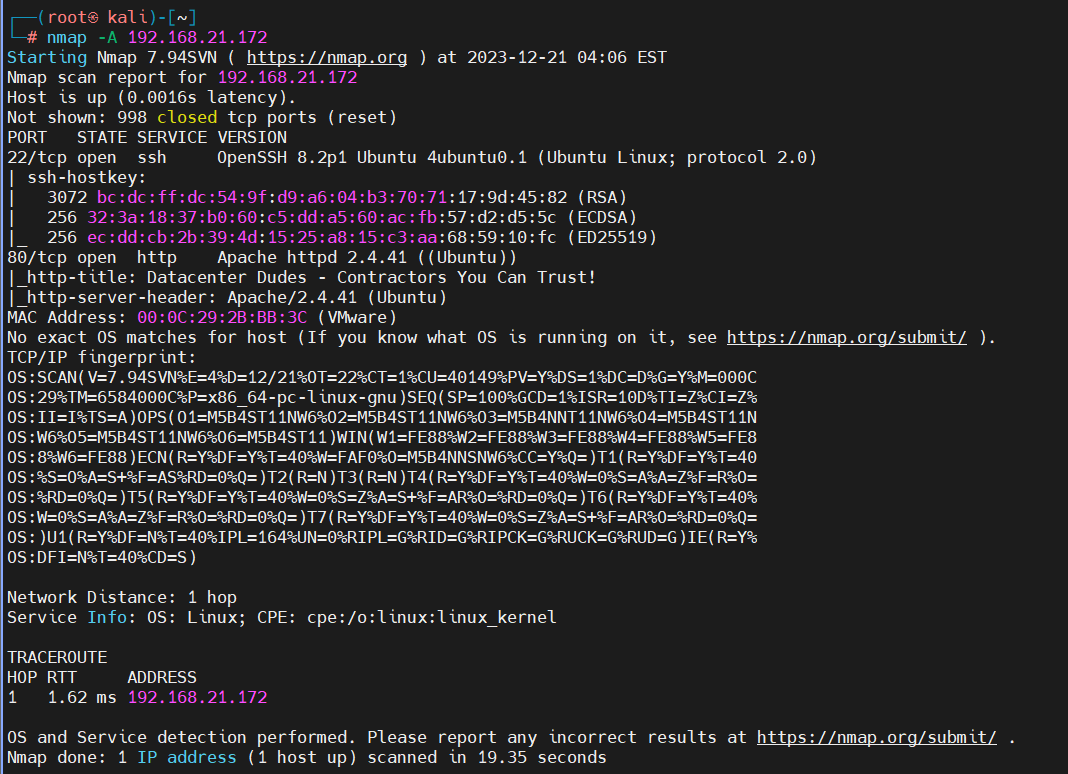
端口服务扫描





漏洞扫描

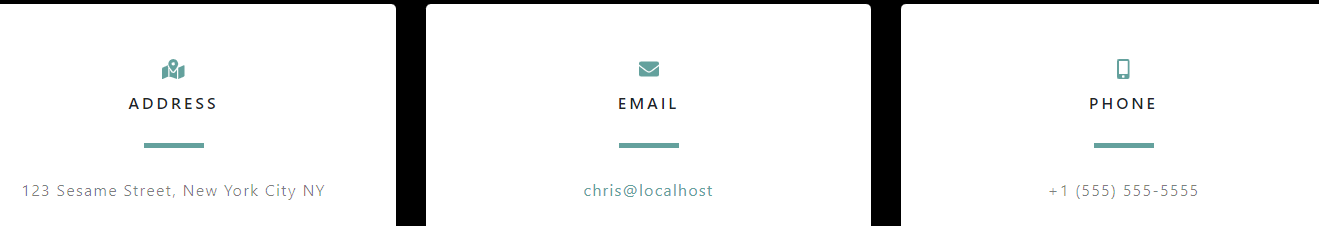




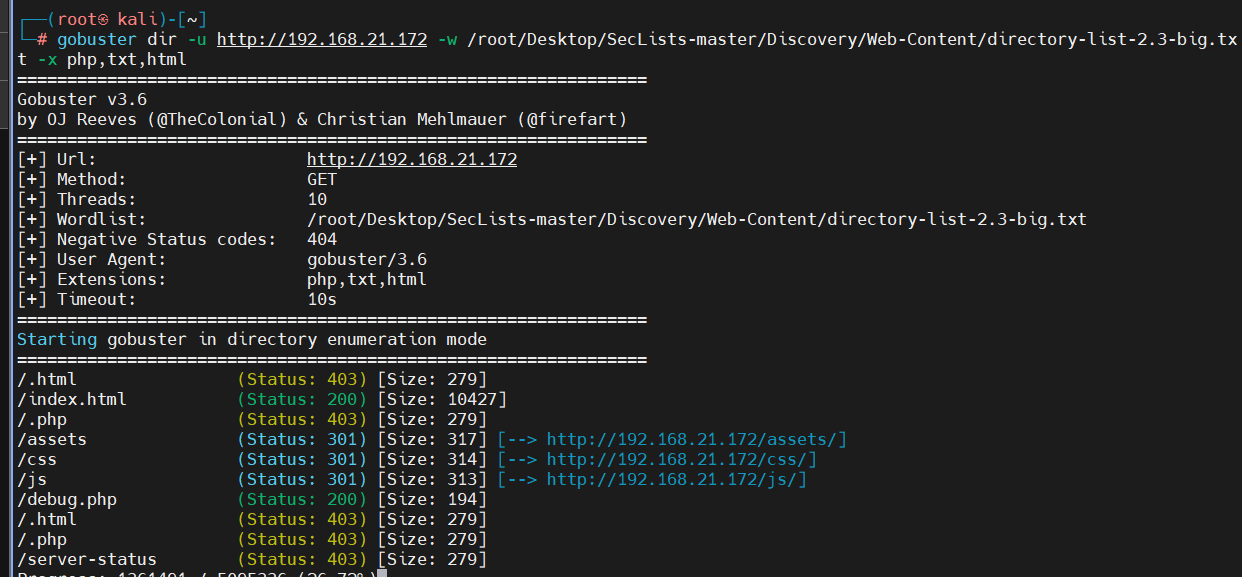
先去看看web



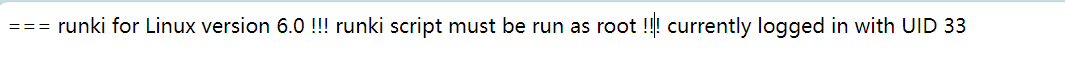
web上面只有这些信息



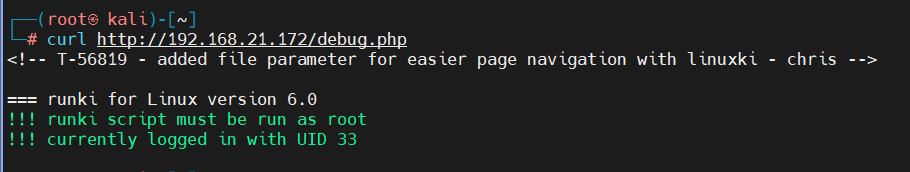
那就目录扫描



发现debugphp那就一定要去看看



游览器访问感觉有点问题

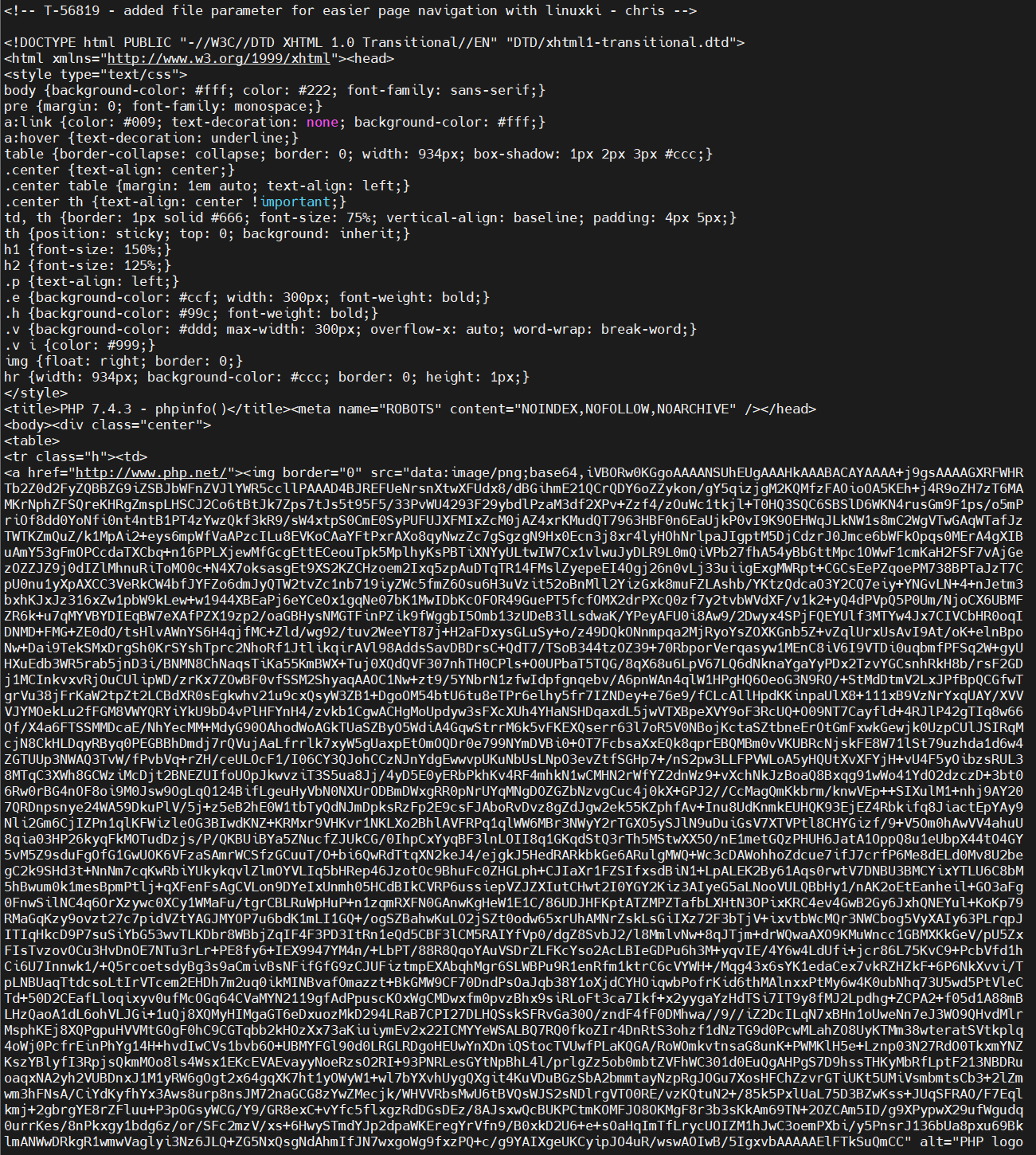


看来猜想是对的

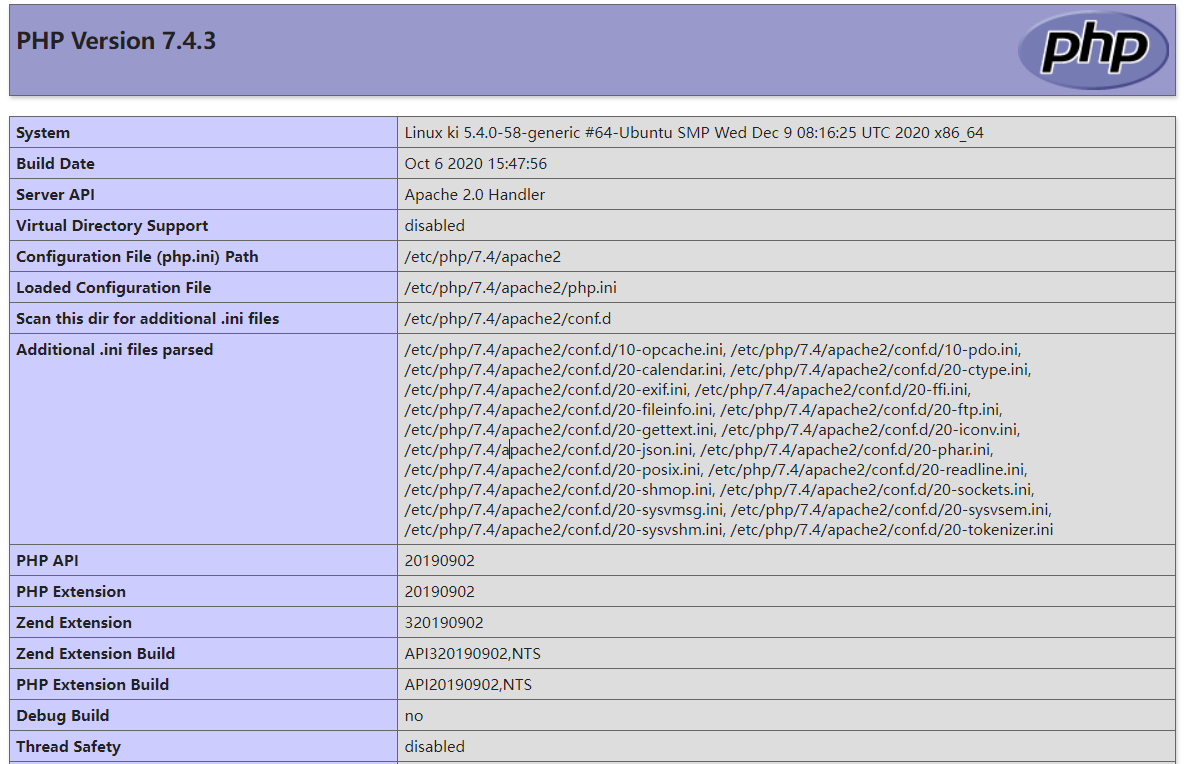
要我们登入而且这个runki脚本是root跑的

那就爆破变量

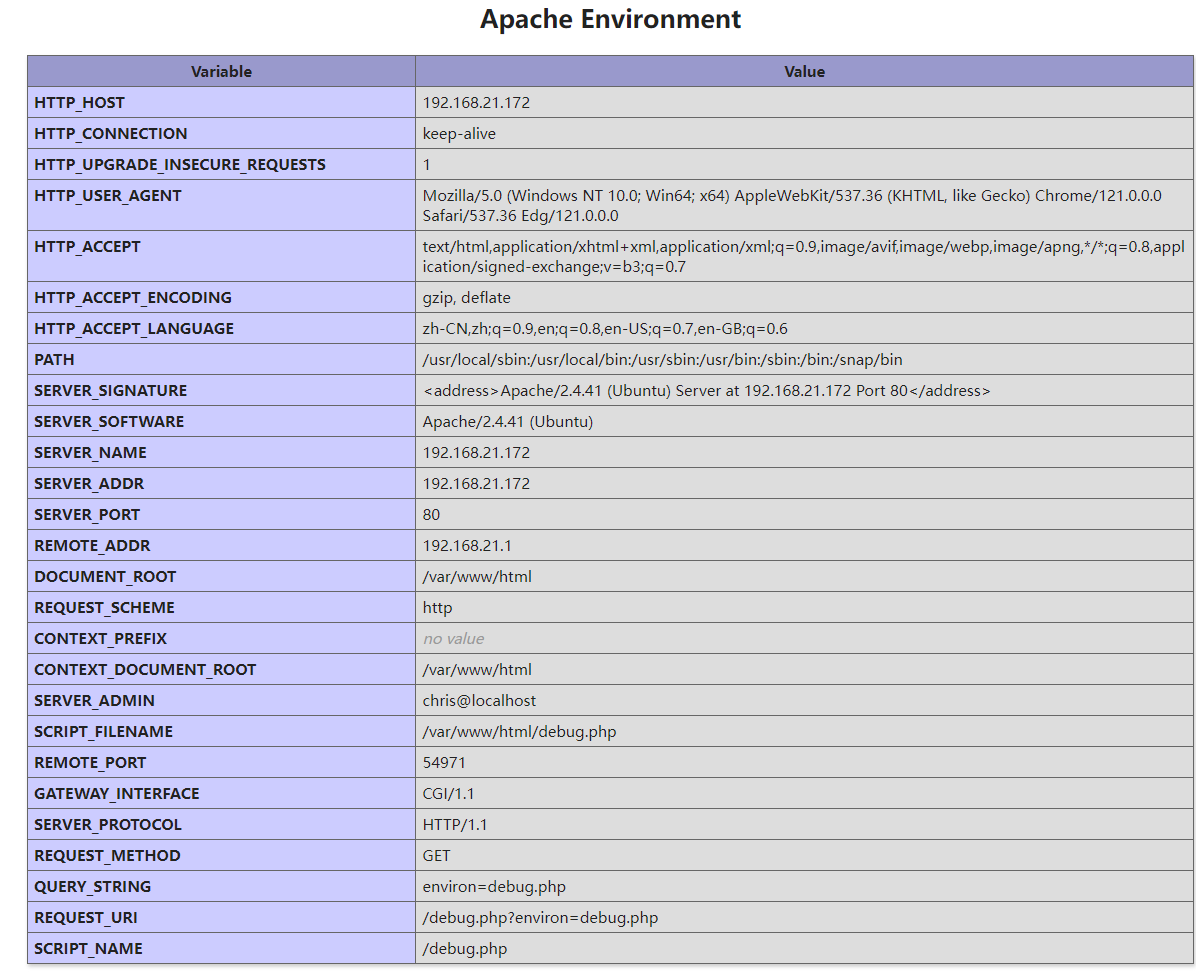
爆破出来后查看一下源代码



离谱看看web吧

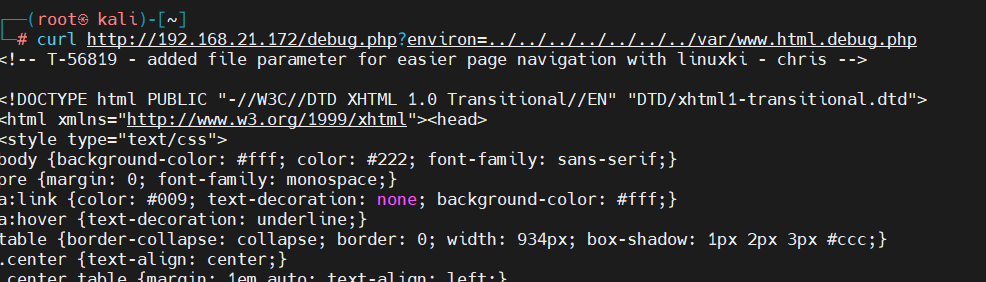


这个是个好东西

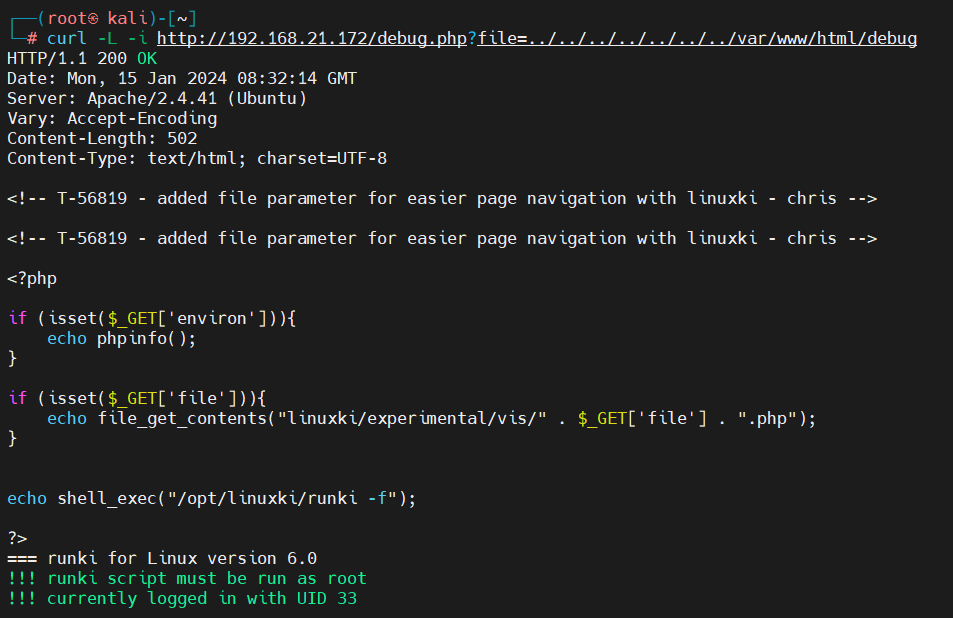


好的能合理解释了（apache的环境变量写成了debug.php）

那么不是我们传参的那个php（注意路径哦）



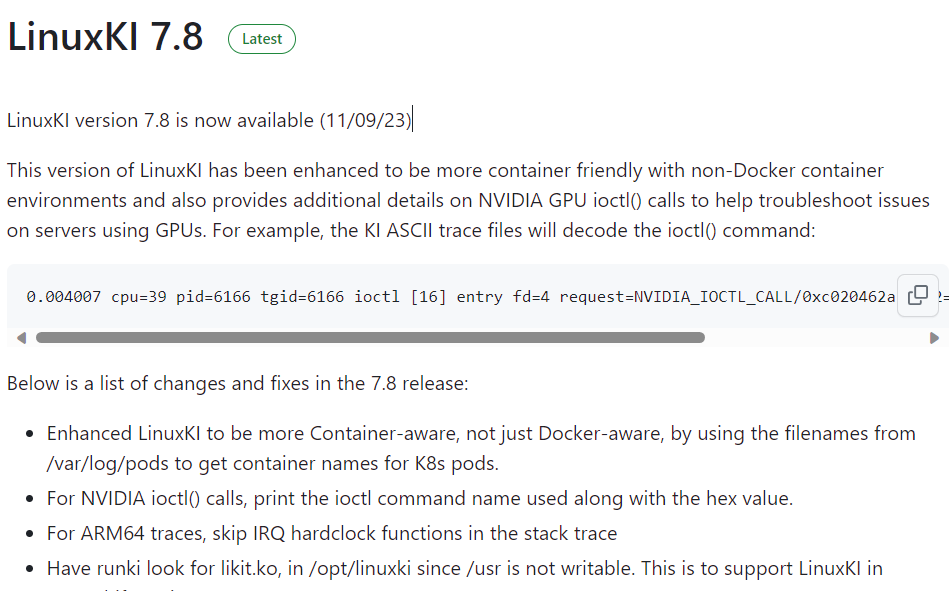
这个回显是一样的，线索好像断了，但是注意一下前面我们只是爆破了带有后缀的文件linux文件是可以没有后缀的



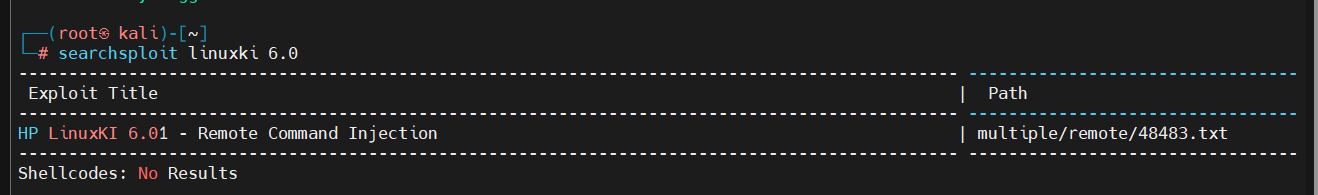
看到这我觉得前面的命令需要优化一下了



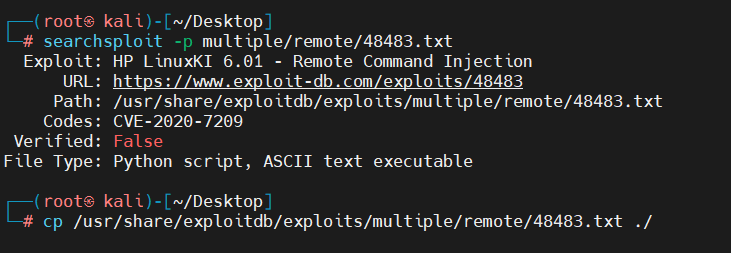
由此还剩下代码里面的runki没有办法解决

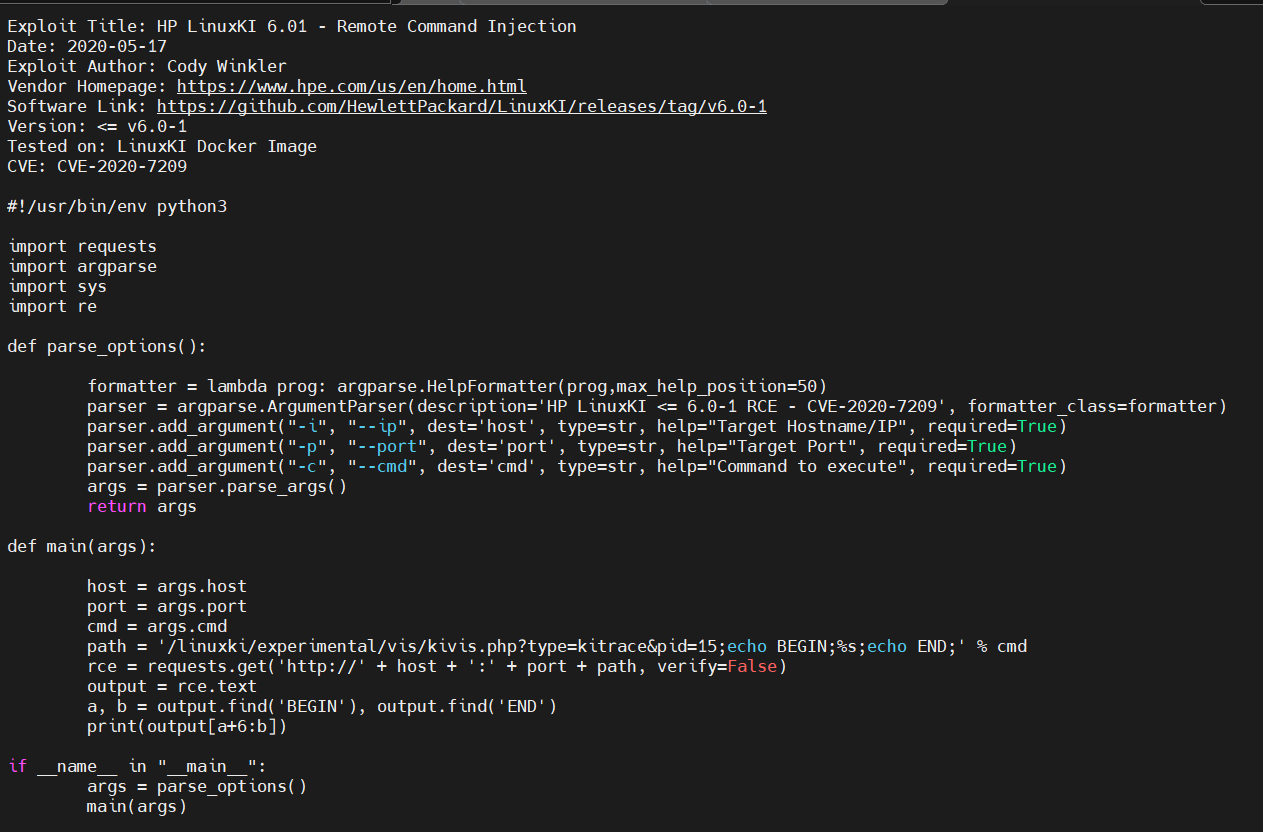


哦名字其实叫linuxki好办了



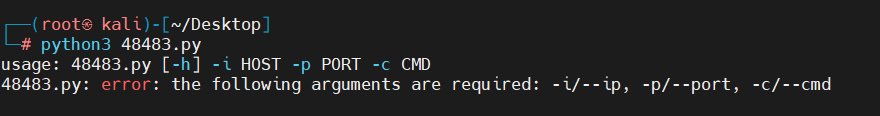
看看

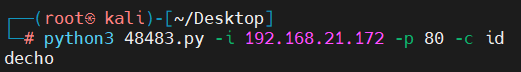




python3的脚本

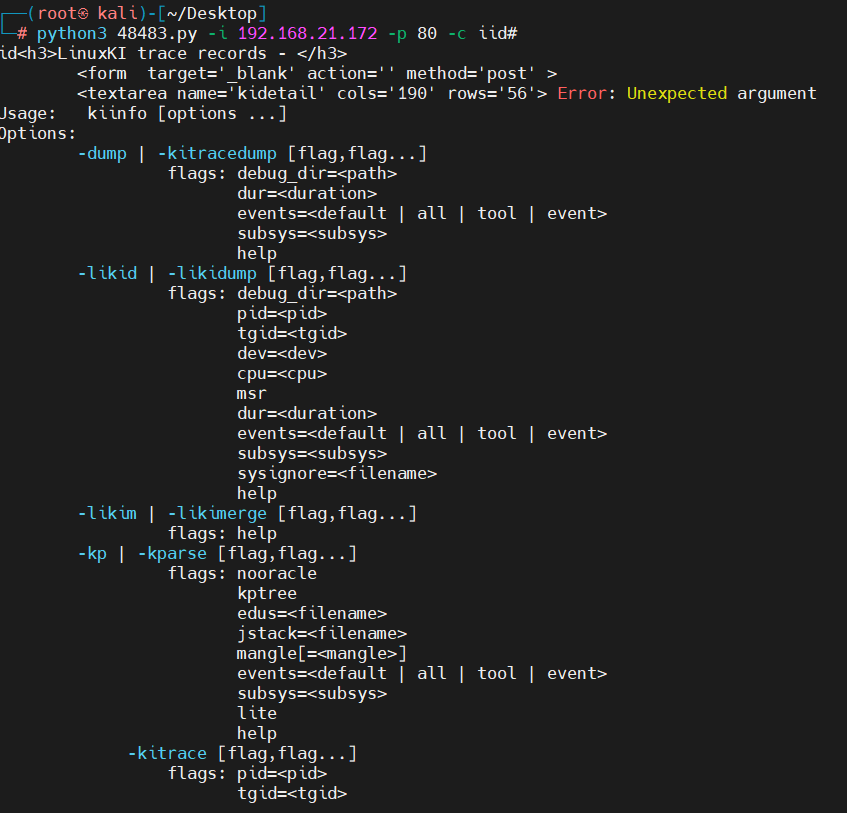
把前面没注释的东西去掉，顺便改一下名字



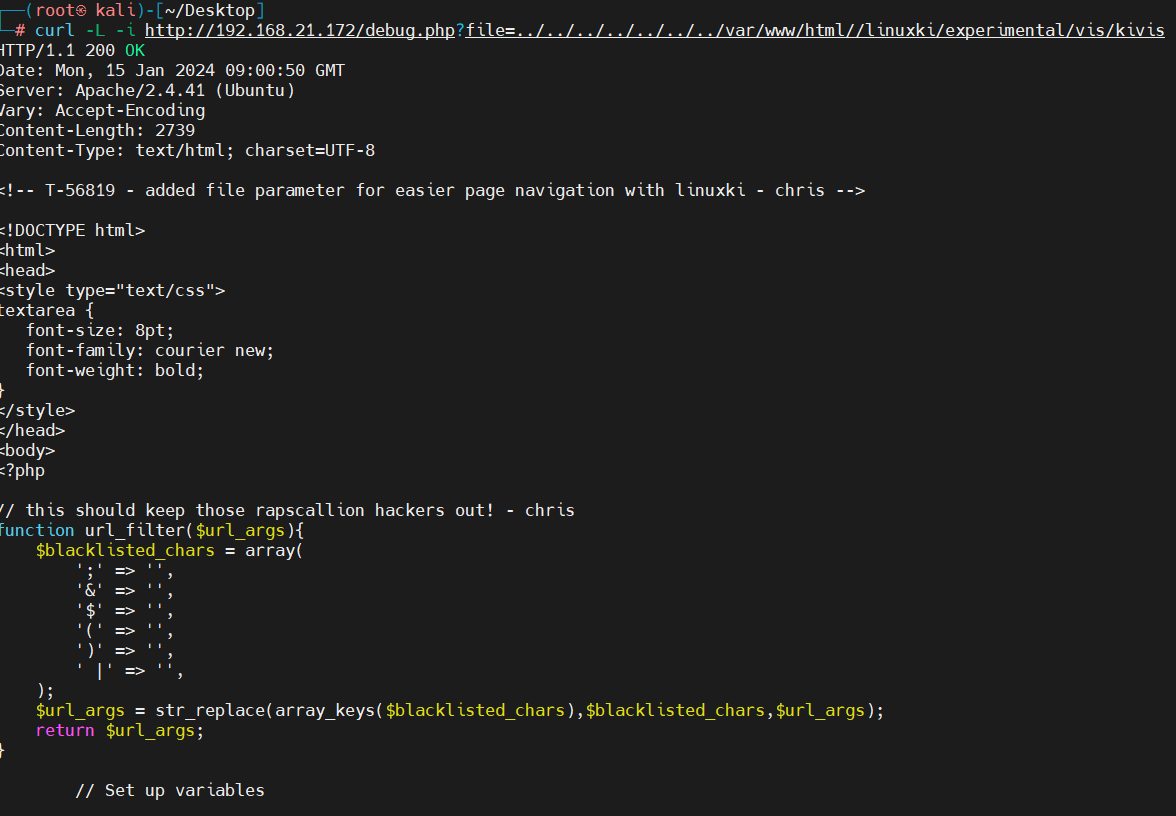


输出好像有点问题，应该是在利用程序里面找线索了，感觉应该是字符串分割





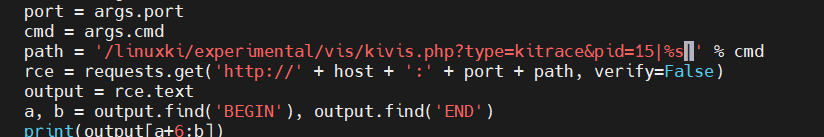
出来了点东西但是还是要看看

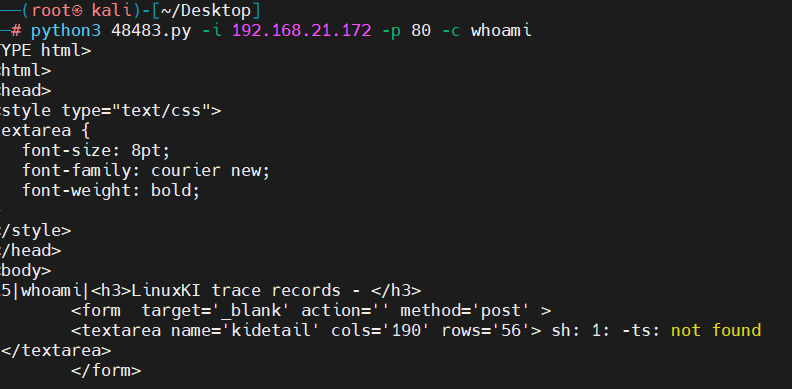


脚本利用的是pid上面正好截到了有关信息，去查看有关pid的程序

这里就是命令执行了（注意最后一行是有空格的）

那么要改脚本了

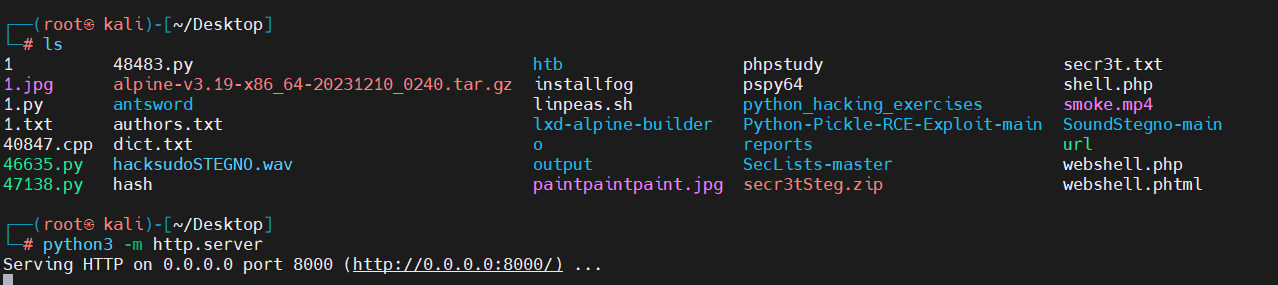




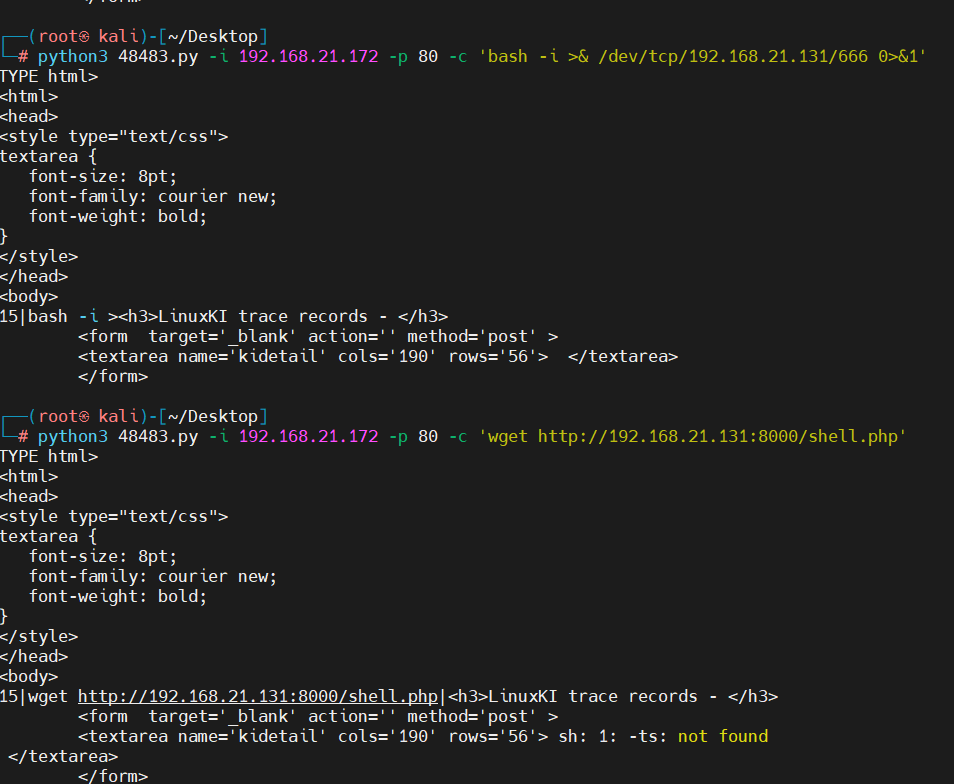
我们在这里只需要反弹shell就可以

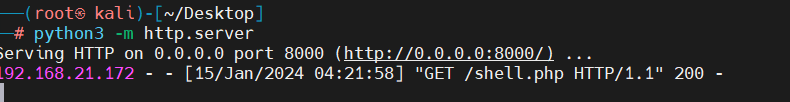


bash好像用不了（因该是没权限）换一个

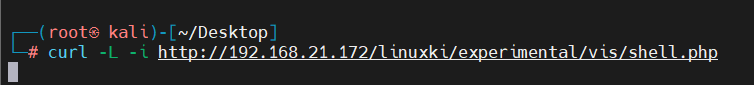


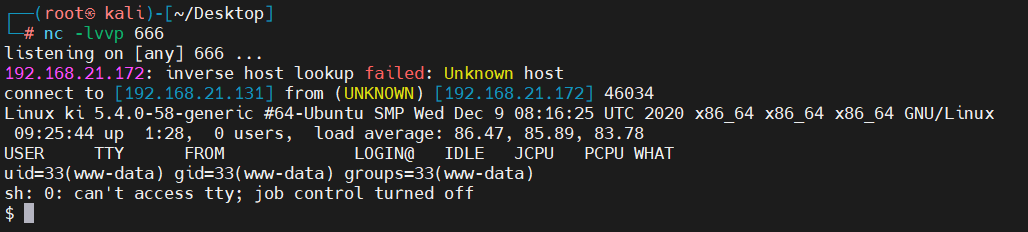
我之前由php的shell就直接用了





访问

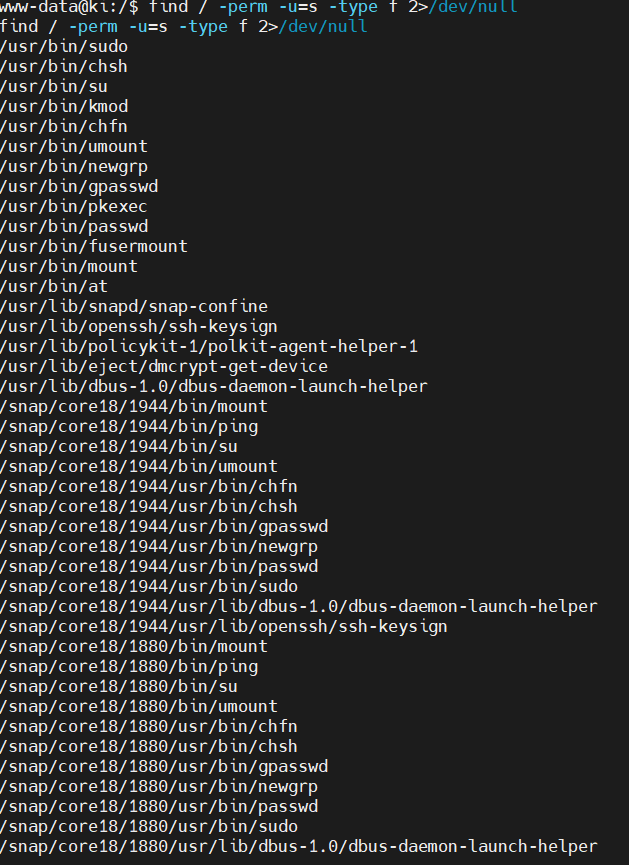






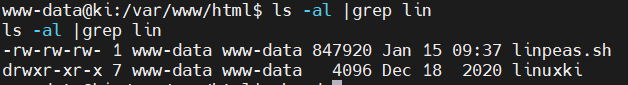
接下来就是提权了

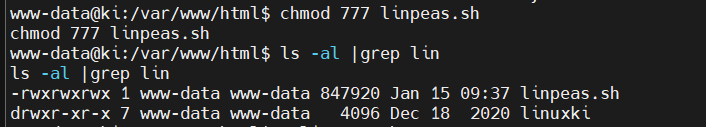
先到普通用户身上

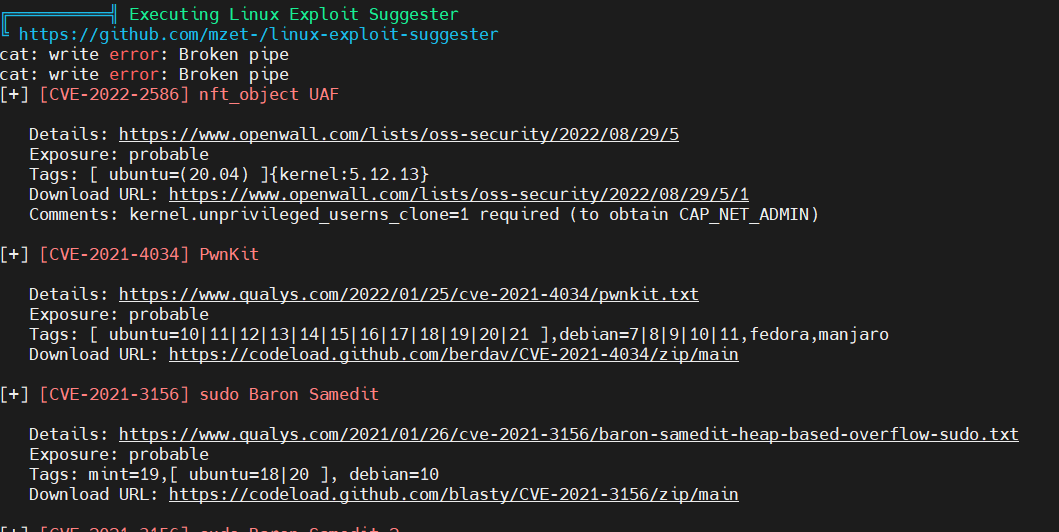


那就用linpeas

下一个

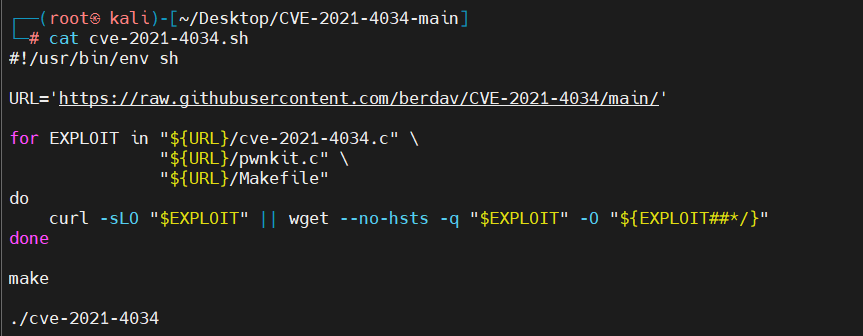






一个一个试吧

下载后解压缩在传进去



需要的文件

一个个下

