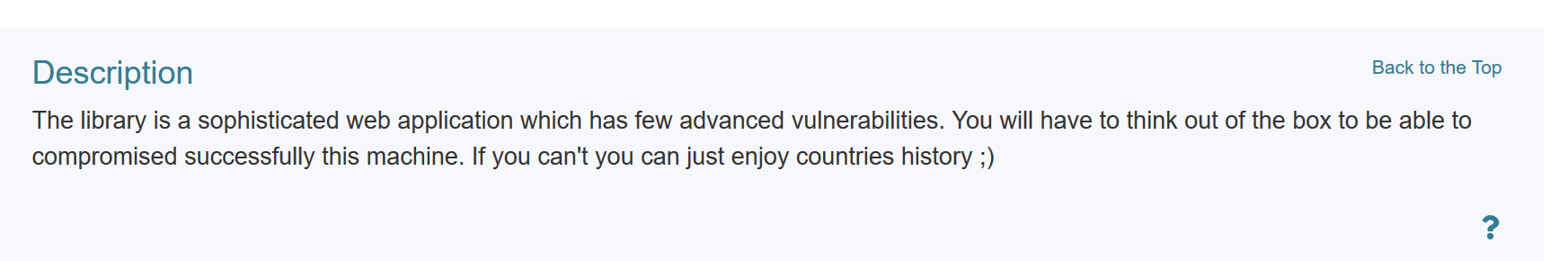
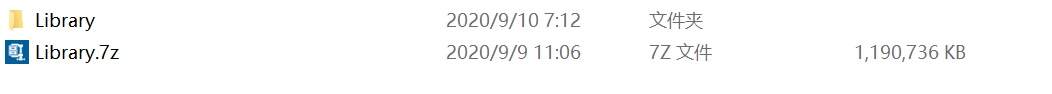
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/the-library-1,334/>

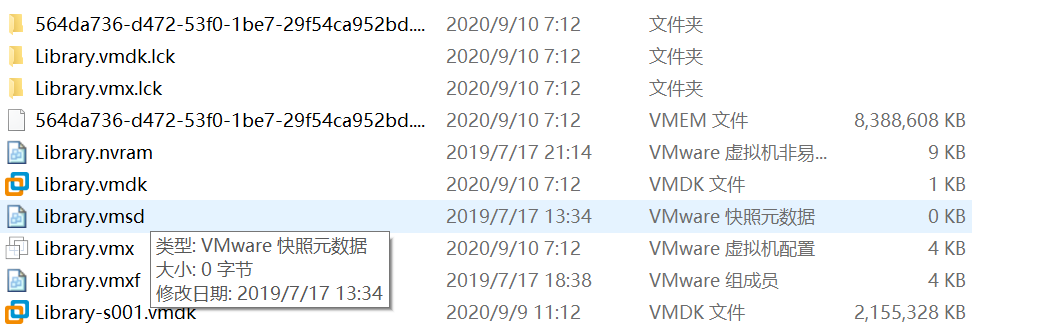
Emmm只是说有很多漏洞，应该是要拿到root权限



解压以后得到一个文件夹，跟进



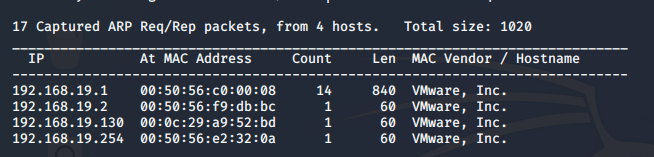
直接点击.vmx就可以了，顺便调回NAT模式就可以攻击了



# 0x01:探测靶机

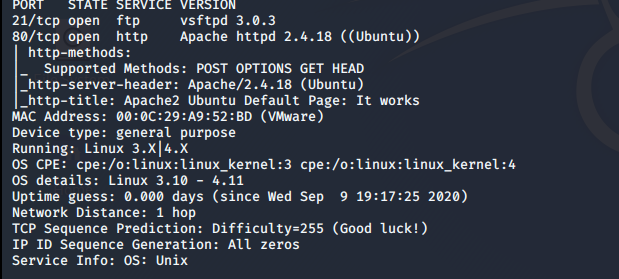
先用netdiscover 探测波靶机,排除.1,.2和.254可以确认靶机IP为192.168.19.130

命令:netdiscover -r 192.168.19.0/16

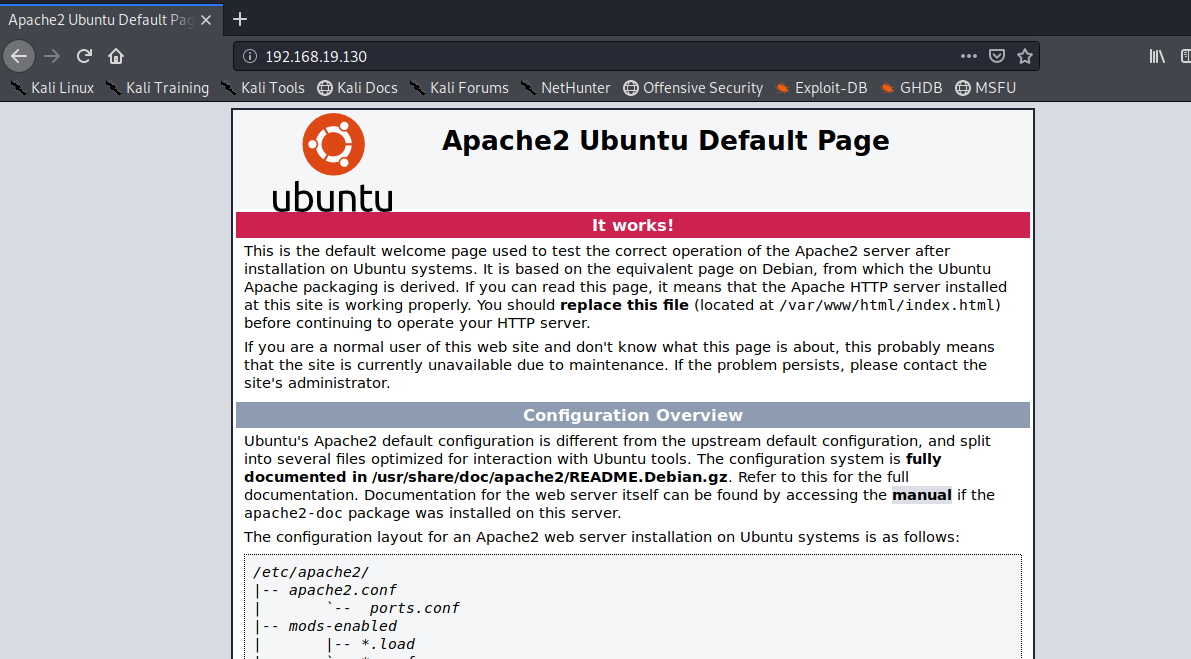


用nmap扫一波端口,只开了21和80端口

命令:nmap -A -sS -sV -v -p- 192.168.19.130

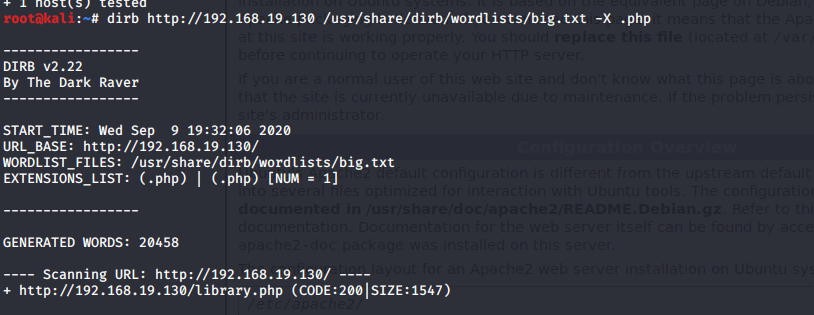


访问波IP可以正常访问开搞

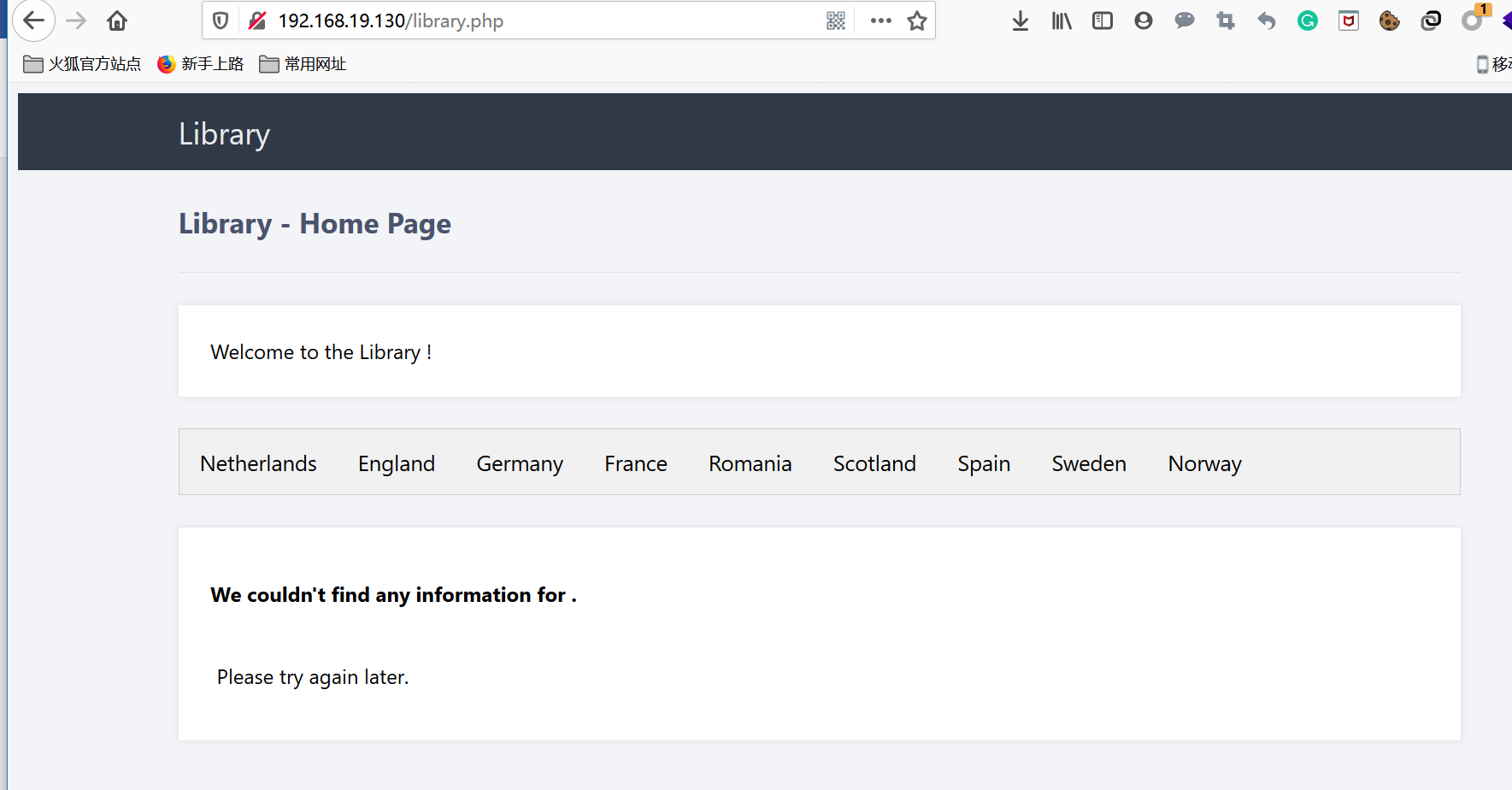


# 0x02:挖掘漏洞

首先正常用dirb扫描目录结果没扫到什么出来，那么只能用 -X .php最后扫出一个library出来



跟进一下Library是这样的



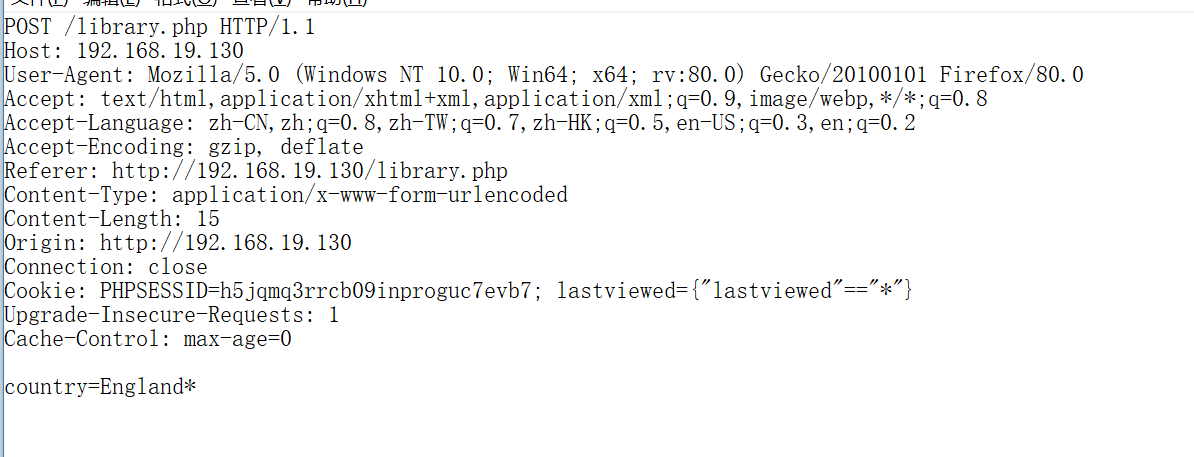
用Burp抓包的时候发现数据是这样的



Lastviewed后面是一堆乱码，直接用burp的解密功能，发现也是England也就是说当我们点击England这个标签的时候，country为England而且cookie也是一样也就是可能存在cookie注入



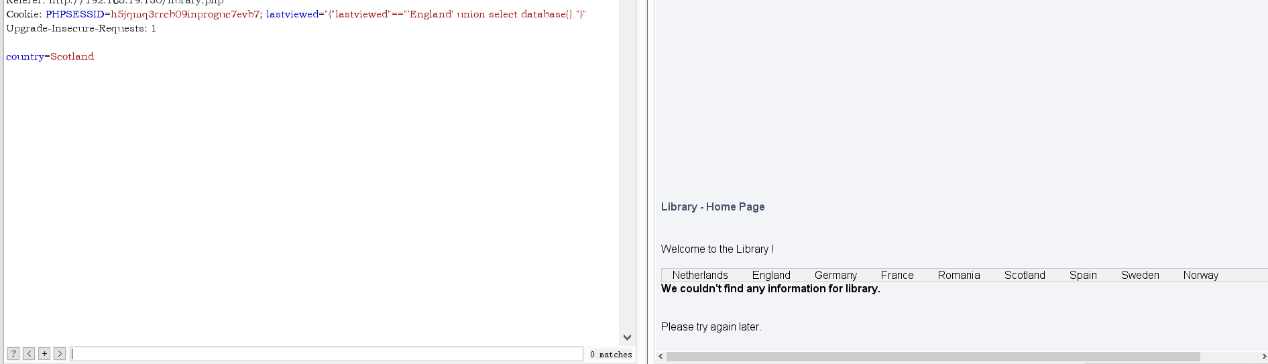
把文本复制下来让sqlmap去跑



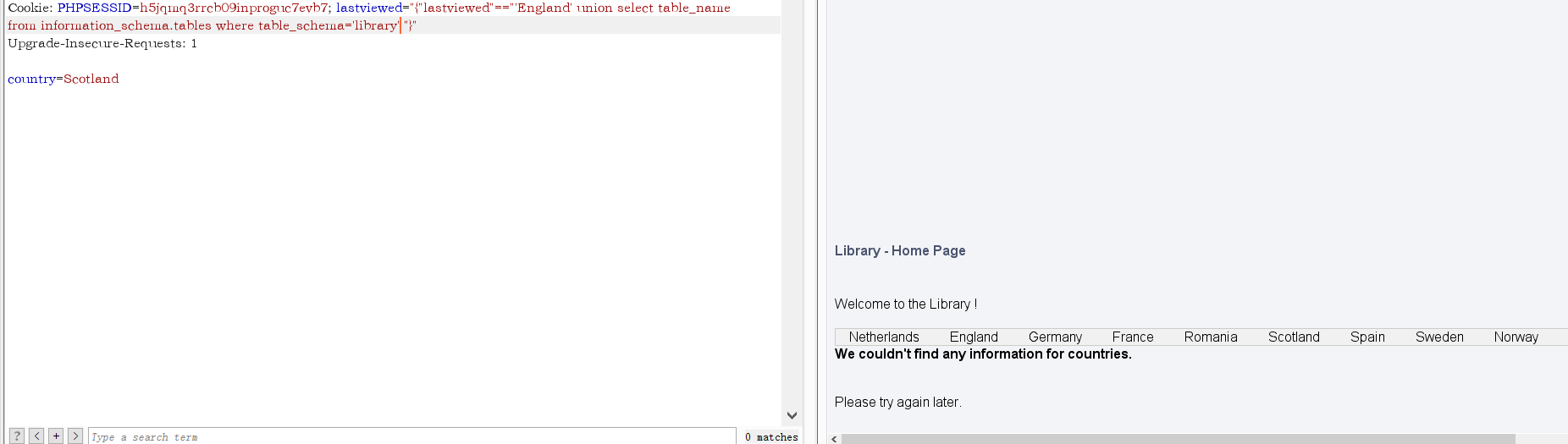
# 0x03:挖掘cookie注入

由于sqlmap死活跑不出来，被迫手注先找到库名为library

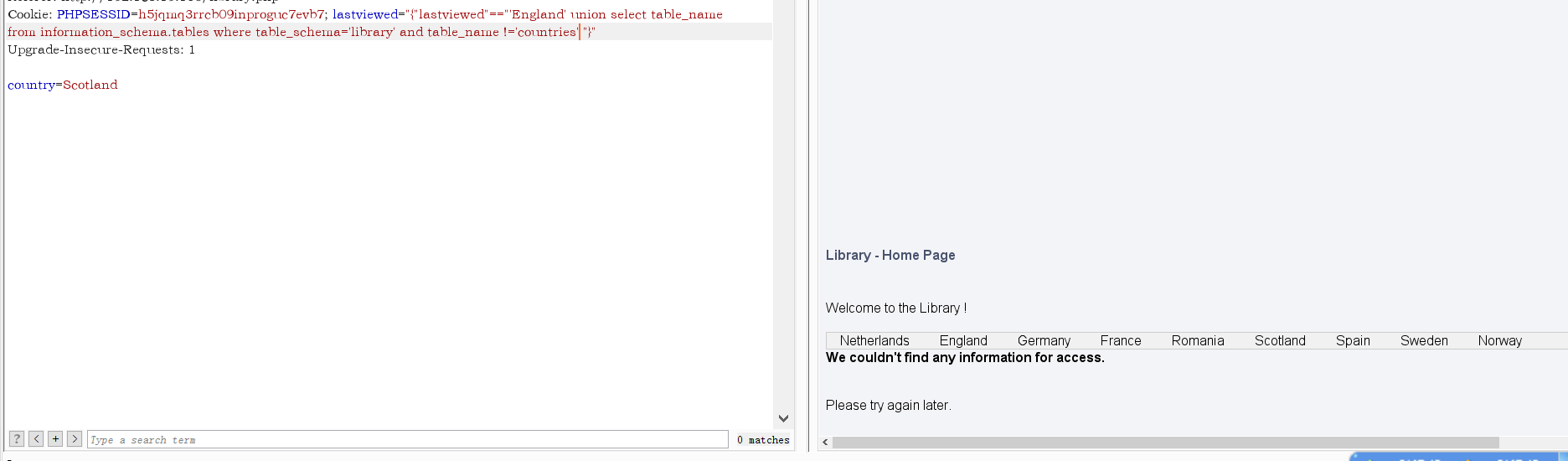
lastviewed="{"lastviewed"=="'England' union select database() "}"



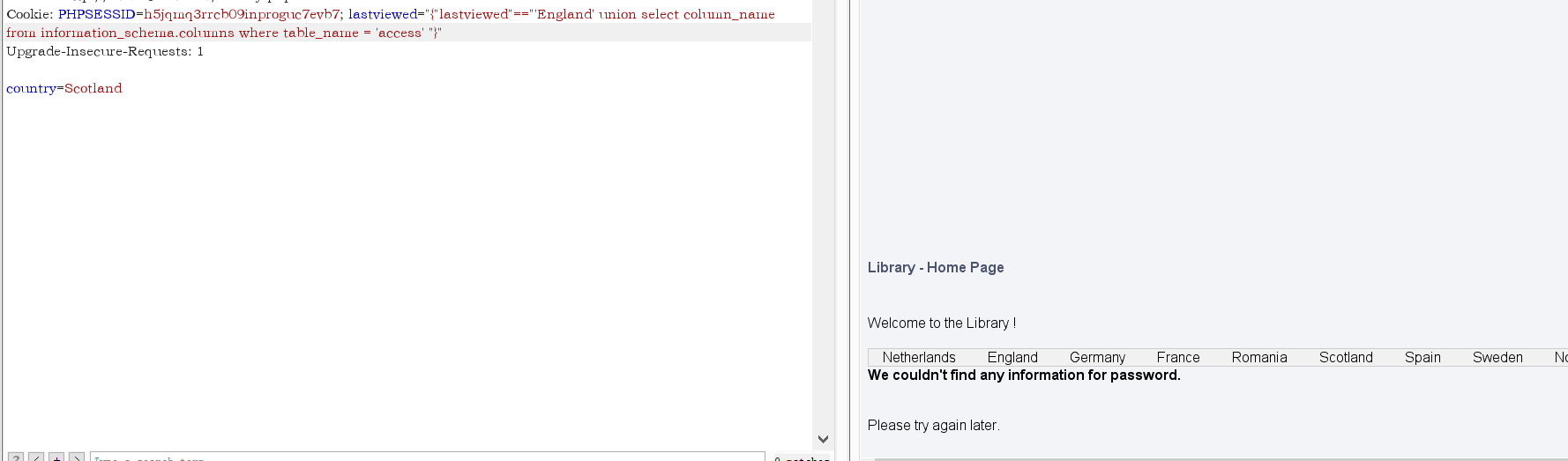
继续跟进库名到表名为countries



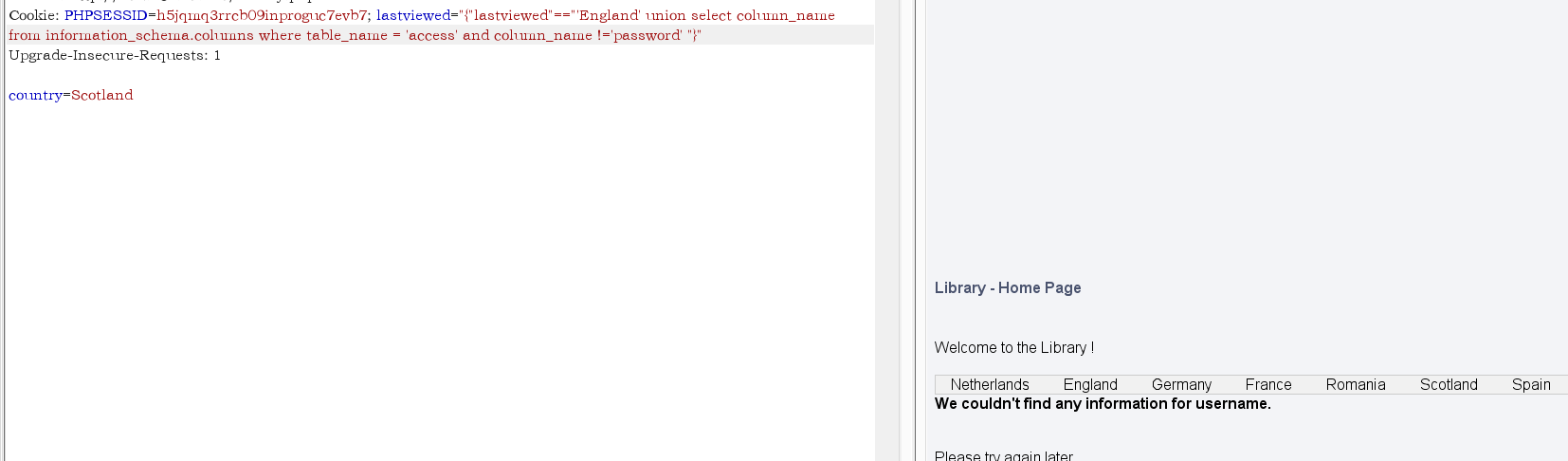
再跟进还有另外一个表access



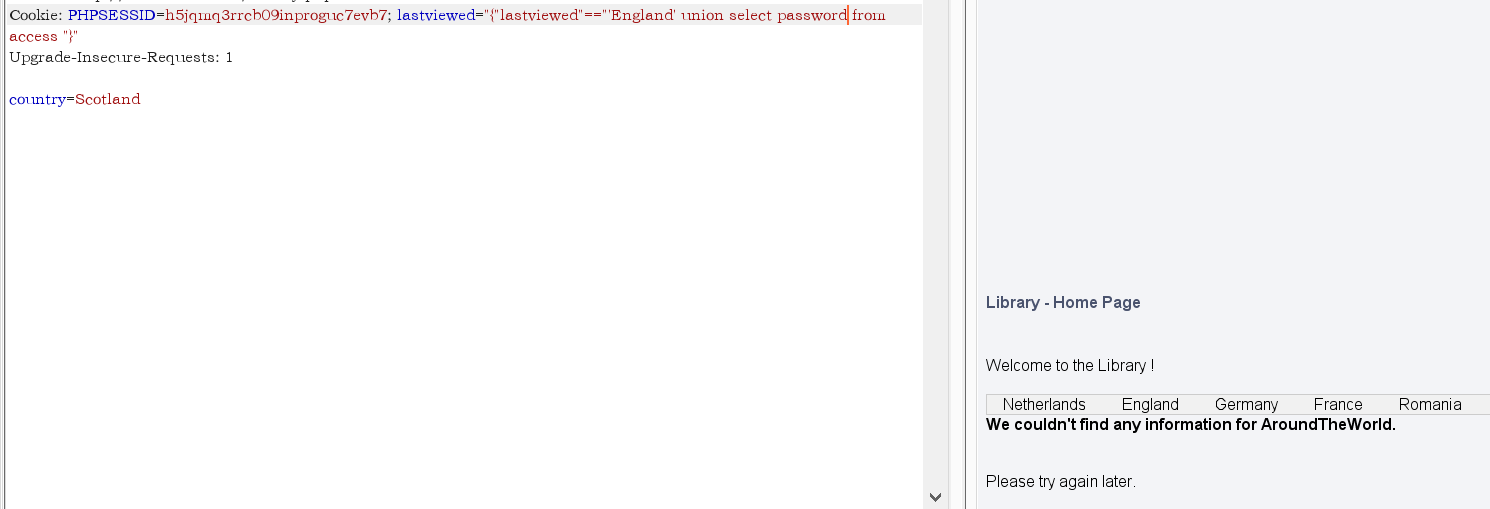
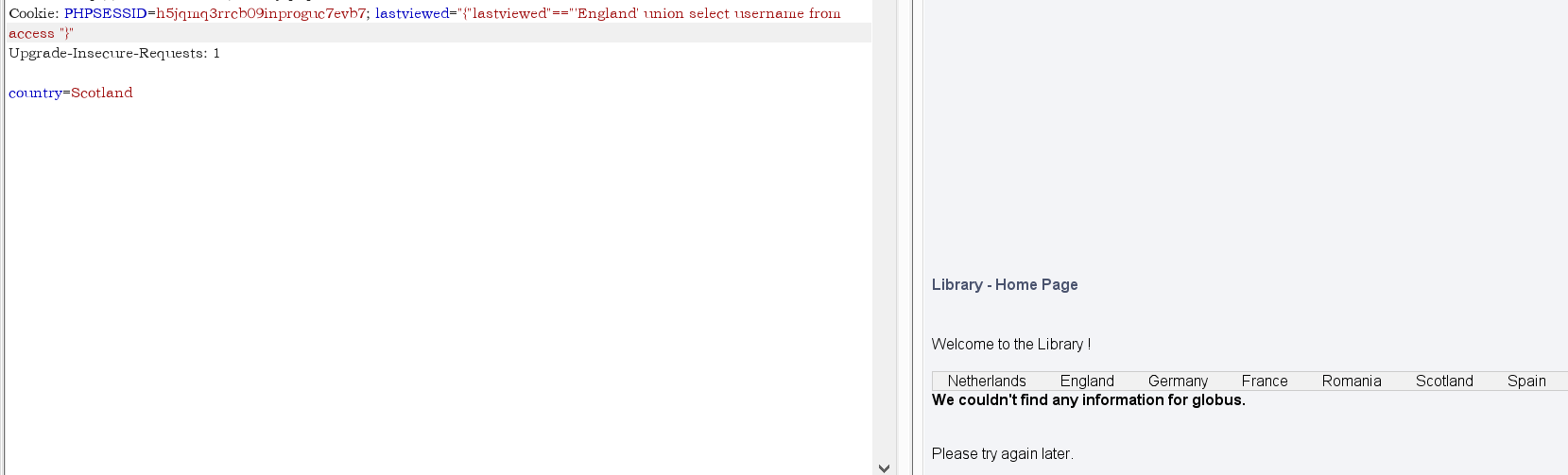
然后就没有了，选择其中的access表进行跟进发现一个password字段



继续跟进发现另外一个关键词字段username

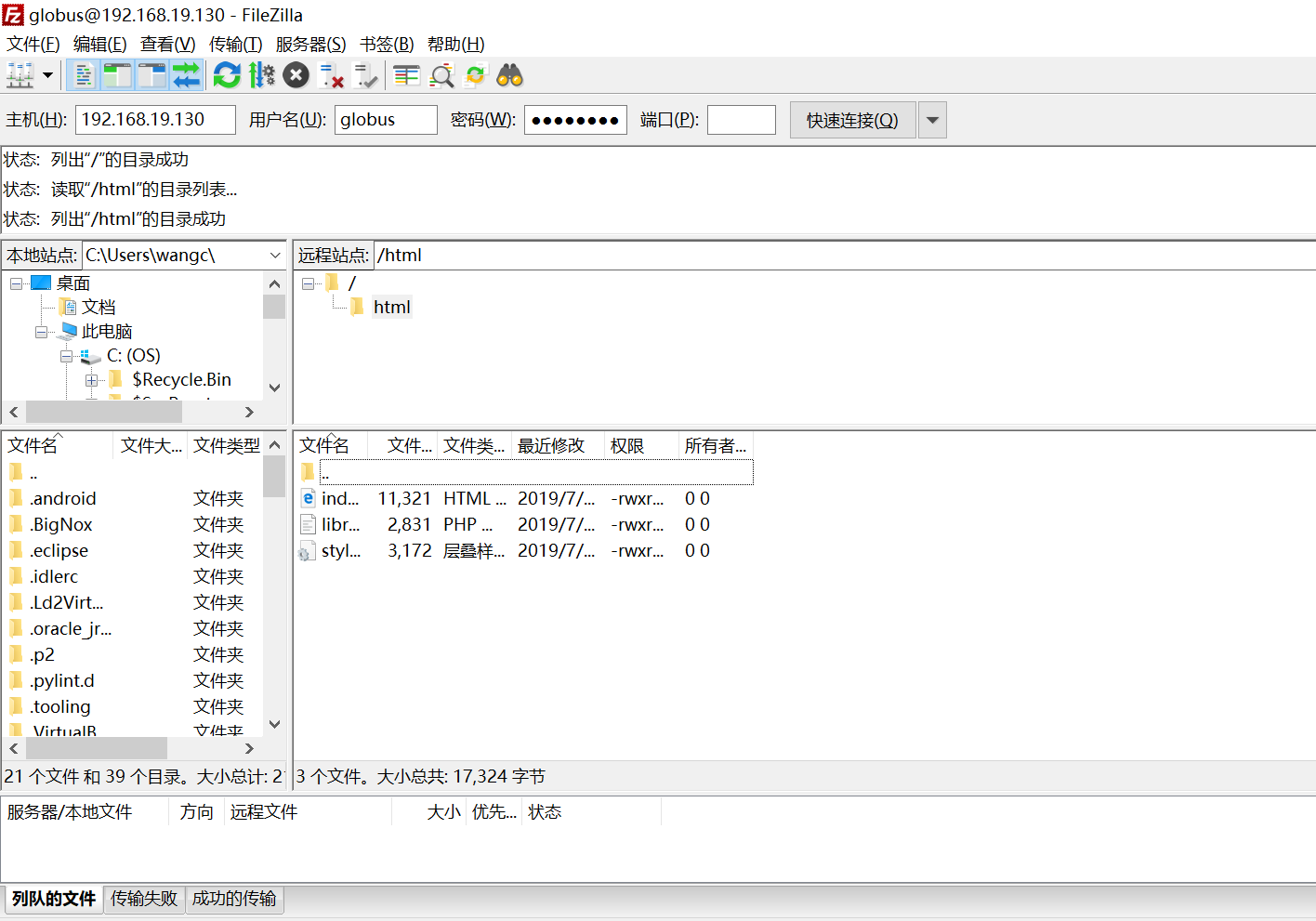


开始提取里面的信息得到username为globus,password为AroundTheWorld

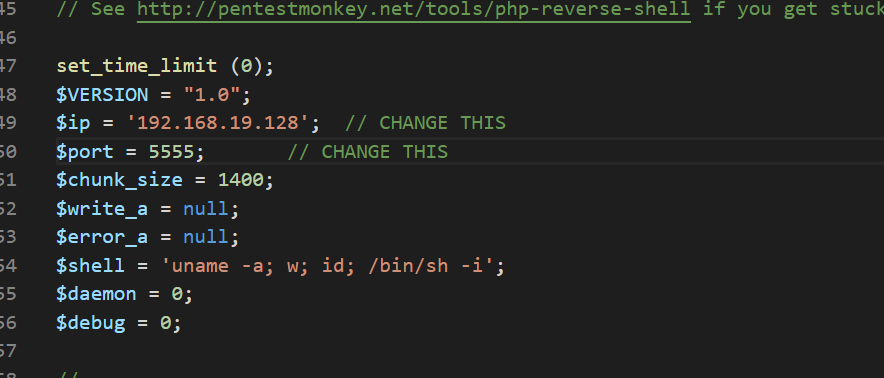


# 0x04:上传反弹shell

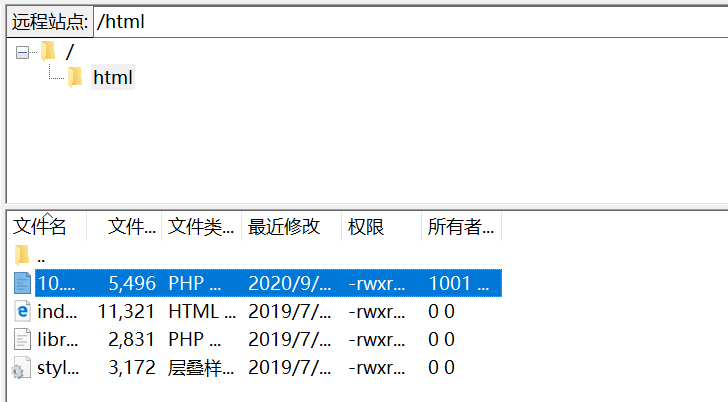
这里我为了操作方便用FileZilla连上去输入刚才得到的密码成功连上



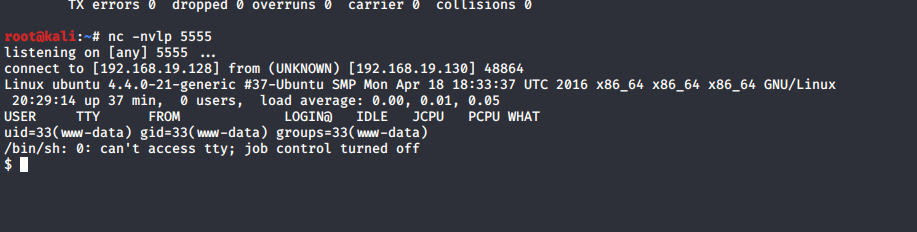
然后更改下kali自带的反弹shell



传上去，10.php就是我的反弹shell(一定要给权限为777否则是运行不了的)

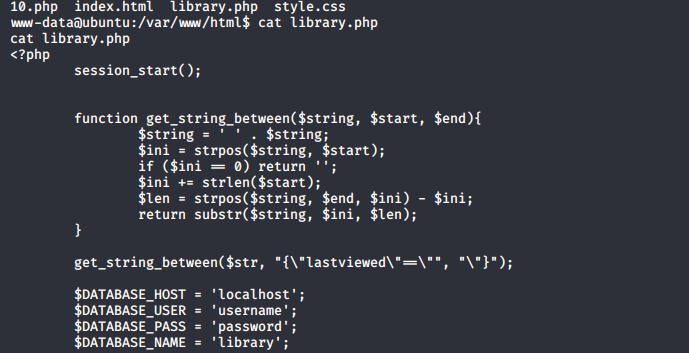


提前开启netcat然后访问页面得到反弹shell



# 0x05:提权

提权有多种方法，这里我偷懒选择最简单的拿到反弹shell以后cat一下library.php发现其它信息有个pass为password



然后直接su root输入密码为Password就可以了。。。。。

