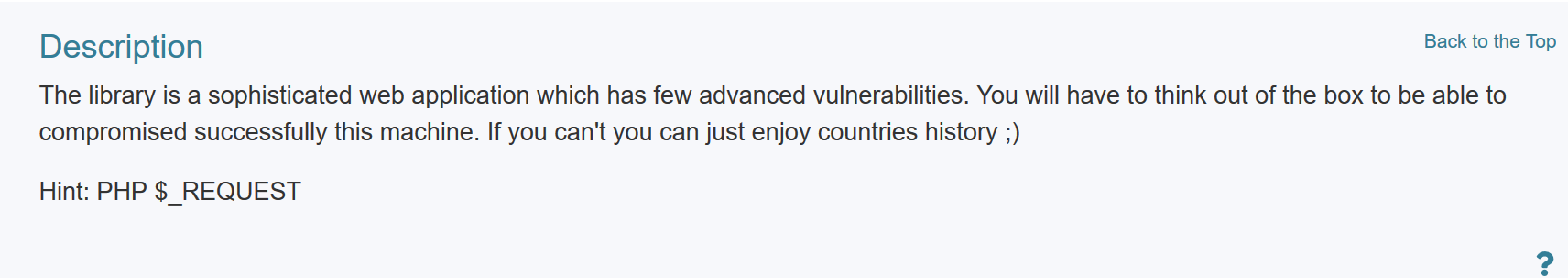
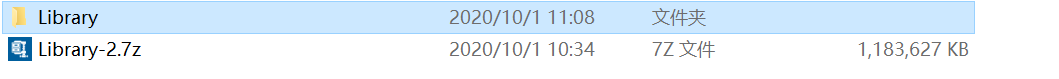
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/the-library-2,335/>

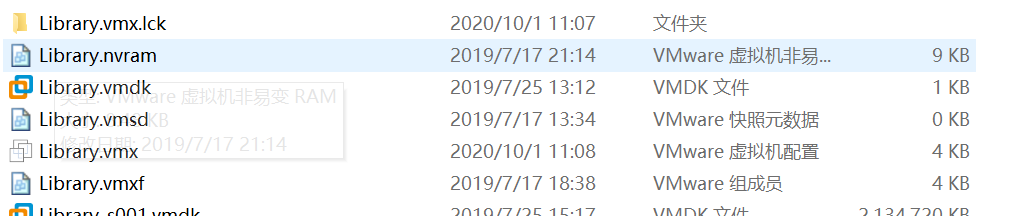
好像没啥有用的信息。。。。。



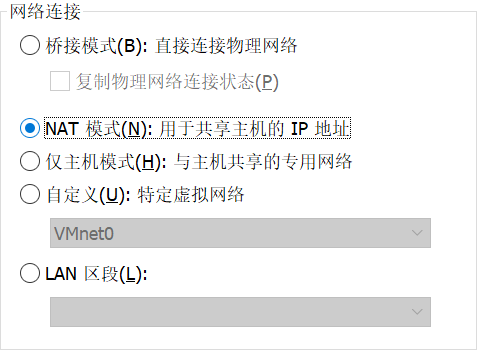
下载完后解压有个文件夹跟进



跟进以后双击.vmx文件



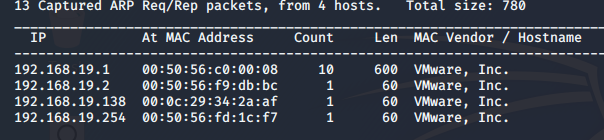
自动安装好，然后记得调回NAT模式就可以运行了



# 0x01:探测靶机

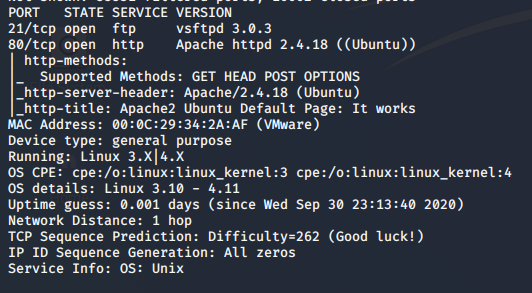
还是先用netdiscover探测波靶机，排除.1,.2和.254可以确认靶机IP为192.168.19.138

命令:netdiscover -r 192.168.19.0/16

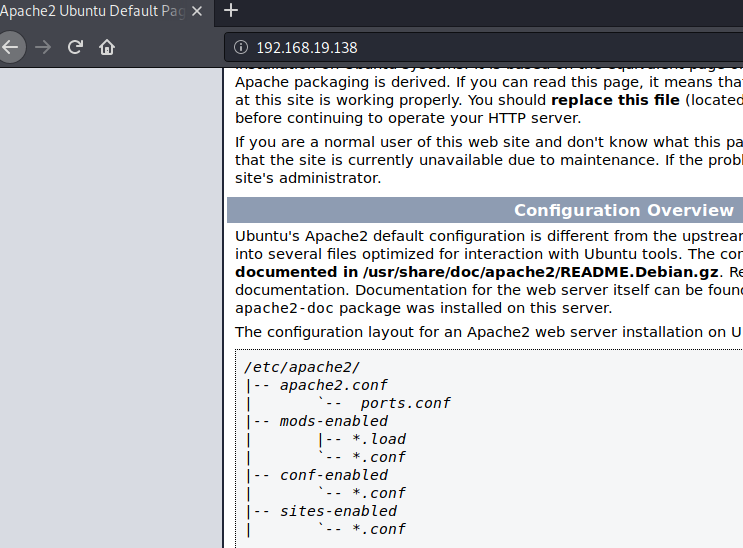


然后开始用Nmap探测波端口,这次只开了21和80端口

命令:nmap -A -sS -sV -v -p- 192.168.19.138

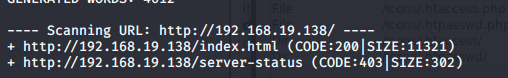


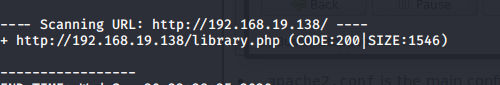
访问波IP正常回显，开搞



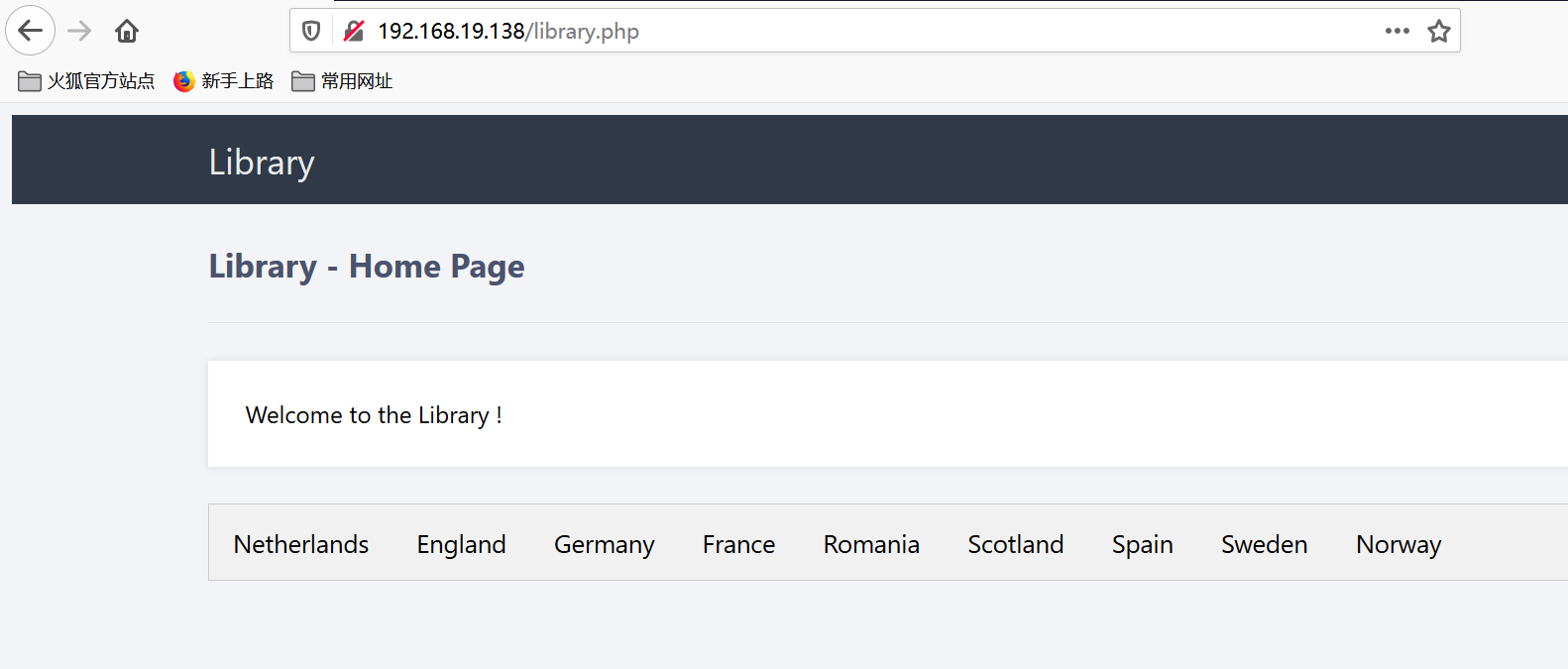
# 0x02:漏洞挖掘

由于不是正常的HTTP服务先用dirb探探路，由于点进去以后都不是正常页面只能扩展后缀名扫到一个library.php的

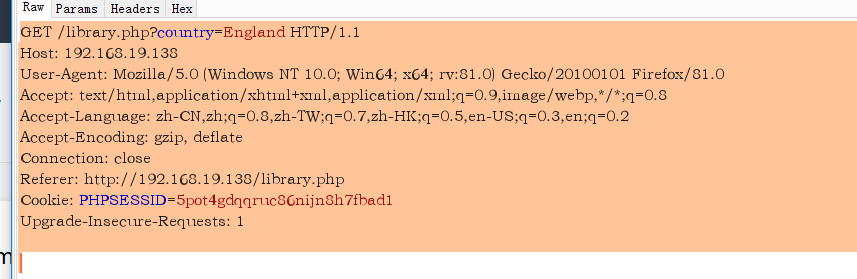




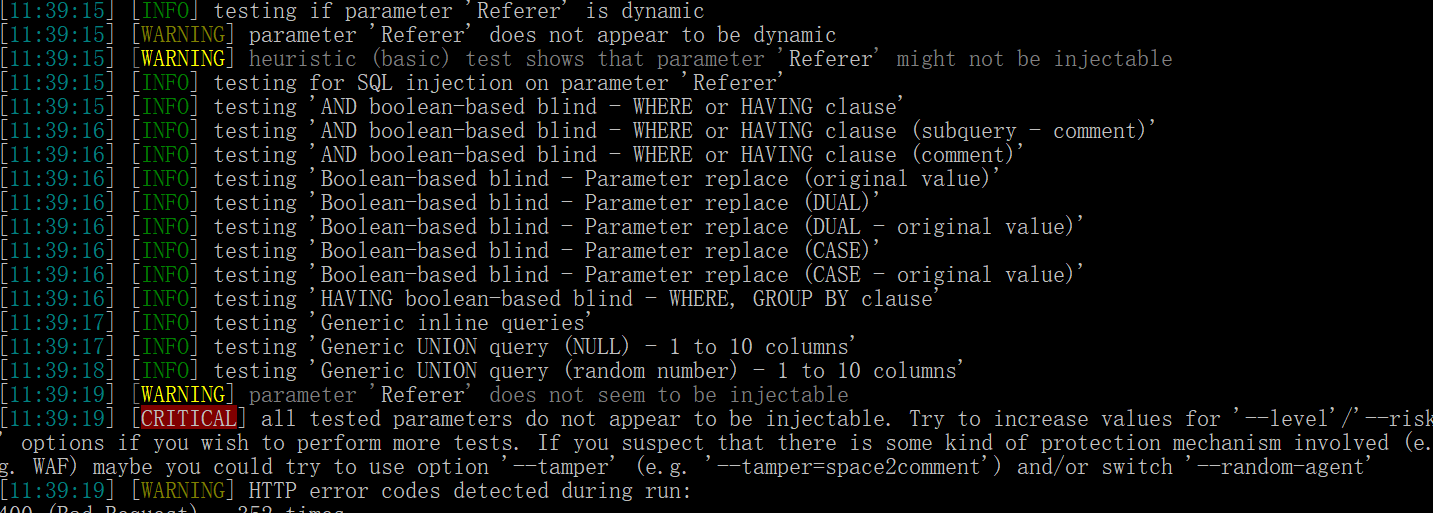
跟进一下是个有功能的页面了



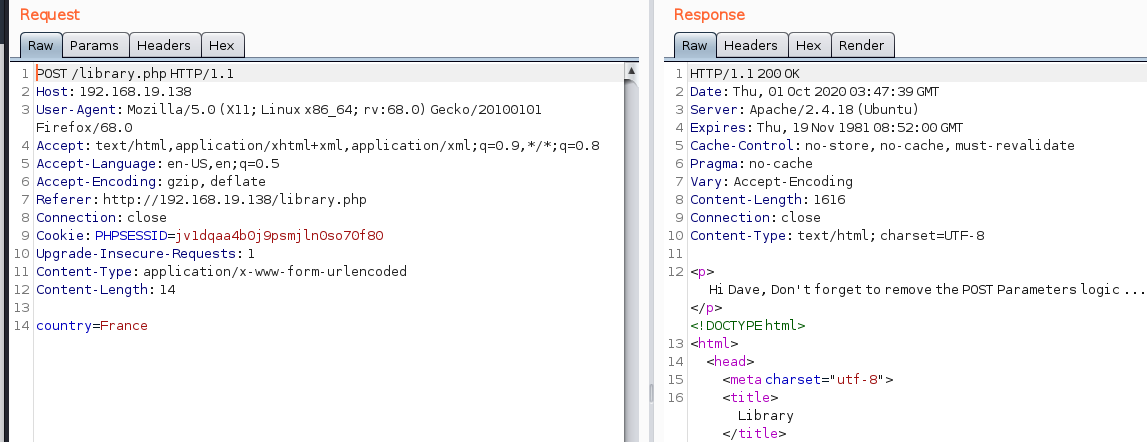
然后尝试抓包发现有参数可控，那么尝试丢到sqlmap里面



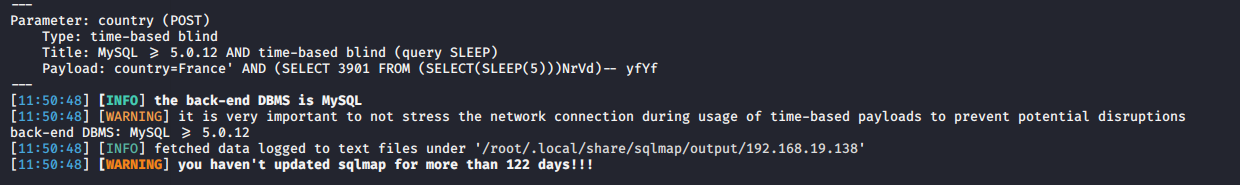
然而失败了



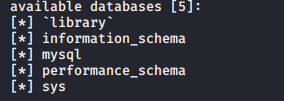
既然这样不行就尝试把GET换成POST也是正常回显



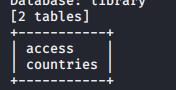
那么保存然后丢到sqlmap里面这次可以跑出来了



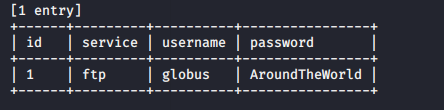
输入—dbs以后发现有几个库



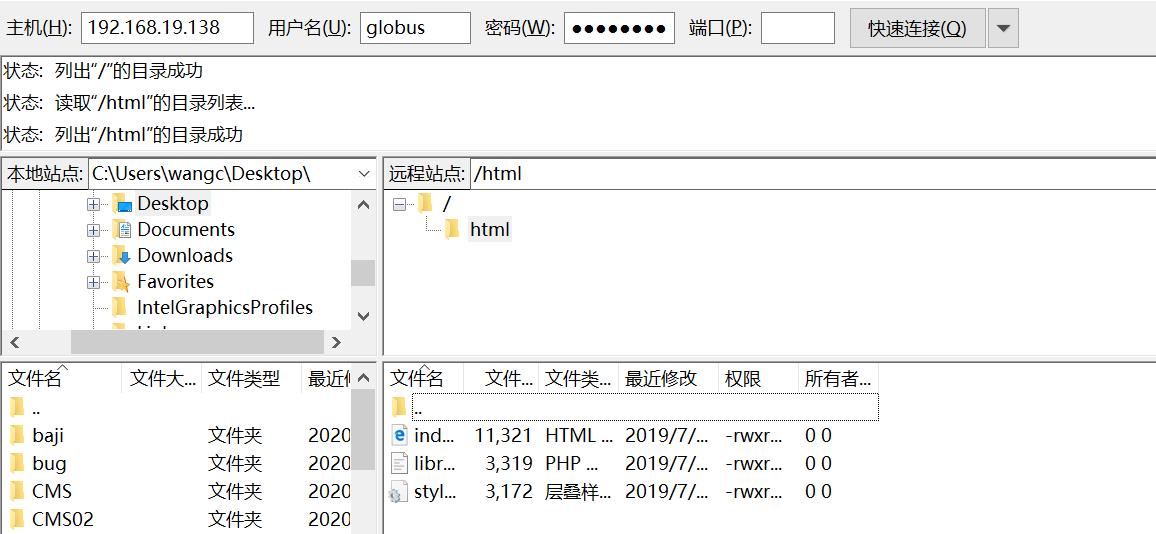
这里发现library莫名其妙多出个单引号实际上是不需要的，由于是靶机直接狠点指定Library先不要—dump先看看里面有什么表，然后发现有个access 和countries



直接开始—dump跑access表里面的内容，得到一个ftp的账号和密码

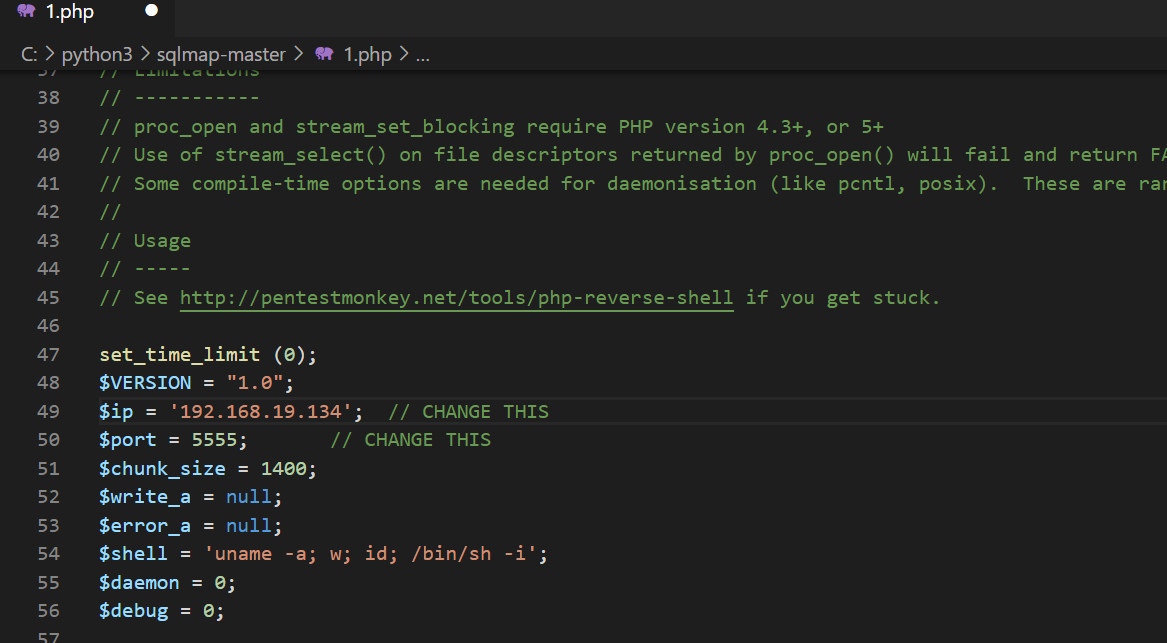


之前在扫描端口的时候知道开了21端口直接上FileZilla

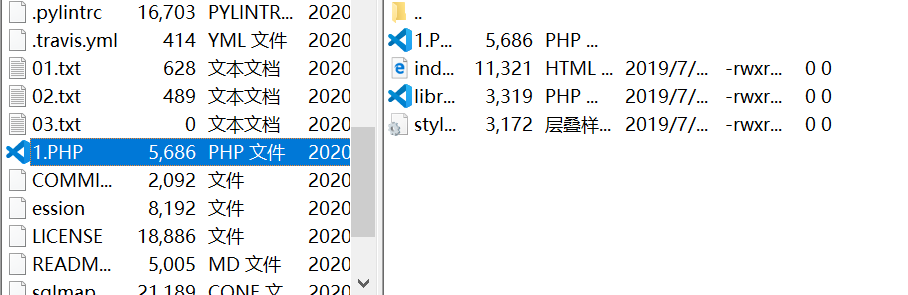


# 0x03:上传反弹shell

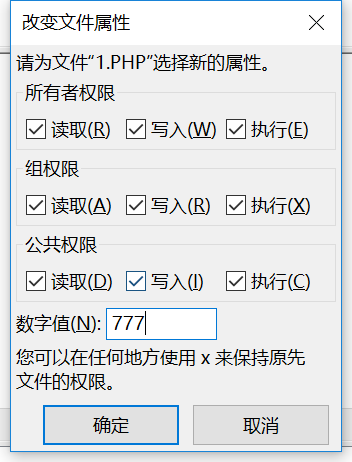
既然在html下放的是对应的文件，理论上来说把反弹shell放进去然后在访问它就可以得到一个shell的，这里我把kali的反弹shell复制到本地上，方便等下上传。



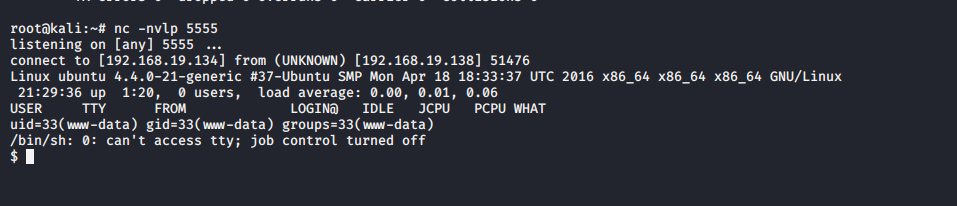
这里正常上传的话似乎做了点限制.php无法上传，变成.PHP以后可以绕过上传



权限记得给为777方便运行



然后提前开启netcat和端口，前端访问一波/1.PHP就可以得到反弹shell了



# 0x04:挖掘信息

本次没有提权，在浏览信息跑到/var/mail/welcome那里可以直接得到root的密码直接su切换成功

