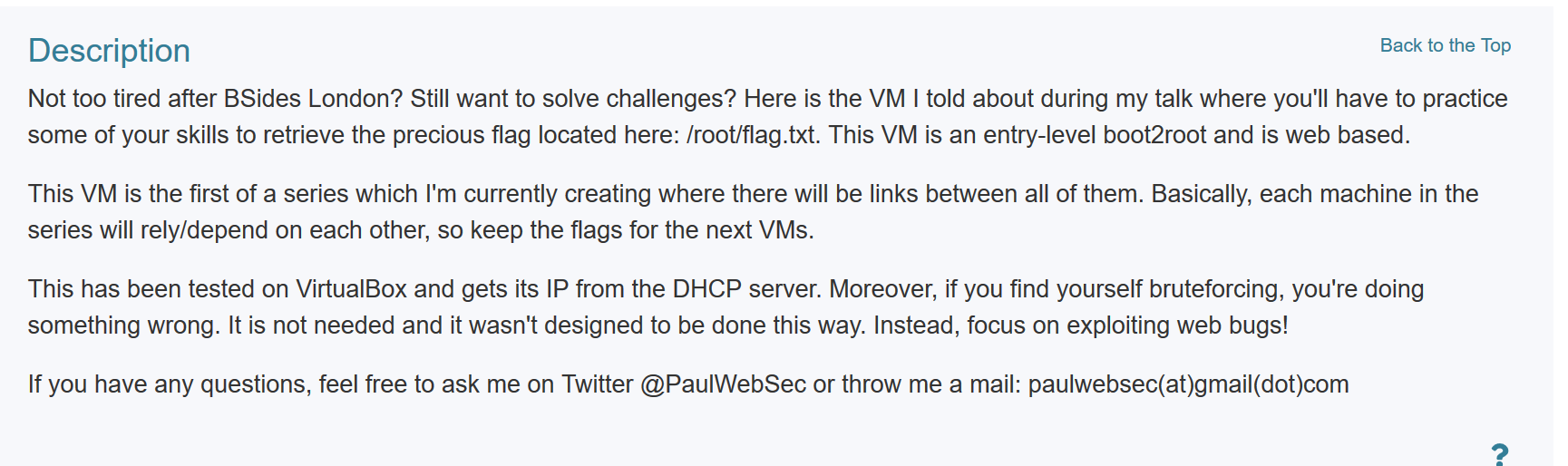
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/secos-1,88/>



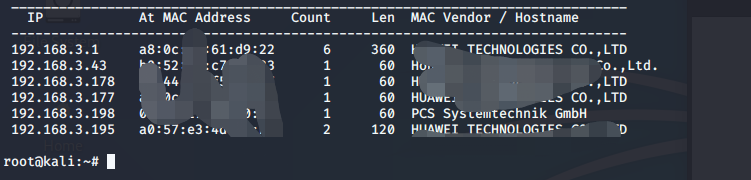
目标是拿到/root目录下的flag同时建议用VirutalBox来运行靶机

由于是用VirtualBox所以解压后打开设置成桥接模式就可开搞了

# 0x01:探测靶机

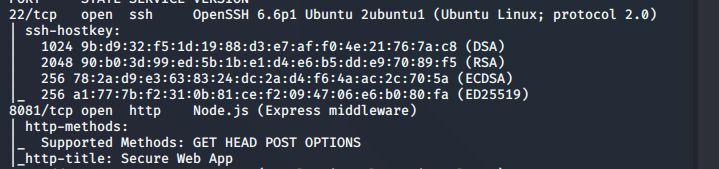
还是先用netdiscover探测波靶机,直接找PCS，确认靶机IP为192.168.3.198

命令:netdiscover -r 192.168.3.0/16

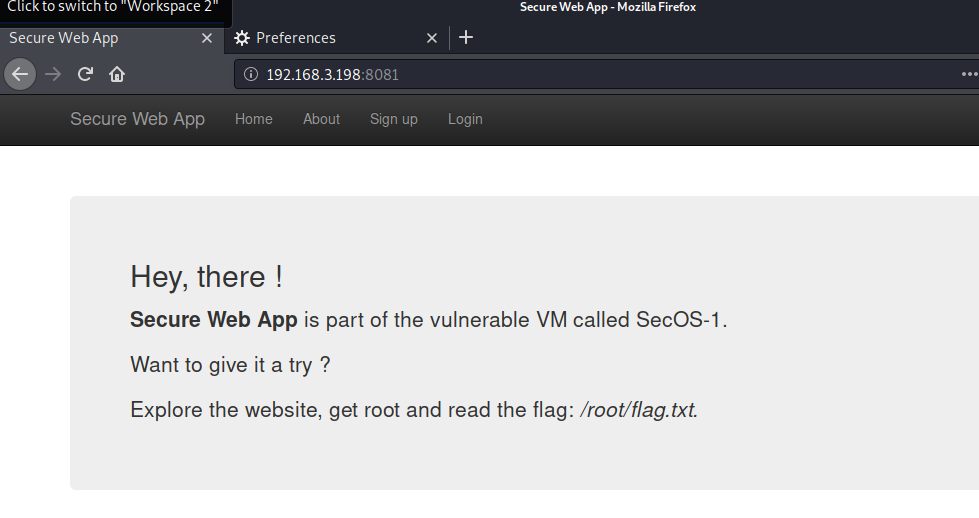


然后开始用nmap探测一下端口，发现居然没有开80而是8081有点奇怪。。。。

命令:nmap -A -sS -sV -v -p- 192.168.3.198

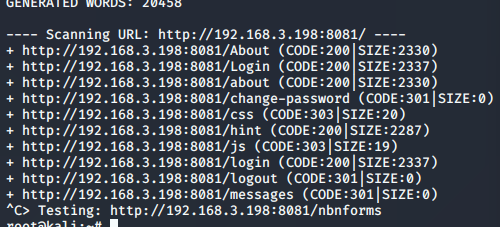


访问一下IP可以正常回显开搞



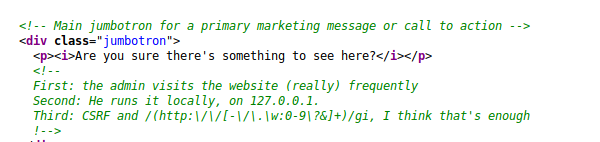
# 0x02:挖掘漏洞

先用dirb扫到一个Hint



跟进一下

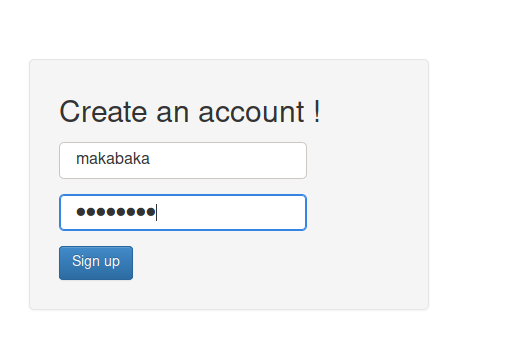
首先是admin经常访问页面，第二他是本地运行，第三存在CSRF漏洞



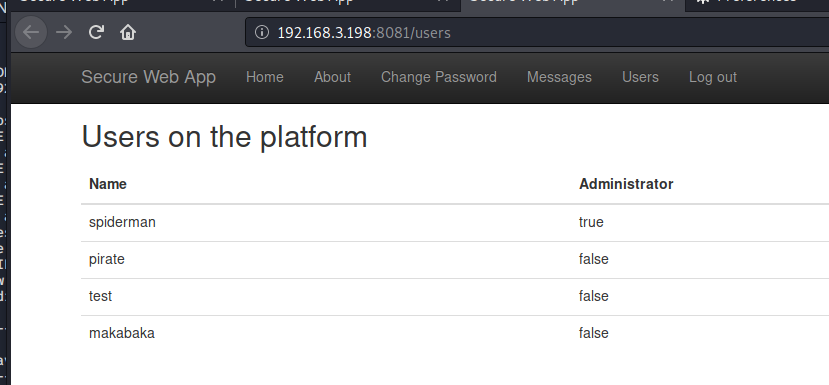
既然这里有个注册页面那先注册一个号

Makabaka

makabaka

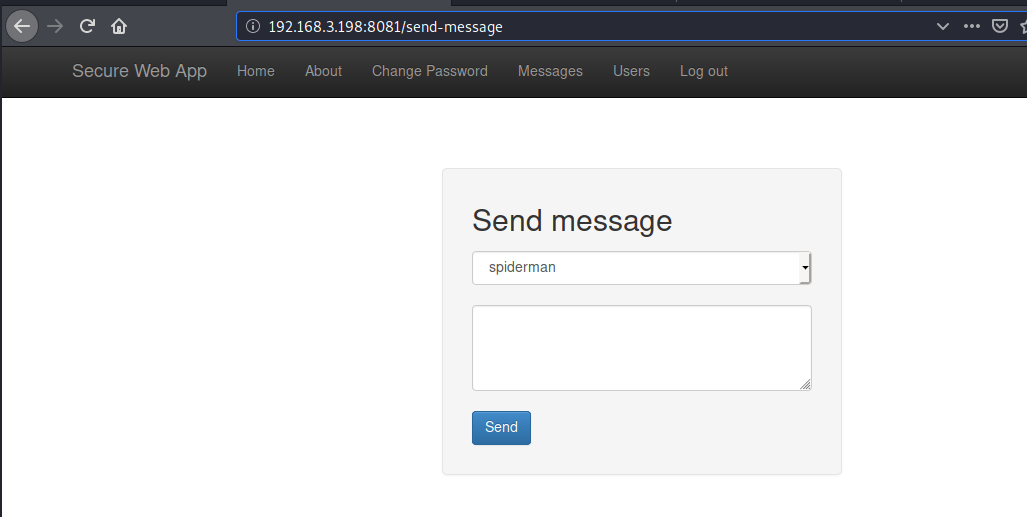


登录以后多了两个功能一个是查看用户组

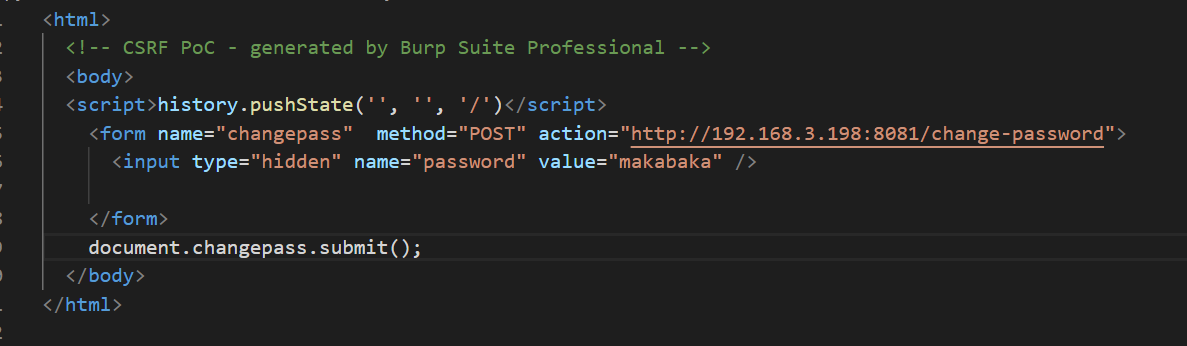


# 0x03:利用CSRF漏洞

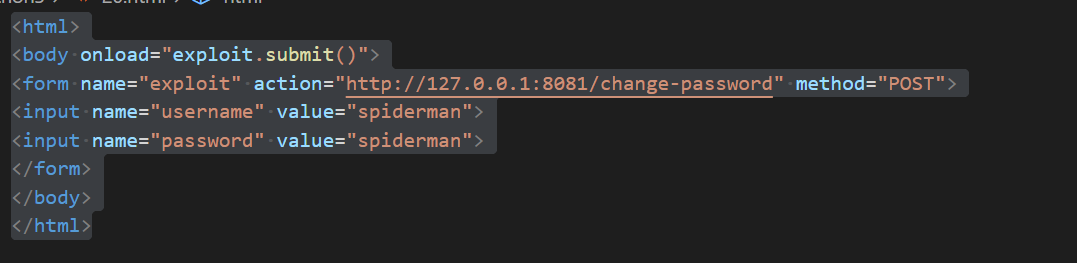
一个是给管理员发送信息，既然是可以发信息给管理员那么就存在一个漏洞，在修改密码那里把当前用户改成管理员用户用BURP生成POC发给管理员



用burp的生成CSRF功能复制代码到VC里面，顺便更改一下触发条件保存成20.html(burp的CSRFpayload其实并不是那么好，要更改触发条件)



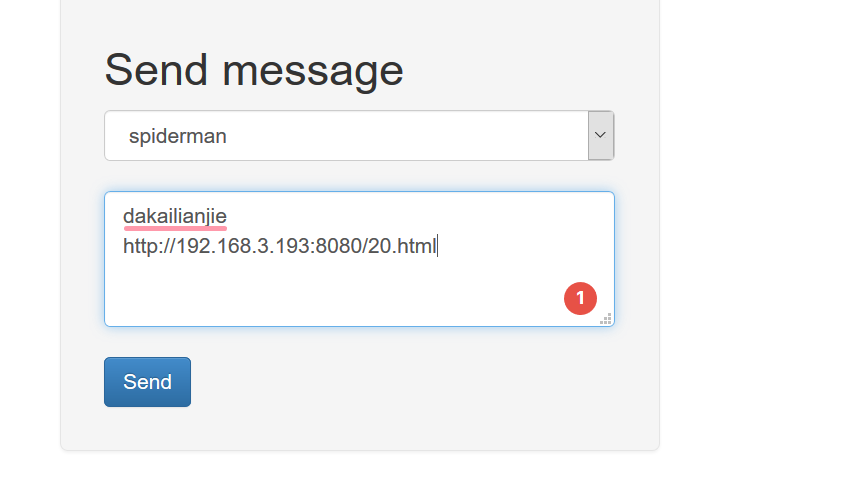
当然这个版本并不成功还得改一下最后变成这样



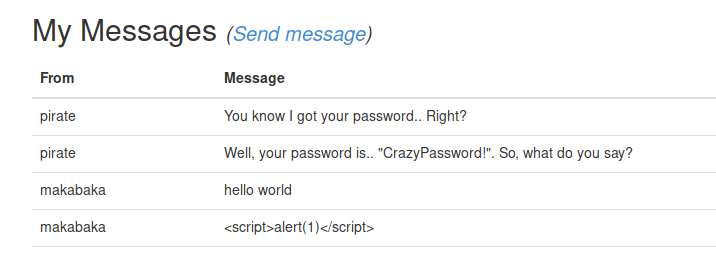
然后把该文件传到kali上面去，顺便在上面开启python共享模式方便管理员访问



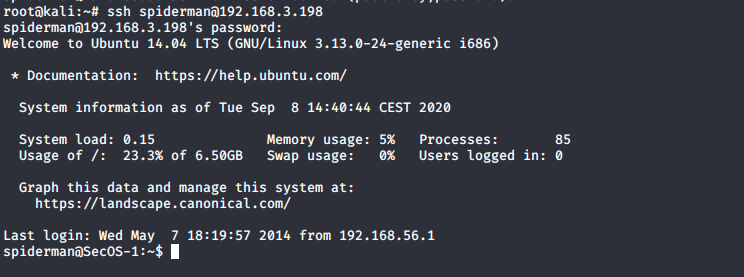
在发送信息这里加上链接等待管理员点开就行了



几分钟后输入spiderman的新账号以后成功登录，顺便在message这里看到一个密码



把密码复制下来尝试登录一波SSH，成功登录



# 0x04:提权

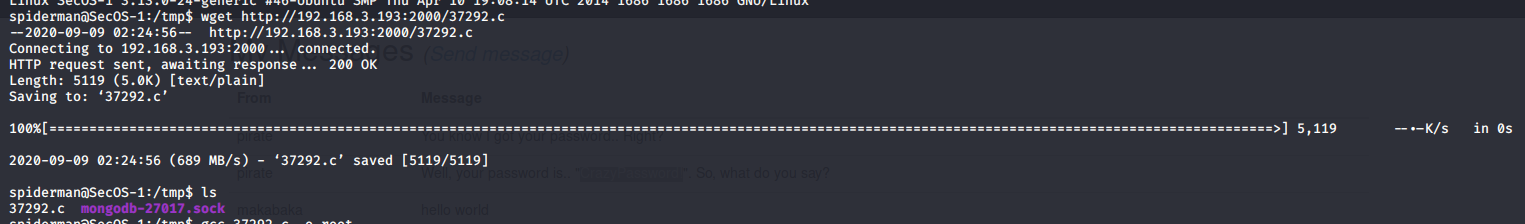
先用了sudo -l结果还是一如既往的失败，换成Uname -a，查到版本号为3.13



在exploitdb上找到一个



传上去



运行方法很简单直接gcc 37292.c -o root 然后./root就可以运行成功了，得到root权限顺便读到flag

