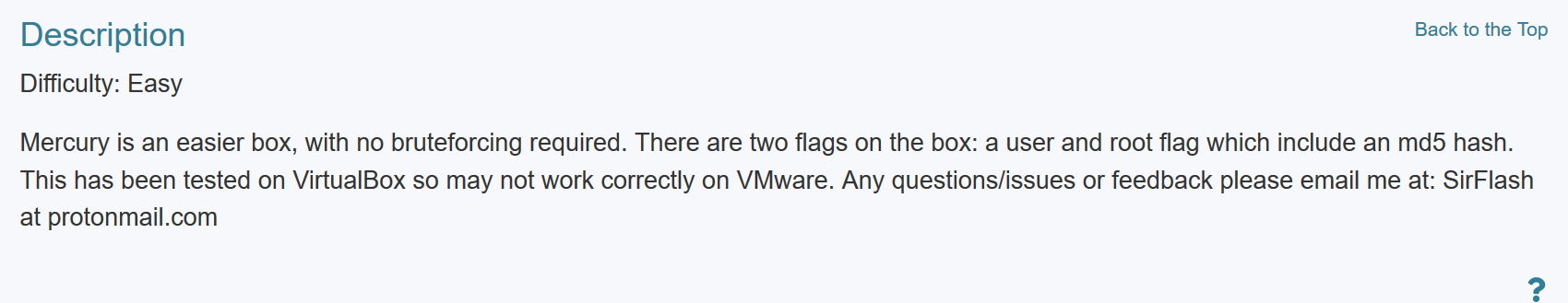
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/the-planets-mercury,544/>

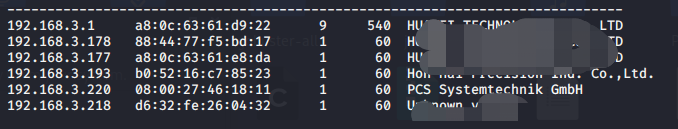
简单级别，2个flag建议在virtualbox下运行



# 0x01:探测靶机

由于是在virtualbox这里就偷懒了，netdiscover启动，直接找PCS确定靶机IP为192.168.3.220

命令:netdiscover -r 192.168.3.0/16

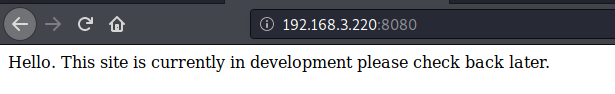


开始用nmap探测端口，这次只开了22和80端口

命令:nmap -A -sS -sV -v -p- 192.168.3.220



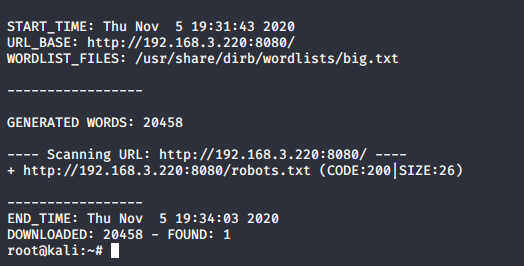
访问一波8080端口可以正常访问



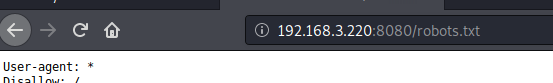
# 0x02:挖掘隐藏目录

这里首先肯定用目录扫描器探路一波，然而有点奇怪的是只扫出个/robots.txt

命令:dirb <http://192.168.3.220:8080> /usr/share/wordlists/big.txt



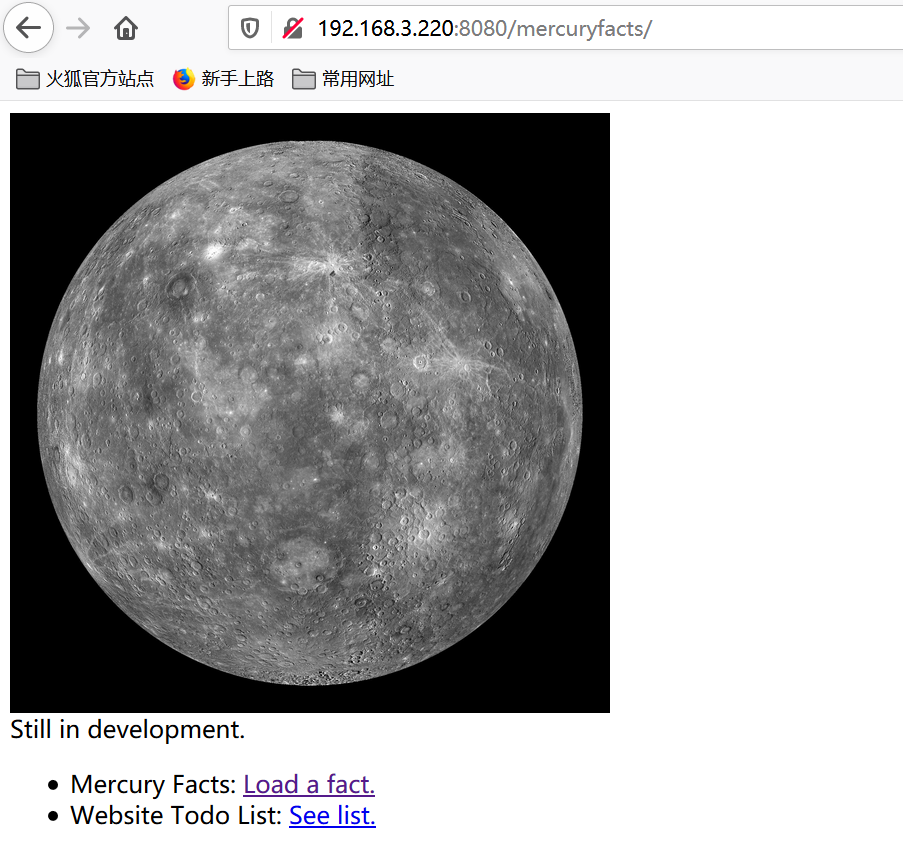
跟进一下也没什么东西



这里只能输入常见目录哦吼但是看到有个东西/mercuryfacts

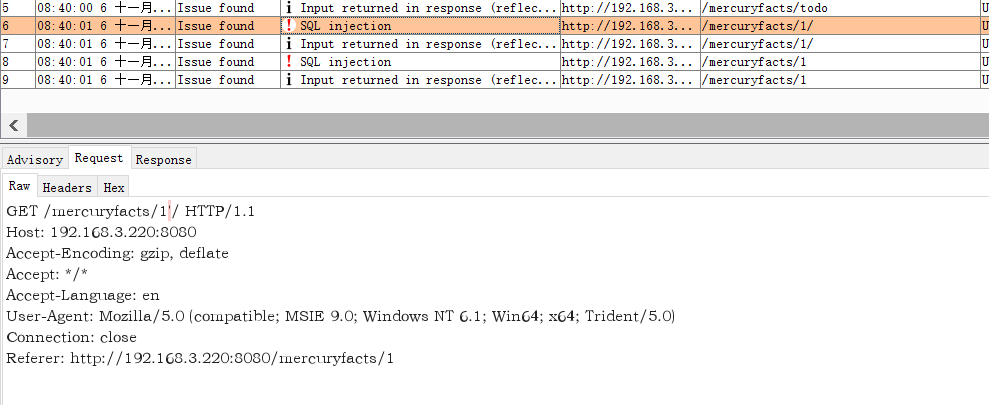


同时终于有个正常页面了



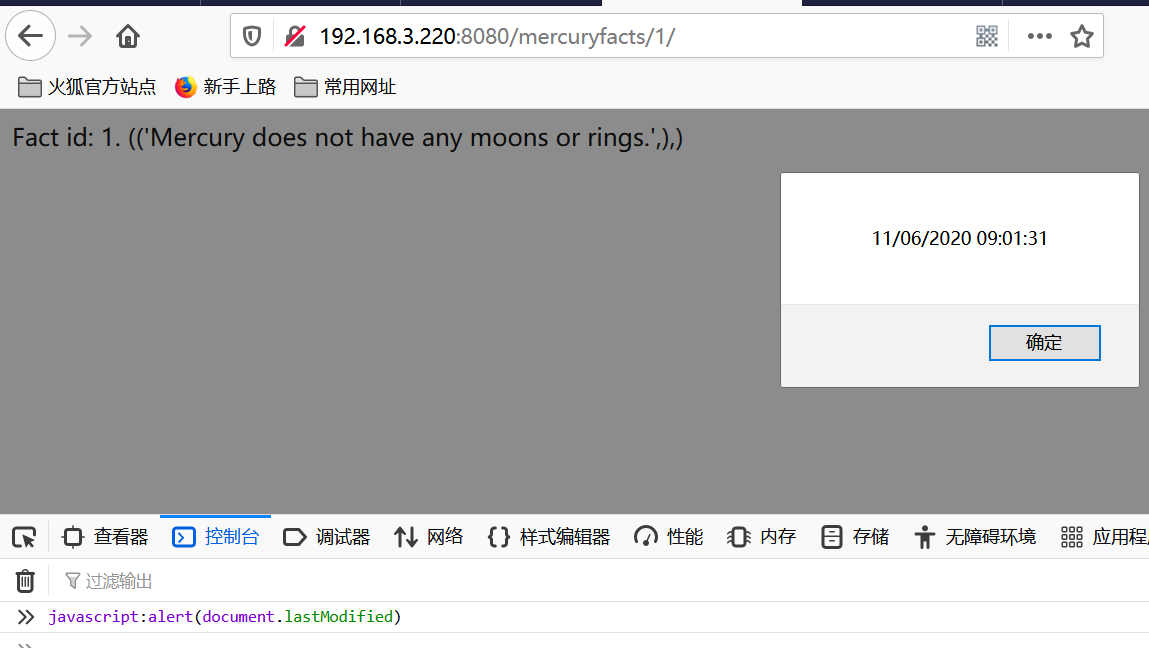
# 0x03:挖掘伪静态注入

这里既然得到/mercuryfacts这个页面，由于是自己的靶机，直接BURP active scan启动，找到了一些SQL注入漏洞，原来是伪静态注入

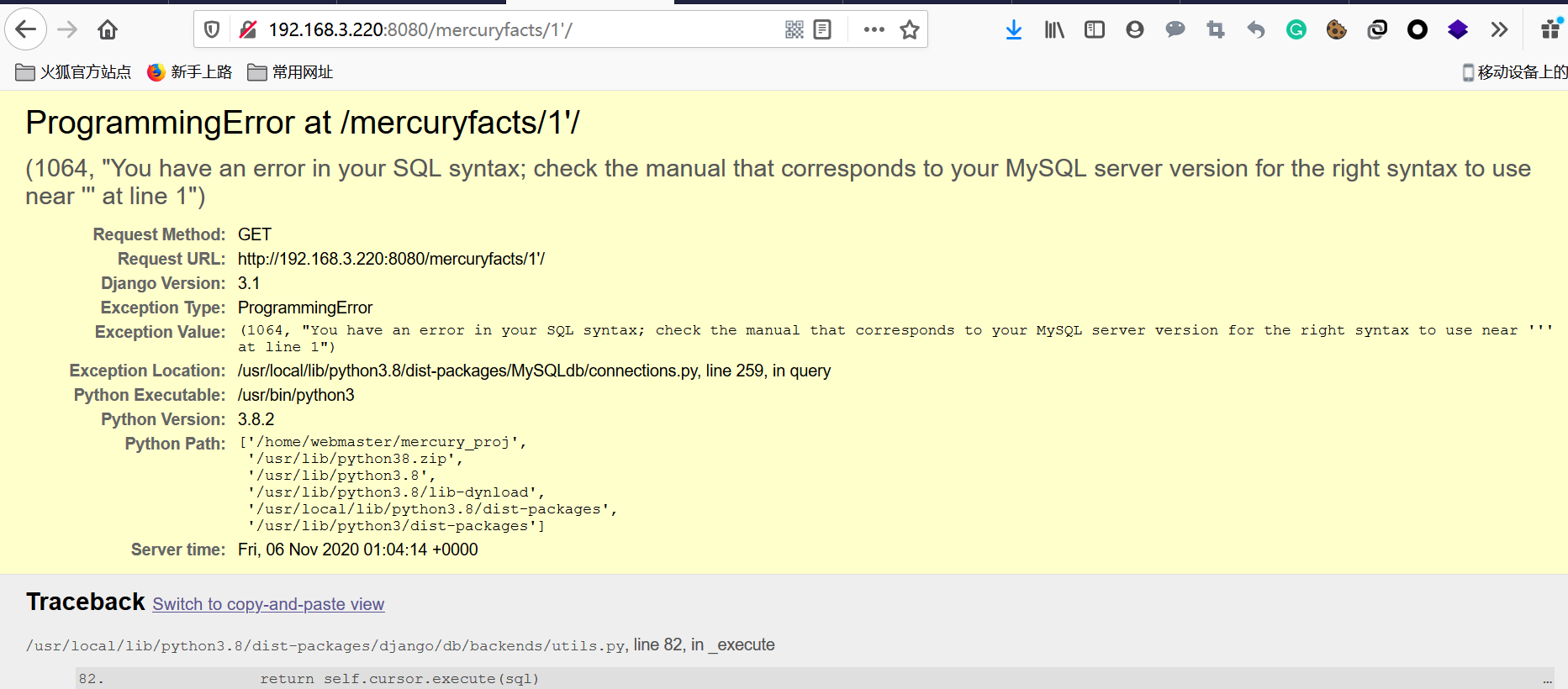


这里说一下伪静态注入，平时我们挖掘SQL漏洞，大部分页面是.php?id=xx这样子的，而有些页面为了保护自己，会把自己伪装成表面上看上去是静态页面(比如.html,htm和/这样),实际上仍然是动态页面，并且存在数据交互的网站

这里在<http://192.168.3.220:8080/mercuryfacts/1/，按F12>打开控制台输入javascript:alert(document.lastModified)，如果弹窗了就证明是一个伪静态的页面

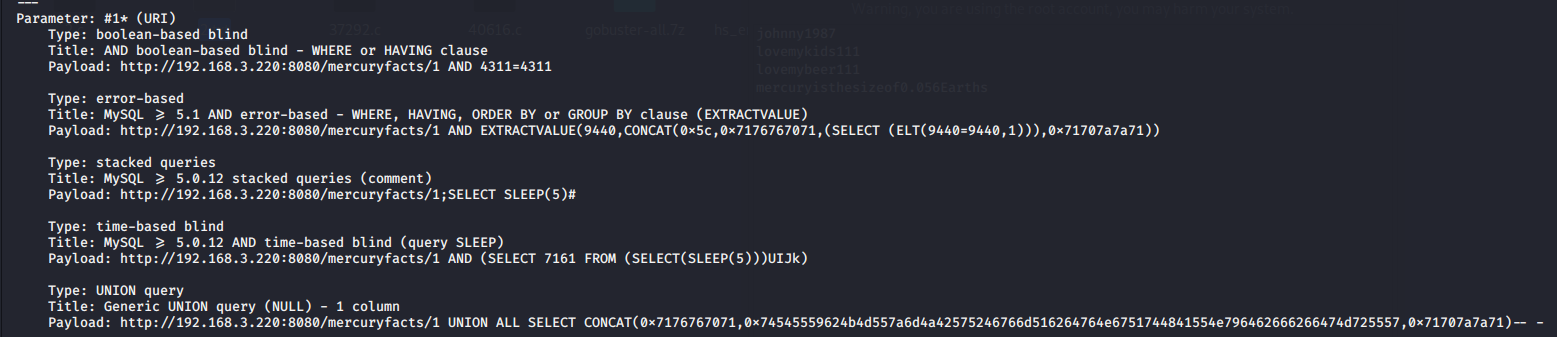


同时加入’直接报错



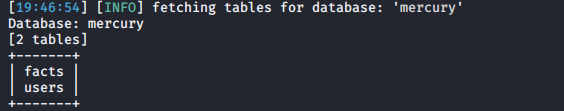
Sqlmap启动,可以跑出来

命令: sqlmap -u <http://192.168.3.220:8080/mercuryfacts/1> --batch



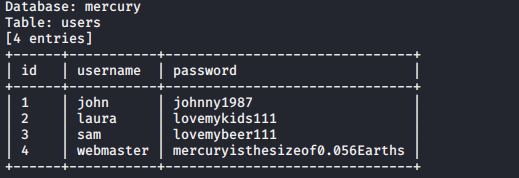
然后跑数据库名字，果断选择User

命令: sqlmap -u <http://192.168.3.220:8080/mercuryfacts/1> --dbs --batch

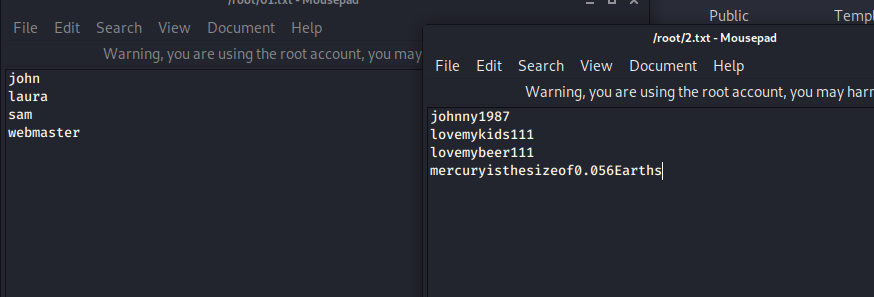


直接对着user撸数据出来

命令: sqlmap -u <http://192.168.3.220:8080/mercuryfacts/1> --dbs -D users --dump --batch

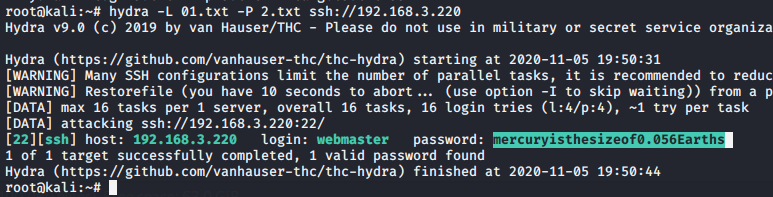


保存下来

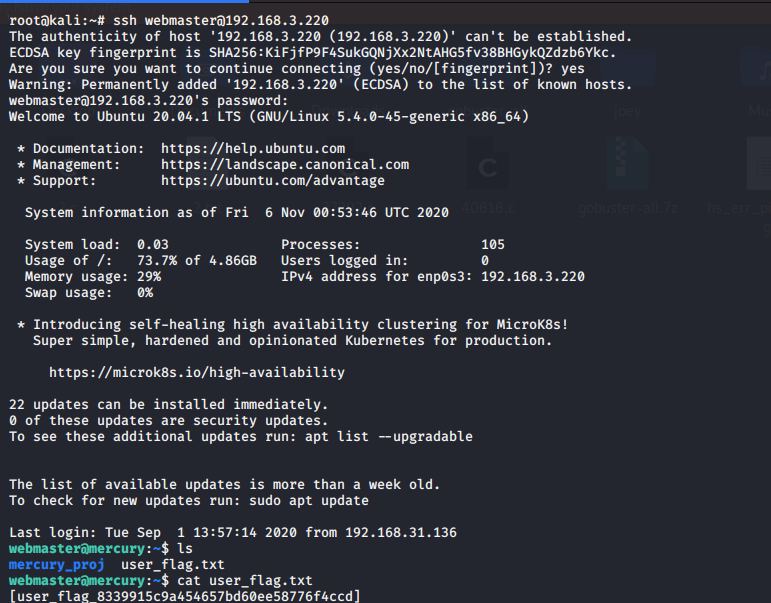


# 0x04:爆破SSH端口

这里由于得到一批账号密码尝试爆破一波22端口，爆破成功

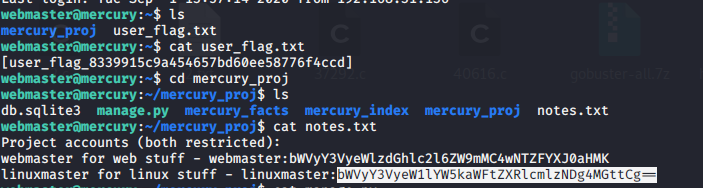


登录以后成功得到Userflag

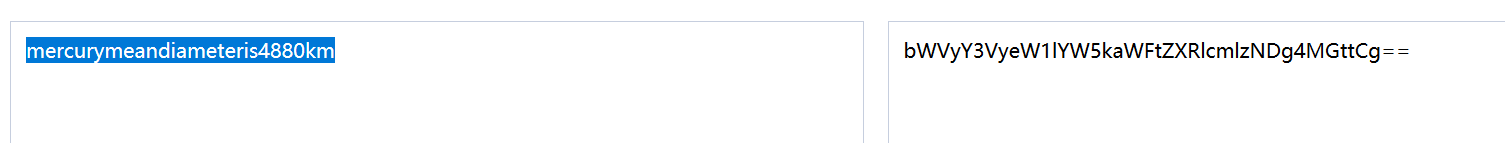


# 0x05:挖掘信息

这里在ls一下，发现mercury\_proj目录跟进一波有个Notes.txt，cat一下得到另外一个账号linuxmaster还有密码应该是base64加密的



解密成功

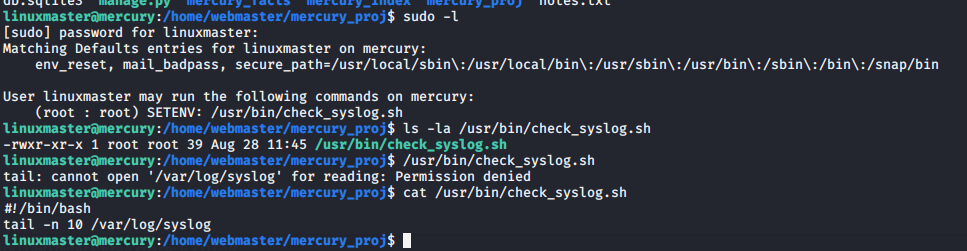


利用su直接切换用户



# 0x06:提权

这次sudo -l终于可以正常运行了，只不过这次没那么容易了，好像不能直接抄答案提权了



这里在网上查了一下这次得用到环境变量提权<https://www.freebuf.com/articles/system/173903.html> 的symlink命令



这里模仿一下先进行符号连接一波，然后设置好PATH



然后利用sudo设置好环境变量，设置好以后会进入vim,记得一定要运行:!/bin/bash才能变成root

