TryHackMe Room Write-up

Title: MD2PDF

Description: TopTierConversions LTD is proud to present its latest product launch.

Author: Igor Buszta

Challenge

Description: Hello Hacker!

TopTierConversions LTD is proud to announce its latest and greatest product launch: MD2PDF.

This easy-to-use utility converts markdown files to PDF and is totally secure! Right...?

Note: Please allow 3-5 minutes for the VM to boot up fully before attempting the challenge.

Objective: What is the flag?

Tools: Kali Linux, nmap

Let's kick things off with a classic nmap.

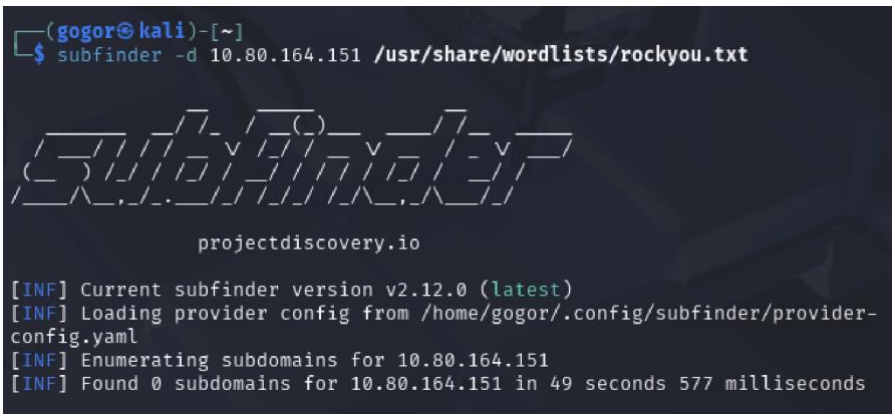
```
┌──(gogor㉿kali)-[~/Downloads]
└─$ nmap 10.81.144.150
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-11 20:08 GMT
Nmap scan report for 10.81.144.150
Host is up (0.047s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 2.44 seconds
```

Picture 1: nmap output performed on Target Machine.

Port 5000 seems promising, ssh doesn't seem like a way here. Let's scan the IP with subfinder and gobuster for subdomains and catalogs.

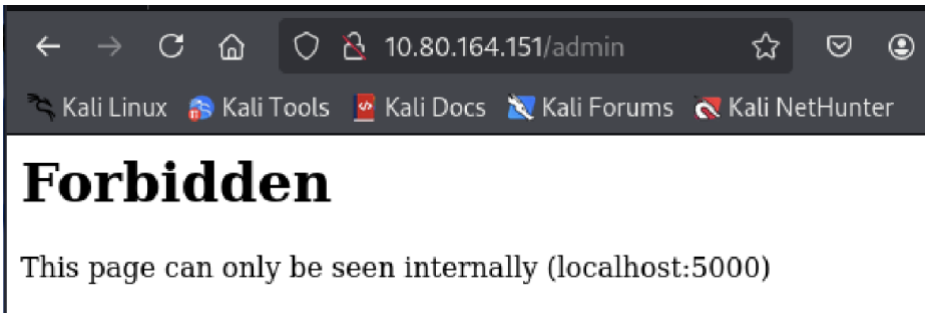
```
┌──(gogor㉿kali)-[~]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medi
um.txt -u 10.80.164.151
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.80.164.151
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list
-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 403) [Size: 166]
/convert              (Status: 405) [Size: 178]
```

Picture 2: gobuster output.



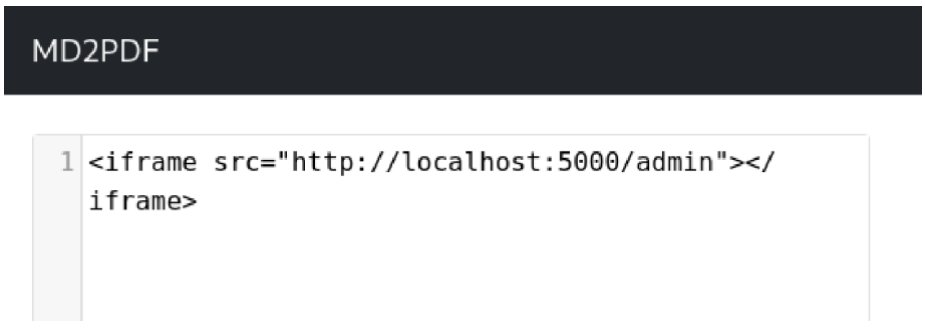
Picture 3: subfinder output.

There are no subdomains but there is forbidden admin catalog on the server (code 403).



Picture 4: Browser's [target ip]/admin output

From the webpage we can tell that we need to access it by localhost:5000. We've seen on our nmap results, that port 5000 is open. We can try to crack the vault open now.



Picture 5: Server Side Request Forgery performed.

The web page transforms Markdown markup language into PDF, so we use it's semantics to run the code server-side to give us a look inside the admin forbidden panel.