Room Link: https://tryhackme.com/room/md2pdf

This room shows how to exploit mistakes made in server-side PDF conversion by using iframe injection to execute an XSS attack and access restricted pages. We'll use nmap, Gobuster, and html to complete this room.

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...?

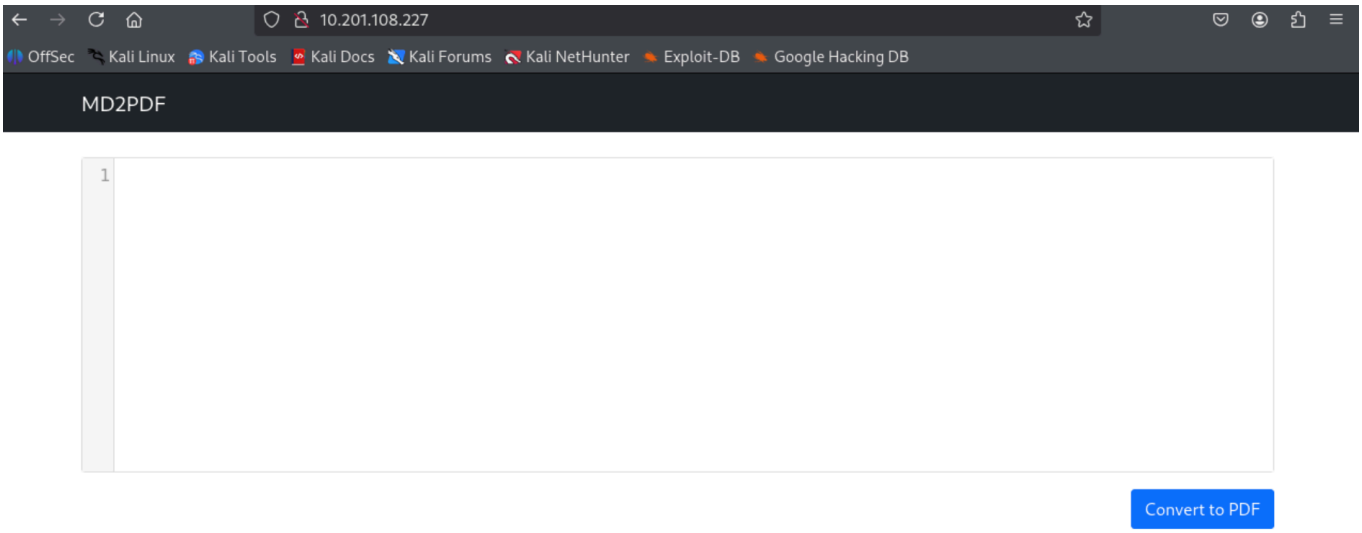
Recon

First, I'll run a quick nmap scan to see what ports are open.

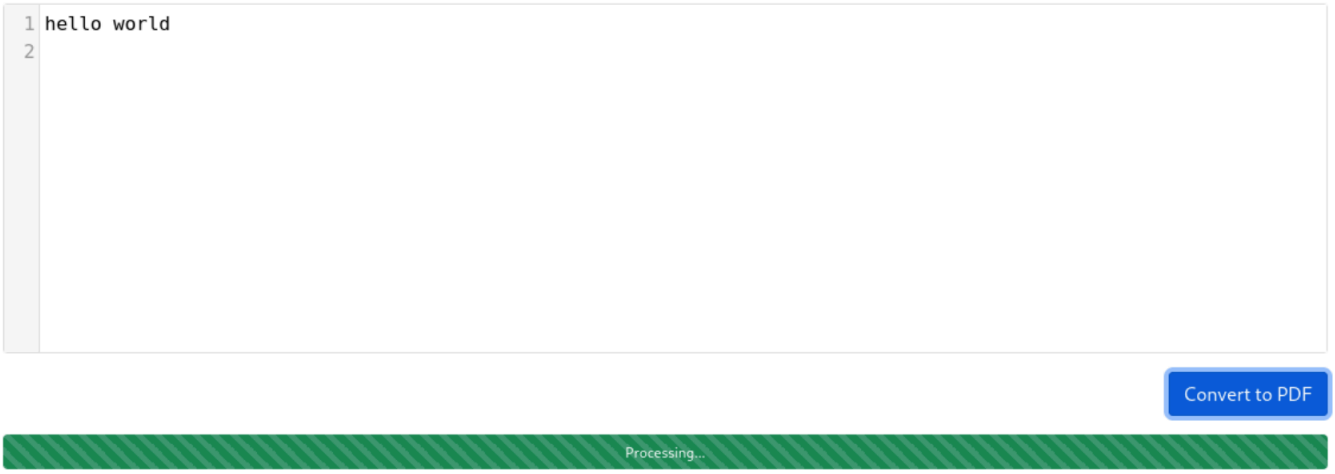
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.201.108.227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-01 13:10 EDT
Nmap scan report for 10.201.108.227
Host is up (0.014s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

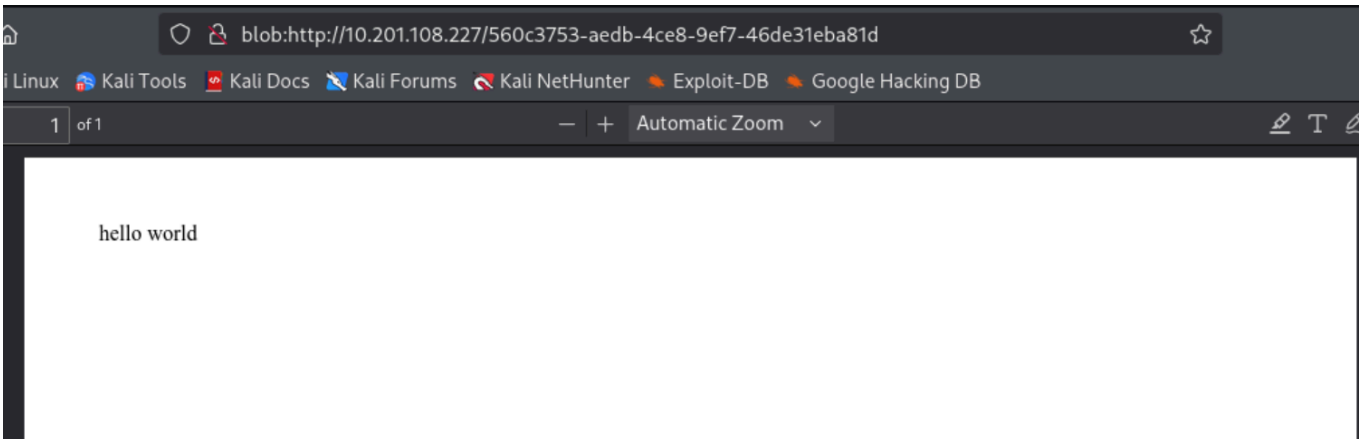
The target machine is running http on port 80, which draws my attention as a possible way into the machine.



I enter the target IP into my browser to see what the webpage looks like. To test the program, I run a sample string through the converter.



Hitting "convert to PDF" opens a new tab displaying my converted pdf!



Next, I'm going to use Gobuster to enumerate subdirectories of the target IP. We'll use the "-u" flag to specify the url of the target. The "-w" flag denotes the location of the wordlist on my

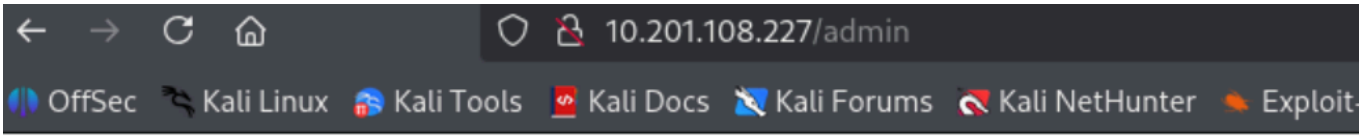
virtual machine. I'm using small list from the directory buster folder first, and if that fails to find anything interesting, I'll escalate things and use the big list.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.201.108.227 -w /usr/share/wordlists/dirb/small.txt
```

Result:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.201.108.227
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/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: 959 / 960 (99.90%)
===============================================================
Finished
===============================================================
```

This shows promising results! The target IP has an admin subdirectory. We'll navigate to that now.



Forbidden

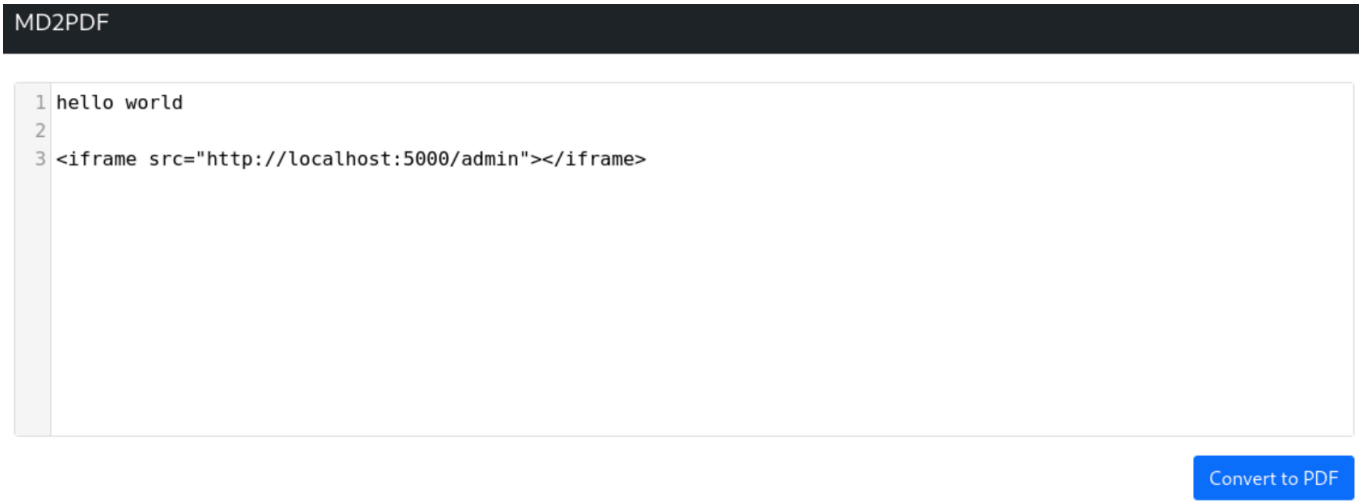
This page can only be seen internally (localhost:5000)

Looks like the page is only accessible locally from the server itself. Clearly there is something being hidden here.

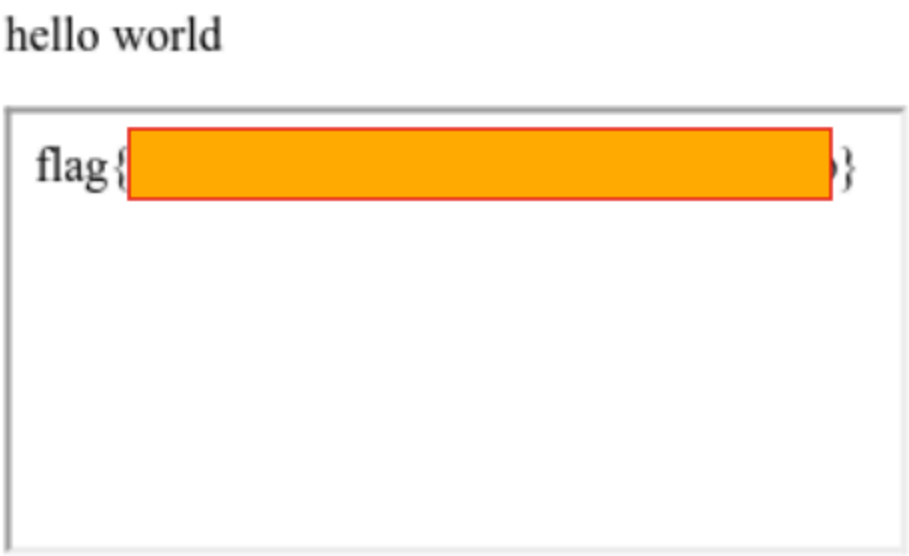
Find Flag

The page we want to access is locked to only be viewed from the local machine. We're going to try to trick the local machine into showing it to us.

Let's see if we can use a simple iframe injection to exploit the markdown parsing inside the PDF converter. This iframe tells the markdown parser to embed a view of the page located at "http://localhost:5000/admin".



Result:



Success! Our iframe injection yields the flag we need, and we can complete the room.

Conclusion

This was a quick room to gain some experience using iframe injection to complete a XSS attack. It was a great room to complete in between classes.