TRY HACK ME

LO-FI [CTF Report]

AUTHOR: TOM SHINJO THOMAS

ROOM NAME: LO-FI

This machine is rated as easy and focuses on Local File Inclusion (LFI) vulnerabilities and Directory Traversal techniques.

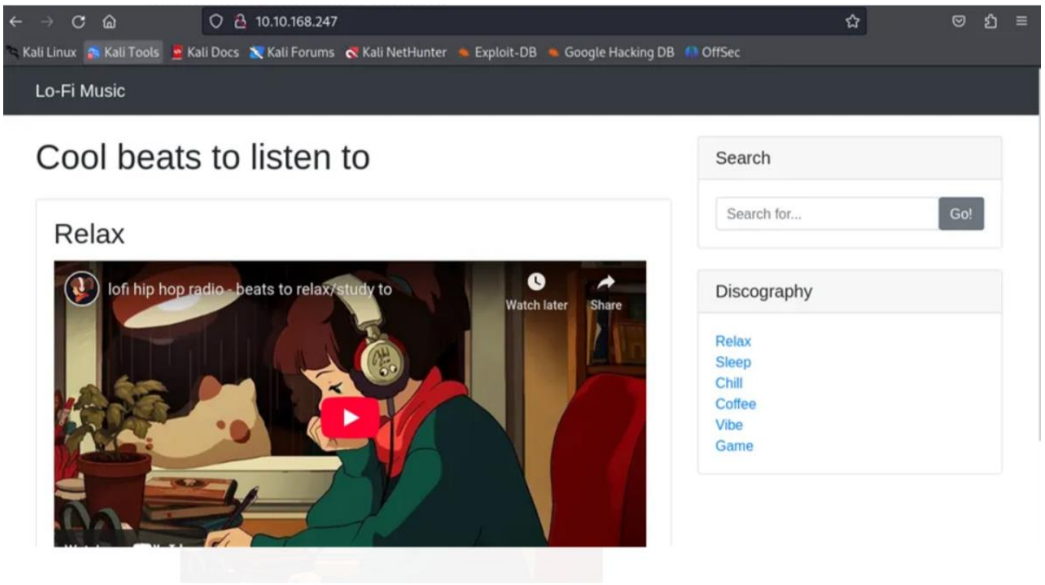
STEPS:

1. the first thing that interests us is to scan the target machine and see which ports and services are open. We will do this by using the command:

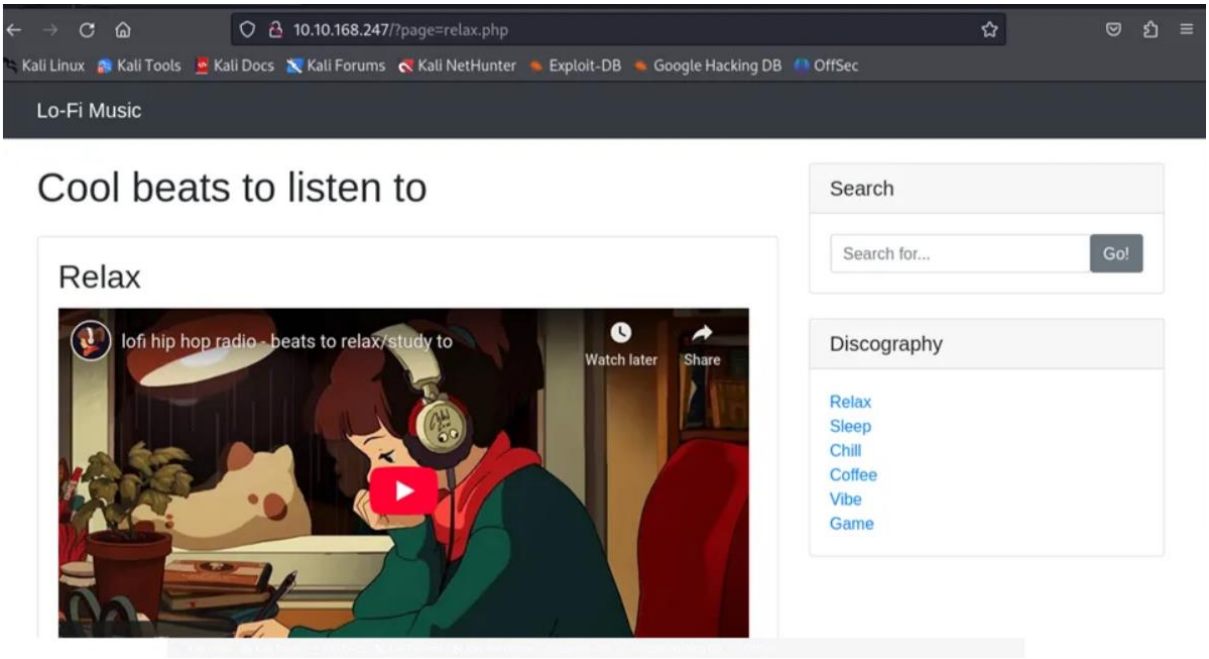
```
nmap 10.10.168.247
```

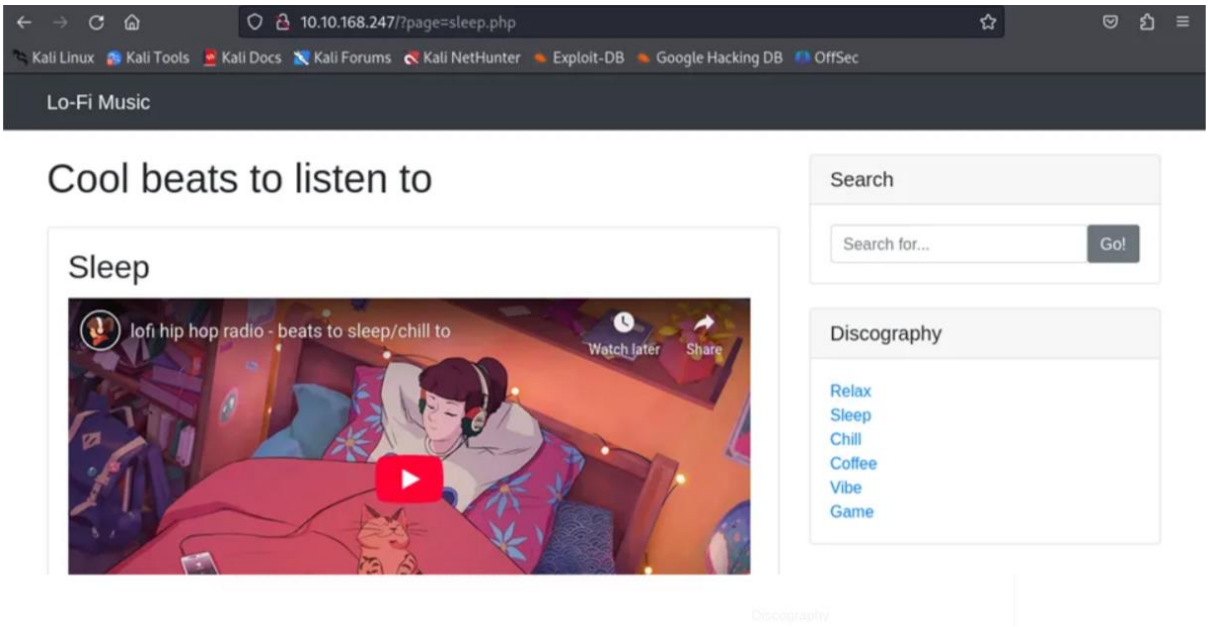
```
└$ nmap 10.10.168.247
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-09 06:45 EDT
Nmap scan report for 10.10.168.247
Host is up (0.079s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds
```

After the scan was completed, we discovered that there are 2 open ports: port 80 and port 22. Since we found that port 80 is open, we can access the machine's IP through a browser.

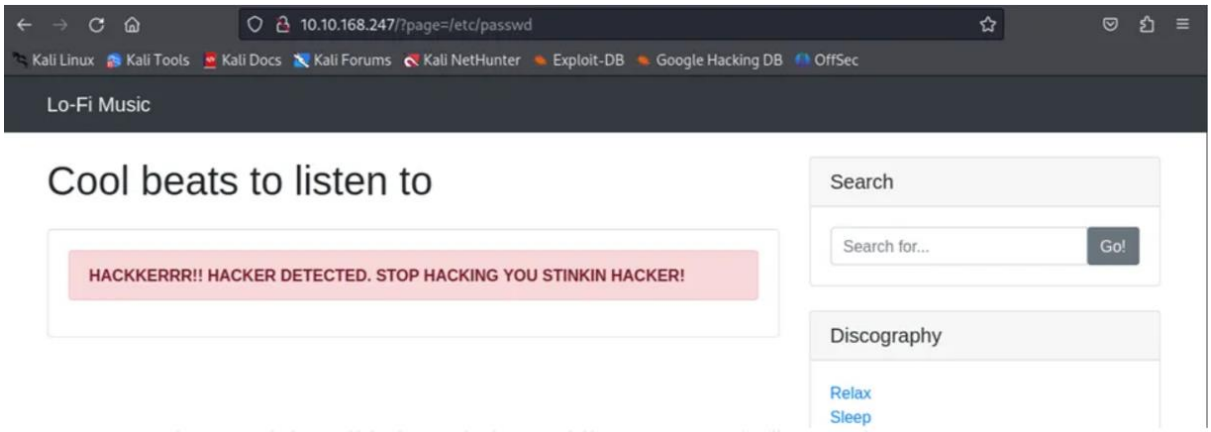


When we switch between the music genres, we'll see that our page equals some value.

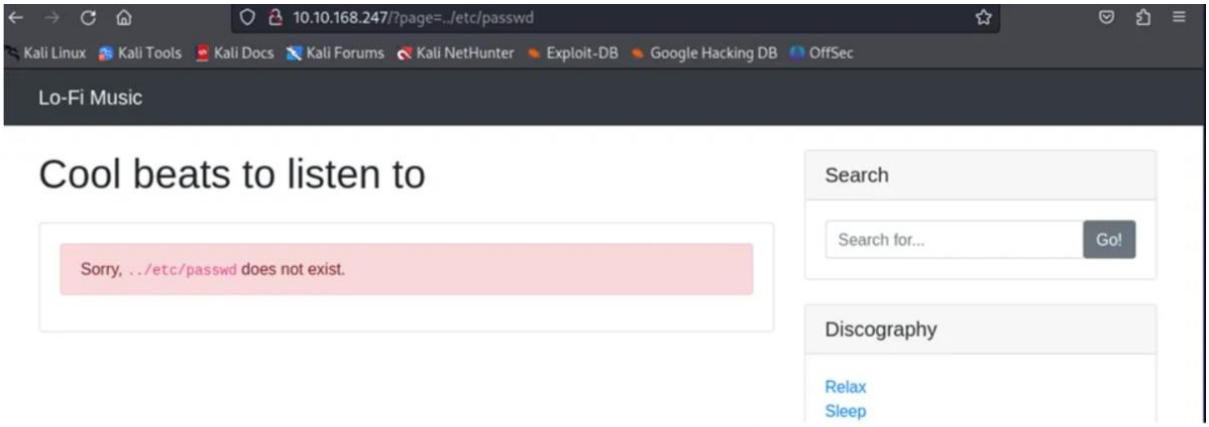




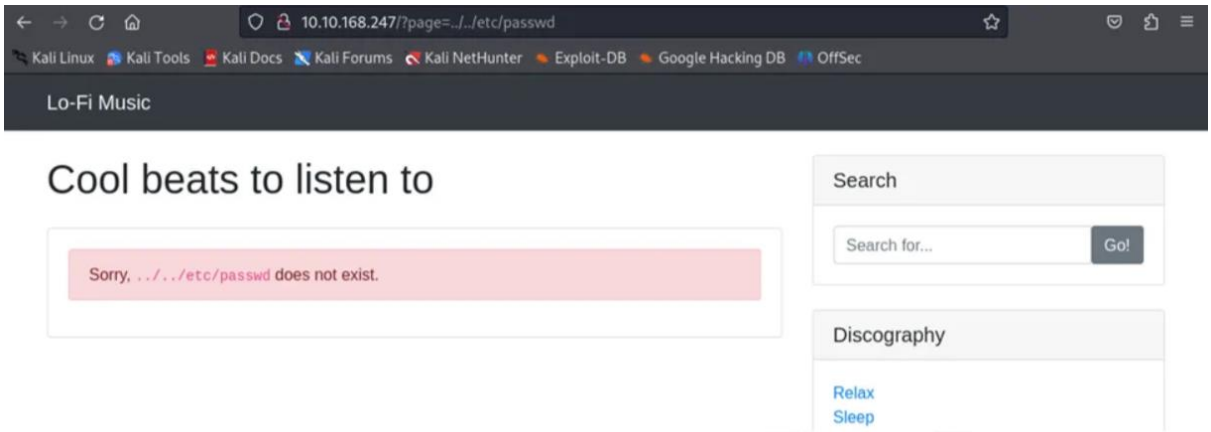
When we encounter a situation like this, there's a high chance of a local file inclusion. Therefore, we'll change the value to /etc/passwd to inspect information about the system's users.



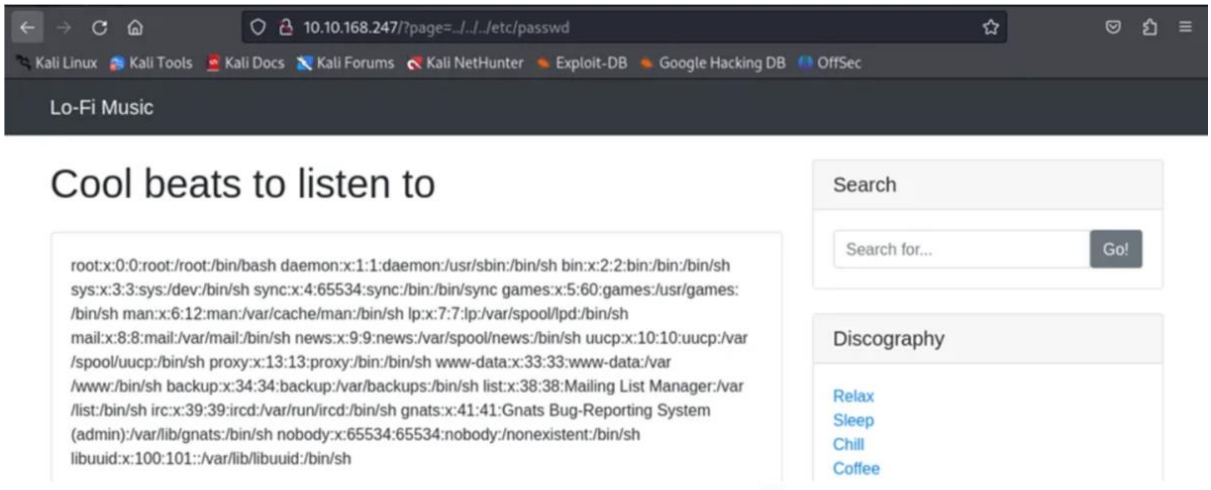
We notice an error message — let's now prepend "../" to /etc/passwd to proceed.



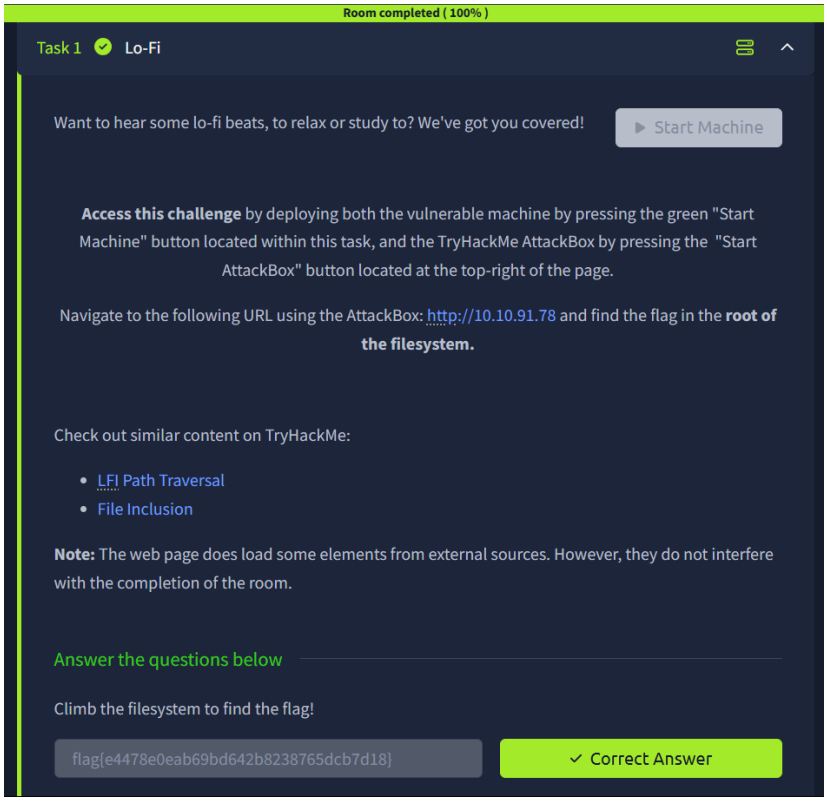
We're now seeing a different error message, which indicates that we've bypassed the validation — let's try adding one more "../" to continue.



We got the same message again, so let's add another one because we don't know the actual path where the file is located.



We're able to view the users list, but that's not our goal. To complete the room, we need to locate the flag file located in the root directory. So instead of /etc/passwd, let's try flag.txt and send the request again.



We managed to solve the challenge.