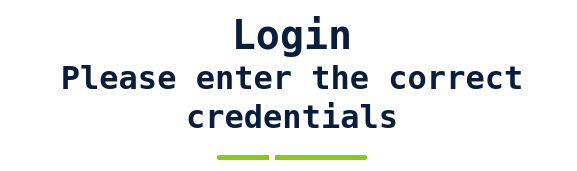
The URL given: <http://10.10.48.192/login.php>

The website itself is a simple login page.

A screen shot of a computer

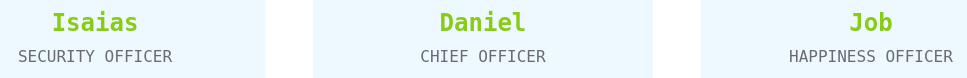
Description automatically generated

I decided to try default passwords and usernames.



This gave an error message. Using this error message, I can use WFUZZ or HYDRA to crack. But first I need to find usernames and passwords.

Snooping around the website, I found a webpage that contained the names of all of the team members.



This is extremely useful.

I have chosen to go a max depth of 2 and a min-word length of 5. I also decided it is probably smartest choice to use the default page as the starting point. I then also want to include words with numbers in them.

This is the brute force command I used to get the password and username combination.

**Note**: The FUZZ keyword is purposely written as FUZ2Z NOT FUZZ!!!

This is the valid credentials.



I was able to successfully login. The default page was the dashboard and it showed emails of the current user. I found one that had ‘confidential message’ mentioned in the subject line and found the flag.

A screenshot of a computer

Description automatically generatedThe flag below.