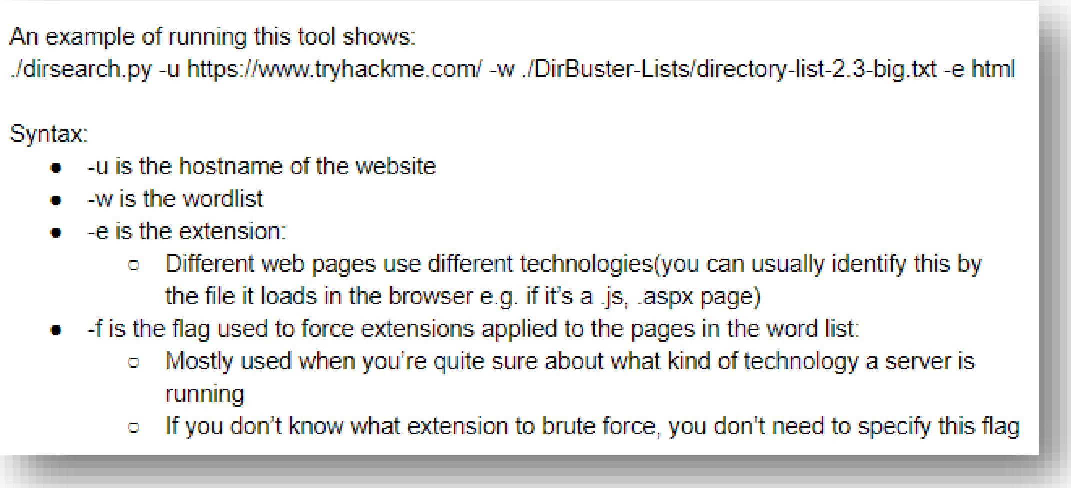
https://docs.google.com/document/d/1622ejYtCmLOS0zd16CyfhA1xgQk8l55gYWMY8fnpHfQ/edit

[Task 7] [Day 2] Arctic Forum

1. **What is the path of the hidden page?**
   - Use DirSearch python tool to brute force dictionary attack and search a website's directories for valid responses

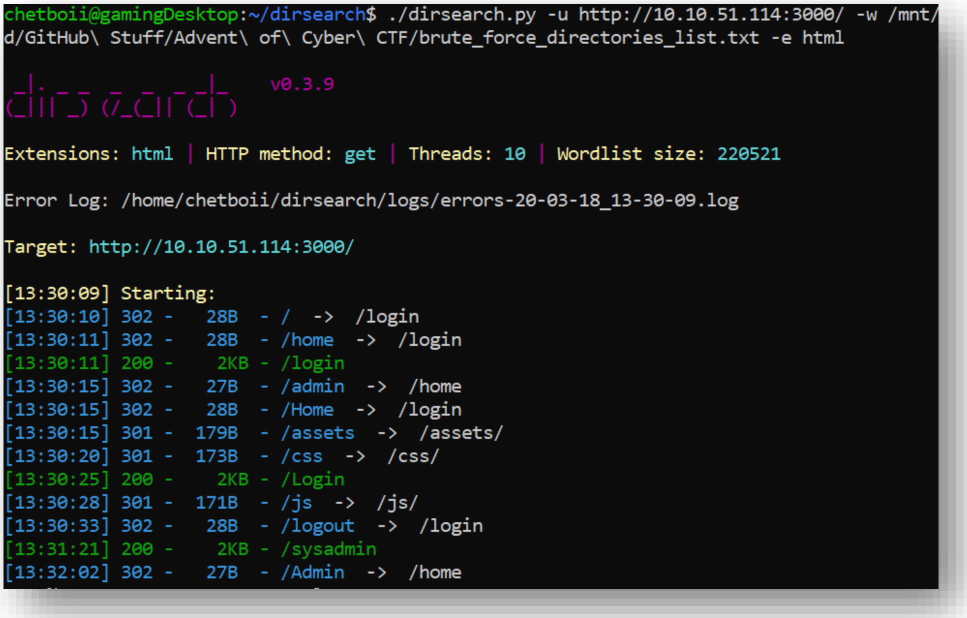


An example of running this tool shows:
./dirsearch.py -u https://www.tryhackme.com/ -w ./DirBuster-Lists/directory-list-2.3-big.txt -e html

Syntax:

- -u is the hostname of the website
- -w is the wordlist
- -e is the extension:
  - Different web pages use different technologies(you can usually identify this by the file it loads in the browser e.g. if it's a .js, .aspx page)
- -f is the flag used to force extensions applied to the pages in the word list:
  - Mostly used when you're quite sure about what kind of technology a server is running
  - If you don't know what extension to brute force, you don't need to specify this flag

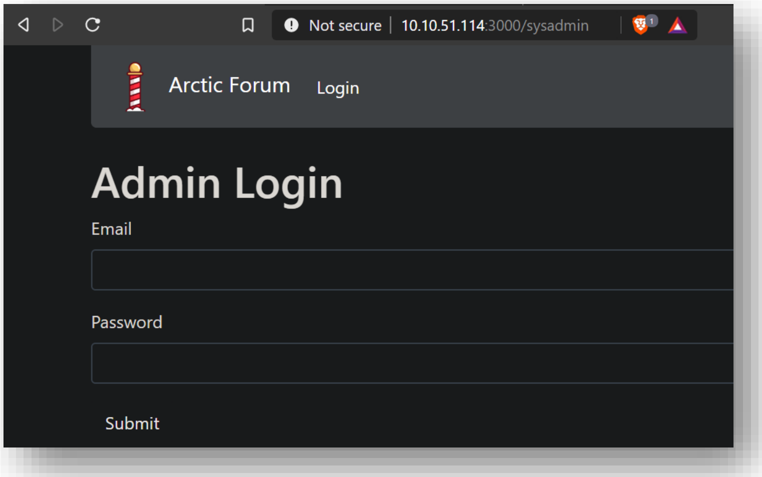
   - ./dirsearch.py -u http:// http://10.10.51.114:3000/ -w /mnt/d/GitHub\ Stuff/Advent\ of\ Cyber\ CTF/brute_force_directories_list.txt -e html



```
chetboii@gamingDesktop:~/dirsearch$ ./dirsearch.py -u http://10.10.51.114:3000/ -w /mnt/
d/GitHub\ Stuff/Advent\ of\ Cyber\ CTF/brute_force_directories_list.txt -e html

 _|. _ _  _  _  _ _|_    v0.3.9
(_||| _) (/_(_|| (_| )

Extensions: html | HTTP method: get | Threads: 10 | Wordlist size: 220521

Error Log: /home/chetboii/dirsearch/logs/errors-20-03-18_13-30-09.log

Target: http://10.10.51.114:3000/

[13:30:09] Starting:
[13:30:10] 302 -   28B  - /  ->  /login
[13:30:11] 302 -   28B  - /home  ->  /login
[13:30:11] 200 -    2KB - /login
[13:30:15] 302 -   27B  - /admin  ->  /home
[13:30:15] 302 -   28B  - /Home  ->  /login
[13:30:15] 301 -  179B  - /assets  ->  /assets/
[13:30:20] 301 -  173B  - /css  ->  /css/
[13:30:25] 200 -    2KB - /Login
[13:30:28] 301 -  171B  - /js  ->  /js/
[13:30:33] 302 -   28B  - /logout  ->  /login
[13:31:21] 200 -    2KB - /sysadmin
[13:32:02] 302 -   27B  - /Admin  ->  /home
```

   - Try to access http://<machine_ip>:3000/sysadmin

2. What is the password you found?
   - To find the password, lets look around the page



Not secure | 10.10.51.114:3000/sysadmin

Arctic Forum Login

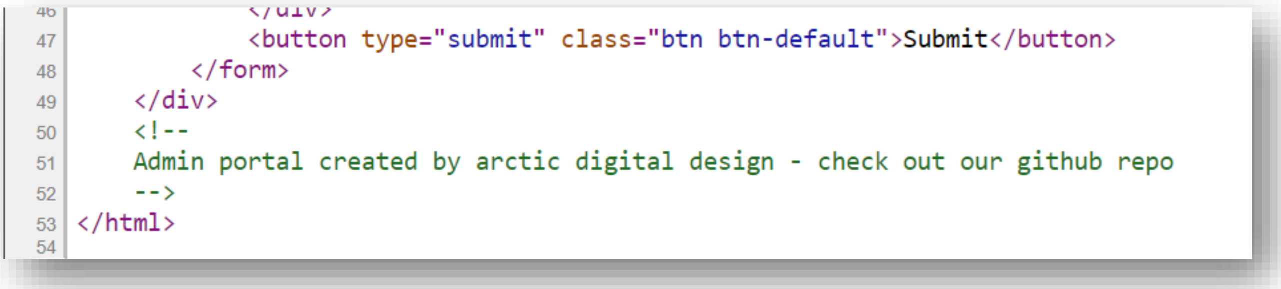
Admin Login

Email

Password

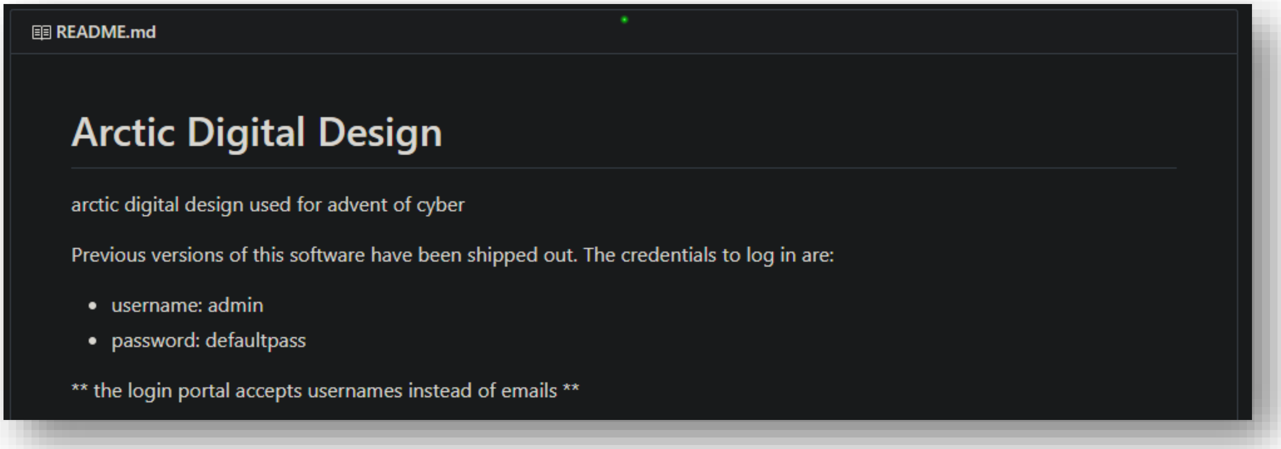
Submit

- Right-click and inspect page source:



```
                </div>
                <button type="submit" class="btn btn-default">Submit</button>
            </form>
        </div>
        <!--
        Admin portal created by arctic digital design - check out our github repo
        -->
</html>
```

- Go to github and search arctic digital design:
- Password is defaultpass



README.md

Arctic Digital Design

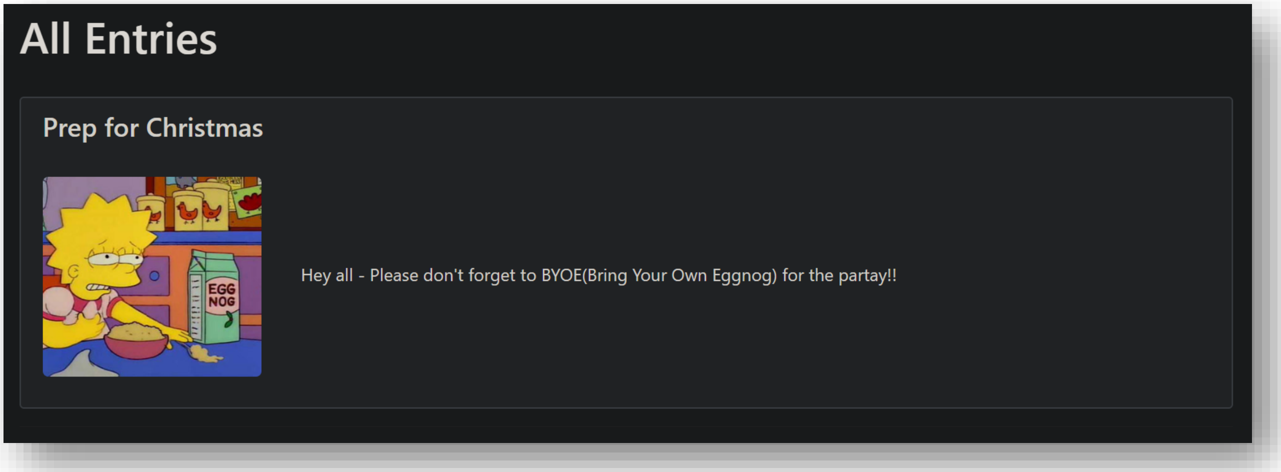
arctic digital design used for advent of cyber

Previous versions of this software have been shipped out. The credentials to log in are:

- username: admin
- password: defaultpass

** the login portal accepts usernames instead of emails **

3. What do you have to take to the 'partay'
   - After loggin in as admin, we are met with:



All Entries

Prep for Christmas

Hey all - Please don't forget to BYOE(Bring Your Own Eggnog) for the partay!!

   - BYO Eggnog