

Day 2 - Artic Forum

Scenario

Task 7 [Day 2] Arctic Forum



Deploy

A big part of working at the best festival company is the social live! The elves have always loved interacting with everyone. Unfortunately, the christmas monster took down their main form of communication - the arctic forum!

Elf McForum has been sobbing away McElferson's office. *How could the monster take down the forum!* In an attempt to make McElferson happy, she sends you to McForum's office to help.

P.S. Challenge may a take up to 5 minutes to boot up and configure!

Access the page at [http://\[your-ip-here\]:3000](http://[your-ip-here]:3000)

Check out the supporting material [here!](#)


checking the webpage & we found a regular elf login page

Arctic Forum | Login

To Base64 - CyberChef

10.10.212.57:3000/login

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensi

 Arctic Forum Login

Regular Elf Login



Username

Password

let's try to perform web directory fuzzing
//as for the 302 status code it'll be the directories & will redirect us to another page
//so the hidden page will be status code 200 which will be sysadmin

```
[+] Url: http://10.10.212.57:3000/
[+] Threads: 40
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
```

```
2020/11/28 07:25:55 Starting gobuster
```

```
/admin (Status: 302)
/Admin (Status: 302)
/ADMIN (Status: 302)
/assets (Status: 301)
/css (Status: 301)
/home (Status: 302)
/Home (Status: 302)
/js (Status: 301)
/login (Status: 200)
/Login (Status: 200)
/logout (Status: 302)
/sysadmin (Status: 200)
/SysAdmin (Status: 200)
```


2020/11/28 07:26:20 Finished

& when we check it out we've end up in the admin login page

Arctic Forum | Admin Login x http://10.10.212.57:3000/log x To Base64 - CyberChe

← → ↻ 🏠 10.10.212.57:3000/sysadmin

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

 Arctic Forum Login

Admin Login

Email

Password

Submit

Question: What is the path of the hidden page?
-/sysadmin

if we check out the /sysadmin source code we'll notice that this page have a github repo

```
3     </form>
3   </div>
3   <!--
1   Admin portal created by arctic digital design - check out our github repo
2   -->
3 </html>
1
```

so let's use googleFu to find the github repo, & we'll be able to find the github repo that's belong to ashu-savani

🔗 master ▾

🔗 1 branch

🔖 0 tags



ashu-savani Update README.md

7d5ba



README.md

Update README.md

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 default credential to login will be admin:defaultpass, so let's try it out see the default credential able to use or not

//& it works!, now we've login into admin account

Arctic Forum | Admin page × To Base64 - CyberChef × GitHub - ash

← → ↻ 🏠 10.10.212.57:3000/admin

🔗 Kali Linux 🔗 Kali Training 🔗 Kali Tools 📄 Kali Docs 🔗 Kali Forums 🔗 Net

 Arctic Forum Logout

Add Users

Email

Name

--

Question: What is the password you found?
-defaultpass

& now we've found an entries here for Prep for Christmas
//they need to bring Egnog for the partay

All Entries

Prep for Christmas



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

Question: What do you have to take to the 'partay'
-Eggnog