# CyberHeroes



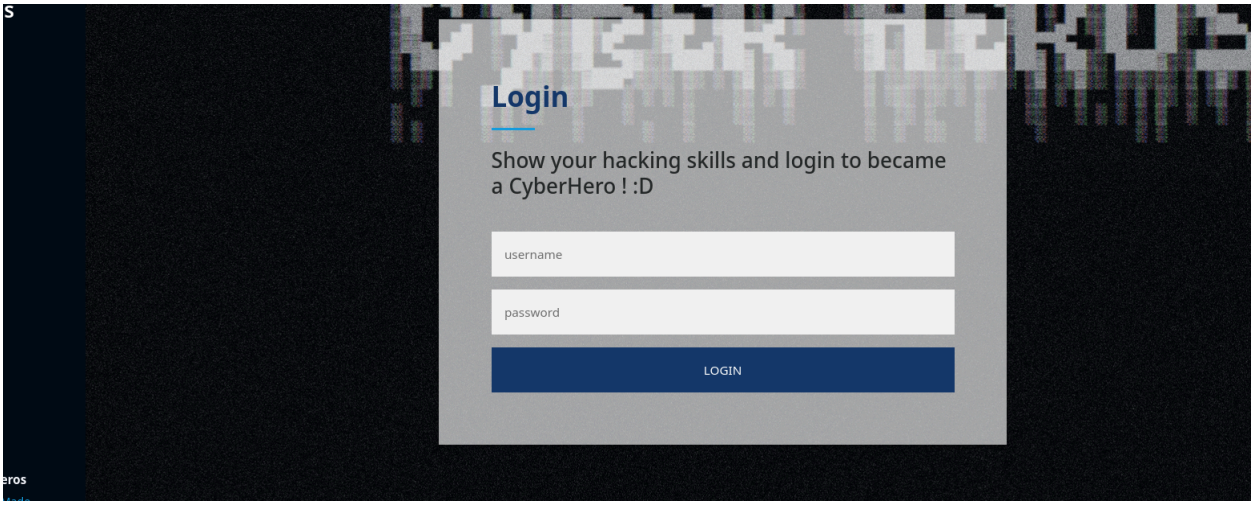
# Enumeration

## Nmap Scan

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Li
| ssh-hostkey:
|   3072 27:ed:7d:88:a4:f5:2d:c3:db:34:d5:75:cf:b1:f4:1e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDrOi/LJO/biEv/dSTHe0I6AZk
|   256 d5:41:29:9d:b8:16:76:81:26:bc:70:19:c8:1a:1d:da (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
|   256 c0:ef:a4:83:46:f3:f1:a8:2c:ef:79:b9:e3:91:76:40 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK40MtYwEqaKFgCKWt/JnLRTNu

80/tcp open  http    syn-ack ttl 60 Apache httpd 2.4.48 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-favicon: Unknown favicon MD5: 03983666D3C4B72ECAAB464BD200E6F
|_http-server-header: Apache/2.4.48 (Ubuntu)
|_http-title: CyberHeros : Index
Warning: OSScan results may be unreliable because we could not find at least 1 c
OS fingerprint not ideal because: Missing a closed TCP port so results incomplet
```

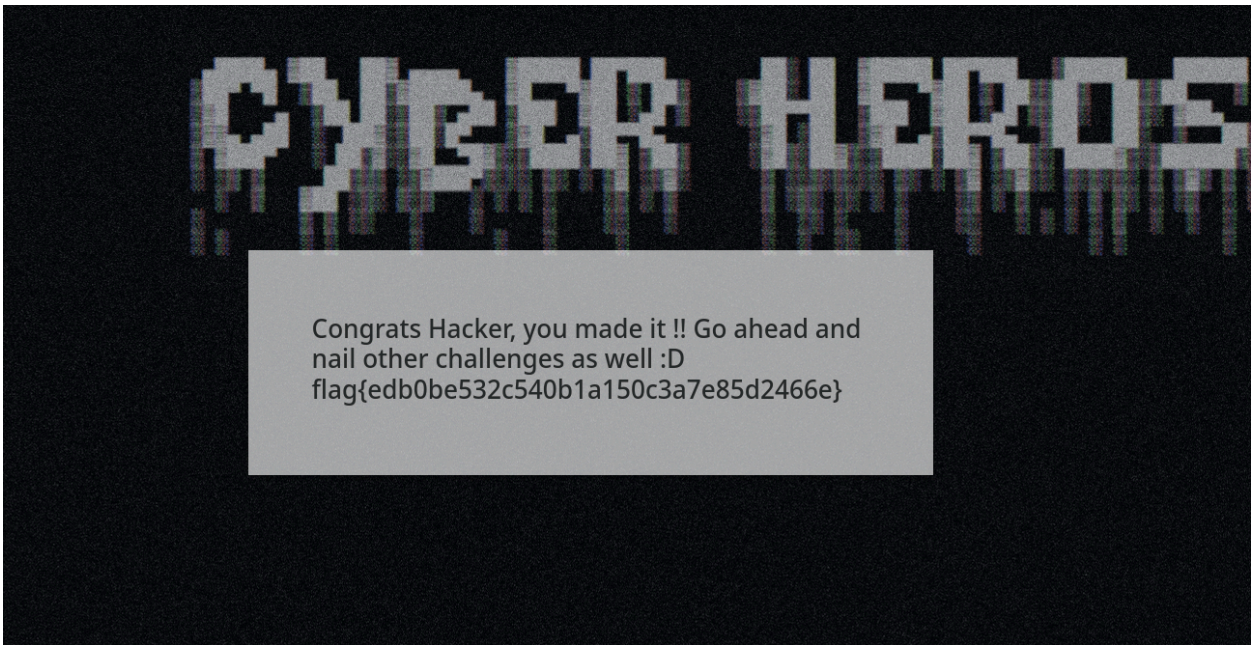
# Exploitation




```
<script>
  function authenticate() {
    a = document.getElementById('uname')
    b = document.getElementById('pass')
    const RevereString = str => [...str].reverse().join('');
    if (a.value=="h3ck3rBoi" & b.value==RevereString("54321@terceSrepuS")) {
      var xhttp = new XMLHttpRequest();
      xhttp.onreadystatechange = function() {
        if (this.readyState == 4 && this.status == 200) {
          document.getElementById("flag").innerHTML = this.responseText ;
          document.getElementById("todel").innerHTML = "";
          document.getElementById("rm").remove() ;
        }
      };
      xhttp.open("GET", "RandomLo0o0o0o0o0o0o0o0o0o0gpath12345_Flag_"+a.value+"_"+b.value+".txt", true);
      xhttp.send();
    }
    else {
      alert("Incorrect Password, try again.. you got this hacker !")
    }
  }
</script>
```

username: h3ck3rBoi

password: SuperSecret@12345


CYBER HEROES
Congrats Hacker, you made it !! Go ahead and nail other challenges as well :D
flag{edb0be532c540b1a150c3a7e85d2466e}