cyber heroes

Keşif ile başlıyoruz.

web taramasını yapıyoruz.

```
🖵 gobuster dir -u http://10.10.144.243 -w /usr/share/dirbuster/wordlists/directory-list-2
.3-medium.txt -t 10
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:
                              http://10.10.144.243
[+] Method:
[+] Threads:
                              GET
                              10
[+] Wordlist:
                              /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:
                             404
[+] User Agent:
                              gobuster/3.5
[+] Timeout:
                              10s
2024/04/03 06:39:09 Starting gobuster in directory enumeration mode
                      (Status: 301) [Size: 315] [→ http://10.10.144.243/assets/]
/assets
```

<u>Name</u>	<u>Last modified</u>	Size Description
Parent Directory		-
css/	2022-03-02 19:08	-
<u>img/</u>	2022-03-02 19:08	-
<u>js/</u>	2022-03-02 19:08	-
<u>vendor/</u>	2022-03-02 19:07	-
Apache/2.4.48 (Ubuntu) Server at 10.1	10.144.243 Port 80

Bu klasörleri kurcaladım. Bir şey bulamadım.

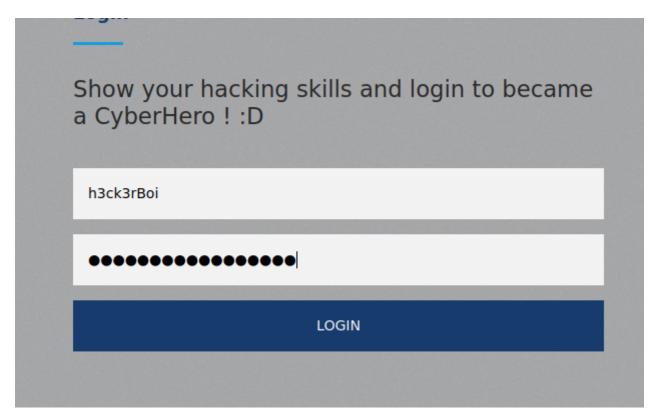
login.html adlı bir sayfa keşfediyoruz. Bunun üzerinden taramaya devam ediyoruz. Kaynak kodu incelediğimizde aşağıdaki kısım dikkatimizi çekiyor.

```
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) {
```

Metni ters çeviriyoruz.

```
$ echo "54321@terceSrepuS" | rev
SuperSecret@12345
```

Kullanıcı adı h3ck3rBoi parola ise SuperSecret@12345 olduğunu keşfediyoruz.



Giriş yapıyor. Görev başarılı.

