#easy #tryhackme #web-pentest

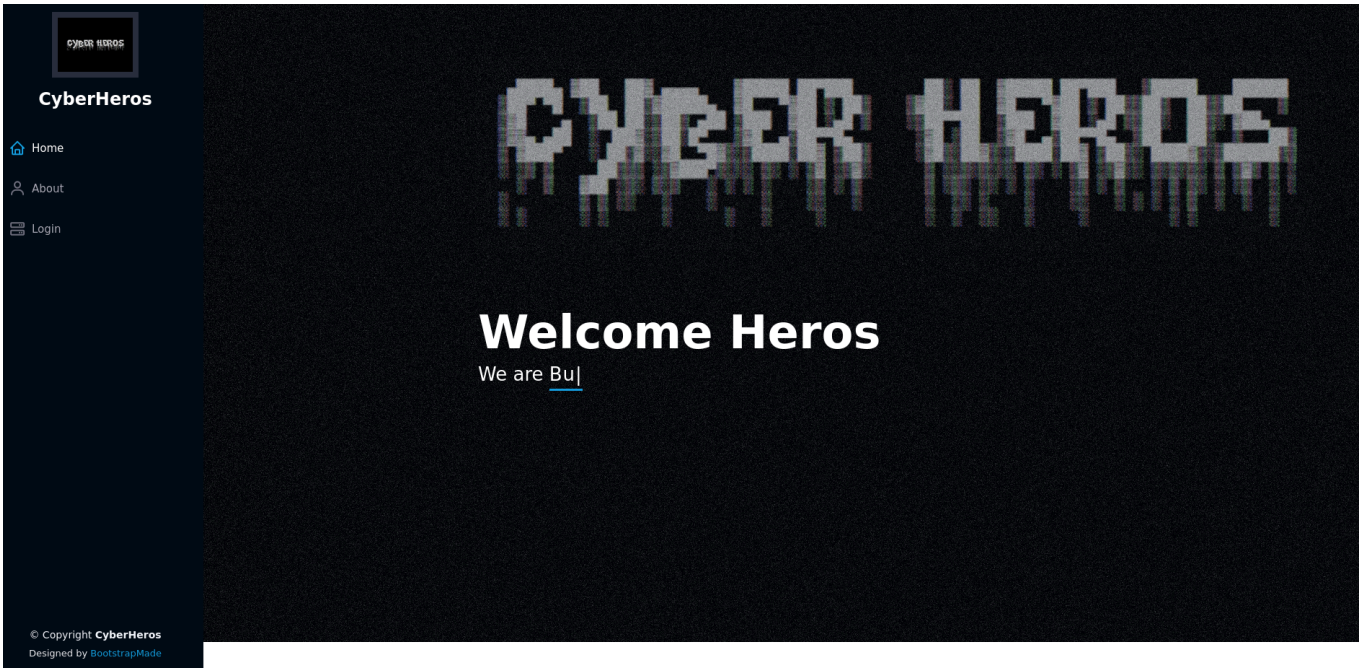
Сбор данных

Машинка сплойтилась со слледующим IP адресом:
`10.80.166.101`
В качестве подсказки былло написано: Authentication Bypass (обход аутентификации)
Пройдемся nmap-ом

```
nmap -sC -sV 10.80.166.101
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.80.166.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 17:30 EST
Nmap scan report for 10.80.166.101
Host is up (0.064s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 90:77:fc:70:0d:88:68:94:35:c3:c2:a5:f8:be:7a:db (RSA)
|   256 07:80:e5:62:1f:05:3f:86:33:54:f6:b5:71:3c:9b:52 (ECDSA)
|_  256 a5:3c:ae:e6:b9:ca:70:0a:6d:94:cb:ac:d4:50:cb:4a (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Ubuntu))
|_http-server-header: Apache/2.4.48 (Ubuntu)
|_http-title: CyberHeros : Index
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.33 seconds
```

Открыт 22 и 80 порт. Откроем страничку в браузере.



Запустим dirsearch:

```
dirsearch -u 10.80.166.101
```

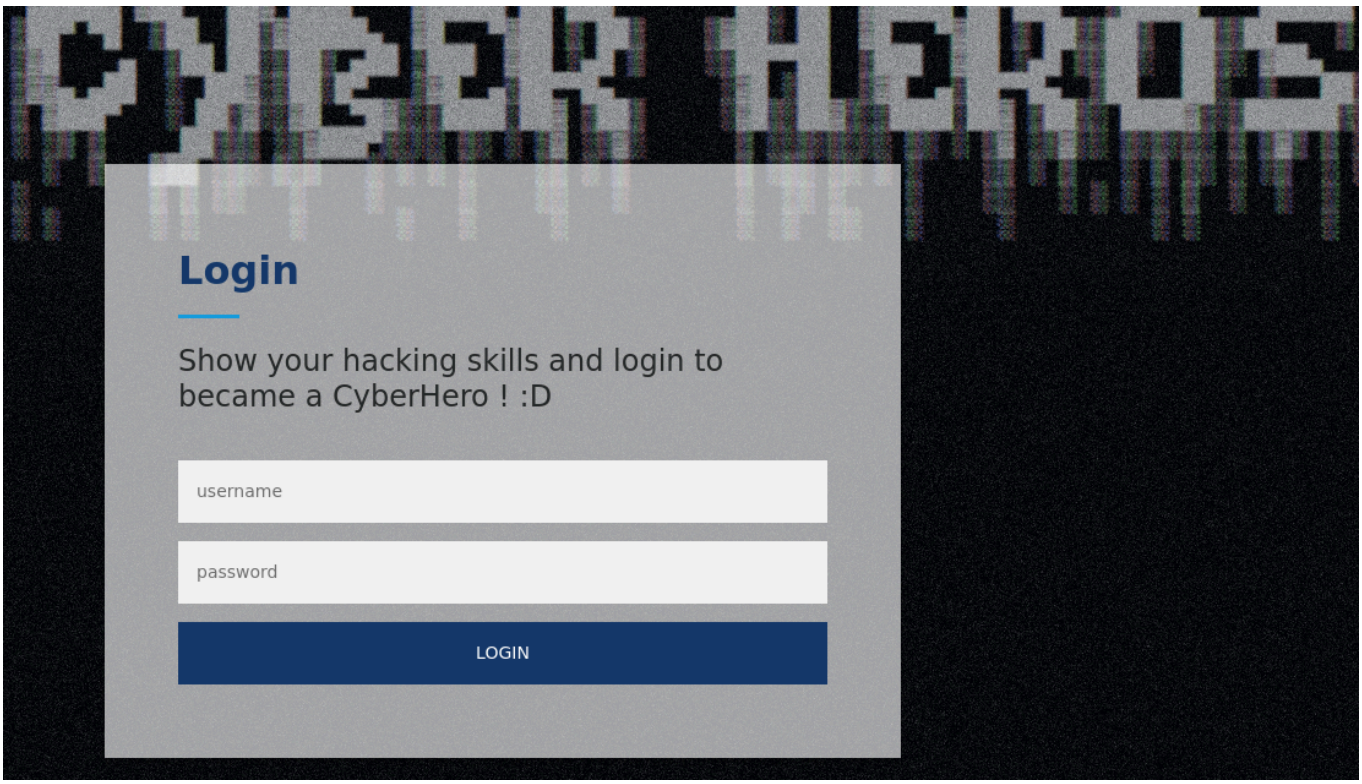
```
Target: http://10.80.166.101/

[17:32:32] Starting:
[17:32:36] 403 -  278B  - /.ht_wsr.txt
[17:32:36] 403 -  278B  - /.htaccess.save
[17:32:36] 403 -  278B  - /.htaccess.orig
[17:32:36] 403 -  278B  - /.htaccess.bak1
[17:32:36] 403 -  278B  - /.htaccess.sample
[17:32:36] 403 -  278B  - /.htaccess_extra
[17:32:36] 403 -  278B  - /.htaccess_orig
[17:32:36] 403 -  278B  - /.htaccess_sc
[17:32:36] 403 -  278B  - /.htaccessOLD
[17:32:36] 403 -  278B  - /.htaccessBAK
[17:32:36] 403 -  278B  - /.htaccessOLD2
[17:32:37] 403 -  278B  - /.htm
[17:32:37] 403 -  278B  - /.html
[17:32:37] 403 -  278B  - /.htpasswd_test
[17:32:37] 403 -  278B  - /.httr-oauth
[17:32:37] 403 -  278B  - /.htpasswds
[17:32:49] 200 -  478B  - /assets/
[17:32:49] 301 -  315B  - /assets  →  http://10.80.166.101/assets/
[17:32:51] 200 -  725B  - /changelog.txt
[17:33:03] 200 -    2KB - /login.html
[17:33:14] 403 -  278B  - /server-status/
[17:33:14] 403 -  278B  - /server-status

Task Completed
```

Глянем changelog.txt

```
Version: 3.7.0
  - Updated Bootstrap to version 5.1.3
  - Updated all outdated third party vendor libraries to their latest versions

Version: 3.6.0
  - Updated Bootstrap to version 5.1.2
  - Updated all outdated third party vendor libraries to their latest versions

Version: 3.5.0
  - Fixed slider issue in testimonials and portfolio details sections

Version: 3.4.0
  - Updated Bootstrap to version 5.1.1
  - Updated all outdated third party vendor libraries to their latest versions
  - Improved and updated dev version gulp scripts

Version: 3.3.0
  - Updated Bootstrap to version 5.0.1
  - Updated all outdated third party vendor libraries to their latest versions
  - Fixed navigation links focus color

Version: 3.2.0
  - Updated Bootstrap to version 5.0.0 Final
  - Updated all outdated third party vendor libraries to their latest versions

Version: 3.1.0
  - Updated Bootstrap to version 5.0.0-beta3
  - Updated all outdated third party vendor libraries to their latest versions
  - Updated the PHP Email Form to V3.1

Version: 3.0.1
  - Updated Bootstrap to version 5.0.0-beta2
  - Updated all outdated third party vendor libraries to their latest versions
```

Ничего интересного тут особо нет.

Перейдем на страничку авторизации:



Попробовал залогиниться с кредами: admin admin
Они не подошли, но при отправке я заметил некотрые странности:

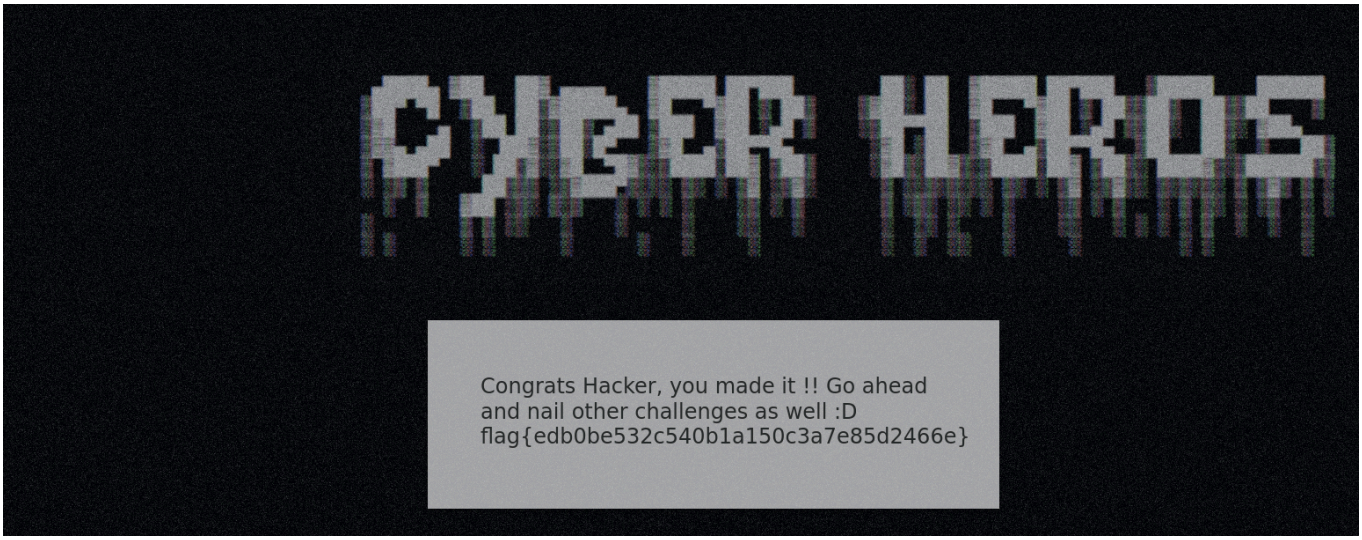
1. ответ пришел мгновенно
2. вылетело окошко браузера
   Можно предположить, что обработка происходит на frontend-е.
   Жмем F12 и идем в инструменты разработчика, глянем файл login.html
   Удалось найти интересную функцию js

```
<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>
```

Эта функция как раз и обрабатывает наш ввод:
'if (a.value"h3ck3rBoi" & b.valueRevereString("54321@terceSrepuS"))'
54321@terceSrepuS - пароль наоборот (SuperSecret@12345)

```
login:     h3ck3rBoi
password:  SuperSecret@12345
```

Зайдем под этими кредами через окошко авторизации:



Круто, мы нашли флаг)

```
flag{edb0be532c540b1a150c3a7e85d2466e}
```