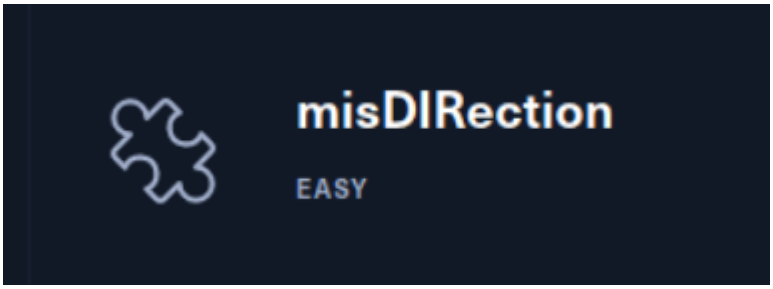
WU GROUP 2 ke 4

Muhammad Mazaya R. S.
Seraphine Amanda Honoris

1. HackTheBox “misDIRection”



Pertama-tama, download dulu filenya. Lalu kita extract.

```
┌──(seraphine㉿kali)-[~/Desktop/htb]
└─$ ls
BabyEncryption  BabyEncryption.zip  misDIRection.zip
```

Namun, setelah di extract tidak muncul apa-apa. Oleh karena itu saya mencoba command ls -la.

```
┌──(seraphine㉿kali)-[~/Desktop/htb]
└─$ ls -la
total 40
drwxr-xr-x  5 seraphine seraphine  4096 Nov 10 16:36  .
drwxr-xr-x 12 seraphine seraphine  4096 Sep 30 23:26  ..
drwxr-xr-x  2 seraphine seraphine  4096 Sep  9 16:30  BabyEncryption
-rw-r--r--  1 seraphine seraphine   631 Sep  9 14:00  BabyEncryption.zip
-rw-r--r--  1 seraphine seraphine 15804 Nov 10 16:35  misDIRection.zip
drwxr-xr-x 64 seraphine seraphine  4096 May  2  2018  .secret
drwxr-xr-x 64 seraphine seraphine  4096 May  2  2018 '.secret (2)'
```

Ternyata misDIRection.zip sudah terextract. Namun bentuknya memang hidden folder.
Lalu saya coba buka untuk melihat isi folder dari .secret

```
┌──(seraphine㉿kali)-[~/Desktop/htb/.secret]
└─$ ls
0  3  6  9  b  C  e  F  h  I  k  L  n  O  q  R  t  U  w  X  z
1  4  7  a  B  d  E  g  H  j  K  m  N  p  Q  s  T  v  W  y  Z
2  5  8  A  c  D  f  G  i  J  l  M  o  P  r  S  u  V  x  Y
```

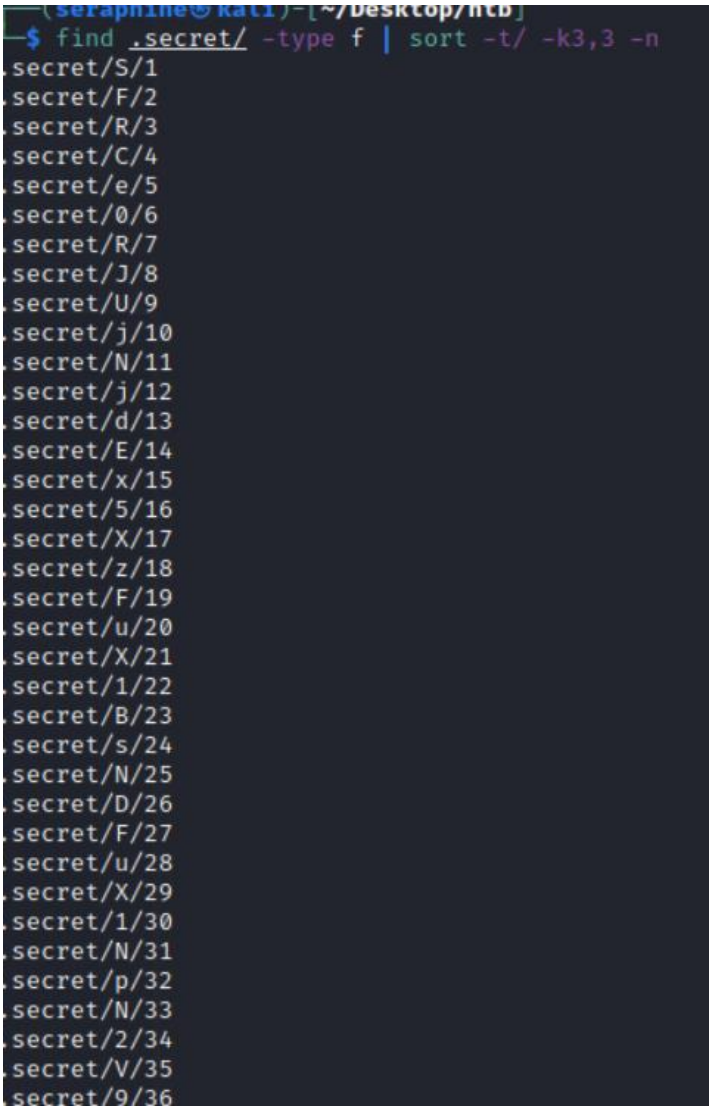
Jadi saya coba cek isi tiap folder seperti apa

```
┌──(seraphine㉿kali)-[~/Desktop/htb/.secret]
└─$ ./1

┌──(seraphine㉿kali)-[~/Desktop/htb/.secret/1]
└─$ ls
22  30

┌──(seraphine㉿kali)-[~/Desktop/htb/.secret/1]
└─$ cd ..

┌──(seraphine㉿kali)-[~/Desktop/htb/.secret]
└─$ ./2

┌──(seraphine㉿kali)-[~/Desktop/htb/.secret/2]
└─$ ls
34
```

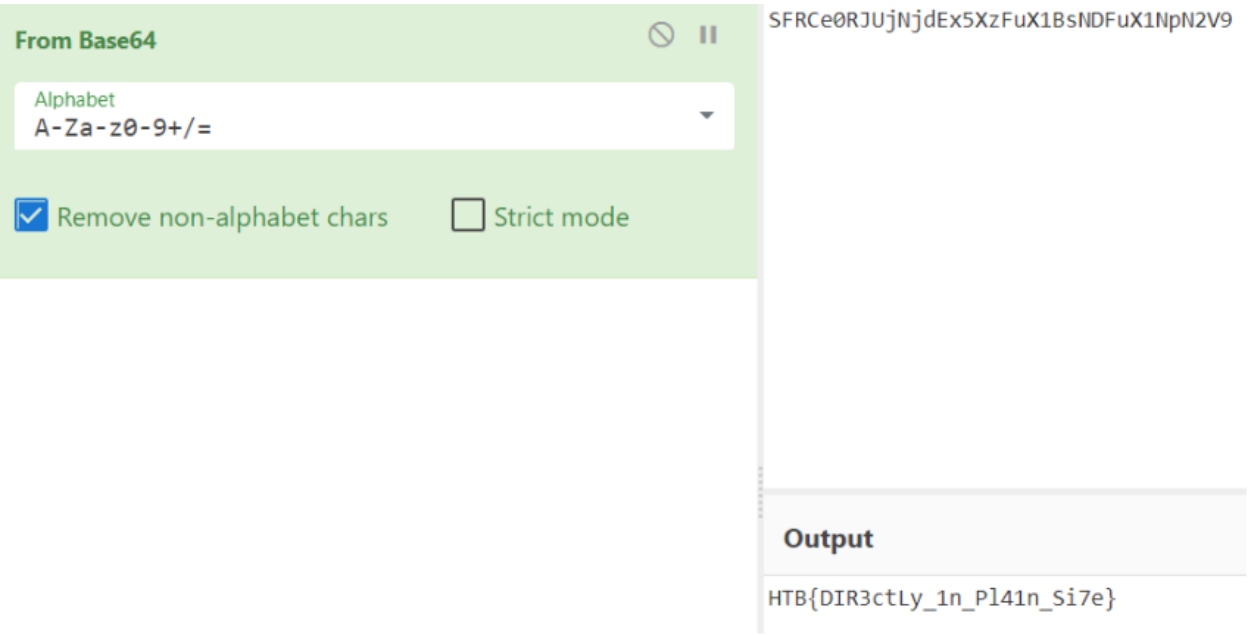
Ternyata di beberapa folder ada angka. Sehingga saya menggunakan command yang bisa membantu membuka folder secara bersamaan.

```
┌──(seraphine㉿kali)-[~/Desktop/htb]
└─$ unzip misDIRection.zip
Archive:  misDIRection.zip
[misDIRection.zip] .secret/S/1 password:
replace .secret/S/1? [y]es, [n]o, [A]ll, [N]one, [r]ename: A
 extracting: .secret/S/1
 extracting: .secret/V/35
 extracting: .secret/F/2
 extracting: .secret/F/19
 extracting: .secret/F/27
 extracting: .secret/B/23
 extracting: .secret/2/34
 extracting: .secret/R/7
 extracting: .secret/R/3
 extracting: .secret/z/18
 extracting: .secret/j/10
 extracting: .secret/j/12
 extracting: .secret/d/13
 extracting: .secret/U/9
 extracting: .secret/p/32
 extracting: .secret/N/25
 extracting: .secret/N/11
 extracting: .secret/N/31
 extracting: .secret/N/33
 extracting: .secret/e/5
 extracting: .secret/1/30
 extracting: .secret/1/22
 extracting: .secret/s/24
 extracting: .secret/D/26
 extracting: .secret/X/29
 extracting: .secret/X/21
 extracting: .secret/X/17
 extracting: .secret/9/36
 extracting: .secret/J/8
 extracting: .secret/C/4
 extracting: .secret/0/6
 extracting: .secret/E/14
 extracting: .secret/5/16
 extracting: .secret/x/15
 extracting: .secret/u/20
 extracting: .secret/u/28
```

Dari sini kita bisa melihat bahwa untuk kata tertentu, ada angka yang menjadi pengurutnya. Maka dari itu saya berusaha mengurutkan dari angka satu sampai angka terakhir.



Sehingga didapatkan string berupa = SFRCe0RJUjNjdEx5XzFuX1BsNDFuX1NpN2V9
Oleh karena itu, saya coba decode dengan base64



Akhirnya didapatkanlah flagnya.
Flag = HTB{DIR3ctLy_1n_Pl41n_Si7e}

2. TryHackMe PICKLE RICK

Start Machine

This Rick and Morty themed challenge requires you to exploit a webserver to find 3 ingredients that will help Rick make his potion to transform himself back into a human from a pickle.

Deploy the virtual machine on this task and explore the web application: 10.10.121.53

You can also access the web app using the following link: https://10-10-121-53.p.thmlabs.com (this will update when the machine has fully started)

Kali ini saya mencoba mengerjakan sebuah machine yang bernama Pickle Rick.
Kita disuruh mencari 3 ingredients atau flag dalam machine tersebut.
Seperti biasa, saya mulai dengan NMAP

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Li
ux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Android 5.1 (92%), Linux 3.13 (92%), Linux 3.2 - 3.16 (92%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

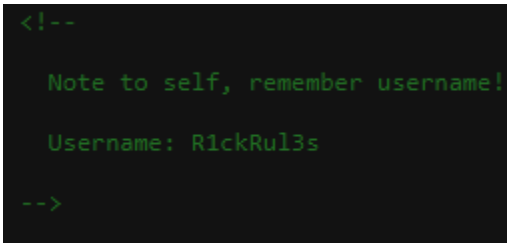
NMAP menemukan 2 port yang terbuka, yaitu port 22 dan 80.
Pada port 22, ada openSSH
Pada port 80, ada http

Help Morty!

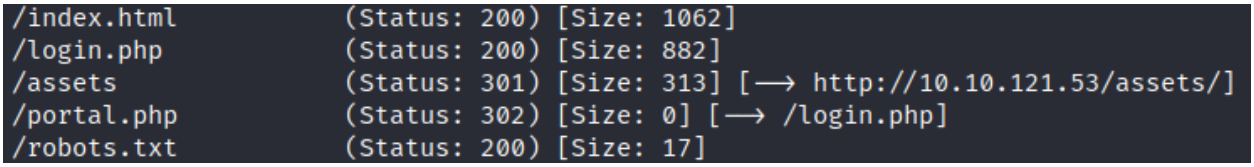
Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to *__BURRRP__*....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the *__BURRRRRRRP__*, password was! Help Morty, Help!

Jika dibuka melalui browser akan muncul page seperti ini.
Saya langsung mencoba gobuster untuk mencari hidden directory atau files
Sambil menunggu gobuster selesai saya coba buka sourcenya



Di source ada sebuah pesan yang berisikan username.
Mungkin ini akan berguna nanti.



Hasil gobuster menunjukan ada directory /login.php dan sebuah file robots.txt
login.php, seperti namanya merupakan sebuah login page

Portal Login Page

Username:

Password:

Login

Robots.txt berisikan sebuah string catch phrase

`Wubbalubbadubdub`

Sejauh ini kita sudah menemukan sebuah login page, username dan sebuah string yang mungkin adalah password
Langsung saja dicoba

Dan setelah itu muncul page seperti ini

Rick Portal | Commands | Potions | Creatures | Potions | Beth Clone Notes

Command Panel

Commands

Execute

Ada sebuah Command Panel
Dan jika dicoba beberapa command seperti ls dia akan menjalankannya

Command Panel

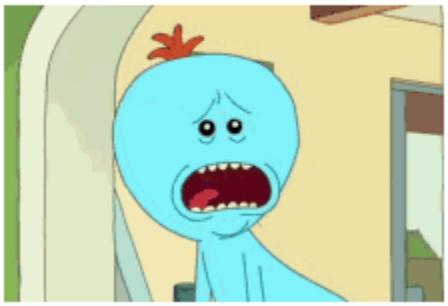
Commands

Execute

```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

Namun jika dicoba membuka dengan command cat akan muncul seperti ini

Command disabled to make it hard for future **PICKLEEEE RICCCKKKK**.



Saya coba menggunakan grep . [nama file]
Dan ternyata bisa

```
mr. meeseek hair
```

Sepertinya ini adalah salah satu ingredients yang kita cari.

Selanjutnya saya coba cuka clue.txt dengan cara yang sama
Muncul pesan seperti ini

```
Look around the file system for the other ingredient.
```

Sepertinya masih ada file yang tersembunyi
Saya coba ls /home, sebuah nama directory yang sangat common
Dan ternyata ada nama usernya.
Langsung saja ls /home/rick
Muncul seperti ini

```
second ingredients
```

Saya coba menggunakan command less
less '/home/rick/second ingredients'
Ternyata bisa dan sekarang kita dapat ingredient yang kedua

```
1 jerry tear
```

Untuk yang terakhir saya coba melihat apa yang ada di root directory
Menggunakan sudo ls /root

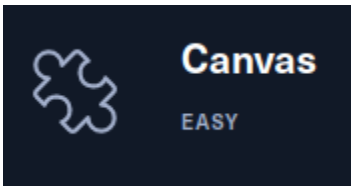
```
3rd.txt
snap
```

Nah ingredient terakhir sepertinya ada dalam 3rd.txt
Dengan command sudo grep . /root/3rd.txt seharusnya file tersebut bisa terbaca

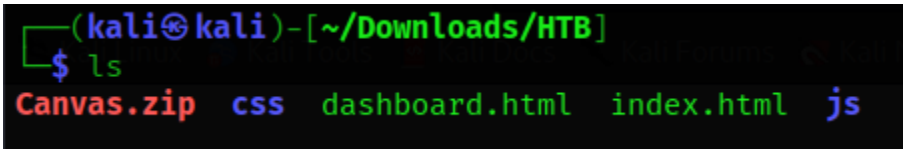
```
3rd ingredients: fleeb juice
```

Ternyata benar ingredient terakhir sudah di temukan.

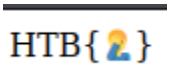
3. HackTheBox “Canvas”



Kali ini saya mencoba Canvas dari HTB
Diberikan beberapa file

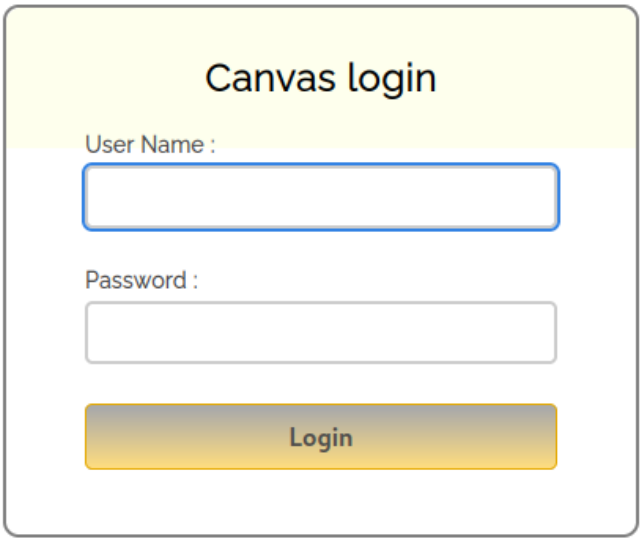


dashboard.html berisikan sebuah string seperti flag



Namun itu salah
Kemudian saya coba buka index.html

index.html berisi sebuah login page



Saya coba beberapa username dan password default, seperti admin,root,toor
Ternyata admin lah yang benar

Ternyata hanya diredirect ke dashboard.html

Saya coba buka file css

```css
@import url(http://fonts.googleapis.com/css?family=Raleway);
h2{
background-color: #FEFFED;
padding: 30px 35px;
margin: -10px -50px;
text-align:center;
border-radius: 10px 10px 0 0;
}
hr{
margin: 10px -50px;
border: 0;
border-top: 1px solid #ccc;
margin-bottom: 40px;
}
div.container{
width: 900px;
height: 610px;
margin:35px auto;
font-family: 'Raleway', sans-serif;
}
div.main{
width: 300px;
padding: 10px 50px 25px;
border: 2px solid gray;
border-radius: 10px;
font-family: raleway;
float:left;
margin-top:50px;
}
input[type=text],input[type=password]{
width: 100%;
height: 40px;
padding: 5px;
margin-bottom: 25px;
margin-top: 5px;
```

Sepertinya tidak ada yang sus amogus

Selanjutnya saya coba lihat file yang bernama login.js

Sepertinya ada text yang terenkrpsi

Setelah mencari di internet, ternyata ini ada code js yang sudah ter obfuscate.

Code obfuscation digunakan untuk mempersulit reverse engineering dari source code.

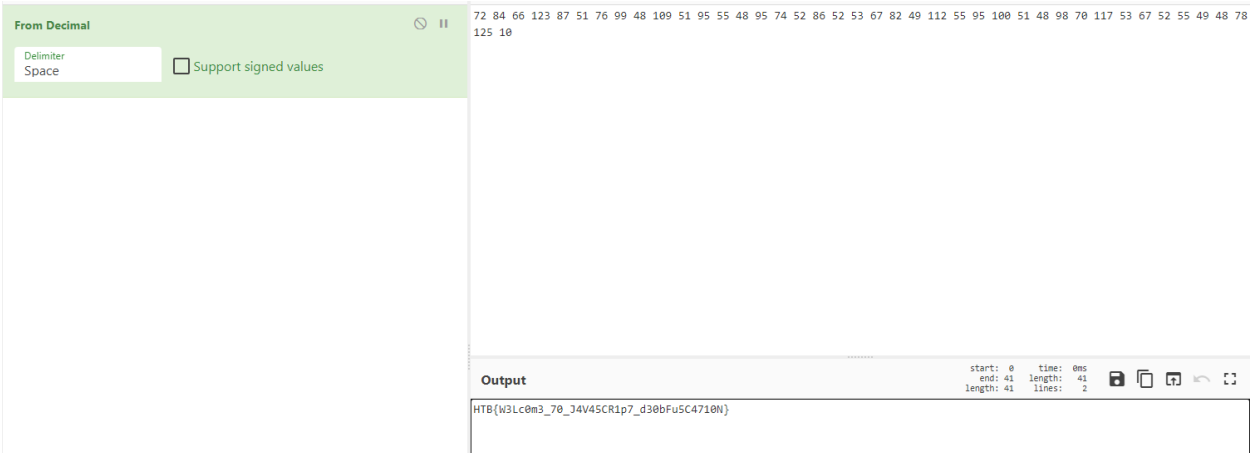
Setelah saya deofuscate code tersebut hasilnya seperti ini

```
var monikah = ["toString", "username", "console", "getElementById", "log", "bind", "disabled", "apply", "admin",
(function (kimbelry, nithya) {
  var fitzpatrick = function (abraya) {
    while (--abraya) {
      kimbelry.push(kimbelry.shift());
    }
  }, vriha = function () {
    var xoi = {data: {key: "cookie", value: "timeout"}, setCookie: function (larisha, ahlam, elaise, kyzaiah) {
      kyzaiah = kyzaiah || {};
      var felizia = ahlam + "=" + elaise, ambria = 0;
      for (var gerrilynn = 0, mailon = larisha.length; gerrilynn < mailon; gerrilynn++) {
        var delycia = larisha[gerrilynn];
        felizia += "; " + delycia;
        var samanvita = larisha[delycia];
        larisha.push(samanvita), mailon = larisha.length, samanvita !== !![] && (felizia += "=" + samanvita);
      }
      kyzaiah.cookie = felizia;
    }, removeCookie: function () {
      return "dev";
    }, getCookie: function (yuhanna, shawntaya) {
      yuhanna = yuhanna || function (lisel) {
        return lisel;
      };
      var sixto = yuhanna(new RegExp("(?:^|; )" + shawntaya.replace(/([.$?*|{}()[]\/+^])/g, "$1") + "=([^;]*)"));
```

Saya coba baca code tersebut dan saya menemukan sesuatu yang mencurigakan pada line terakhir

```
var res = String.fromCharCode(72, 84, 66, 123, 87, 51, 76, 99, 48, 109, 51, 95, 55, 48, 95, 74, 52, 86, 52, 53, 6
```

Saya coba hilangkan komma dan masukkan ke Cyberchef
Ini lah hasilnya




```
HTB{W3Lc0m3_70_J4V45CR1p7_d30bFu5C4710N}
```