TENESYS

IAM9ROOT

Akinari X ZheeK

NeverLAN CTF

➢ Cookie Monster (25 Point)   -WEB-

It's a classic https://challenges.neverlanctf.com:1110

Diberikan sebuah website yang berisi tulisan

He's my favorite Red guy

Karena judul merupakan Cookie berarti Cookie harus diganti. Di Website mengatakan favorite Red guy berarti Cookie harus diganti dengan nama karakter berwarna merah dan ku ingat jika kalian dulu pernah nonton **Jalan Sesama** atau **Sesame Street** ada karakter berwarna merah yaitu **Elmo**

Lalu, ganti Cookie dengan nama **Elmo** dengan **EditThisCookies**

You got it! flag{YummyC00k13s}

Flag : flag{YummyC00k13s}

➢ React To This (50 Point)   -WEB-

It looks like someone set up their react site wrong…

https://challenges.neverlanctf.com:1145

Diberikan sebuah website yang berisikan

Disini kita hanya membutuhkan sebuah source files bisa dengan Inspect -> Sources lalu pilih admin.js maka didapatkan flagnya
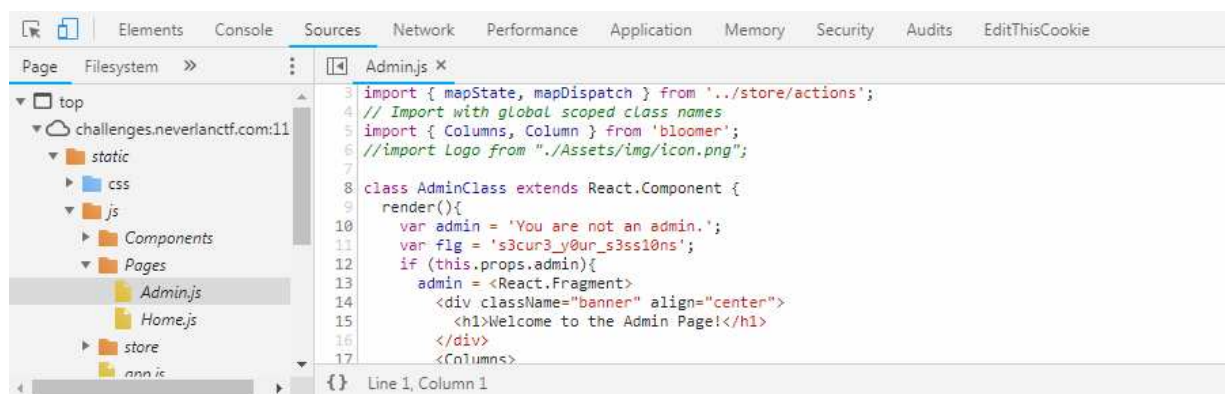
Flag : s3cur3_y0ur_s3ss10ns

➢ Dirty Validate (50 Point)   -WEB-

To keep my server from doing a lot of work, I made javascript do the heavy lifting of checking a user's password

https://challenges.neverlanctf.com:1135/

Diberikan sebuah website yang berisikan

Welcome. Login in to continue

Username [username]   Password [password]

Lalu, disini kita melihat View-Source terlebih dahulu terdapat webhooks/get_username.php
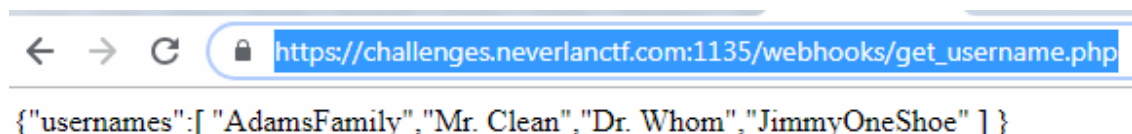
```
// For element with id='name', when a key is pressed run this function
$('#name').on('keypress',function(){
  // get the value that is in element with id='name'
  var that = $('#name');
  // make an ajax request to get the expected username
  $.ajax('webhooks/get_username.php',{})
  .done(function(data)
  { // once the request has been completed, run this function
      data = JSON.parse(data);
      if( data.usernames.indexOf(that.val()) != -1 ){ // see if the username is in the list
```

Webhooks/get_password.php

```
// For the password input now
// This is a BAD idea, never validate sensitive data in javascript
$('#pass').on('keypress', function(){
  // get value for element with id='pass'
  var that = $('#pass');
  // make an ajax request to get the expected password for the given username
  $.ajax('webhooks/get_password.php?user='+encodeURIComponent($('#name').val()),{})
  .done(function(data)
  {// once the request has completed, run this function
      // remove whitespace from data
      data = data.replace(/(\r\n|\n|\r)/gm,"");
      // check if the data matches the given value
      if(window.atob(data) == that.val()){
```

Untuk melihat username yang digunakan
https://challenges.neverlanctf.com:1135/webhooks/get_username.php

← → C 🔒 https://challenges.neverlanctf.com:1135/webhooks/get_username.php

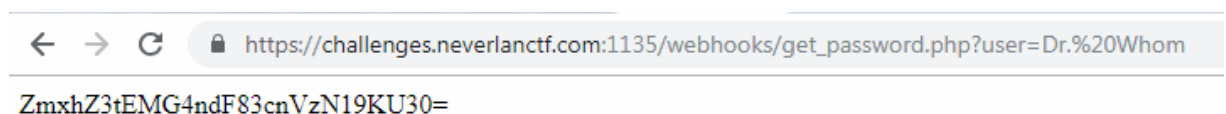{"usernames":["AdamsFamily","Mr. Clean","Dr. Whom","JimmyOneShoe"] }

Lalu untuk masuk ke data username tersebut bisa dengan
https://challenges.neverlanctf.com:1135/webhooks/get_password.php?user=input

Lakukan percobaan satu persatu dan ditemukanlah

← → C 🔒 https://challenges.neverlanctf.com:1135/webhooks/get_password.php?user=Dr.%20Whom

ZmxhZ3tEMG4ndF83cnVzN19KU30=

Lalu decode base64 to text dan didapatkan flagnya

Input value to Encode or Decode:

flag{D0n't_7rus7_JS}

Flag : flag{D0n't_7rus7_JS}

➢ Things are not always what they seem (50 Point) -WEB-

If you can't find it you're not looking hard enough

https://challenges.neverlanctf.com:1165/hello.html

Diberikan sebuah website yang berisi gambar bergerak dan beberapa rantai kata.

Welcome to the most fluid, quickest loading site you have ever encountered in your entire career. Available on every browser, every platform, everywhere. You're welcome...

CTRL + A dan flag kemudian terlihat

Welcome to the most fluid, quickest loading site you have ever encountered in your entire career. Available on every browser, every platform, everywhere. You're welcome...

Well, look at you go! You can see that sometimes everything isn't as it appears... flag{Whale_w0u1d_y0u_l00k3y_th3r3}

©Claude Rains

Flag : flag{Whale_w0u1d_y0u_l00k3y_th3r3}

➢ SQL Fun 1 (75 Point)   - WEB -

> REPORT: 'My Customer forgot his Password. His Fname is Jimmy. Can you get his password for me? It should be in the users table'
>
> https://challenges.neverlanctf.com:1150

Diberikan sebuah website dimana kita harus melakukan inputan sql query ke server

REPORT: 'My Customer forgot his `Password`. His `Fname` is Jimmy. Can you get his password for me? It should be in the `users` table'

[   ] Submit

Isi inputan dengan
SELECT * FROM users WHERE Fname='Jimmy'

id	Username	Fname	Lname	Email	Password
2	JimWill	Jimmy	Willman	SQL@example.com	flag{SQL_F0r_Th3_W1n}

REPORT: 'My Customer forgot his `Password`. His `Fname` is Jimmy. Can you get his password for me? It should be in the `users` table'

[   ] Submit

Flag : flag{SQL_F0r_Th3_W1n}

REPORT: A Client forgot his Password... again. Could you get it for me? He has a users account and his Lname is Miller if that helps at all. Oh! and Ken was saying something about a new table called passwd; said it was better to separate things

https://challenges.neverlanctf.com:1155

Diberikan sebuah website seperti challenge sebelumnya tetapi password berada di table lain, panggil menggunakan relasi antar table dengan query

SELECT a.Lname, b.Password FROM users a, passwd b WHERE a.Lname='Miller'

REPORT: A Client forgot his `Password`... again. Could you get it for me? He has a `users` account and his `Lname` is Miller if that helps at all Oh! and Ken was saying something about a new table called `passwd`; said it was better to separate things

Lname	Password
Miller	Tm9wZS4uLiBXcm9uZyB1c2Vy
Miller	ZmxhZ3tXMWxsX1kwdV9KMDFOX00zP30=
Miller	Tm9wZS4uLiBXcm9uZyB1c2Vy
Miller	Tm9wZS4uLiBXcm9uZyB1c2Vy
Miller	Tm9wZS4uLiBXcm9uZyB1c2Vy

maybe try JOINing another table

Decode string base64 tersebut dan didapatkan flagnya

Flag : flag{W1ll_Y0u_J01N_M3?}

➤ Console (75 Points)   - WEB -

You control the browser

https://challenges.neverlanctf.com:1120

Diberikan sebuah website dimana inputan akan memanggil fungsi what() pada javascript dan inputan tersebut akan dibandingkan dengan md5, terdapat pula fungsi getThat(strg) dimana fungsi tersebut jika berisi value 'Y' akan menampilkan flag dan value 'N' akan menghasilkan nilai false

```javascript
function what(){
    var input = document.getElementById("pass").value;
    if( md5(input) == "7b1ece53a46f4a5a2995b9cf901bf457" ){
        getThat('Y');
    }else{getThat('N')}
}
function getThat(strg){
    if(strg == 'Y'){
        // Note: There is no data sent to the key.php file...
        // jquery ajax reference: https://api.jquery.com/jQuery.ajax/
        $.ajax({
            type: 'GET',
            url: '1/key.php',
            success: function (file_html) {
                // success
                foo.innerHTML=(file_html)
            }
        });
    }else{
        foo.innerHTML = "Nope, try again";

    }
}
```

Kita bisa manipulasi tombol button agar langsung memanggil fungsi getThat() tentunya dengan value 'Y'

```
">
            "
  <input type="text" id="pass" value>
  <button type="submit" onclick="what()">submit</button> == $0
  <p id="p">Nope, try again</p>
</form>
<script>…</script>
/hody\
```
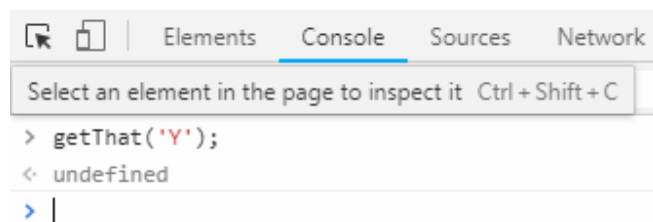
Menjadi

```
            "
  <input type="text" id="pass" value>
  <button type="submit" onclick="getThat('Y')">submit</button> == $0
  <p id="p">Password: flag{console_controls_js}</p>
</form>
<script>…</script>
'body>
:ml>
```

Atau dengan menggunakan console pada browser


```
        Elements   Console   Sources   Network

Select an element in the page to inspect it   Ctrl + Shift + C

> getThat('Y');
< undefined
> |
```

Nanti akan langsung menampilkan flag pada browser


```
>  [            ]  submit
```

Password: flag{console_controls_js}

Flag : flag{console_controls_js}

➢ Das Blog (125 Points)   - WEB -

Word on the street, Johnny's got a blog. Seems he doesn't know how to escape his inputs.

https://challenges.neverlanctf.com:1125

You have stumbled upon Das Blog

Hi, my name is Johnny and this is my blog

You must login to view posts

Diberikan sebuah website dimana kita harus login untuk melihat postnya. Lakukan basic sql injection pada halaman login

Please login here

Username Johnny'--
Password
Login

You have ADMIN permissions

The Key, Oh my, The Key

I know this post is only available for admins, and since I am the only admin on the blog, I decided to start keeping my passwords on here for quick access. Everyone says that it isin't a good idea, but I don't care, nobody reads this blog anyway...

flag{3sc4pe_Y0ur_1npu7s}

The First Entry

This is my first time writing a blog for my very own, custom made, website!!!!

I can set posts to only show for users with special permissions!

Yet another log entry that you probably won't read

so... it turns out not a whole lot of people actually visit my blog... maybe I should host it on a public server?

Flag : flag{3sc4pe_Y0ur_1npu7s}

➢ Das Blog 2(150 Points)   - WEB -

Well, we really showed Johnny. It looks like he made some changes... But he still isn't escaping his inputs. Teach him a lesson.

https://challenges.neverlanctf.com:1130

Sama seperti challenge sebelumnya yang berbeda adalah adanya hak akses 'admin' dan 'default'

Jika kita menggunakan injeksi seperti sebelumnya maka yang tampil akan seperti ini

Welcome Johnny

You have DEFAULT permissions

The First Entry

This is my first time writing a blog for my very own, custom made, website!!!!

I can set posts to only show for users with special permissions!

Yet another log entry that you probably won't read

so... it turns out not a whole lot of people actually visit my blog... maybe I should host it on a public server?

Kita akan melakukan injeksi terhadap akun pertama, kedua, ketiga,dst sampai didapatkan akun 'admin'. Untuk akun pertama kita coba dengan injeksi seperti ini

' or 1=1 limit 0,1#

Didapatkan login dengan akun 'default'. Lakukan dengan injeksi pada akun kedua dengan injeksi sebagai berikut

' or 1=1 limit 1,1#

You have ADMIN permissions

The Key, Oh my, The Key

I know this post is only available for admins, and since I am the only admin on the blog, I decided to start keeping my passwords on here for quick access.
Everyone says that it isin't a good idea, but I don't care, nobody reads this blog anyway...

flag{Pwn3d_W1th_SQL}

The First Entry

This is my first time writing a blog for my very own, custom made, website!!!!

I can set posts to only show for users with special permissions!

Yet another log entry that you probably won't read

so... it turns out not a whole lot of people actually visit my blog... maybe I should host it on a public server?

Didapatkanlah akun admin yang berada pada id ke 2 pada tabel.

Flag : flag{Pwn3d_W1th_SQL}

➤ SQL Trivia 1 (20 Points)   – Trivia –

> The oldest SQL Injection Vulnerability. The flag is the vulnerability ID.

Soal trivia dimana kita harus mengetahui Vuln ID pada SQL Injection tertua.
Dapat dicari pada website CVE

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SQL+Injection

CVE-2000-1233   SQL injection vulnerability in read.php3 and other scripts in Phorum 3.0.7 allows remote attackers to execute arbitrary SQL queries via the sSQL parameter.

Dimana SQL Injection tertua menyerang php3 dan penyerang dapat
mengeksekusi SQL Query melalui sSQL parameter

Flag : CVE-2000-1233

➤ SQL Trivia 2 (20 Points)   – Trivia –

> In MSSQL Injection Whats the query to see what version it is?

Soal trivia selanjutnya, pertanyaan pada MSSQL Injection query apa yang
digunakan untuk melihat versi

Flag : SELECT @@version

➤ Sea Quail (20 Points)   – Trivia –

> A domain-specific language used in programming and designed for managing
> data held in a relational database management system, or for stream processing
> in a relational data stream management system.

Soal trivia selanjutnya. Ez life

Flag : SQL

➢ 64 Characters (20 Points)   – Trivia –

A group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation.

Soal trivia lagi …

Flag : Base64

➢ With Some Milk (20 Points)   – Trivia –

A small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.

Soal Trivia juga …

Flag : cookies

➢ Beep Boop (20 Points)   – Trivia –

A standard used by websites to communicate with web crawlers and other web robots. The standard specifies how to inform the web robot about which areas of the website should not be processed or scanned

Soal trivia gan …

Flag : Robots exclusion standard

➢ C'Mere Piggy (20 Points)   – Trivia –

Why make bacon when you can make a cipher instead ?

If only I could remember what it's called...

Karena cluenya "make bacon when you can make a cipher" disini saya search dengan "make bacon in cipher" muncul dengan nama baconian cipher lalu ku menemukan pigpen cipher karena bacon = pig ku coba Pigpen dan benar.

Flag : Pigpen

➢ Alright.. Who is this ? (20 Points)   – Trivia –

A command line tool that tells you whois hosting a particular website.

Hanya soal trivia…

Flag : WHOIS

➢ Cover the BASEs (20 Points)   – Crypto –

ZmxhZ3tEMWRfeTB1X2QwX3RoM19QcjNfQ1RGfQ==

Diberikan sebuah encode base64 lalu di decode dan didapatkan

Input value to Encode or Decode:

flag{D1d_y0u_d0_th3_Pr3_CTF}

Flag : flag{D1d_y0u_d0_th3_Pr3_CTF}

➢ Oink Oink (75 Points)   – Crypto –

⊏�{⊐0∇⊡_⌐⊡⊐_⊐1Γ7⊲}

Diberikan sebuah gambar , soal ini muncul ketika sudah solve soal trivia yaitu "C'Mere Piggy" sehingga gambar ini merupakan sebuah Pigpen. Lalu, didecode dengan https://www.dcode.fr/pigpen-cipher dan didapatkan

(Original) ♯,♯•,×,×   FLAG DWNANDDRY

Karena ada angka dan sesuai format sehingga didapatkan sebuah flag

Flag : FLAG{D0WN_AND_D1R7Y}

➢ Alphabet Soup (125 Points)   – Crypto –

MKXU IDKMI DM BDASKMI NLU XCPJNDICFQ! K VDMGUC KW PDT GKG NLKB HP LFMG DC TBUG PDTC CUBDTCXUB. K'Q BTCU MDV PDT VFMN F WAFI BD LUCU KN KB WAFI GDKMINLKBHPLFMGKBQDCUWTMNLFMFMDMAKMUNDDA

Diberikan sebuah karakter lalu disini saya decode dengan quipqiup.com dan didapatkan

```
NICE GOING ON SO??ING THE CRY?TOGRA?! I WONDER IF YOU DID
THIS BY HAND OR USED YOUR RESOURCES. I'? SURE NOW YOU WANT A
F?AG SO HERE IT IS F?AG
DOINGTHISBYHANDIS?OREFUNTHANANON?INETOO?
```

Karena, ada yang tidak diketahui lalu disini ku menambahkan sendiri yaitu A = L , Q = M sehingga menjadi bahasa inggris yang dimengerti dan didapatkan flagnya

```
NICE GOING ON SOLVING THE CRY?TOGRAF! I WONDER IF YOU DID
THIS BY HAND OR USED YOUR RESOURCES. I'M SURE NOW YOU WANT A
FLAG SO HERE IT IS FLAG
DOINGTHISBYHANDISMOREFUNTHANANONLINETOOL
```

Flag : DOINGTHISBYHANDISMOREFUNTHANANONLINETOOL

➢ Super Old School (150 Points)   – Crypto –
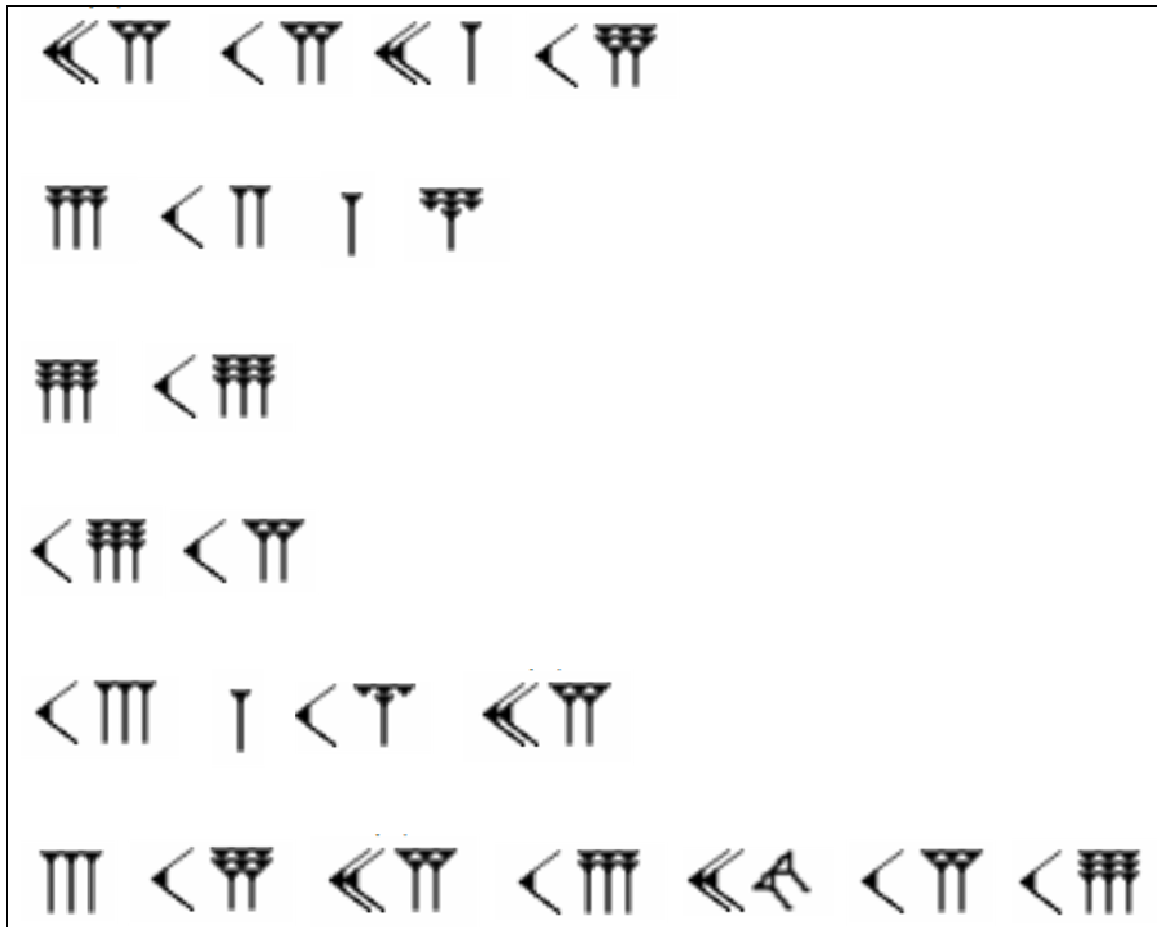
Diberikan sebuah gambar symbol, lalu disini saya melakukan **"The Power of Searching"** sehingga didapatkan sebuah asumsi yang pertama sebuah gambar yaitu cuneiform

Lalu, saya mencoba mendecode dan ternyata ada yang berbeda sehingga saya mencari yang lain karena ini hampir mirip dengan gambar soal maka saya

asumsikan bahwa ini tidak jauh jauh dari cuneiform maka saya mencari tau tentang cuneiform dan didapatkan Babylonian lalu ku asumsikan bahwa ini adalah Babylonian

Lalu, saya decode Si **Baby** ini dan didapatkan

25 15 21 18 6 12 17 9 19 19 15 13 1 14 25 3 18 25 16 20 15 19

Lalu, angka tersebut didecode ke Alphabet
YOUR FLAG IS SOMANYCRYPTOS

Flag : SOMANYCRYPTOS

➤ Z3ro Cool Bruh! (150 Points)　　　　　　　– Crypto –

Hackers keep secrets

Diberikan sebuah gambar lalu disini kita menggunakan steghide awalnya disini kita kesusahan mencari passwordnya dan ternyata passwordnya cuman "neverlanctf" tanpa ada capslock dan spasi ☹

```
D:\Tool\steghide-0.5.1\steghide-0.5.1\steghide>steghide.exe extract -sf hackers.
jpeg
Enter passphrase:
wrote extracted data to "Ohno.txt".
```

Didapatkan sebuah txt yang berisikan sebuah enkripsi dari vigenere cipher

I wonder what this is????
Fowbjcsniuwcwscotsxvevvko

Lalu disini kami decode dengan v2.cryptii.com lalu dimasukan cipher text tersebut dengan key "hackers" kenapa hackers? Karena gambar merupakan film hackers jadi diasumsikan bahwa key adalah hackers.

Key	hackers		Transform	Lowercase letters ▼
Fowbjcsniuwcwscotsxvevvko			yourflagismyfavoritemovie	

Flag : myfavoritemovie

➢ February 14th (150 Point)   - Crypto -

3,9,13,15,18,7,20,1,4,14,5,21,6,2,17,10,8,16,12,11,19

Please input the flag with no spaces! :)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
	J	O	W	W	A	S	Q	L	L	W	E	I	U	S	B	A	E	S	I	P	L
	O	W	W	A	Q	A	P	K	E	Q	I	O	O	Q	D	Z	R	D	O	U	E
	E	D	E	F	B	W	I	J	M	I	K	M	L	W	E	C	Y	E	I	R	O
	D	Z	S	D	M	P	W	H	L	A	L	K	M	E	L	K	U	W	Q	T	W
	L	D	D	L	V	I	D	W	O	S	G	I	N	Z	U	K	K	I	Z	G	D
	Z	M	H	M	D	W	A	Q	Y	L	I	S	B	V	E	P	M	P	B	Q	Z
	E	B	G	I	J	Q	S	A	T	M	S	W	J	C	W	L	V	Q	H	M	S
	G	N	U	O	O	D	F	Z	D	B	A	T	K	N	R	U	D	K	I	P	L
	S	P	I	L	R	F	Q	B	H	H	B	U	O	Q	T	U	I	L	F	U	K
	W	I	O	Q	P	L	I	V	A	G	I	I	U	A	H	Y	P	Y	L	T	Y
	F	Y	K	W	D	K	K	C	Q	O	O	Z	R	W	K	T	S	T	O	R	D
	C	Q	M	A	J	L	F	O	W	Y	R	B	W	D	M	G	O	E	I	D	T
	V	L	E	Z	Q	H	V	I	I	W	S	O	Q	F	N	N	M	D	K	Q	P
	H	A	W	M	S	Q	L	Y	O	I	M	Y	A	K	F	W	I	F	U	J	I
	Y	Q	T	L	A	W	O	H	P	R	Q	W	S	O	Q	S	T	N	W	N	O
	R	U	Y	O	X	S	E	E	L	I	W	X	D	P	A	A	P	O	E	D	U
	F	I	P	P	C	A	W	S	S	P	S	Z	X	T	S	I	O	Y	X	W	T
	M	K	Q	I	H	D	C	O	A	W	Z	W	Z	U	P	O	U	W	N	P	G
	K	L	Z	Y	U	X	F	K	Z	S	S	V	J	G	K	P	R	K	M	K	H
	I	G	S	U	W	G	I	M	X	Z	E	S	L	C	G	E	F	J	Q	Z	V
	U	F	A	R	Q	H	U	K	B	D	U	L	P	F	L	W	T	H	R	X	B

Diberikan sebuah table berisikan sebuah alphabet dan sebuah angka 3,9,13,15,18,7,20,1,4,14,5,21,6,2,17,10,8,16,12,11,19 yang merupakan clue dimana cluenya diurutkan berdasarkan angka tersebut dan didapatkanlah flag

```
W  L  U  B  S  Q  P  J  W  S  A  L  S  O  E  W  L  A  I  E  I
W  E  O  D  D  P  U  O  A  Q  Q  E  A  W  R  Q  K  Z  O  I  O
E  M  L  E  E  I  R  E  F  W  B  O  W  D  Y  I  J  C  M  K  I
S  L  M  L  W  W  T  D  D  E  M  W  P  Z  U  A  H  K  K  L  Q
D  O  N  U  I  D  G  L  L  Z  V  D  I  D  K  S  W  K  I  G  Z
H  Y  B  E  P  A  Q  Z  M  V  D  Z  W  M  M  L  Q  P  S  I  B
G  T  J  W  Q  S  M  E  I  C  J  S  Q  B  V  M  A  L  W  S  H
U  D  K  R  K  F  P  G  O  N  O  L  D  N  D  B  Z  U  T  A  I
I  H  O  T  L  Q  U  S  L  Q  R  K  F  P  I  H  B  U  U  B  F
O  A  U  H  Y  I  T  W  Q  A  P  Y  L  I  P  G  V  Y  I  I  L
K  Q  R  K  T  K  R  F  W  W  D  D  K  Y  S  O  C  T  Z  O  O
M  W  W  M  E  F  D  C  A  D  J  T  L  Q  O  Y  O  G  B  R  I
E  I  Q  N  D  V  Q  V  Z  F  Q  P  H  L  M  W  I  N  O  S  K
W  O  A  F  F  L  J  H  M  K  S  I  Q  A  I  I  Y  W  Y  M  U
T  P  S  Q  N  O  N  Y  L  O  A  O  W  Q  T  R  H  S  W  Q  W
Y  L  D  A  O  E  D  R  O  P  X  U  S  U  P  I  E  A  X  W  E
P  S  X  S  Y  W  W  F  P  T  C  T  A  I  O  P  S  I  Z  S  X
Q  A  Z  P  W  C  P  M  I  U  H  G  D  K  U  W  O  O  W  Z  N
Z  Z  J  K  K  F  K  K  Y  G  U  H  X  L  R  S  K  P  V  S  M
S  X  L  G  J  I  Z  I  U  C  W  V  G  G  F  Z  M  E  S  E  Q
A  B  P  L  H  U  X  U  R  F  Q  B  H  F  T  D  K  W  L  U  R
```

Flag : WELLIAMGLADTHATISOVER

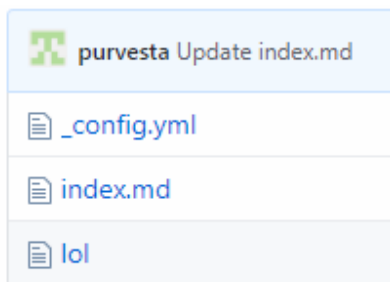## ➤ purvesta (75 Points)   – Recon –

I love Github. Use it all the time! Just wish they could host a webpage...

Diberikan sebuah clue yaitu sebuah github lalu didapatkan
https://github.com/purvesta lalu klik https://github.com/purvesta/purvesta.github.io

Lalu klik lol maka didapatkan flangnya..

Flag : flag{Th1s_g1thub_l00ks_a_l1l_sparc3}

➢ Let's go way back (100 Points)   – Recon –

Back in the day, Zesty hid a flag in the first version of our website

Diberikan sebuah clue yaitu "Let's go way back" dimana disini kita harus kembali ke masa lalu untuk mengingat masa masa indah bersama ~~Mantan~~

Disini kita ke web masa lalu dengan
https://web.archive.org/web/20160618105549/https://neverlanctf.com/
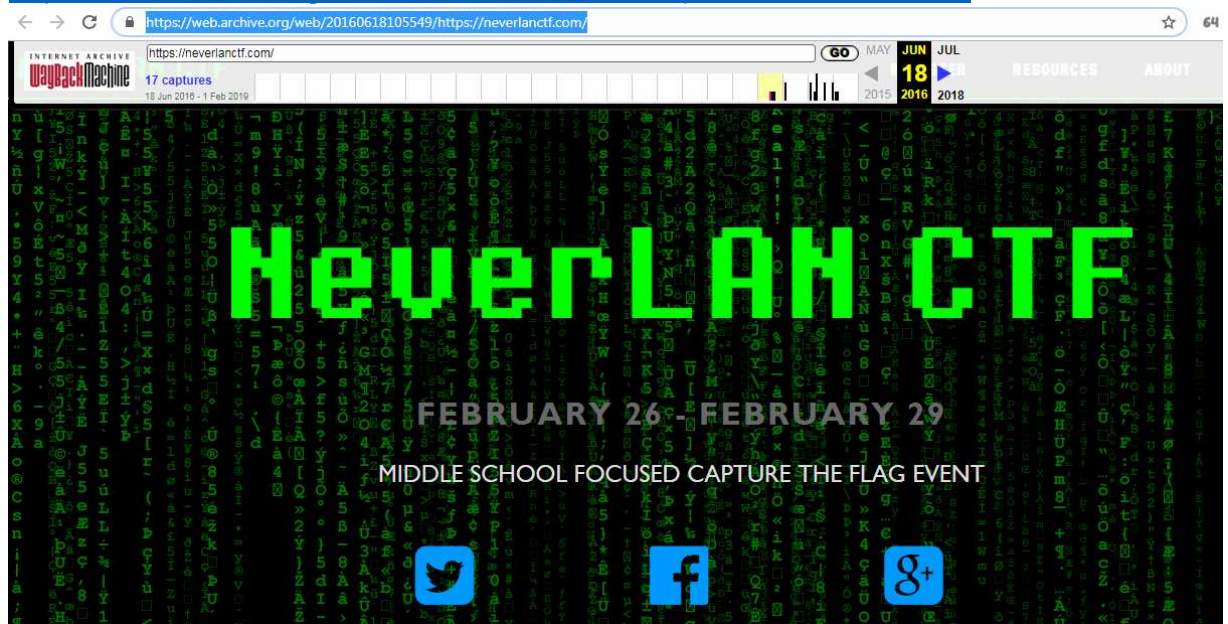
Lalu disini kita asumsikan bahwa flagnya terdapat pada gambar background untuk melihat gambarnya berikut linknya
https://web.archive.org/web/20170308143437im_/https://neverlanctf.com/img/matrix2.png

Lalu didapatkan flagnya

Flag : TheMatrixIsReal!!!

➢ Jackalope's Live Set (200 Points)   – Recon –

Need to watch to see!

Live.neverlanctf.com

Diberikan sebuah live streaming DJ dimana disini kita melihat , mendengarkan sambil bergoyang https://chew.tv/s7a73farm/dj-jackalopes-neverlanctf-mix

Flag : flag{MISSJACKALOPEDOTCOM}

➢ Tineh Nimjeh's Live Set (200 Points)   – Recon –

Whats with all the DJs having flags??

Watch to catch it

live.neverlanctf.com

Diberikan sebuah live streaming DJ dimana disini kita melihat , mendengarkan sambil bergoyang https://chew.tv/s7a73farm/tineh-nimjehs-neverlanctfs-mix

Flag : flag{HE_IS_A_TURTLE_NINJA}

➤ S7a73farm Live Set (300 Points)　　　　　– Recon –

Watch the Live DJ stream Feb 2nd 7pm MST 2am UTC url: live.neverlanctf.com
Did you see it?

Diberikan sebuah live streaming DJ dimana disini kita melihat , mendengarkan sambil bergoyang https://chew.tv/s7a73farm/neverlanctf-2019
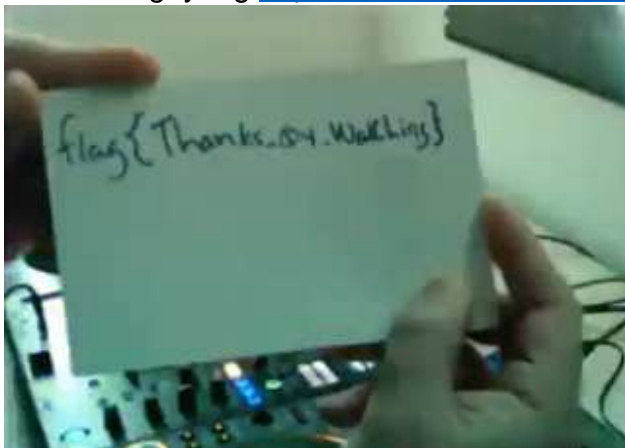
Dan didapatkan flagnya untuk mendapatkan flagnya harus teliti karena DJ yang ngasih gerak gerak dan tulisan tidak terlalu jelas ☹

Flag : flag{Thanks_04_Watching}

➢ TeachThemToHack (300 Points)　　　　　　　– Recon –

In 2018 NeverlanCTF was one of the Keynotes for a security conference. There is a video of it on youtube. I remember seeing a flag. This one is not as easy as you think.

Diberikan sebuah clue dimana kita harus mencari flag pada saat mereka mejadi sebuah pembicara di konferensi lalu mencoba search "neverlanctf 2018 conference" di youtube
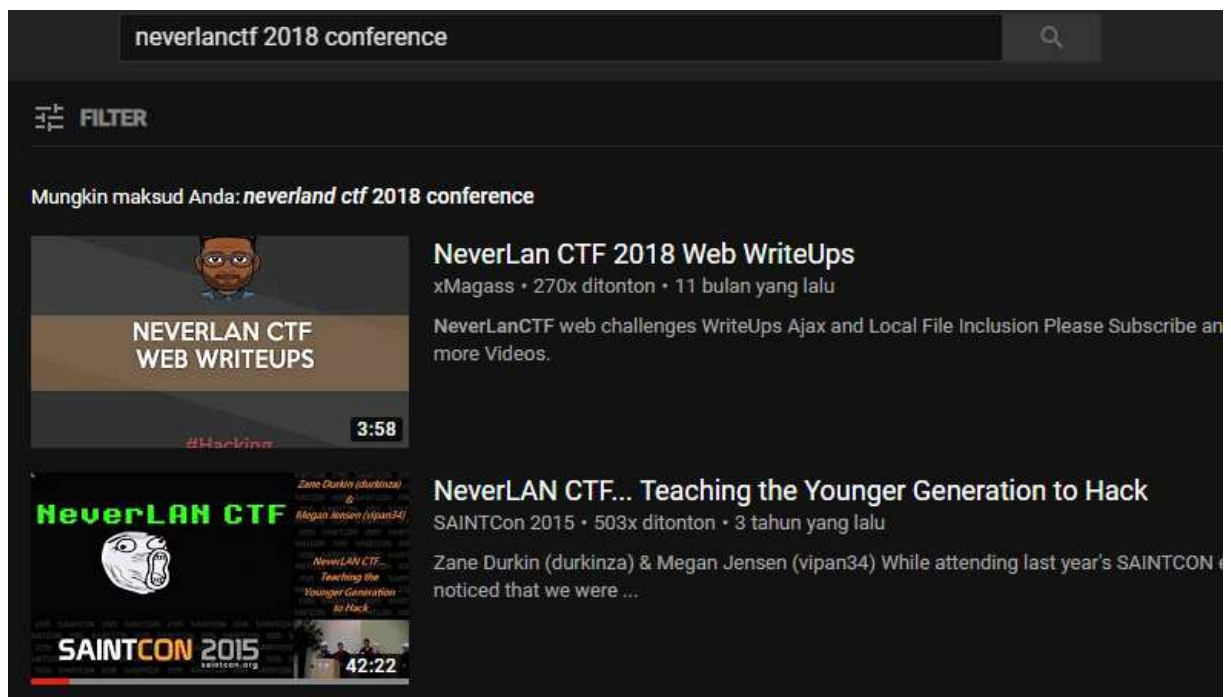
Disini kita mendapatkan clue lagi bahwa mereka pernah mengisi di konferensi SAINTCON lalu search SAINTCON untuk menemukan channel tersebut.
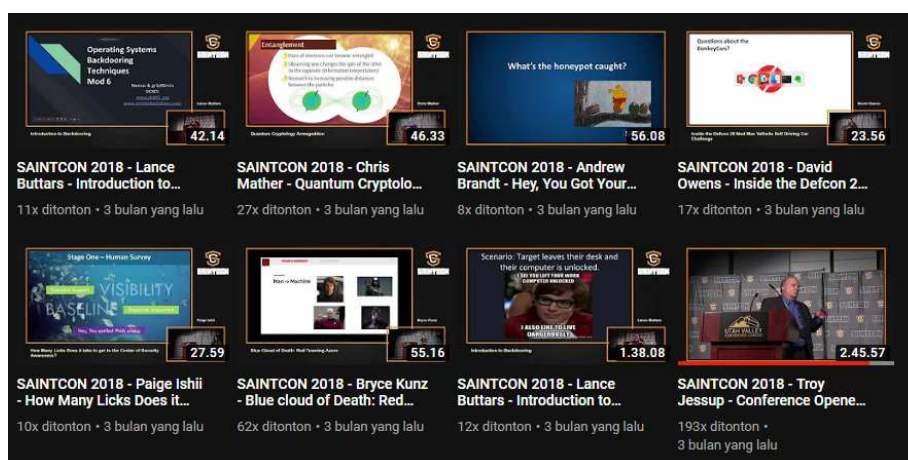
Lalu ditonton dan cari bagian dimana mereka melakuakan presentasi konferensi dan didapatkan flagnya
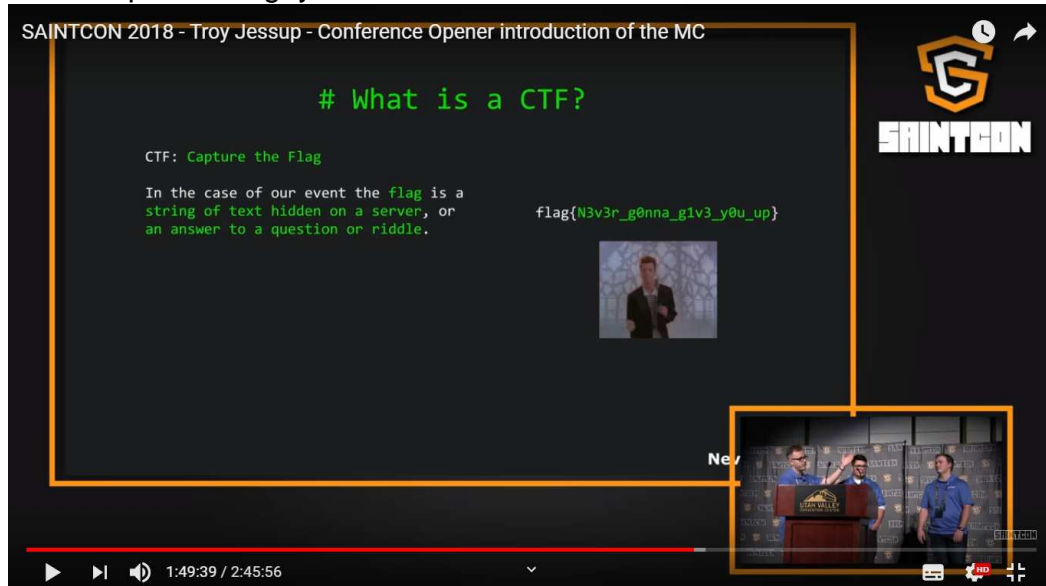
Flag : flag{N3v3r_g0nna_g1v3_y0u_up}

➢ Binary 1 (100 Points)   – Binary –

A user accidentally installed malware on their computer and now the user database is unavailable. Can you recover the data and the flag?

Flag is All Caps

6579776964584e6c636a45694f6e7369626d46745a534936496b566d5a6d

6c6c49466468636d51694c434a3163325679626d46745a534936496b4674

5a5778354c6b4a6864574e6f496977695a573168615777694f694a426147

31685a43354362326468626b426f6233355459576c734c6d4e7662534973

496d466b5a484a6c63334d694f6e7369633352795a575630496a6f6951447

39335a53425162334a3063794973496e4e316158526c526c496a6f6951584

4c6941774e5459694c434a6a61585235496a6f69695327435624746796247

Dst……

Diberikan sebuah file user_db yang berisikan hexadecimal lalu di decode menjadi base 64 lalu didecode lagi menjadi teks user database.
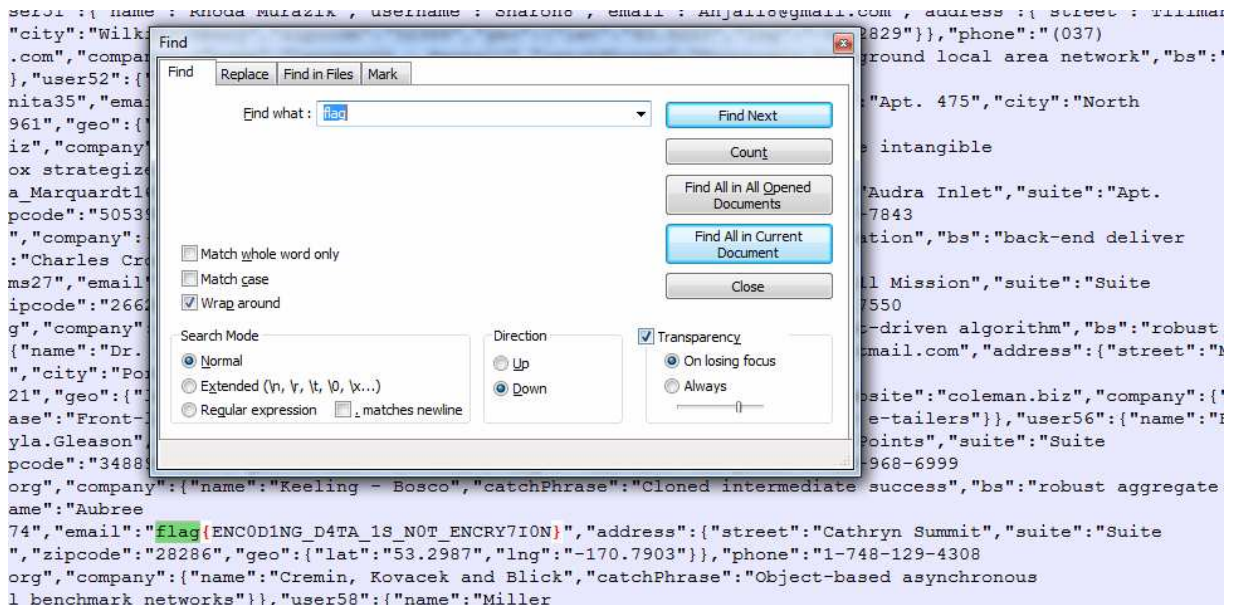
Lalu, CTRL+F flag maka ditemukan flagnya.

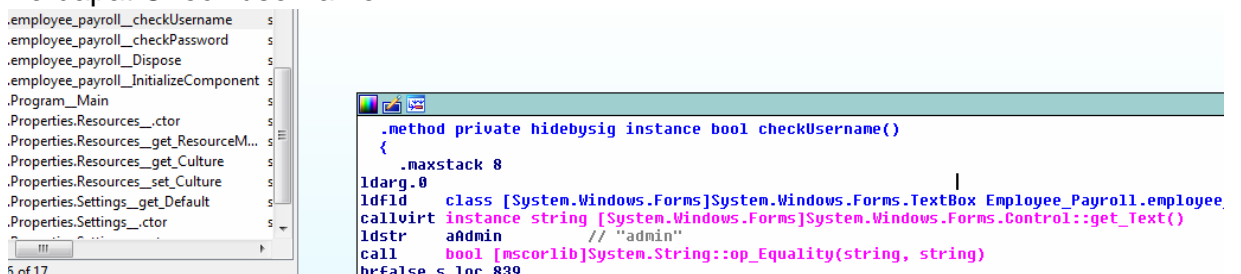Flag : flag{ENC0D1NG_D4TA_1S_N0T_ENCRY7I0N}

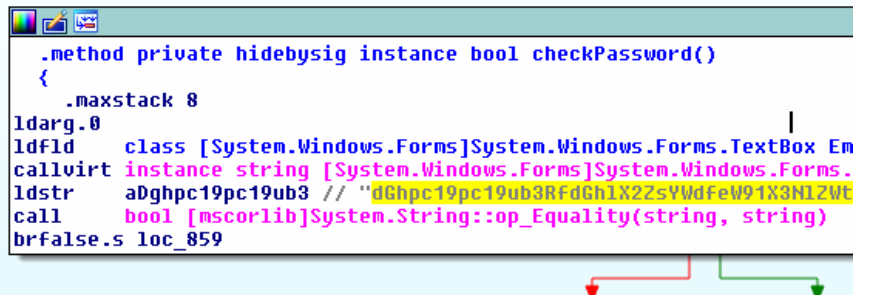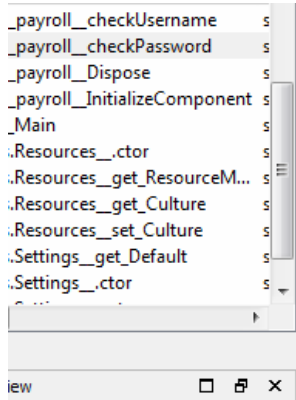## ➢ Binary 2 (200 Points)   – Binary –

> Our lead Software Engineer recently left and deleted all the source code and changed the login information for our employee payroll application. Without the login info none of the employees will be paid. Can you help us by finding login creds

Diberikan sebuah file .EXE lalu disini kami membuka dengan IDA Pro 64-bit

Terdapat Check username

Check Password

```
_payroll__checkUsername      s
_payroll__checkPassword      s
_payroll__Dispose            s
_payroll__InitializeComponent s
_Main                        s
.Resources_.ctor             s
.Resources__get_ResourceM... s
.Resources__get_Culture      s
.Resources__set_Culture      s
.Settings__get_Default       s
.Settings__.ctor             s
iew              □  🗗  ✕
```

```
.method private hidebysig instance bool checkPassword()
{
   .maxstack 8
ldarg.0
ldfld    class [System.Windows.Forms]System.Windows.Forms.TextBox Em
callvirt instance string [System.Windows.Forms]System.Windows.Forms.
ldstr    aDghpc19pc19ub3 // "dGhpc19pc19ub3RfdGhlX2ZsYWdfeW91X3N1ZWt
call     bool [mscorlib]System.String::op_Equality(string, string)
brfalse.s loc_859
```

Lalu dimasukkan admin dan password tersebut dan didapatkan flagnya

flag{ST0RING_STAT1C_PA55WORDS_1N_FIL3S_1S_N0T_S3CUR3}

Flag : flag{ST0RING_STAT1C_PA55WORDS_1N_FIL3S_1S_N0T_S3CUR3}

➢ WebCipher (300 Points)   – Scripting –

To verify that only computers can access the website, you must reverse the
Caesar cipher There are a list of possible words that the cipher may be here

https://challenges.neverlanctf.com:1160

Diberikan sebuah website, awalnya saya bingung mau ngapain seperti mikirin
~~gebetan~~

jllnunajcxa

[   ] Submit

Lalu, saya coba jllnunajcxa decode dengan quipqiup.com dan dapatkan
accelerator. Awalnya ini ku kira adalah clue lalu saya mencoba submit dengan
accelerator dan didapatkan

You got it!

flag{H3llo_c4es3r}

Flag : flag{H3llo_c4es3r}