

Write Up Nathan CTF

24 Mei 2024



Oleh Tim SatpamJaringan

1. Bryan Mogens Warren
2. Gabriell Gonardo
3. Christopher Ryan

Total Poin : 618 Points

Cryptography

1. MAYDAY, MAYDAY



Soal diatas adalah sandi morse yang menggunakan titik dan garis sebagai kodennya,

-- -- -.- .- .- -/- -.- .- .- /... /... .- .- -/- /... .- .- -/- /... .- .- /-- .- .- /-- .- .-

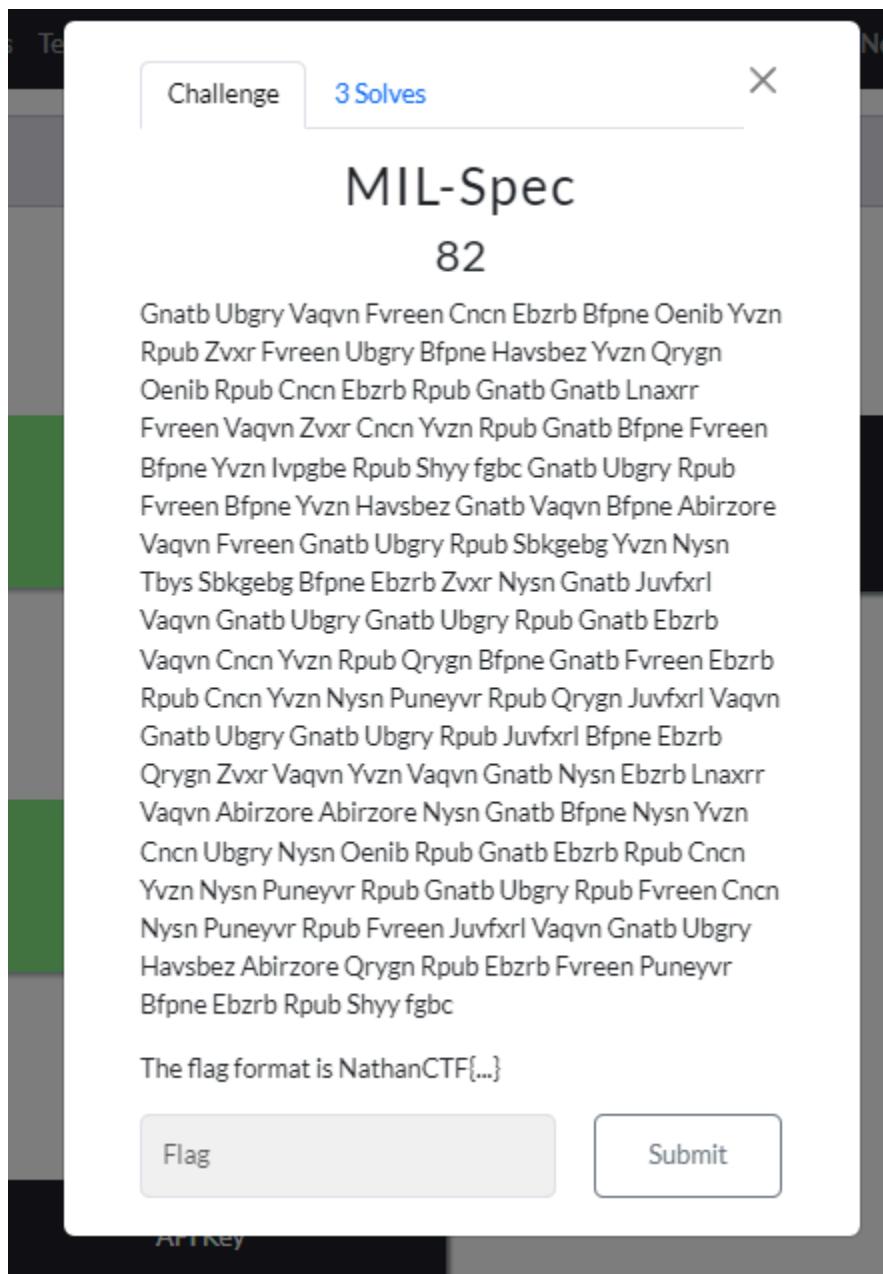
kami menggunakan morse decoder online (<https://morsedecoder.com/>), setelah memasukan kodennya kami mendapatkan pesan

MAYDAY MAYDAY OUR SHIP IS SINKING HERE IS OUR ENCODED FLAG
JZQXI2DBNZBVIRT3N5UF63TPL52GQZK7ONUGS4C7NFZV6Z3PNZSX2==

Melihat text encode diatas kami melihat ada 3 padding di akhir kode encode tersebut yang membuat kami mencurigai code tersebut adalah Base32. Kami menggunakan base 32 decoder online dan memasukan text tersebut menghasilkan flagnya yaitu

NathanCTF{oh_no_the_ship_is_gone}

2. MIL-Spec



Melihat teks diatas secara sekilas, kami mencurigai jika teks tersebut adalah Caesar Cipher, maka dari itu kami mencoba melakukan decrypt dengan caesar decrpytor dengan mencoba semua 26 kombinasi yang ada. Kami mendapatkan hasil pada putaran ke 13, hasilnya seperti di bawah ini.

↑↑	↑↑
	Tango Hotel India Sierra Papa
	Romeo Oscar Bravo Lima Echo Mike
	Sierra Hotel Oscar Uniform Lima
	Delta Bravo Echo Papa Romeo Echo
	Tango Tango Yankee Sierra India
	Mike Papa Lima Echo Tango Oscar
	Sierra Oscar Lima Victor Echo
	Full stop Tango Hotel Echo
	Sierra Oscar Lima Uniform Tango
	India Oscar November India
	Sierra Tango Hotel Echo Foxtrot
	Lima Alfa Golf Foxtrot Oscar
	Romeo Mike Alfa Tango Whiskey
	India Tango Hotel Tango Hotel
	Echo Tango Romeo India Papa Lima
→13 (←13)	Echo Delta Oscar Tango Sierra
	Romeo Echo Papa Lima Alfa
	Charlie Echo Delta Whiskey India
	Tango Hotel Tango Hotel Echo
	Whiskey Oscar Romeo Delta Mike
	India Lima India Tango Alfa
	Romeo Yankee India November
	November Alfa Tango Oscar Alfa
	Lima Papa Hotel Alfa Bravo Echo
	Tango Romeo Echo Papa Lima Alfa
	Charlie Echo Tango Hotel Echo
	Sierra Papa Alfa Charlie Echo
	Sierra Whiskey India Tango Hotel
	Uniform November Delta Echo
	Romeo Sierra Charlie Oscar Romeo
	Echo Full stop

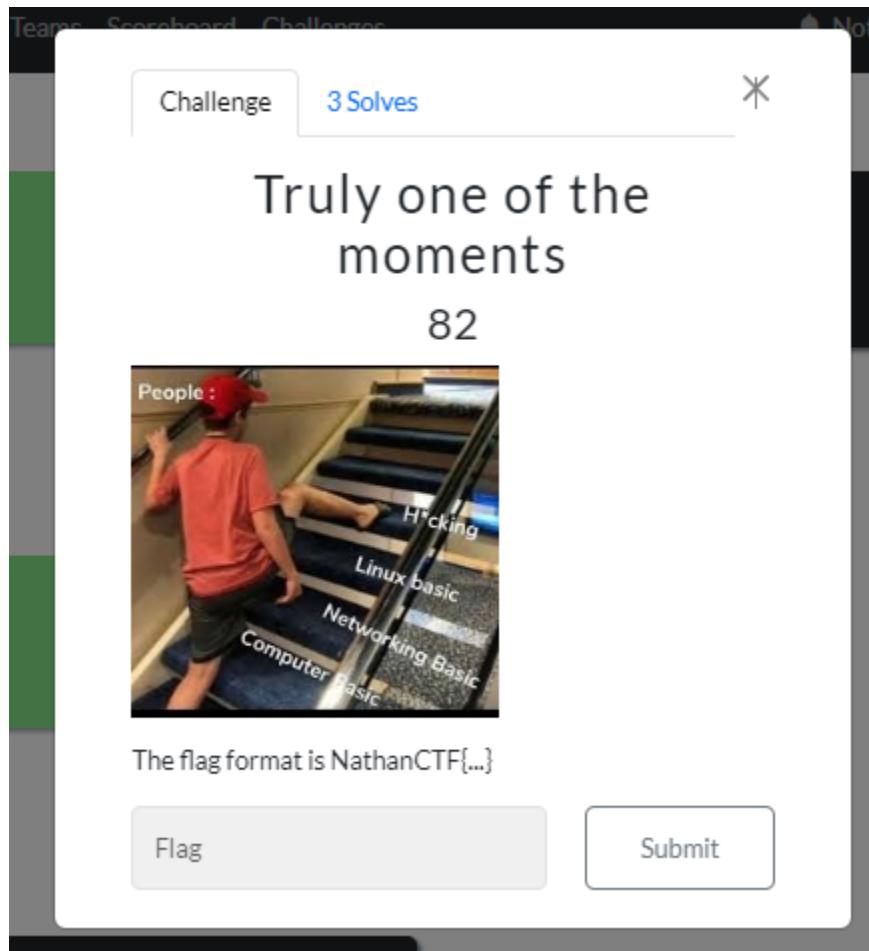
Kami cukup familiar dengan teks tersebut, lalu kami mencoba melakukan searching di google apa itu MIL-Spec, google menunjukan informasi tentang hal-hal yang berhubungan dengan military. Mengetahui hal itu kami mengingat bahwa ada kode-kode yang digunakan oleh kelompok militer yang mana pesan asli dari kode tersebut dapat dilihat dengan melihat setiap huruf depan dari kata yang ada.

Kita melakukan decode secara manual dan mendapatkan pesan akhir yang mengatakan bahwa flagnya adalah format flag dengan mengganti isinya dengan kata MILITARY tetapi dengan NATO Alphabet, dan setiap kata dipisahkan oleh underscore. Maka flagnya adalah

NathanCTF{Mike_India_Lima_India_Tango_Alpha_Romeo_Yankee}

Steganography

1. Truly One Of The Moments



Kita melakukan download pada gambar yang ada, lalu langsung melakukan semua hal yang mungkin di steganography seperti cek properties, exiftool, hexedit. Hingga kami menemukan pada hexedit terdapat flag yang disembunyikan di akhir hex edit.

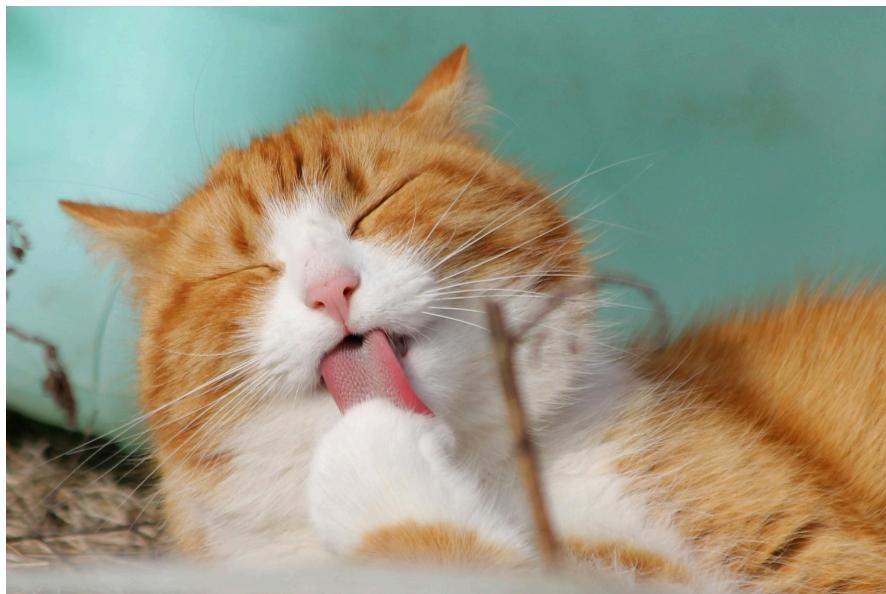
9F EA A5 32 B2 DF EC 1E	. a l K ^ 6fΩÑ2 ∞
15 46 F9 9B CE CA 8B AF	. ß0>+@ . F· c l »
3B 83 8E 61 71 F6 18 43	πΔ`ö . â. ;âÄaq÷. C
02 34 D1 87 61 6C 24 D4	}A. l f ñ. 4=çal\$ L
17 E6 D7 45 AB 89 C7 F7	£W. Ñi≥+ . μ E½ë ≈
FC DC 97 36 CA F0 BA FF	⊤_. 67∞△n ù 6 l
FC DB 9C F7 FF CA F9 FF	iQ. jΩ. T≤n £ ≈ l .
CA ED 51 21 E6 AC 14 4F	l / f. ;ôφQ!μ½. 0
75 0D FF 1F 92 E6 32 74	±.. ±./u. .Æμ2t
49 45 4E 44 AE 42 60 4E	1. `v ... TEND«B`N
7B 6B 33 33 70 5F 6C 33	athanCTF{k33p_l3
6E 64 5F 31 6D 70 72 30	4rnln6_4nd_1mpr0

vln6}é

Flagnya adalah

NathanCTF{k33p_l34rn1n6_4nd_1mpr0v1n6}

2. Stegcat



Pada challenge ini kita mendownload gambar yang ada di challenge lalu kita berusaha untuk mencari dimana letak flag nya berada. Setelah mencari ternyata kita menemukan flag nya dengan cara melakukan zoom in ke bagian kanan pada foto



Lalu kita menemukan ada flag tersembunyi di dalam foto nya

NathanCTF{c475_4r3_1nd33d_cu73}

Website

1. Breaking News!

Pada challenge ini kita mendapatkan suatu website seperti ini :

News App

Big Launching

Welcome to our fancy news website! Built with the latest technology~

New Feature

We have added a new feature to our website! Check it out now~

Bug Fix

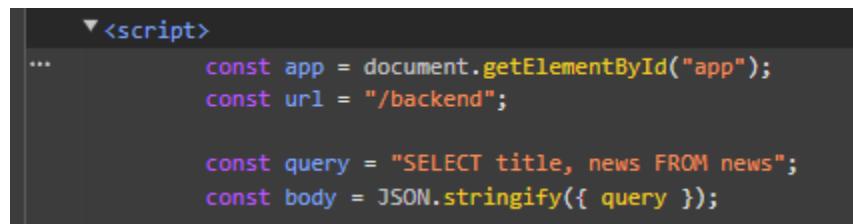
We have fixed a bug that caused the website to crash. Sorry for the inconvenience~

New Update

We have updated our website to the latest version. Enjoy~

Lalu kita mencoba untuk mencari clue/hint terlebih dahulu pada soal. Ternyata pada soal memberi tahu bahwa ada hubungannya dengan backend dan frontend.

Pada frontend kita menemukan ada nya query SQL yang seharusnya tidak ada di sana :

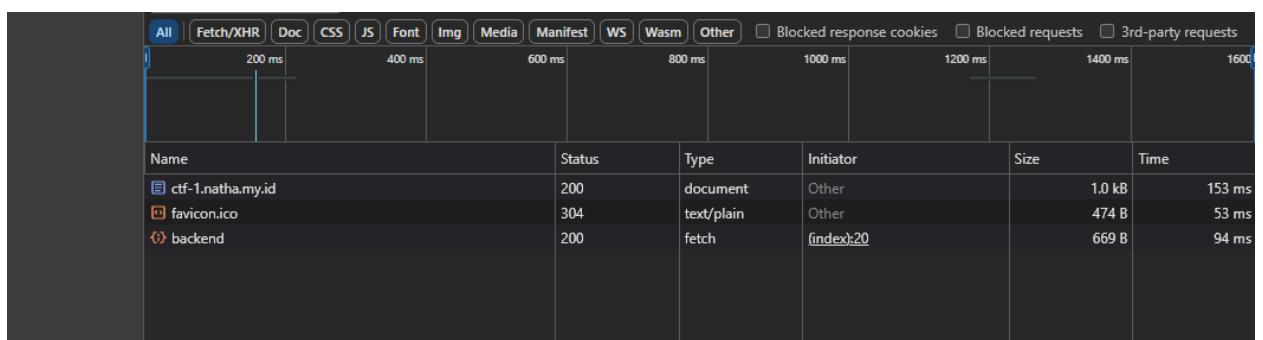


```
<script>
...
    const app = document.getElementById("app");
    const url = "/backend";

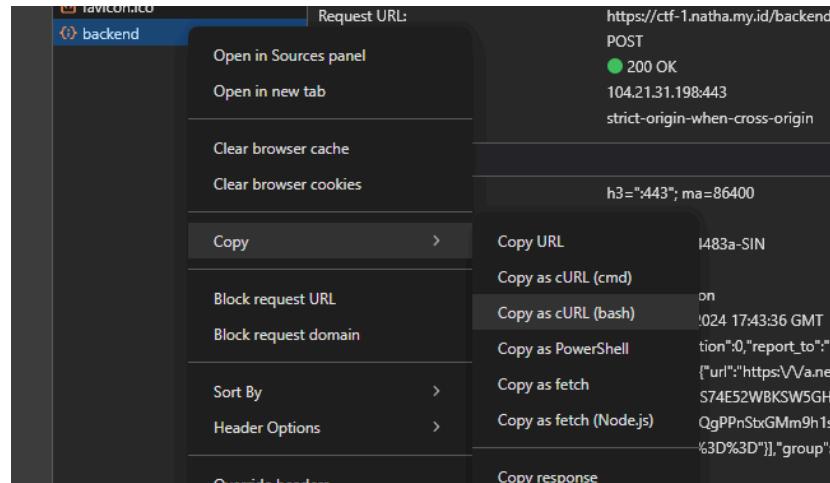
    const query = "SELECT title, news FROM news";
    const body = JSON.stringify({ query });

```

Lalu kita mencoba untuk melihat network dari website ini :



Ternyata terdapat packet “backend”

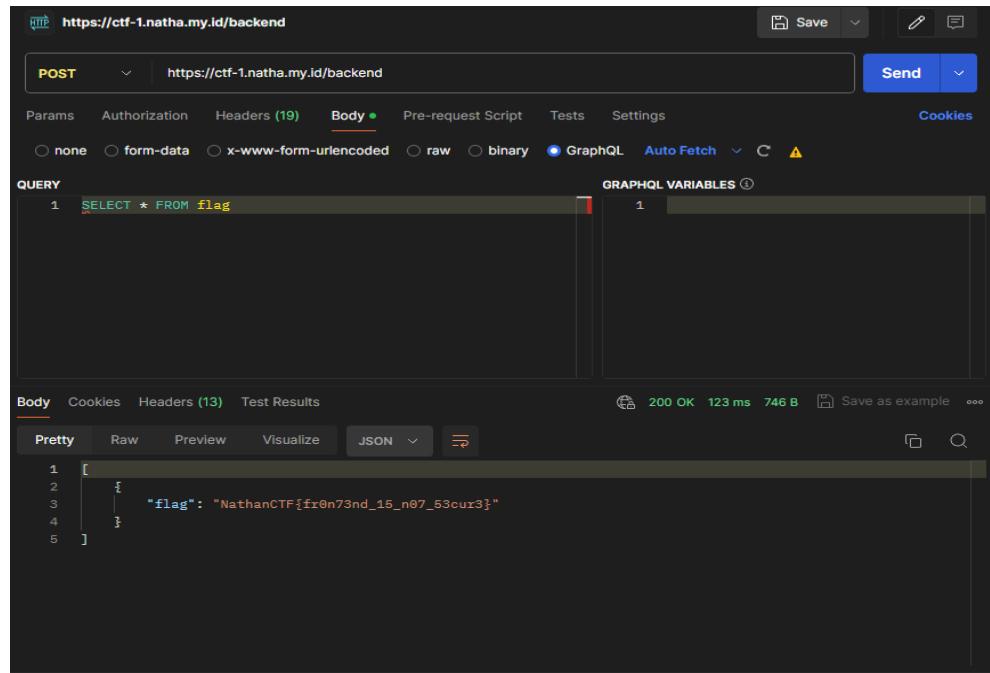


Kita copy terlebih dahulu dalam bentuk bash lalu selanjutnya kita buka menggunakan tools yang bernama POSTMAN

```

1  [ { "title": "Big Launching", "news": "Welcome to our fancy news website! Built with the latest technology~" }, { "title": "New Feature", "news": "We have added a new feature to our website! Check it out now~" }, { "title": "Bug Fix", "news": "We have fixed a bug that caused the website to crash. Sorry for the inconvenience~" } ]
  
```

Di bagian body jika kita SEND terdapat sekumpulan database. Lalu kita coba mengganti query nya dari “SELECT title, news FROM news” menjadi “SELECT * FROM flag” lalu kita SEND kembali



The screenshot shows a Postman interface for a GraphQL query. The URL is `https://ctf-1.natha.my.id/backend`. The method is POST, and the body contains the following GraphQL query:

```
1 SELECT * FROM flag
```

The response status is 200 OK, with 123 ms latency and 746 B size. The JSON response is:

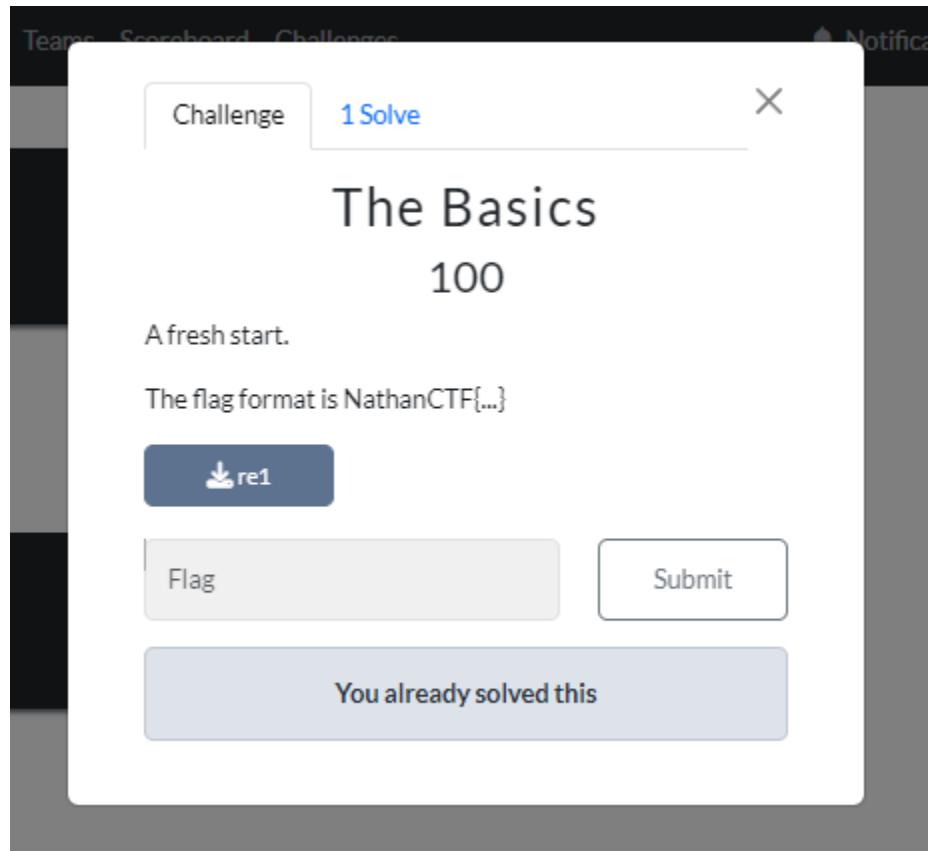
```
1 [  
2   {  
3     "flag": "NathanCTF{fr0n73nd_15_n07_53cur3}"  
4   }  
5 ]
```

Lalu kita mendapatkan flag nya :)

NathanCTF{fr0n73nd_15_n07_53cur3}

Reverse Engineering

1. Re1



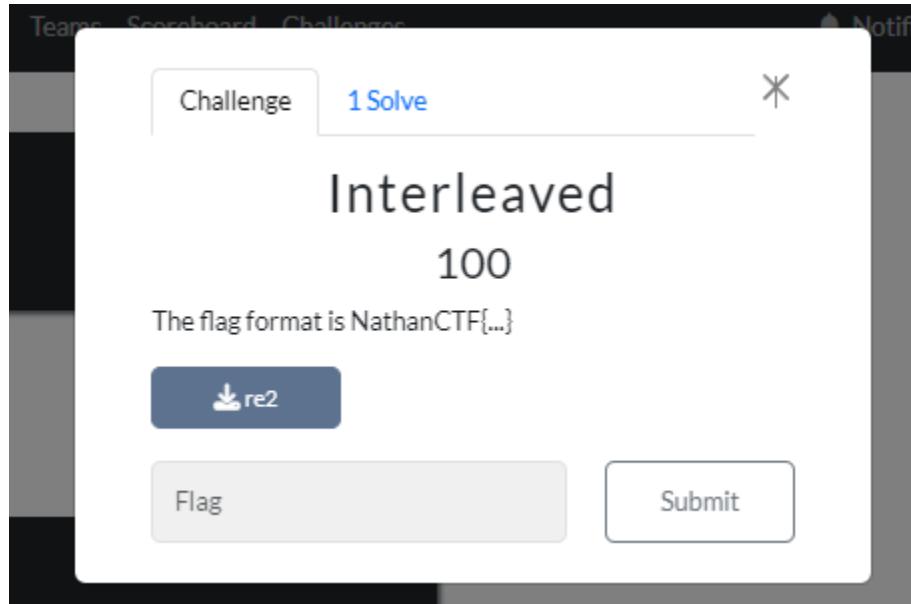
Kami mendownload file tersebut dan membukannya di Ghidra, setelah melakukan auto analyze kami menemukan string yang mencurigakan

```
1
2 undefined8 UndefinedFunction_001010e0(void)
3
4 {
5     int iVar1;
6     long in_FS_OFFSET;
7     char acStack_74 [100];
8     long lStack_10;
9
10    lStack_10 = *(long *) (in_FS_OFFSET + 0x28);
11    __printf_chk(1,"Enter password: ");
12    __isoc99_scanf(&DAT_00102015,acStack_74);
13    iVar1 = strcmp(acStack_74,"fancy password blah");
14    if (iVar1 == 0) {
15        __printf_chk(1,"Correct password! Here\\'s your flag: %c%c%c%c%c%c%c%c%c\n",0x4e,0x61,0x74,
16                    0x68,0x61,0x6e,0x43,0x54,0x46,0x7b,"w3lc0m3_70_r3v3r53_3n61n33rln6",0x7d);
17    }
18    else {
19        puts("Incorrect password!");
20    }
21    if (lStack_10 != *(long *) (in_FS_OFFSET + 0x28)) {
22        /* WARNING: Subroutine does not return */
23        __stack_chk_fail();
24 }
```

Kami mencoba memasukannya ke dalam format flag dan ternyata flag kami diterima, flagnya adalah

NathanCTF{w3lc0m3_70_r3v3r53_3n61n33rln6}

2. Interleaved



Kami mendownload file yang tertera di soal, lalu kami memasukkannya ke Ghidra untuk di analisa. Di dalam Ghidra terdapat string yang mencurigakan

```
    lVar2 = lVar2 + 1;
} while (lVar2 != 0x18);
iVar1 = strcmp(local_80,"NtaCFp4np5wr_n5uc_03hhh");
if (iVar1 == 0) {
    iVar1 = strcmp(local_68,"ahnT(11_450dl_0r3cd_444");
    if (iVar1 == 0) {
        puts("Correct password!");
        uVar3 = 0;
        goto LAB_0010118e;
    }
}
```

Melihat hal tersebut kami menyadari bahwa flagnya dipisah menjadi 2 dengan urutan selang seling. Untuk mengembalikan flagnya kami menggunakan script python.

```
▶ str1 = "NtaCFp4np5wr_n5uc_03hhh}";
str2 = "ahnT{l1_450d1_0r3cd_444";
strTot = "";
for i in range(len(str1)-1):
    strTot += str1[i];
    strTot += str2[i];

print(strTot);
```

```
→ NathanCTF{pl41n_p455w0rd_1n_50urc3_c0d3_h4h4h4}
```

Flagnya adalah

NathanCTF{pl41n_p455w0rd_1n_50urc3_c0d3_h4h4h4}