

Penugasan Oprec Cyber Security OmahTI 2024

Ravif Gayuh Wicaksono — username: Sppsr

Minggu, 17 November 2024

1 Write Up OverTheWire : Bandit

1.1 Level 0

Tujuan

Tujuan dari level ini adalah untuk masuk ke dalam permainan "Bandit" menggunakan SSH dengan host, username, dan password tertentu.

Penyelesaian

Untuk masuk dalam sebuah machine dengan SSH, langkah pertama adalah membuka terminal pada Linux terlebih dahulu. Lalu, dengan mengikuti basic command SSH.

```
ssh <username>@<server> -p <port>
```

Dalam petunjuk pengerjaan, diberi beberapa keterangan seperti

- **Username:** bandit0
- **Host:** bandit.labs.overthewire.org
- **Port:** 2220

Sehingga, dapat kita masukkan user, host, dan port kedalam basic command ssh yang ada pada documentation SSH menjadi,

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Lalu muncul beberapa baris kalimat,

```
(superposer@superposer)-[~/Desktop]
$ ssh bandit0@bandit.labs.overthewire.org -p2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([16.16.163.126]:2220)
' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
```

Selepas itu, kita diminta memasukan password untuk masuk dalam SSH tersebut, dengan password "bandit0"

```
bandit0@bandit.labs.overthewire.org's password:
OverTheWire
www. ver he ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:

* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
* PASSWORDS for each level are stored in /etc/somegame_pass/.
```

Lalu muncul beberapa pop-up yang menunjukkan bahwa kita sudah masuk dalam Over The Wire Bandit.

1.2 Level 0 – Level 1

Tujuan

Tujuan dari level ini adalah untuk masuk ke dalam file readme yang ada pada home directory, disana terdapat password untuk masuk dalam level selanjutnya.

Penyelesaian

Kita gunakan command "ls" untuk mencari semua list yang ada pada directory yang sedang kita masuki saat ini, dan ada satu file bernama readme.

```
bandit0@bandit:~$ ls
readme
```

Lalu, kita menggunakan command "cat" untuk membaca apa yang ada di dalam suatu file, yaitu

```
cat readme
```

```
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNW0Z0Ta6ip5If
```

Lalu muncul password untuk level selanjutnya.

1.3 Level 1 – Level 2

Tujuan

Tujuan dari level ini adalah untuk masuk ke dalam file dengan nama – yang ada pada home directory, dimana disana terdapat password untuk masuk dalam level selanjutnya.

Penyelesaian

Kita gunakan command ”ls” untuk mencari semua list yang ada pada directory yang sedang kita masuki saat ini, lalu terdapat satu file bernama – dalam directory tersebut. Setelah itu, digunakan command ”cat”, namun menggunakan

```
cat .\<filename>
```

Hal itu untuk menghindari ambiguitas command cat - yang dianggap terminal Linux sebagai command yang membaca masukan yang dimasukkan user, yang nantinya akan terus berulang tanpa henti. -2mm

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

Lalu selepas itu, muncul password untuk level selanjutnya.

1.4 Level 2 – Level 3

Tujuan

Tujuan dari level ini adalah untuk membaca password dalam sebuah file, tetapi nama file dipisahkan oleh spasi.

Penyelesaian

Kita gunakan command ”ls” untuk mencari semua list yang ada pada directory yang sedang kita masuki saat ini, lalu terdapat satu file bernama – dalam directory tersebut. Setelah itu, digunakan command ”cat”, namun menggunakan backslash di tiap akhir kata.

```
cat <word1>\ <word2>\
```

Hal itu dilakukan agar terminal Linux memahami bahwa nama file itu dipisahkan spasi, bukan file yang berbeda.

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx
```

Lalu selepas itu, muncul password untuk level selanjutnya.

1.5 Level 3 – Level 4

Tujuan

Tujuan dari level ini adalah untuk membaca password dalam file yang tersembunyi dalam directory inhere.

Penyelesaian

Kita gunakan command **"ls"** untuk mencari semua list yang ada pada directory yang sedang kita masuki saat ini. Kita menemukan satu folder bernama inhere. Lalu, kita mencoba masuk ke dirextory itu dengan command **cd**, yaitu

```
cd inhere/
```

Tetapi, kita harus menambahkan command **-la** setelah **ls** untuk menampilkan semua file yang diawali **"."** dan juga file yang bersifat hidden.

```
ls -la
```

Selepas itu, kita gunakan command **cat** pada file yang telah kita temukan, yaitu **"...Hiding-From-You"**.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Sep 19 07:08 .
drwxr-xr-x 3 root root 4096 Sep 19 07:08 ..
-rw-r----- 1 bandit4 bandit3 33 Sep 19 07:08 ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
ZWmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

Lalu selepas itu, muncul password untuk level selanjutnya.

1.6 Level 4 – Level 5

Tujuan

Tujuan dari level ini adalah untuk membaca password dalam satu-satunya file yang bisa dibaca dalam folder inhere.

Penyelesaian

Kita gunakan command **"ls"** untuk mencari semua list yang ada pada directory yang sedang kita masuki saat ini. Kita menemukan satu folder bernama inhere. Lalu, kita mencoba masuk ke dirextory itu dengan **command cd**.

Selepas masuk dalam folder inhere, dituliskan command **ls -la** untuk mengetahui list file secara mendetail pada folder inhere.

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -la
total 48
drwxr-xr-x 2 root root 4096 Sep 19 07:08 .
drwxr-xr-x 3 root root 4096 Sep 19 07:08 ..
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file00
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file01
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file02
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file03
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file04
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file05
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file06
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file07
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file08
-rw-r----- 1 bandit5 bandit4 33 Sep 19 07:08 -file09
```

Selepas itu, kita akan cek tiap file yang ada pada folder inhere, dengan command file, yaitu:

```
file ./<filename>
```

Untuk mengecek setiap jenis file, kita menggunakan `./.*`. Lalu kita temukan bahwa `-file07` adalah satu-satunya file yang berformat ASCII text. Lalu kita lakukan command `cat` untuk membaca file tersebut.

```
bandit4@bandit:~/inhere$ file ./.*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
cat: ./-file07: No such file or directory
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZ00E005pTW81FB8j8lxXGUQw
```

Di akhir, kita menemukan password untuk level selanjutnya.

1.7 Level 5 – Level 6

Tujuan

Tujuan dari level ini adalah membaca password dari file yang memiliki beberapa kriteria yang ditentukan.

Penyelesaian

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -la
total 88
drwxr-xr-x 22 root bandit5 4096 Sep 19 07:08 .
drwxr-xr-x  3 root root    4096 Sep 19 07:08 ..
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere00
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere01
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere02
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere03
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere04
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere05
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere06
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere07
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere08
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere09
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere10
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere11
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere12
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere13
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere14
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere15
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere16
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere17
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere18
drwxr-xr-x  2 root bandit5 4096 Sep 19 07:08 maybehere19
bandit5@bandit:~/inhere$ find ./ -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

Kita gunakan command `cd inhere` untuk masuk dalam folder inhere. Selepas masuk dalam directory, digunakan command `find` dengan indikator yang telah ditentukan yaitu:

- human-readable
- 1033 bytes in size
- not executable

Lalu, dari indikator itu kita cari menggunakan command find pada terminal Linux. Dengan -size untuk menyeleksi ukuran file sesuai dengan indikator, dan -type untuk mengetahui tipe file.

```
find ./ -size 1033c -type f
```

Selepas itu, ditemukan bahwa file2 dalam folder maybehere07 yang memenuhi indikator tersebut. Untuk mengetahui isi dari file2, kita gunakan command cat. Di akhir, kita mendapatkan password untuk level selanjutnya.

1.8 Level 6 – Level 7

Tujuan

Tujuan dari level ini adalah membaca password yang di store oleh user tertentu pada server tersebut yang memenuhi beberapa indikator.

Penyelesaian

Kita cari file dengan indikator yang ditentukan yaitu,

- owned by user bandit7
- owned by group bandit6
- size 33 byte

Dengan menggunakan command find, dengan parameter type, size, use, dan group, diikuti oleh dev/null untuk membuang semua alert denied permission. Command lengkapnya menjadi,

```
find / -type f -size 33c -user bandit7 -group bandit6 2</dev/null
```

Lalu, kita mendapat directory file yang sama dengan deskripsi yang diberikan, lantas kita gunakan command cat untuk mengetahui apa yang ada di dalamnya.

```
bandit6@bandit:~$ ls -la
total 20
drwxr-xr-x 2 root root 4096 Sep 19 07:08 .
drwxr-xr-x 70 root root 4096 Sep 19 07:09 ..
-rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 root root 3771 Mar 31 2024 .bashrc
-rw-r--r-- 1 root root 807 Mar 31 2024 .profile
bandit6@bandit:~$ find / -type f -size 33c -user bandit7 -group bandit6 2</dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLn0LFVAaj
bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Selepas itu, kita mendapat password untuk level berikutnya.

1.9 Level 7 – Level 8

Tujuan

Tujuan dari level ini adalah membaca password dalam sebuah file, dimana passwordnya terletak setelah kata "millionth".

Penyelesaian

Di awal, kita menggunakan command `ls` untuk mengetahui file apa saja yang ada didalam directory yang kita masuki. Selepas itu, dtitemukan bahwa hanya ada satu file dengan format `.txt`, yaitu `data.txt`.

Selanjutnya, kita akan menggunakan command pipe untuk menggabungkan dua command, yaitu `grep` untuk mencari sebuah string dalam file dan juga `sort` untuk mengurutkan tiap kata. Basic commandnya adalah,

```
sort <filename> | grep <words>
```

Command lengkapnya adalah,

```
sort data.txt | grep millionth
```

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ sort data.txt | grep millionth
millionth      dfwvzFQ14mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

Di samping `millionth`, terdapat sebuah string yang merupakan password dari level selanjutnya.

1.10 Level 8 – Level 9

Tujuan

Tujuan dari level ini adalah membaca password dalam sebuah file, dimana passwordnya adalah satu-satunya baris yang unik.

Penyelesaian

Di awal, kita gunakan command `ls` untuk mengetahui file apa yang akan kita ulik lebih dalam. Ditemukan satu file, yaitu `data.txt`. Setelah itu, kita gunakan pipe command untuk menyatukan command `sort` untuk mengurutkan baris sesuai abjad, dan `uniq`, yang merupakan command untuk memfilter sebuah baris. Karena kita membutuhkan satu-satunya baris yang unik, maka kita gunakan ekstensi `-u` dalam command `uniq`, sehingga commandnya menjadi,

```
sort data.txt | uniq -u
```

Kita tuliskan dalam terminal linux.

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXGqGanal4xvAg0JM
```

Setelah itu, kita mendapatkan password untuk level berikutnya.

1.11 Level 9 – Level 10

Tujuan

Tujuan dari level ini adalah membaca password dalam sebuah file, dimana passwordnya adalah kalimat yang terbaca manusia dan didahului oleh beberapa karakter `"=`".

Penyelesaian

Di awal, kita menggunakan `ls` untuk mengetahui file yang ada dan file apa yang akan kita berikan perintah berikutnya. Didapatkan satu file `data.txt` dalam directory yang kita masuki. Lalu, kita gunakan pipe command untuk menggabungkan dua command, yaitu `strings`, yang merupakan perintah dimana sebuah binary-file dapat kita ketahui teksnya, dan juga `grep` yang akan kita gunakan untuk mencari password, karena diketahui bahwa password didahului oleh banyak karakter `"=`". Commandnya menjadi,

```
strings data.txt | grep =
```

Setelah itu, kita cari strings yang didahului oleh banyak karakter sama dengan, dan cocok menjadi password untuk level selanjutnya. Lalu ditemukan password untuk level selanjutnya.

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep =
}----- the
p\l=
;c<Q=.dEXU!
3JprD----- passwordi
qC(=
~fDV3----- is
7=oc
zP=
~de=
3k-fQ
~o 0
69}=
%"-Y
~tZ-07
D9----- FGUW5i1LVJrxX9kMYMm1N4MgbpfMiqey
N~[!N
zA-?0j
bandit9@bandit:~$
```

1.12 Level 10 – Level 11

Tujuan

Tujuan dari level ini adalah membaca password dalam sebuah file, dimana passwordnya merupakan bilangan basis 64 dan harus dilakukan decode padanya.

Penyelesaian

Di awal, kita menggunakan `ls` untuk mengetahui file yang ada dan file apa yang akan kita berikan perintah berikutnya. Didapatkan satu file `data.txt` dalam directory yang kita masuki. Selepas itu, kita mencoba untuk melihat apa yang ada di dalam `data.txt` dengan command `cat`. Selepas itu, kita coba decode isi dari `data.txt` dengan command `base64` dengan ekstensi `-d` di terminal Linux. Command ini merupakan decoder/encoder yang disediakan secara default oleh Kali Linux yang berfungsi melakukan decode/encode pada sebuah bilangan basis 64. Commandnya menjadi,

```
base64 -d data.txt
```



```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMLJXbnBOVmozcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSgsg2RWnpNVj3qRr
```

Lalu kita dapatkan hasil decode dari string di dalam data.txt, dan kita berhasil menemukan password untuk level berikutnya.

1.13 Level 11 – Level 12

Tujuan

Tujuan dari level ini adalah membaca password dalam sebuah file bernama data.txt, dimana passwordnya kita dapat setelah melakukan operasi ROT13 pada string didalamnya.

Penyelesaian

Saya rasa tidak perlu melakukan perintah ls, karena secara gamblang dideskripsikan bahwa passwordnya ada pada string yang terdapat di dalam file data.txt.

Sebab hal itu, kita langsung menuju ke pipe command, dimana kita akan mengombinasikan dua command, yaitu cat dan tr untuk translating, deleting, atau squeezing sebuah string. Pada konteks level ini, perintah tr digunakan untuk merotasikan huruf, dengan teknis,

- A – M diubah menjadi N – Z
- N – Z diubah menjadi A – M
- a – m diubah menjadi n – z
- n – z diubah menjadi a – m

Hal itu diaplikasikan pada command tr menjadi,

```
cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-m'
```

Lalu,

```
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-m'
The password is 7x16WNeHIi5YkIHwsfFIqoognUTyj9Q4
```

Akhirnya muncul password untuk level selanjutnya.

2 Write Up PicoCTF

2.1 Useless : General Skill (Medium)

Deskripsi

Diberikan sebuah skrip yang melakukan beberapa perhitungan dasar. Jelajahi skrip tersebut dan temukan sebuah flag.

Penyelesaian

Di awal, ide saya adalah untuk mengecek sebenarnya skrip apa yang ada dalam directory utama pada SSH yang diberikan. Maka dari itu langkah pertama yang saya coba gunakan adalah dengan melakukan command `ls` agar setidaknya saya tahu nama file yang ada dalam directory tersebut.

```
picoplayer@challenge:~$ ls
useless
```

Setelah mengetahui bahwa nama file tersebut adalah "useless". Ide saya selanjutnya adalah apa bentuk file itu sebenarnya. Caranya adalah dengan menggunakan command

```
file useless
```

Menggunakan command tersebut, saya mengetahui bahwa file itu adalah sebuah bash script. Mengingat bahwa itu adalah bash script, saya mencoba untuk membaca apa yang ada didalam skrip itu menggunakan command

```
cat useless
```

```
picoplayer@challenge:~$ file useless
useless: Bourne-Again shell script, ASCII text executable
picoplayer@challenge:~$ cat useless
#!/bin/bash
# Basic mathematical operations via command-line arguments

if [ $# != 3 ]
then
    echo "Read the code first"
else
    if [[ "$1" == "add" ]]
    then
        sum=$(( $2 + $3 ))
        echo "The Sum is: $sum"

    elif [[ "$1" == "sub" ]]
    then
        sub=$(( $2 - $3 ))
        echo "The Subtract is: $sub"

    elif [[ "$1" == "div" ]]
    then
        div=$(( $2 / $3 ))
        echo "The quotient is: $div"
```

Pada akhir skrip saya menemukan sesuatu yang menarik, karena hal tersebut bukan merupakan operasi aritmatika.

```
        elif [[ "$1" == "mul" ]]
        then
            mul=$(( $2 * $3 ))
            echo "The product is: $mul"

        else
            echo "Read the manual"

        fi
    fi
```

Kita diminta untuk membaca manual dari CTF tersebut. Terdapat beberapa tag, seperti "Medium", "General Skills", "PicoCTF 2023", dan "man". Setelah membuka semua tag, hanya satu tag yang unik dan tak ditemukan pada CTF challenges lainnya, yaitu tag "**man**"

useless 

Medium General Skills picoCTF 2023 man

Tentu mendapatkan kata kunci seperti itu akan sangat membantu walktrough kita. Selanjutnya, mari kita coba itu menjadi sebuah perintah pada terminal Linux, dengan command

```
man useless
```

```
picoPlayer@challenge:~$ man useless
useless
useless, -- This is a simple calculator script

SYNOPSIS
    useless, [add sub mul div] number1 number2

DESCRIPTION
    Use the useless, macro to make simple calculations like addition, subtraction, multiplication and division.

Examples
    ./useless add 1 2
    This will add 1 and 2 and return 3

    ./useless mul 2 3
    This will return 6 as a product of 2 and 3

    ./useless div 6 3
    This will return 2 as a quotient of 6 and 3

    ./useless sub 6 5
    This will return 1 as a remainder of subtraction of 5 from 6

Authors
    This script was designed and developed by Cylab Africa
    picoCTF{us3l3ss_ch4ll3ng3_3xp10it3d_5657}
```

Pada akhir kode itu, kita mendapatkan sebuah flag.

Flag

```
picoCTF{us3l3ss_ch4ll3ng3_3xp10it3d_5657}
```

2.2 Rotation : Cryptography (Medium)

Deskripsi

Diberikan sebuah string pada file encrypted.txt. Kita diminta untuk melakukan decrypting pada string tersebut.

Penyelesaian

Berdasarkan penjelasan dan hint yang ada dalam kolom manual Rotation. Kita diminta untuk melakukan operasi rotasi pada string yang ada di dalam file encrypted.txt.

rotation

Medium
Cryptography
picoCTF 2023

AUTHOR: LOIC SHEMA

Description

You will find the flag after decrypting this file
Download the encrypted flag [here](#).

Hints

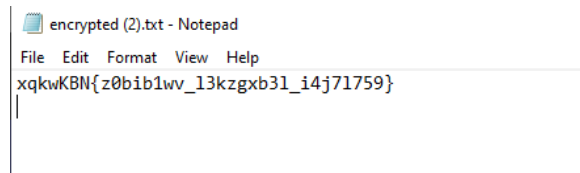
1

Sometimes rotation is right

Dalam file tersebut terlihat muncul sebuah baris huruf,

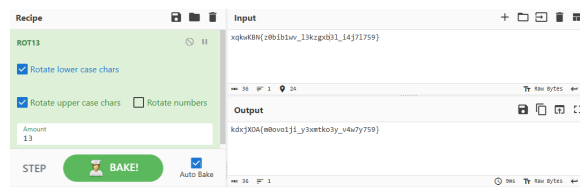
```
xqkwKBN{z0bib1wv_13kzgxb31_i4j71759}
```

Untuk menyelesaikannya, kita harus mencoba melakukan analisis pada tiap char dalam string tersebut. Dalam semua challenge PicoCTF, flag selalu punya template picoCTF. Sedangkan char pertama pada string yang ada di dalam file encrypted adalah "x".

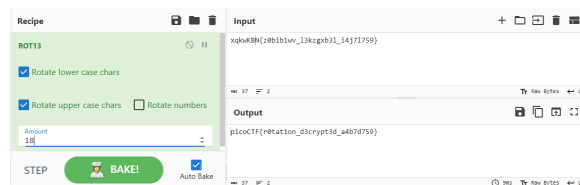


Bila kita melakukan operasi ROT13 pada Cyber Chef, yang dihasilkan bukan picoCTF, tetapi,

```
kdxjX0A{m0ovo1ji_y3xmtko3y_v4w7y759}
```





Melalui mekanisme rotasi 13, kita tahu bahwa a akan diganti n, karena a ditambah 13 adalah 14, dan huruf ke-14 adalah n. Sedangkan untuk mengganti x menjadi p, kita harus menambahnya dengan 18. Begitu pula dengan char selanjutnya. Maka kita akan menggunakan ROT18 untuk mendapatkan flagnya.



picoCTF{rotation_d3crypt3d_a4b7d759}

Deskripsi

PcapPoisoning



MediumForensicspicoCTF 2023pcap

AUTHOR: MUBARAK MIKAIL

Description

How about some hide and seek heh?

Download [this file](#) and find the flag.


Hints ?

(None)

13.876 users solved

79%

Liked

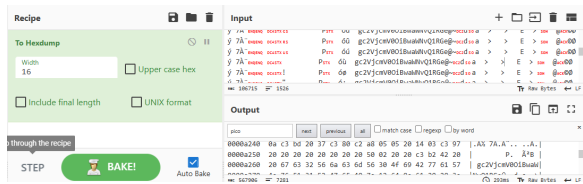
 picoCTF{FLAG}

Submit Flag

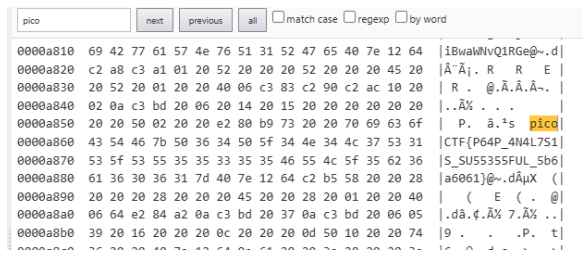
Pertama, saya mencoba untuk mengubah file pcap tersebut ke dalam txt, untuk mengetahui skrip dari file dengan ekstensi pcap tersebut.

[illegible]

Selepas itu saya menggunakan Cyber Chef untuk mengubah skrip itu kedalam sebuah hexdump.



Lantas, saya mencari kata kunci pico dalam hexdump tersebut dan saya menemukan sebuah flag dalam hexdump itu.



Flag

picoCTF{P64P_4N4L7S1S_SU55355FUL_5b6a6061}

2.4 Binary Search : General Skills (Easy)

Deskripsi

Diberikan sebuah permainan dimana kita harus menebak sebuah angka dari 1-1000 dalam 10 kesempatan, dimana program hanya akan memberi tahu kita apakah angka itu lebih kecil atau lebih besar.

EasyGeneral Skills

AUTHOR: JEFFERY JOHN

Description

Want to play a game? As you use more of the shell, you might be interested in how they work! Binary search is a classic algorithm used to quickly find an item in a sorted list. Can you find the flag? You'll have 1000 possibilities and only 10 guesses.

Cyber security often has a huge amount of data to look through - from logs, vulnerability reports, and forensics. Practicing the fundamentals manually might help you in the future when you have to write your own tools!

You can download the challenge files here:

- [challenge.zip](#)

This challenge launches an instance on demand.

Its current status is:

RUNNING

Instance Time Remaining:

28:49

Restart Instance

Hints

1 2 3

Penyelesaian

Ketika pertama melihat deskripsi dari tantangan ini, konsep pertama yang terpikirkan oleh saya adalah divide and conquer, yaitu membagi jumlahan angka pertama dan angka terakhir dengan 2 terus menerus hingga kita berhasil menemukan angka yang benar.

```
ssh -p 62477 ctf-player@atlas.picoctf.net
superposer-picoctf@webshell:~$ ssh -p 62477 ctf-player@atlas.picoctf.net
The authenticity of host '[atlas.picoctf.net]:62477 ([18.217.83.136]):6247
ED25519 key fingerprint is SHA256:M8hXanE81/Yzfs8luxNsufL4vCzCKE11M/3hp01
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[atlas.picoctf.net]:62477' (ED25519) to the l
ctf-player@atlas.picoctf.net's password:
Welcome to the Binary Search Game!
I'm thinking of a number between 1 and 1000.
Enter your guess: 500
Higher! Try again.
Enter your guess: 750
Lower! Try again.
Enter your guess: 625
Lower! Try again.
Enter your guess: 563
Higher! Try again.
Enter your guess: 594
Lower! Try again.
Enter your guess: 578
Higher! Try again.
Enter your guess: 586
Lower! Try again.
Enter your guess: 582
Lower! Try again.
Enter your guess: 580
Lower! Try again.
Enter your guess: 579
Congratulations! You guessed the correct number: 579
Here's your flag: picoCTF{g00d_gu355_de9570b0}
Connection to atlas.picoctf.net closed.
superposer-picoctf@webshell:~$ timed out waiting for input: auto-logout
Webshell session has ended.
```

Dalam permainan saya, saya menggunakan 10 percobaan, mulai dari 500, 750, 625, dan seterusnya. Lalu, selepas berhasil menemukan angka yang benar, ditemukan sebuah flag untuk challenge kali ini.

Flag

picoCTF{g00d_gu355_de9570b0}

2.5 interencdec : Cryptography (Easy)

Deskripsi

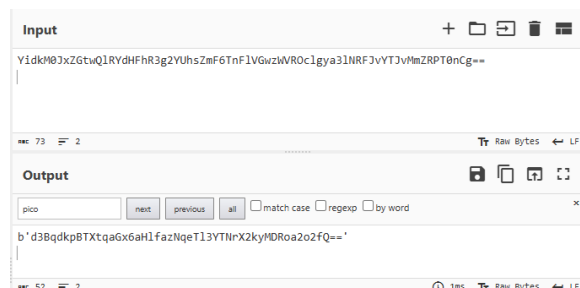
Diberikan sebuah kode, kita diminta untuk menerjemahkan itu menjadi sebuah flag yang benar.

Penyelesaian

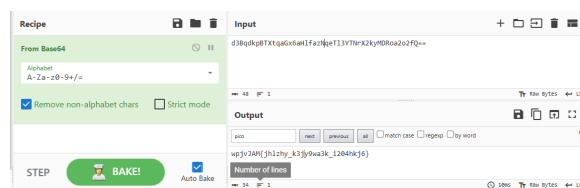
Saya mengubah ekstensinya menjadi .txt dan melihat strings yang ada di dalam enc flag. Setelah melihat susunan karakter di dalam string tersebut. Saya menyimpulkan bahwa kemungkinan besar itu adalah karakter basis 64 karena dua karakter "=" di akhir string.

```
enc_flag (3).txt - Notepad
File Edit Format View Help
YidkM03xZGtwQ1RYdHFhR3g2YUhsZmF6TnF1VGwzWVR0c1gya31NRF3vYTJvMmZRPT0nCG==
```

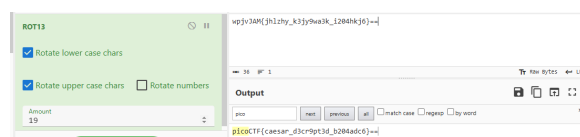
Sehingga, saya mencoba mengolahnya di Cyber Chef menggunakan tools From Base64.



Lalu dihasilkan sebuah string yang diawali b. Tetapi, melihat string di dalam petik, saya mengasumsikan bahwa string itu adalah karakter basis 64 lagi karena diakhiri oleh dua karakter "==". Selepas itu, diolah lagi menggunakan Cyber Chef dengan tools yang sama, tentu dengan mengecualikan b.



Dihasilkan sebuah string mirip dengan template picoCTF. Lalu, asumsi saya mengarah pada kita harus merotasikan string yang dihasilkan dari pengolahan tadi. Dengan menggunakan ROT amount 19, kita mampu mendapatkan sebuah flag yang sesuai dengan apa yang diminta oleh picoCTF.



Flag

picoCTF{caesar_d3cr9pt3d_b204adc6}

3 Write Up Bonus Challenges : OTI

3.1 OSINT : WH4T TH3 S1GM4 CH.1

Challenge

18 Solves

×

WH4T TH3 S1GM4 CH. 1

500

author: Mr. Vanum

Try rizzing your laptop

Difficulty: EASY

Format: OTI24{...}

▶ Unlock Hint for 0 points

▶ Unlock Hint for 0 points

▶ Unlock Hint for 0 points

▶ Unlock Hint for 50 points

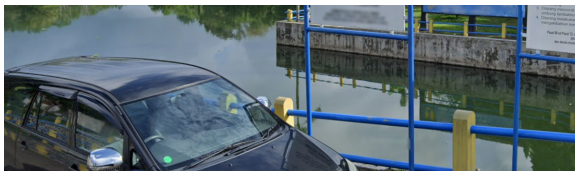
↓ chall.zip

Flag

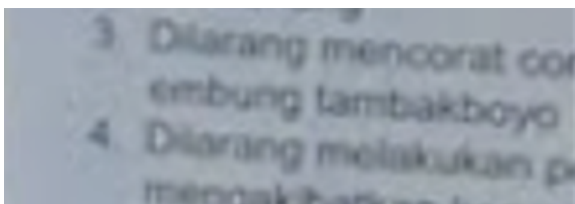
Submit

Penyelesaian

Diberikan satu file berbentuk zip yang berisi tiga gambar dengan ekstensi png dan satu file dengan ekstensi pdf. Ketika menyelam lebih jauh pada ketiga gambar, gambar kedua dan ketiga cukup membuat saya tertarik. Tetapi sesuatu yang sangat menarik ada pada gambar kedua



Bila dilihat lebih dekat lagi, kita akan menemukan sesuatu yang benar-benar menjadi kunci untuk menyelesaikan tantangan ini.



Sorry for the blurry images. Namun, terlihat jelas bahwa itu adalah **Embung Tambakboyo**.

Karena kita sudah menemukan nama dari lokasi yang kita cari. Dari penjelasan pdf yang ada pada file .zip, kita harus menuliskannya dengan huruf besar dan dipisahkan oleh underscore, bukan spasi. Sehingga, flagnya menjadi,

OTI24{EMBUNG_TAMBAKBOYO}

3.2 OSINT : WH4T TH3 S1GM4 CH.2

Challenge

14 Solves

×

WH4T TH3 S1GM4 CH.2

500


Mr. Vanum

Have you mog today?

Difficulty: MEDIUM

Format: OTI24{...}

- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 50 points

 chall.zip

Flag

Submit

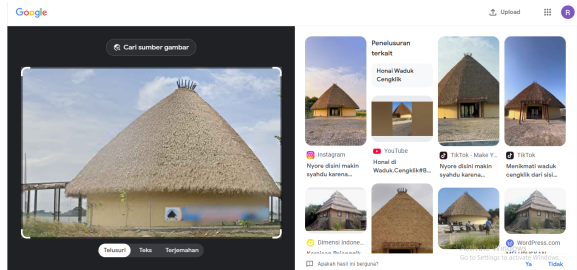
Penyelesaian

Diberikan satu file berbentuk zip yang berisi satu gambar dan satu pdf. Setelah itu, karena melihat gambar yang sangat blurry.



Saya mencoba untuk mengenhance itu agar ketika melakukan pencarian dengan image search menjadi lebih akurat.

Saya memutuskan menggunakan google image search sebagai pilihan, karena ketika menyelam pada Yandex dan Bing, saya tak menemukan titik terang sama sekali. Hasilnya sangat positif, saya menemukan tempat yang sama persis dengan apa yang ada pada tantangan itu.



Hasilnya adalah **"Rumah Honai Waduk Cengklik"**. Setelah mencoba beberapa kemungkinan flag, saya mendapatkan flag yang berhasil menyelesaikan tantangan ini, yaitu,

OTI24{HONAI_WADUK_CENGLIK}

3.3 Forensic : THE LOST JOURNEY

Challenge
10 Solves

A LONG JOURNEY

1000

author: NINOK

The first half of the flag is hidden in this photo, but the rest? It's on a wild goose chase through the author profiles and bios!

P.s. i stole the author's password: {OmahtiSlogan}, and I heard that the author never types with spaces. What a weird guy

Difficulty: Ya begitulah :)

Format: OTI24{...}

- Unlock Hint for 0 points
- Unlock Hint for 0 points
- Unlock Hint for 50 points

suprise.png

Dalam hint pertama, author memberikan sebuah petunjuk untuk menggunakan stegosuite, salah satu tools dalam Linux. Digunakan command,

stegosuite extract -k <key> path/filename

Lalu, siapa yang akan dijadikan target, tentunya adalah satu-satunya lampiran, yaitu surprise.png. Dari hint "I stole the author's password", kita tahu bahwa password atau key dari file itu adalah slogan OmahTI. Kita semua tahu, yaitu "We Make IT For Everyone", tapi dengan huruf kecil dan tanpa spasi.

Karena hal tersebut, command lengkapnya adalah:

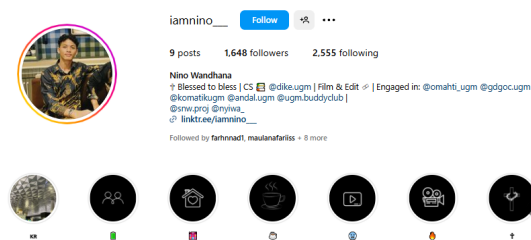
```
stegosuite extract -k wemakeitforeveryone Desktop/surprise.png
```

```
(superposer@superposer)-[~]
$ stegosuite extract -k wemakeitforeveryone Desktop/surprise.png
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Loading png image from /home/superposer/Desktop/surprise.png
Extracting data...
Extracting completed
Extracted message: hi there ;)
Extracted file saved to /home/superposer/Desktop/kiwkiw.txt
```

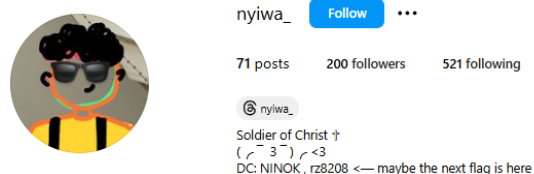
Kita mendapatkan file ekstraksi dan disimpan ke kiwkiw.txt yang berisi flag bagian pertama.

```
pTI24{D1C1UM_OT1_CH417 (1ST FLAG)
```

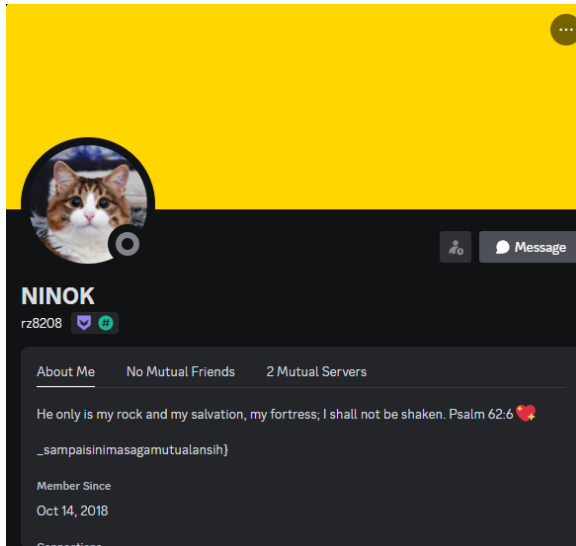
Setelah itu, kita beranjak pada hint kedua, yaitu kita harus melakukan stalking pada sosial media author.



Melalui sosial media utama author, kita menemukan second account yang memberikan kita clue lebih lanjut lagi, yaitu menuju discord author yang mungkin akan memberikan kita jalan menuju flag part kedua.

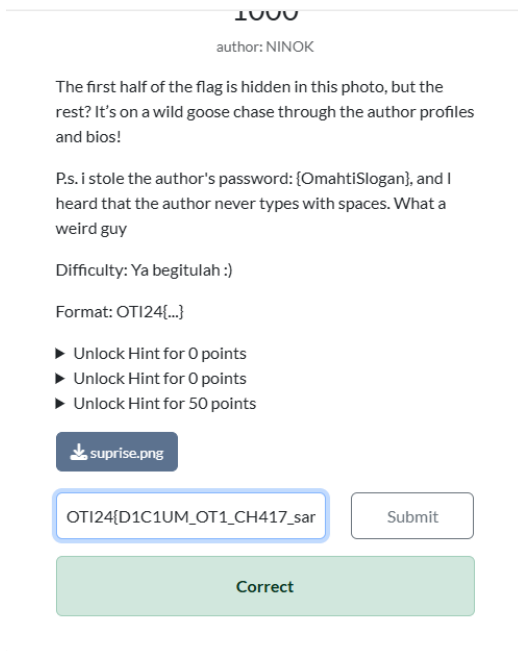


Berbekal id "rz8208", kita bisa menemukan akun discord dengan username NINOK, yang memberikan kita flag bagian kedua.



Lalu setelah itu, tahap terakhir adalah menggabungkan dua part flag yang telah kita dapatkan menjadi

```
OTI24{D1C1UM_OT1_CH417_sampaisinimasagamutualansih}
```



3.4 MISC : Color Blind

Challenge

11 Solves

✕

Color Blind


500

Mr. Vanum

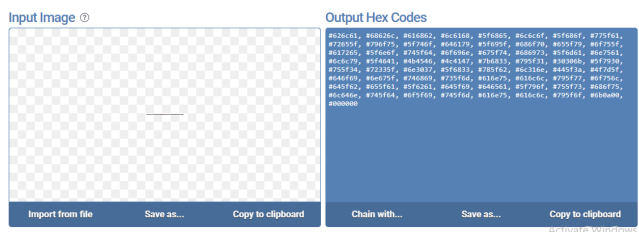
Are you color blind?

Difficulty: Medium, Annoying

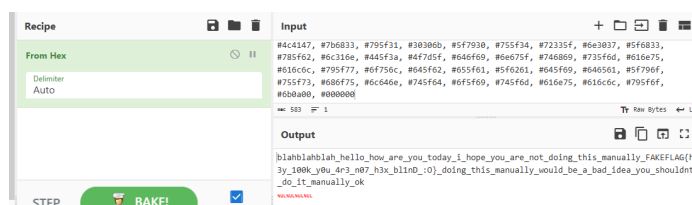
- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 200 points
- ▶ Unlock Hint for 1000 points

 colors.png

Diberikan satu file berbentuk png, dan dua hint yang "sangat membantu". Pada hint pertama, author mengatakan bahwa dalam warna itu merepresentasikan sesuatu. Saya langsung berasumsi bahwa itu hex. Secar teori, tiap warna punya dua kode, yaitu RGB dan HEX. Mengapa HEX? Alasannya adalah karena nantinya HEX bisa diubah menjadi sebuah teks. Maka dari itu, kita mengubah colors.png menjadi sebuah baris kode HEX menggunakan tools yang tersedia secara online.



Tidak berhentisampai situ, karena HEX sangat sulit untuk dibaca, maka kita menggunakan Cyber Chef sekali lagi untuk mengubah kode HEX menjadi teks yang biasa kita gunakan sehari-hari.



Oke, kita menemukan suatu hal yang menarik, yaitu **FAKEFLAG** yang ada di hasil keluaran.

```
'_FAKEFLAG{h3y_100k_y0u_4r3_n07_h3x_b11nD_:0}_'
```

Tentu saja FLAG itu masih palsu dan salah, karena flag itu tidak sesuai dengan template yang diberikan oleh OTI. Mari kita ganti awalnya menjadi OTI24.

Color Blind


500

Mr. Vanum

Are you color blind?

Difficulty: Medium, Annoying

- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 200 points
- ▶ Unlock Hint for 1000 points

 colors.png

You already solved this

Dengan mengganti awalnya menjadi OTI24, kita berhasil menyelesaikan challenge ini dengan flag

```
OTI24{h3y_100k_y0u_4r3_n07_h3x_b11nD_:0}
```

3.5 Web Exploitation : ez

Challenge

15 Solves

×

ez

500

author: kremie

it's ez

Difficulty: EZ

<https://oprec2.fitrafep.com>

source.zip

Flag

Submit

Diberikan sebuah website dengan domain **oprec2.fitrafep.com**

← ↻ 🔒 https://oprec2.fitrafep.com/login

Login

Username

Password

Login

Setelah dibuka, ternyata website tersebut berisi login page. Seperti biasa, ketika terdapat login page, reflek pake SQL Injection :b. Kita mencoba untuk melakukan bypass pada login page ini menggunakan SQLI.

← ↻ 🔒 https://oprec2.fitrafep.com/login

Login

" or "1"="1

.....

Login

Lantas kita injeksi beberapa karakter yang mampu memanipulasi SQL website tersebut. Ada beberapa cara, tetapi kita bisa memakai,

```
' or '1'='1
```

Selepas itu, kita berhasil melakukan bypass pada halaman login tersebut. Lalu, kita mendapatkan bagian pertama dari flag yang ingin kita dapatkan untuk menyelesaikan challenge ini .

OTI24{welcome_

Your notes

- [Test](#)
- [Test2](#)

[Logout](#)

Mendapatkan bagian pertama tak cukup untuk menyelesaikan tantangan ini, selanjutnya kita harus melakukan eksplorasi lebih lanjut terhadap halaman baru yang kita masuki.

Mari kita coba, untuk masuk dalam halaman Test dan Test2. Ada sedikit yang janggal pada parameter yang ada pada url mereka berdua.



Bila teman-teman perhatikan, parameternya melompat. Dari satu ke tiga, meninggalkan parameter kedua. Mari kita eksplorasi ada apa pada getnote/2 ini.



Sesuai dengan harapan, kita mendapatkan bagian kedua dari flag tersebut. Sehingga flagnya menjadi

OTI24{welcome_kidz_it's_ez_right}

3.6 Forensic : LOST IN SOUND

Challenge

12 Solves

×

LOST IN SOUND

500


author: NINOK

Legend has it, a mischievous DJ hid a secret message in this audio file. It's said that only those with the keenest ears (and perhaps a pinch of patience) can uncover it. Will you be able to crack the code, or will you just end up humming along to sweet, sweet nothing?

Difficulty: Medium - Hard

Format: OT124{...}

- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 50 points

 chall.wav

Flag

Submit

Kita diminta untuk melakukan ekstraksi pesan rahasia yang diberikan author pada audio file yang dilampirkan, yaitu chall.wav.

Pada hint kedua, diberikan suatu petunjuk bahwa kita harus menggunakan tools bernama audistego, untuk mengekstraksi pesan rahasia tersebut (meski mengorbankan 50 poin, tapi ini worth it).

Instalasi tools audistego, dan setelah selesai melakukan instalasi, step selanjutnya adalah memindahkan file chall.wav ke dir AudioStego agar mampu kita ekstrak dengan tools AudioStego, caranya adalah,

```
(superposer@superposer)-[~]  
$ sudo cp Desktop/chall.wav /AudioStego
```

Selepas melakukan copy chall.wav ke dir AudioStego, hal yang harus kita lakukan selanjutnya adalah menuliskan command,

```
ExtractMsg.py -f chall.wav
```

Sehingga, tools audistego melakukan kerjanya dan mampu mengekstrak teks rahasia yang ada pada chall.wav. Sesuai dengan harapan, teks rahasia yang disembunyikan dalam file tersebut adalah flag yang kita butuhkan.

```

  A n n o u n c e m e n t
Created By
sh: 1: toilet: not found
For Any Queries Mail Us!!!
Mail: thedarktech.yt@gmail.com
YouTube Page: https://www.youtube.com/channel/UC6_l3aewNjpPYSkG0TpxSCA

Initializing.....!!!
Extracted Secrate Msg : OTI24{C017GR4T5_Y0u_C4n_kn0W_c0mmun1c4t3_w1th_4ud10_h3h3h3h3}

(superposer@superposer)-[~/AudioStego]
$
```

Sehingga kita berhasil menemukan sebuah flag, yaitu

OTI24{C017GR4T5_Y0u_C4n_kn0W_c0mmun1c4t3_w1th_4ud10_h3h3h3h3}

3.7 Web Exploitation : The Costumer Is Always Right

Challenge

9 Solves

×

The Customer is Always Right

750

I've opened up a new flag market. For total transparency, we're allowing refunds on any product at any time for any reason. After all, the customer is always right!

<https://chall2.fitrafep.com>

Format: OTI24{...}

Submit

Diberikan suatu website, dan dalam manualnya tertulis bahwa untuk transparansi total, kita dipersilahkan untuk melakukan refund pada produk yang ada di sana.

```
Flag Market

For all your flag needs, both fake and
real.
User balance: $10
Transactions

Fake Flag Buy for $10
Real Flag Buy for $100

Source
```

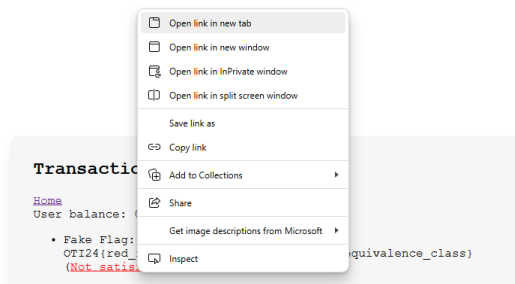
Selepas masuk pada halaman web, kita diberikan uang sebanyak 10 dollar untuk melakukan pembelian produk yang ada di dalam website tersebut. Dalam website tersebut ada dua pilihan produk, fake flag dengan harga 10 dollar dan real flag dengan harga 100 dollar. Mari kita coba eksplorasi dengan membeli fake flag terlebih dahulu.

```
Transactions

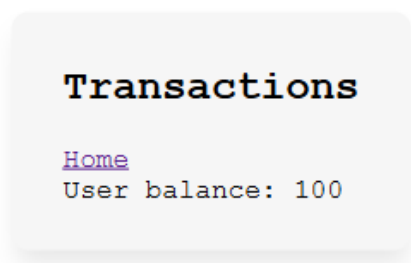
Home
User balance: 0

• Fake Flag:
  OTI24(red_flags_and_fake_flags_form_an_equivalence_class)
  (Not_satisfied?)
```

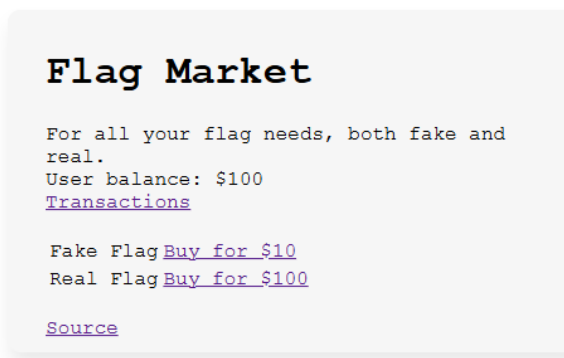
Selepas membeli fake flag, sama seperti manual, terapat pilihan "not satisfied" untuk melakukan refund. Namun, hal itu hanya akan mengembalikan 10 dollar kita tanpa menambah apapun. Dari manual, saya memiliki asumsi bahwa kuncinya ada pada sistem refund ini. Saya mencoba untuk membuka link refund itu tab baru.



Ternyata, kita bisa melakukan eksploitasi di sini, dimana kita mampu untuk menambah uang kita secara terus-menerus tak henti dengan melakukan pengembalian pada tab yang baru. Tetapi, kita harus membuka semua tab, yaitu 10 tab terlebih dahulu sebelum melakukan klik pada button refund.



Sehingga, uang yang kita dapatkan adalah 100 dollar.



Selepas itu, kita bisa membeli produk real flag, dan mengetahui apa isi di dalamnya.

Transactions

[Home](#)

User balance: 0

- Real Flag: OTI24{4s1kS8TpuWj37kdjDKFywRN5JLuh9D8z} ([Not satisfied?](#))

Beruntungnya, produk itu menghasilkan flag yang dapat menyelesaikan tantangan ini, yaitu

OTI24{4s1kS8TpuWj37kdjDKFywRN5JLuh9D8z}

3.8 Cryptography : Beauty and the Beast

uname: Spsr

750

Mr. Vanum

Once upon a time, a noble prince was cursed by a wicked witch, his form twisted into a terrifying Beast by a powerful hex. The hex could only be broken if the Beast solved an ancient spell, filled with cryptic riddles and symbols, but the key to unlocking it lay beyond his understanding. One day, as you, a traveler, wandered through the enchanted forest, you encountered the Beast and Beauty, desperate for help. They turned to you and asked, "Can you help us solve the complex spell and break the hex that binds me?"

4f544932347b485461685f65745f6877616f747273645f5f6a6175727365745f5f7761655f6964726964765f656272757374695f6f746e685f696973665f5f6979736f5f5f7461686e65735f776b656572795f5f74416862617274615f6379616f6475615f6261727261655f5f74776872656f5f6e7367705f656d6c756c615f68696173685f616e686f5f77735f69626b72656f5f6b6265756e747d0d0a

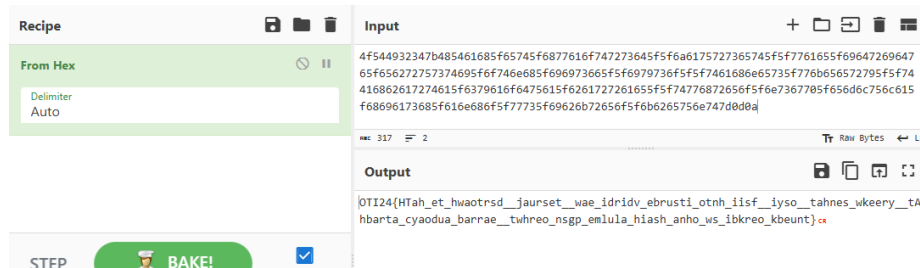
Difficulty: Medium

▼ Unlock Hint for 0 points

The story is so heart-wrenching

Kita diberikan sebuah narasi panjang tentang beauty and the beast, terima kasih atas cerita yang sangat mengharukan :D Tetapi, ada beberapa clue dalam cerita itu. Yang saya temukan pertama adalah penggunaan **Hex** yang terus berulang. Apa itu hex, yak saya berasumsi bahwa itu hexadecimal. Mengingat, kode itu juga sangat mirip dengan kode hexadecimal jika dilihat secara lebih jauh.

Maka dari itu kita bisa mencoba melakukan decrypt dari Hexadecimal menuju ASCII text menggunakan Cyber Chef, dan hasilnya cukup memuaskan.

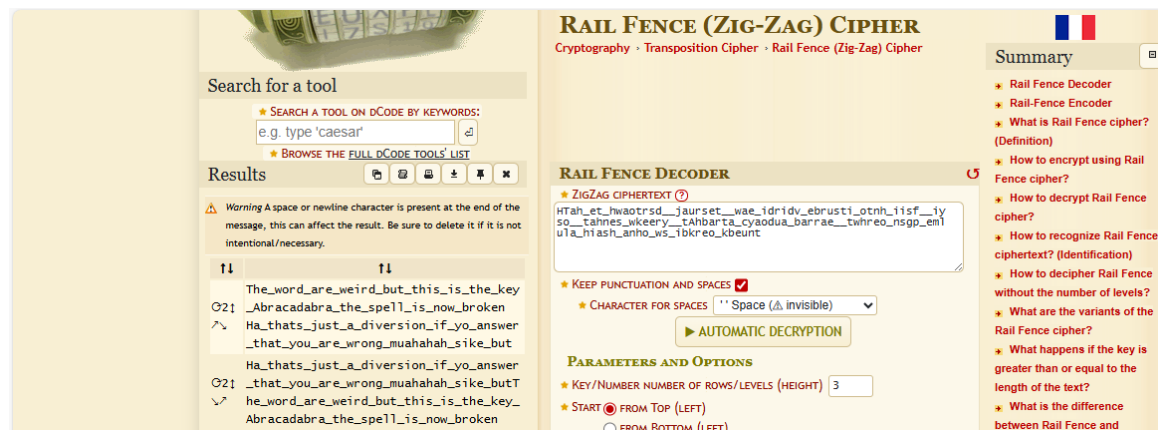


Kita mendapatkan sebuah string yang sudah mendekati apa yang kita inginkan, yaitu:

```
OTI24{HTah_et_hwaotrsd__jaurset__wae_idridv_ebrusti_otnh_iisf__iyso__tahnes_wkeery__tAhbarta_cyaodua_barrae__twhreo_nsgp_emlula_hiash_anho_ws_ibkreo_kbeunt}
```

Tetapi, apa yang ada di dalam kurung kurawal bukanlah flag yang sebenarnya. Sekali lagi saya melakukan eksplorasi yang lebih dalam. Dengan analisis sederhana, saya memahami bahwa ada dua underscore yang saling samping-sampingan, sehingga kita perlu memisah antara underscore satu dengan yang lainnya agar mendapatkan sebuah kalimat yang benar.

Apakah saya mempunyai ide, tentu di awal tidak. Saya mencoba membaca ulang beberapa hand-book cryptography dan menemukan bahwa ada beberapa kemungkinan. Caesar cipher, Vignere, Transpositional, dan Rail Fence. Sayangnya karena kurangnya pengetahuan saya, saya melakukan brute force pada tiap metode cipher dan akhirnya menemukan sesuatu pada rail fence cipher.



Ada dua hasil decrypt yang sangat mendekati flag kita, alasannya karena kita telah menemukan kalimat yang bisa dibaca manusia normal seperti saya. Tetapi kalimat itu masih sangat ambigu. Tetapi ditunjukkan bahwa sebenarnya key nya ada pada Abdacadabra sampai broken. Meski saya cukup kaget dengan kalimat setelahnya, tetapi ketika kita mencoba memasukan

```
OTI24{Abracadabra_the_spell_is_now_broken}
```

Difficulty: Medium

► Unlock Hint for 0 points

OTI24(Abracadabra the spell is n

Submit

Kita berhasil menyelesaikan tantangan ini.