

Cyber Security Community

WRITEUPS 2



Nama Lengkap : Satya Kusuma & Vincentius Farrel
NIM : 2540124740 & 2602084054
Discord Username : Q.#0863 & chomusuke#7595

Web Exploitation: Secrets

Secrets 

 | 200 points

Tags: **picoCTF 2022** **Web Exploitation**

AUTHOR: GEOFFREY NJOGU

Description

We have several pages hidden. Can you find the one with the flag?
The website is running [here](#).

Hints ?

1

folders folders folders

10,156 solves / 10,509 users attempted (97%)

67% Liked



🚩 picoCTF{FLAG}

Submit Flag

Hints:

- folders folders folders

1. Ketika membuka websitenya, akan muncul tampilan seperti dibawah. Dan kalau dibuka bagian about dan contact, tidak ditemukan hint-hint tertentu yang dapat memberikan flagnya.



2. Jadi kita lakukan inspect disini (index.html). Disini kita bisa melihat apa saja yang ditampilkan di websitenya. Sekilas nampak normal-normal saja, tapi disini ada bagian yang nge-link CSS tapi kayak ada folder-foldernya (ini sesuai sama hints dari pico),

jadi kita coba masukkan secret/assets/index.css ke dalam linknya, dan akan menampilkan isi dari CSSnya.

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="UTF-8" />
5     <meta
6       name="viewport"
7       content="width=device-width, initial-scale=1, shrink-to-fit=no"
8     />
9     <meta name="description" content="" />
10    <!-- Bootstrap core CSS -->
11    <link href="vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet" />
12    <!-- title -->
13    <title>home</title>
14    <!-- CSS -->
15    <link href="secret/assets/index.css" rel="stylesheet" />
16  </head>
17  <body>
18    <!-- ***** Header Area Start ***** -->
19    <div class="topnav">
20      <a class="active" href="#home">Home</a>
21      <a href="about.html">About</a>
22      <a href="contact.html">Contact</a>
23    </div>
24
25    <div class="imgcontainer">
26      
31      <div class="top-left">
32        <h1>If security wasn't your job, would you do it as a hobby?</h1>
33      </div>
34    </div>
35  </body>
36 </html>
37
```

```
/* Add a black background color to the top navigation */
.topnav {
  background-color: #333;
  overflow: hidden;
}

/* Style the links inside the navigation bar */
.topnav a {
  float: left;
  color: #f2f2f2;
  text-align: center;
  padding: 14px 16px;
  text-decoration: none;
  font-size: 17px;
}

/* Change the color of links on hover */
.topnav a:hover {
  background-color: #ddd;
  color: black;
}
```

3. Karena sepertinya kita sudah ada di jalan yang benar, coba kita mundurkan menjadi secret/assets. Ternyata hasilnya adalah forbidden.

403 Forbidden

nginx/1.21.6

4. Kalau begitu coba kita mundurkan satu kali lagi menjadi secret/ saja. Dan ternyata memang benar, jadi coba kita lakukan inspect lagi.

Finally. You almost found me. you are doing well



5. Ternyata sama seperti sebelumnya, pada bagian ini juga memiliki folder untuk menampilkan CSSnya. Kalau begitu, kita coba masukkan hidden/ ke dalam pathnya.

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title></title>
5     <link rel="stylesheet" href="hidden/file.css" />
6   </head>
7
8   <body>
9     <h1>Finally. You almost found me. you are doing well</h1>
10    
7   </head>
8   <body>
9     <form>
10      <div class="container">
11        <form method="" action="/secret/assets/popup.js">
12          <div class="row">
13            <h2 style="text-align: center">
14              Login with Social Media or Manually
15            </h2>
16            <div class="v1">
17              <span class="v1-innertext">or</span>
18            </div>
```

7. Ternyata benar, setelah dilakukan inspect masih ada folder superhidden/, jadi langsung kita masukkan ke dalam pathnya dan akan memberikan tampilan seperti dibawah

Finally. You found me. But can you see me

8. Nah seperti yang dilihat, flagnya tidak ada. Untuk melihat flagnya ada 2 cara, kita dapat langsung melihatnya di inspect atau kita ubah warnanya menjadi hitam di css.

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title></title>
5     <link rel="stylesheet" href="mycss.css" />
6   </head>
7
8   <body>
9     <h1>Finally. You found me. But can you see me</h1>
10    <h3 class="flag">picoCTF{succ3ss_@h3n1c@10n_790d2615}</h3>
11  </body>
12 </html>
```

```
1 h1 {
2   text-align: center;
3   color: black;
4   background-color: white;
5 }
6 .flag {
7   background-color: white;
8   color: white;
9 }
10 /* it was real */
11
```

```
1 h1 {
2   text-align: center;
3   color: black;
4   background-color: white;
5 }
6 .flag {
7   background-color: white;
8   color: black;
9 }
10 /* it was real */
11
```

Finally. You found me. But can you see me

picoCTF{succ3ss_@h3n1c@10n_790d2615}

FLAG: picoCTF{succ3ss_@h3n1c@10n_790d2615}

Scavenger Hunt - <http://mercury.picoctf.net:39698/>

Scavenger Hunt



👤 | 50 points ✕

Tags: **picoCTF 2021** **Web Exploitation**

AUTHOR: MADSTACKS

Hints ?

Description

1

There is some interesting information hidden around this site <http://mercury.picoctf.net:39698/>. Can you find it?

30,236 solves / 35,587 users attempted (85%)



62%

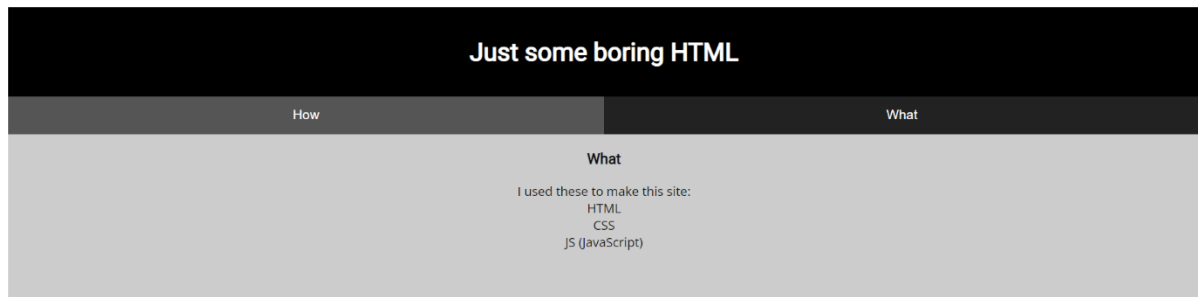
Liked



🚩 picoCTF{FLAG}

Submit
Flag

Soal yang berisi alamat link website, website merupakan website sederhana.



Terdapat clue di dalam website yaitu HTML, CSS, dan Js. Jadi saya coba untuk buka source code pada website dengan inspect element.

```

        CSS <br/>
        JS (JavaScript)
    </p>
    <!-- Here's the first part of the flag: picoCTF{t -->
</div>

```

Pada file HTML terdapat flag pertama.

```

intro { background-color: #ccc; }
about { background-color: #ccc; }

JS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_10 */

```

Pada file CSS terdapat flag kedua.

```

window.onload = function() {
    openTab('tabintro', this, '#222');
}

/* How can I keep Google from indexing my website? */

```

Pada file Js tidak ada flag, namun ada clue.

Apa itu indexing?

Indexing adalah proses ketika search engine mengatur informasi sebelum adanya pencarian, yang artinya search engine menggunakan search engine bots untuk scan website-website yang ada di internet dan mencari konten yang menarik lalu dimasukan di dalam data basenya, data tersebut akan digunakan Ketika user mencari konten yang user ingin cari.

Setelah mengetahui apa itu indexing, pada umumnya developer web tidak mau semua isi website diindexkan oleh bot. Jadi mereka menggunakan robots.txt untuk mengatur yang boleh diindex dan yang tidak boleh diindex.

← → ↻ ⚠ Not secure | mercury.picoctf.net:39698/robots.txt

```

User-agent: *
Disallow: /index.html
# Part 3: t_of_pl4c
# I think this is an apache server... can you Access the next flag?

```

Pada contoh robot.txt terdapat “Disallow: “ yang artinya bot tidak boleh masuk pada file /index.html, yang otomatis tidak diindexkan oleh bot. lalu terdapat flag ke 3 dan clue selanjutnya.

I think this is an apache server... can you Access the next flag?
Cluenya cukup menarik karena pada kata “Access” huruf A kapital, lalu saya coba search di google dengan kata kunci “apache server access file” karena mungkin berhubungan dengan file. Di dalam website terdapat direktori yang bernama ./htaccess file singkatan dari hypertext access, ./htaccess merupakan file yang berfungsi untuk mengatur peraturan dalam website.

Kegunaan file tersebut untuk URL redirection, caching, rewrite URL, Error handling.

← → ↻ ⚠ Not secure | mercury.picoctf.net:39698/.htaccess

Part 4: 3s_2_100k

I love making websites on my Mac, I can Store a lot of information there.

Flag ke-4 sudah didapatkan dengan clue selanjutnya

I love making websites on my Mac, I can Store a lot of information there.

Clue selanjutnya sangat menarik karena kata “Store” huruf “S” kapital sama seperti clue sebelumnya. Pada clue ada yang berhubungan dengan Mac dan juga Store. Saya coba search di google dengan kata kunci “Mac Store file in website”, pada OS apple terdapat hidden file yang bernama .DS_Store. Pada konteks website seorang developer yang ingin mengirim file ke server bisa saja tidak sengaja memasukkan .DS_Store ke dalam server.

← → ↻ ⚠ Not secure | mercury.picoctf.net:39698/.DS_Store



Congrats! You completed the scavenger hunt. Part 5: _fa04427c}

Ketika kit acari /.DS_Store maka akan ketemu flag terakhir.

Flag = picoCTF{th4ts_4_l0t_of_pl4c3s_2_l00k_d375c750}

Cryptography: Flags

Flags 

 | 200 points 

Tags: picoCTF 2019 Cryptography

AUTHOR: DANNY

Description

What do the [flags](#) mean?

Hints 

1

The flag is in the format PICOCTF{}

11,617 solves / 12,363 users attempted (94%)



58% Liked



 picoCTF{FLAG}

Submit Flag

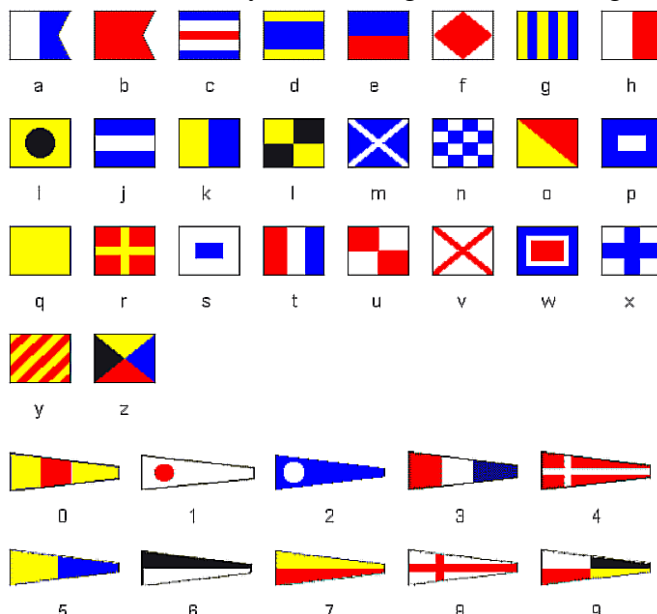
Hints:

- The flag in the format PICOCTF{}

1. Setelah membuka filenya, ternyata berisikan lambang-lambang yang aneh.



2. Jadi saya mencoba mencari tahu tentang ini bermodalkan description yang diberikan. Dan ternyata memang benar, lambang-lambang tersebut memiliki arti.

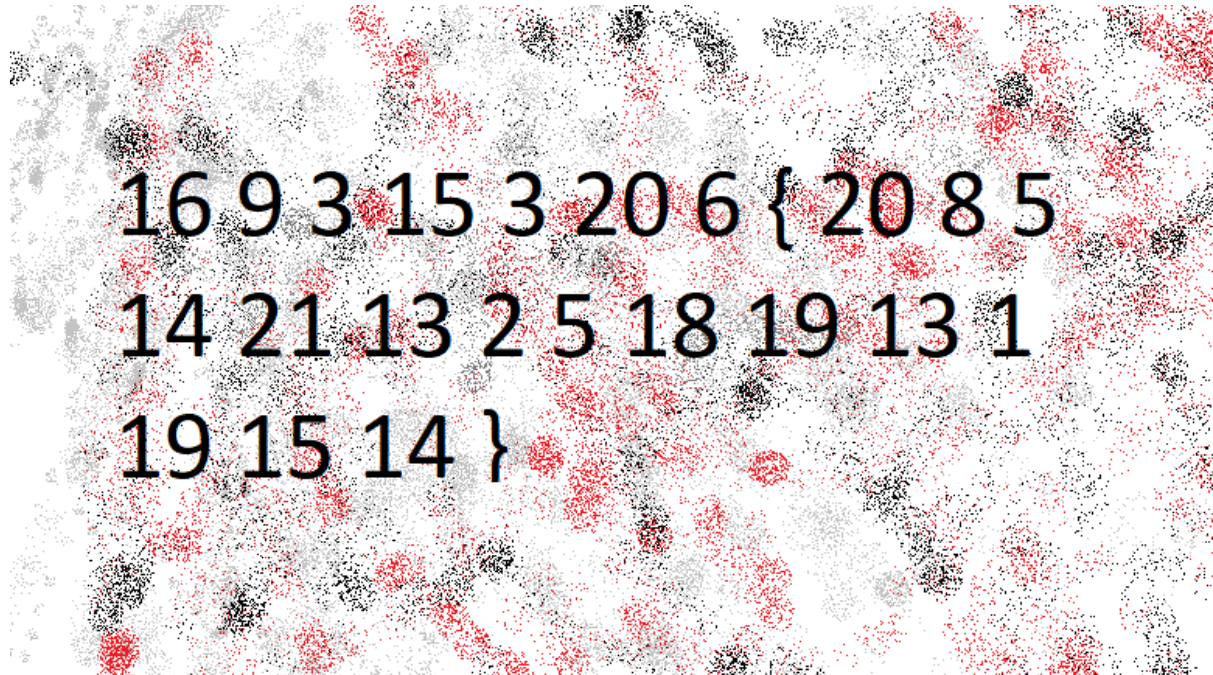


3. Dengan begini, kita bisa langsung decode lambang-lambang tersebut.

FLAG: PICOCTF{F1AG5AND5TUFF}

The Numbers -

<https://play.picoctf.org/practice/challenge/68?category=2&page=1>



Dari soal diberikan gambar yang berjudul The Numbers.png, pada gambar terdapat karakter yang unik yaitu { dan }. Saya langsung coba masukan alphabet sesuai nomor urutnya secara manual karena menurut saya masuk akal karena angka terkecil yaitu angka satu dan yang terbesar yaitu angka dua puluh satu.

```
16 9 3 15 3 20 6 { 20 8 5 14 21 13 2 5 18 19 13 1 19 15 14 }
```

```
picocftf{thenumbersmason}
```

```
Flag = PICOCTF{thenumbersmason}
```

Forensic: FindAndOpen

FindAndOpen

200 points

Tags: picoCTF 2023 Forensics

AUTHOR: MUBARAK MIKAIL

Hints ?

Description

Someone might have hidden the password in the trace file.

Find the key to unlock [this](#) file. [This tracefile](#) might be good to analyze.

1,973 solves / 2,548 users attempted (77%)

28% Liked

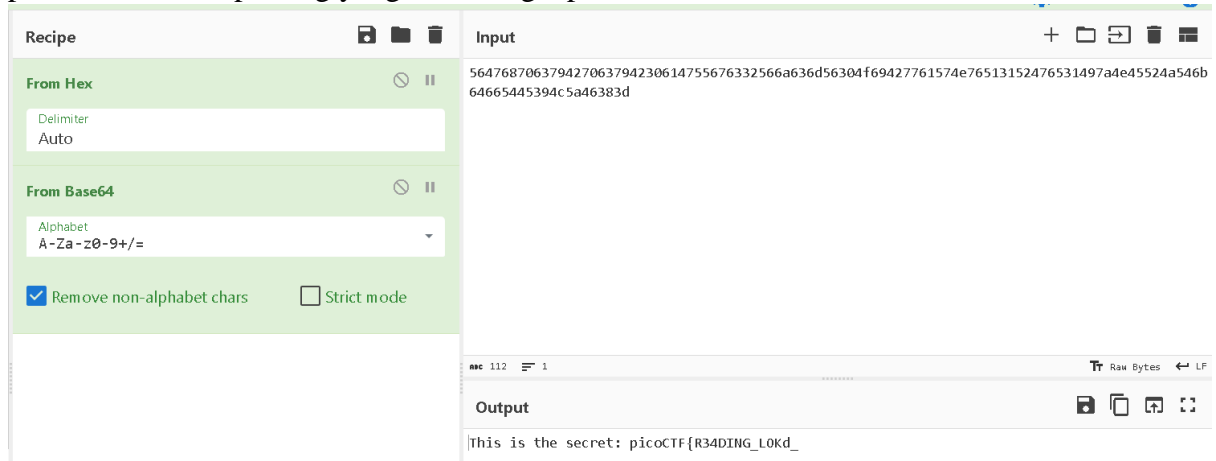
picoCTF{FLAG}

Submit Flag

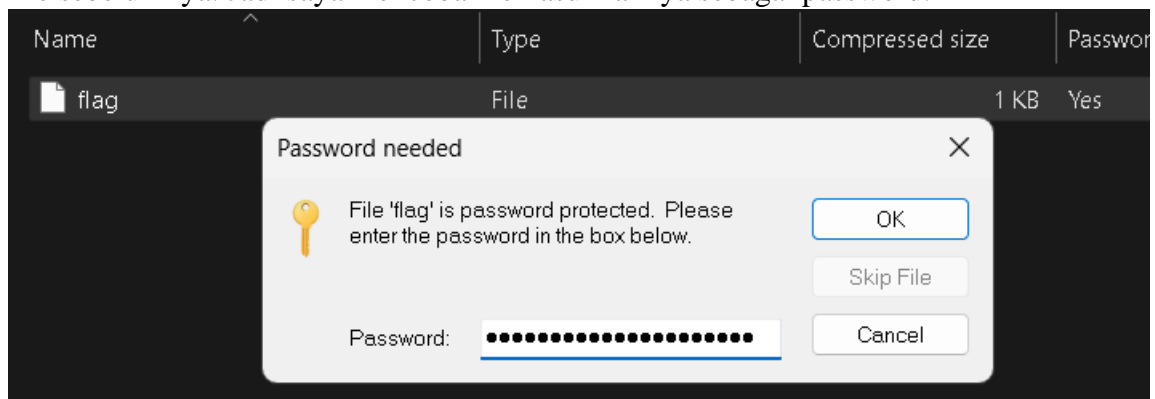
1. Download dulu filenya, disini ada 2 file yang pertama berbentuk zip yang ada passwordnya dan yang ke dua, file memiliki extension .pcap yang mana merupakan file wireshark.
2. Tahap selanjutnya membuka file ke 2 di dalam wireshark. Kemudian setelah mencari dari sekian banyak dan ditemukan dua hint kecil yang mengatakan **Flying on Ethernet secret: Is this the flag** dan **Could the flag have been splitted?** Setelah menemukan kedua hint tersebut, saya juga menemukan ada beberapa length yang berbeda dan diantaranya adalah length 70 yang saya rasa memiliki value dari base64.

The screenshot shows the Wireshark interface with a packet capture of Ethernet II frames. The packet list shows multiple frames with length 47 and 46. The packet details pane shows the structure of an Ethernet II frame with a length of 56 bytes. The packet bytes pane shows the raw data in hexadecimal and ASCII, including the ASCII string 'AABHPP' and 'GTRRLK'.

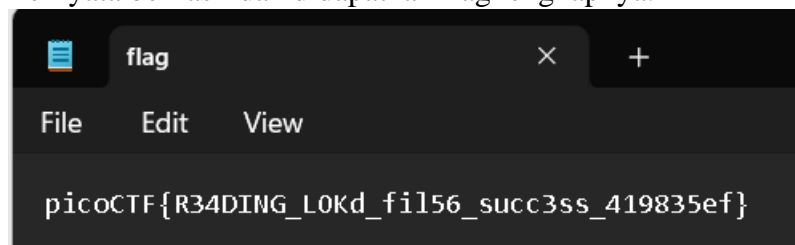
3. Jadi saya copy as value dari wireshark (hex), kemudian decode as base64 dan hasilnya pun terlihat, terdapat flag yang tidak lengkap.



4. Lalu saya berpikir, mungkin saja flag yang sepotong ini merupakan password dari zip file sebelumnya. Jadi saya mencoba memasukkannya sebagai password.



5. Ternyata berhasil dan didapatkan flag lengkapnya.



FLAG: picoCTF{R34DING_L0Kd_fil56_succ3ss_419835ef}

Extensions - <https://play.picoctf.org/practice/challenge/52?category=4&page=2>

extensions 

 | 150 points 

Tags: picoCTF 2019 Forensics

AUTHOR: SANJAY C/DANNY

Hints 

Description

1 2

This is a really weird text file **TXT**? Can you find the flag?

19,327 solves / 19,634 users attempted (98%)



88%
Liked



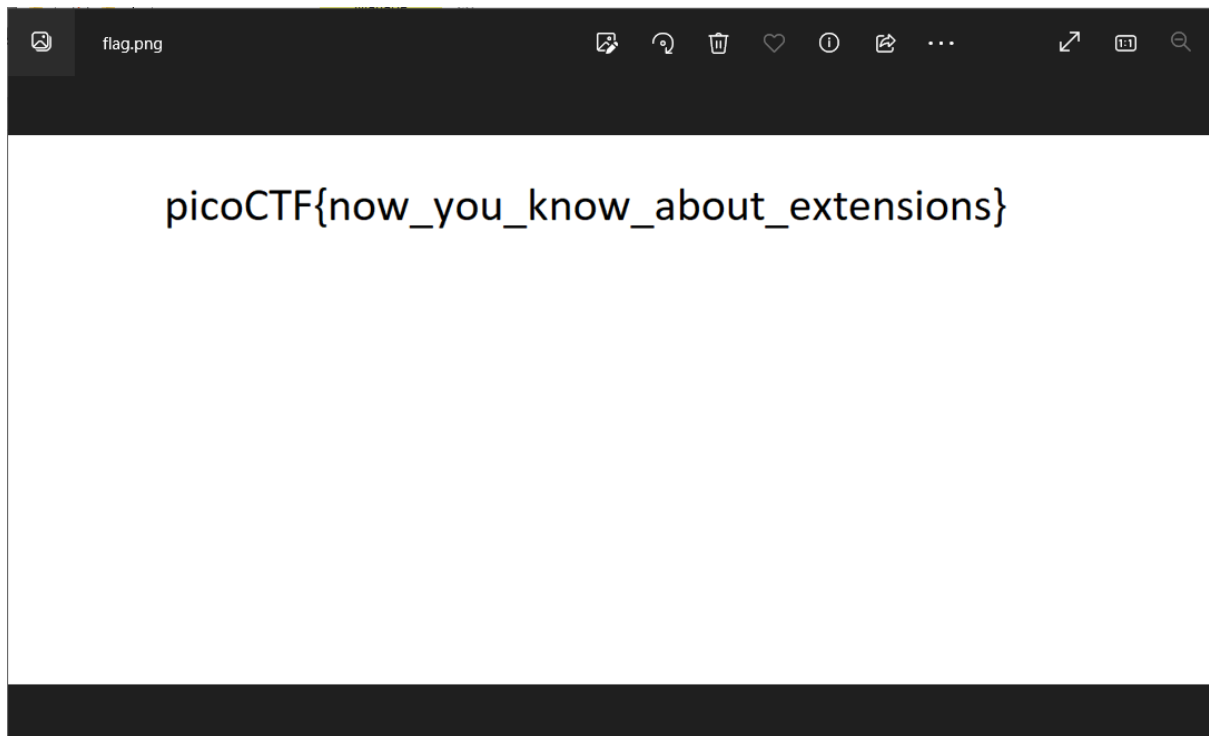
 picoCTF{FLAG}

Submit
Flag

Pada soal diberi file yang bernama “flag.txt”



Pada awal text terdapat kata “PNG” yang merupakan extension, karena nama soalnya extension mungkin saya bisa menggantikan extension “.txt” menjadi “.png”.





Setelah saya ganti muncul gambar yang merupakan flag pada soal ini.

Flag = picoCTF{now_you_know_about_extensions}

Binary Exploitation: two-sum

two-sum 

 | 100 points 

Tags: [picoCTF 2023](#) [Binary Exploitation](#) [C](#) [make](#)

AUTHOR: MUBARAK MIKAIL

Description

Can you solve this?

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.



Its current status is: **NOT_RUNNING**

[Launch Instance](#)

Hints

(None)

2,837 solves / 2,949 users attempted (96%)

 83% Liked 

 picoCTF{FLAG}



[Submit Flag](#)

Hints:

- Integer overflow
- Not necessarily a math problem

1. Ketika kita melakukan launch instance, akan muncul seperti gambar dibawah, yakni nc dan source codenya.

two-sum 

 | 100 points 

Tags: [picoCTF 2023](#) [Binary Exploitation](#) [C](#) [make](#)

AUTHOR: MUBARAK MIKAIL

Description

Can you solve this?

What two positive numbers can make this possible: $n1 > n1 + n2$ OR $n2 > n1 + n2$

Enter them here `nc saturn.picoctf.net 63233`. [Source](#)

This challenge launches an instance on demand.

Its current status is: **RUNNING**


Instance Time Remaining: **14:55**

[Restart Instance](#)

Hints

1 2

2,837 solves / 2,949 users attempted (96%)

 83% Liked 

 picoCTF{FLAG}

[Submit Flag](#)

2. Setelah menyalakan linux dan membuka source codenya. Didapatkan hasil seperti dibawah ketika mengisi angka secara asal.


```
(kali@kali)-[~]  
$ nc saturn.picoctf.net 54451  
n1 > n1 + n2 OR n2 > n1 + n2  
What two positive numbers can make this possible:  
1  
2  
You entered 1 and 2  
No overflow
```

```
#include <stdio.h>  
#include <stdlib.h>  
  
static int addIntOvf(int result, int a, int b) {  
    result = a + b;  
    if(a > 0 && b > 0 && result < 0)  
        return -1;  
    if(a < 0 && b < 0 && result > 0)  
        return -1;  
    return 0;  
}  
  
int main() {  
    int num1, num2, sum;  
    FILE *flag;  
    char c;  
  
    printf("n1 > n1 + n2 OR n2 > n1 + n2 \n");  
    fflush(stdout);  
    printf("What two positive numbers can make this possible: \n");  
    fflush(stdout);  
  
    if (scanf("%d", &num1) && scanf("%d", &num2)) {  
        printf("You entered %d and %d\n", num1, num2);  
        fflush(stdout);  
        sum = num1 + num2;  
        if (addIntOvf(sum, num1, num2) == 0) {  
            printf("No overflow\n");  
            fflush(stdout);  
            exit(0);  
        } else if (addIntOvf(sum, num1, num2) == -1) {  
            printf("You have an integer overflow\n");  
            fflush(stdout);  
        }  
  
        if (num1 > 0 || num2 > 0) {  
            flag = fopen("flag.txt", "r");  
            if(flag == NULL){  
                printf("flag not found: please run this on the  
server\n");  
                fflush(stdout);  
            }  
        }  
    }  
}
```

```

        exit(0);
    }
    char buf[60];
    fgets(buf, 59, flag);
    printf("YOUR FLAG IS: %s\n", buf);
    fflush(stdout);
    exit(0);
}
}
return 0;
}

```

3. Dari source code tersebut, dapat kita lihat pada bagian fungsinya dinyatakan jika $a > 0$ dan $b > 0$ dan hasilnya < 0 , maka akan memberikan hasil "You have an integer overflow" dan akan melanjutkan codenya yang dimana melakukan read file flag.txt. dalam codenya sendiri sudah dituliskan jika tidak ditemukan file flag.txt, maka akan memberikan print "flag not found: please run this on the server". Jadi harus dipastikan ulang sudah menggunakan nc yang diberikan. Dan jika sudah sesuai, maka flagnya akan langsung diberikan.

```

static int addIntOvf(int result, int a, int b) {
    result = a + b;
    if(a > 0 && b > 0 && result < 0)
        return -1;
    if(a < 0 && b < 0 && result > 0)
        return -1;
    return 0;
}

=====
else if (addIntOvf(sum, num1, num2) == -1) {
    printf("You have an integer overflow\n");
    fflush(stdout);
}

=====
if (num1 > 0 || num2 > 0) {
    flag = fopen("flag.txt", "r");
    if(flag == NULL){
        printf("flag not found: please run this on the server\n");
        fflush(stdout);
        exit(0);
    }
    char buf[60];
    fgets(buf, 59, flag);
    printf("YOUR FLAG IS: %s\n", buf);
    fflush(stdout);
    exit(0);
}

```

4. Disini saya menggunakan 2 angka yang merupakan limit dari integer, yakni 2147483647 sebagai a dan bnya. Dan akan menghasilkan flagnya seperti gambar dibawah.

```
(kali@kali)-[~]  
$ nc saturn.picoctf.net 54451  
n1 > n1 + n2 OR n2 > n1 + n2  
What two positive numbers can make this possible:  
2147483647  
2147483647  
You entered 2147483647 and 2147483647  
You have an integer overflow  
YOUR FLAG IS: picoCTF{Tw0_Sum_Integer_Bu773R_0v3rfl0w_482d8fc4}
```

FLAG: picoCTF{Tw0_Sum_Integer_Bu773R_0v3rfl0w_482d8fc4}

Notes

Loh kok bisa? Tentu saja bisa, karna limit dari integer -2147483647 sampai 2147483647 yang dimana kalau lebih dari 2147483647, maka hasilnya akan menjadi minus atau biasa disebut overflow. Makanya ini dibilang integer overflow.

*coba masukkin 10 miliar

```
(kali@kali)-[~]  
$ nc saturn.picoctf.net 59420  
n1 > n1 + n2 OR n2 > n1 + n2  
What two positive numbers can make this possible:  
10000000000  
10000000000  
You entered 1410065408 and 1410065408  
You have an integer overflow  
YOUR FLAG IS: picoCTF{Tw0_Sum_Integer_Bu773R_0v3rfl0w_482d8fc4}
```

buffer overflow 0 -

<https://play.picoctf.org/practice/challenge/257?category=6&page=1>

buffer overflow 0

 | 100 points 

Tags: picoCTF 2022 Binary Exploitation gets

AUTHOR: ALEX FULTON / PALASH OSWAL

Hints 

Description

Smash the stack

Let's start off simple, can you overflow the correct buffer? The program is available [here](#). You can view source [here](#). And connect with it using:

`nc saturn.picoctf.net 63397`

1 2 3

11,010 solves / 11,458 users attempted (96%)



85%



Liked

 picoCTF{FLAG}

Submit
Flag

Pada soal ini diberikan file source code yang berjudul "vuln.c". Tentu saja saya tidak mengerti code C nya. Saya melihat nama soal "buffer overflow 0" dan mencari tau apa itu buffer overflow. Jadi pada programman buffer overflow terjadi ketika volume data melebihi kapasitas penyimpanan buffer memori. Saya mencoba membaca ulang kode C tersebut.

```
#define FLAGSIZE_MAX 64  
  
char flag[FLAGSIZE_MAX];
```

Pada char flag memiliki panjang string 64, mungkin jika saya kasih input lebih dari 64 akan terjadi sesuatu.

```
chomusuke1-picoctf@webshell:~$ nc saturn.picoctf.net 63397
Input: jafiwoioajijawifjavkdnakvjdkajvajfejafijfjaiejfiajfieajfiofiewafjioawfffjaiwejfi
picoCTF{ov3rf10ws_ar3nt_that_bad_8446a0c3}
```

Ternyata benar jika saya masukan input lebih dari 64 akan terjadi buffer overflow dan mendapatkan flagnya

Flag = picoCTF{ov3rf10ws_ar3nt_that_bad_8446a0c3}

Reverse Engineering: vault-door-training

vault-door-training 

 | 50 points 

Tags: picoCTF 2019 Reverse Engineering

AUTHOR: MARK E. HAASE

Description

Your mission is to enter Dr. Evil's laboratory and retrieve the blueprints for his Doomsday Project. The laboratory is protected by a series of locked vault doors. Each door is controlled by a computer and requires a password to open. Unfortunately, our undercover agents have not been able to obtain the secret passwords for the vault doors, but one of our junior agents obtained the source code for each vault's computer! You will need to read the source code for each level to figure out what the password is for that vault door. As a warmup, we have created a replica vault in our training facility. The source code for the training vault is here: [VaultDoorTraining.java](#)

Hints

1

The password is revealed in the program's source code.

40,666 solves / 43,421 users attempted (94%)



72% Liked

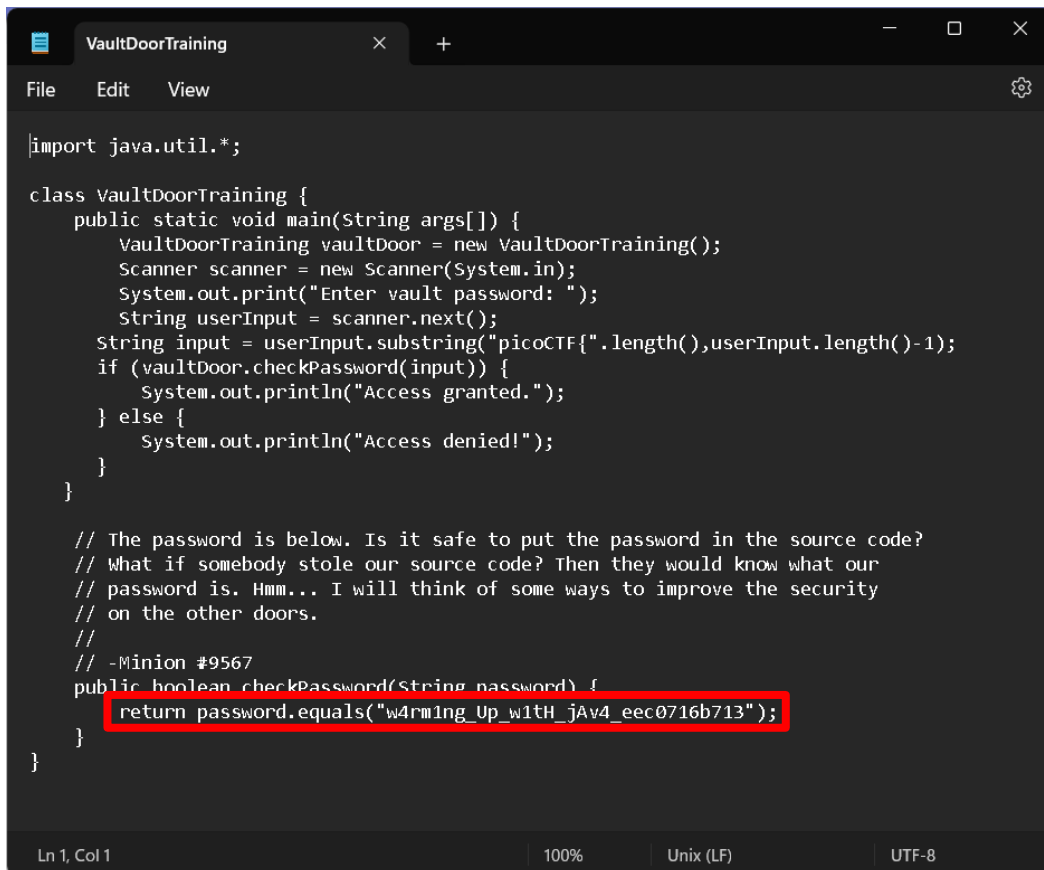


picoCTF{FLAG}

Submit Flag

Hints:

- The password is revealed in the program's source code
1. Download dan buka dulu filenya. Sesuai dengan hint yang diberikan, saya langsung mengecek filenya.



```
import java.util.*;

class VaultDoorTraining {
    public static void main(String args[]) {
        VaultDoorTraining vaultDoor = new VaultDoorTraining();
        Scanner scanner = new Scanner(System.in);
        System.out.print("Enter vault password: ");
        String userInput = scanner.next();
        String input = userInput.substring("picoCTF{".length(),userInput.length()-1);
        if (vaultDoor.checkPassword(input)) {
            System.out.println("Access granted.");
        } else {
            System.out.println("Access denied!");
        }
    }

    // The password is below. Is it safe to put the password in the source code?
    // What if somebody stole our source code? Then they would know what our
    // password is. Hmm... I will think of some ways to improve the security
    // on the other doors.
    //
    // -Minion #9567
    public boolean checkPassword(String password) {
        return password.equals("w4rm1ng_Up_w1tH_jAv4_eec0716b713");
    }
}
```



Ln 1, Col 1 | 100% | Unix (LF) | UTF-8

2. Disini kita langsung menemukan flagnya.

FLAG: picoCTF{w4rm1ng_Up_w1tH_jAv4_eec0716b713}

unpackme.py - <https://play.picoctf.org/practice/challenge/314?category=3&page=2>

unpackme.py 

 | 100 points 

Tags: picoCTF 2022 Reverse Engineering packing

AUTHOR: LT 'SYREAL' JONES

Hints 

Description

(None)

Can you get the flag?

Reverse engineer this [Python program](#).

7,978 solves / 8,165 users attempted (98%)



85%




Liked

 picoCTF{FLAG}

Submit
Flag

Pada soal ini, diberikan sebuah code python yang berjudul “unpackme.flag.py”

```
fernet >  unpackme.flag.py > ...
1  import base64
2  from cryptography.fernet import Fernet
3
4  payload = b'gAAAAABkEnJyDQRwhRctRWgKIhhNCDcqsj5gaQAEIihxiK2NtvYBMwZ2SBoEbwgZV
5
6  key_str = 'correctstaplecorrectstaplecorrec'
7  key_base64 = base64.b64encode(key_str.encode())
8  f = Fernet(key_base64)
9  plain = f.decrypt(payload)
10 exec(plain.decode())
11
```

Code tersebut merupakan file yang harus kita reverse.

Pada variable “payload” terdapat string dalam bentuk bytes.

Variable “key_str” yang merupakan key value untuk membuka “payload”

Variable “key_base64” untuk encode “key_str” menjadi base64.

Variable “plain” merupakan proses decryption yang outputnya berbentuk plain text.

Kita dapat dengan mudah mengganti function exec() menjadi print() untuk melihat plain text tersebut


```

1  import base64
2  from cryptography.fernet import Fernet
3
4  payload = b'gAAAAABkEnJyDQRwhRctRWgKIhhNCDcqsj5g
5
6  key_str = 'correctstaplecorrectstaplecorrec'
7  key_base64 = base64.b64encode(key_str.encode())
8  f = Fernet(key_base64)
9  plain = f.decrypt(payload)
10 print(plain.decode())
11

```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

```

Users/ASUS/AppData/Local/Microsoft/WindowsApps/python
What's the password? batteryhorse
picoCTF{175_chr157m45_5274ff21}
PS C:\Users\ASUS\Documents\Python Stuff\ctf> & C:/Us
uff/ctf/fernet.py"
PS C:\Users\ASUS\Documents\Python Stuff\ctf> & C:/Us
uff/ctf/fernet.py"
PS C:\Users\ASUS\Documents\Python Stuff\ctf> & C:/Us
uff/ctf/fernet/unpackme.flag.py"

pw = input('What\'s the password? ')

if pw == 'batteryhorse':
    print('picoCTF{175_chr157m45_5274ff21}')
else:
    print('That password is incorrect.')

PS C:\Users\ASUS\Documents\Python Stuff\ctf> 

```

Ketika diprint, akan menghasilkan hasil decrypsi dan juga flag picoCTFnya.

Flag = picoCTF{175_chr157m45_5274ff21}