

CTF Class Test intake 082024

| | |
|---------------------|--------------------|
| TP Number: TP067125 | Name: SLOW HAN BIN |
|---------------------|--------------------|

Marking Rubrics for Writeup (5 marks for each required questions)

| | Fail (0-1 mark) | Marginal Fail (2 mark) | Pass (3 marks) | Credit (4 marks) | Distinction (5 marks) |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PLO2 – Cognitive skills | <i>Fail to apply skill / knowledge to a range of approaches in the field of study / work / practice.</i> | <i>Below average skills to apply skill / knowledge to a range of approaches in the field of study / work / practice.</i> | <i>Average skills to apply skill / knowledge to a range of approaches in the field of study / work / practice.</i> | <i>Good skills to apply skill / knowledge to a range of approaches in the field of study / work / practice.</i> | <i>Excellent skills to apply skill / knowledge to a range of approaches in the field of study / work / practice.</i> |
| Writeup showing steps, flow and screenshot (5 marks for each required questions) | Incorrect answer, no write-up provided, no storytelling/ELIF, no screenshots, no demonstration of applying skills / knowledge. | Partially answered, brief write-up provided, no storytelling/ELIF, no screenshots, no demonstration of applying skills / knowledge. | Partially answered, brief write-up provided, minimal storytelling/ELIF, minimal screenshots, no caption, minimal demonstration of applying skills / knowledge. | Correct answer with acceptable details, acceptable storytelling/ELIF, acceptable screenshots with caption, acceptable write-up provided to demonstrate skills / knowledge applied. | Correct answer with excellent details, detailed screenshots with caption, detailed write-up provided to demonstrate skills / knowledge applied. Excellent storytelling/ELIF. |

Writeup showing steps, flow and screenshot for each question:

Question 1.1

- 1) Download the mp3 file from
<https://lms2.apiit.edu.my/pluginfile.php/1274549/question/questiontext/1263515/2/659735/b7acc43c15ed268a1bcb81b528e8a419.mp3>

Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Choose File b7acc43c15...e8a419.mp3

Password (may be blank):

star

- ☒ View raw output as MIME-type
☐ Guess the payload
☐ Prompt to save (you must guess the file type yourself.)

Submit

- 2) Go to <https://futureboy.us/stegano/decinput.html>, upload the mp3 file, then listen to the audio. I heard “star” multiple times. So I guess the password is star
- 3) Got a output which is binary

```
00110110 00110001 00100000 00110111 00110000 00100000 00110111 00110101
00100000 00110100 00110011 00100000 00110101 00110100 00100000 00110100
00110110 00100000 00110111 01100010 00100000 00110110 00110010 00100000
00110011 00110011 00100000 00110101 01100110 00100000 00110110 01100100
00100000 00110101 00111001 00100000 00110101 01100110 00100000 00110101
00110011 00100000 00110101 00110100 00100000 00110011 00110100 00100000
00110101 00110010 00100000 00110101 01100110 00100000 00110011 00110101
00100000 00110111 00110100 00100000 00110111 00110101 00100000 00110110
00110100 00100000 00110011 00110011 00100000 00110110 01100101 00100000
00110111 00110100 00100000 00110010 00110001 00100000 00110111 01100100
```

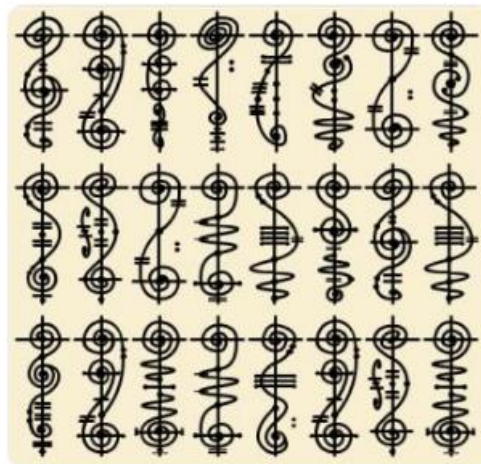
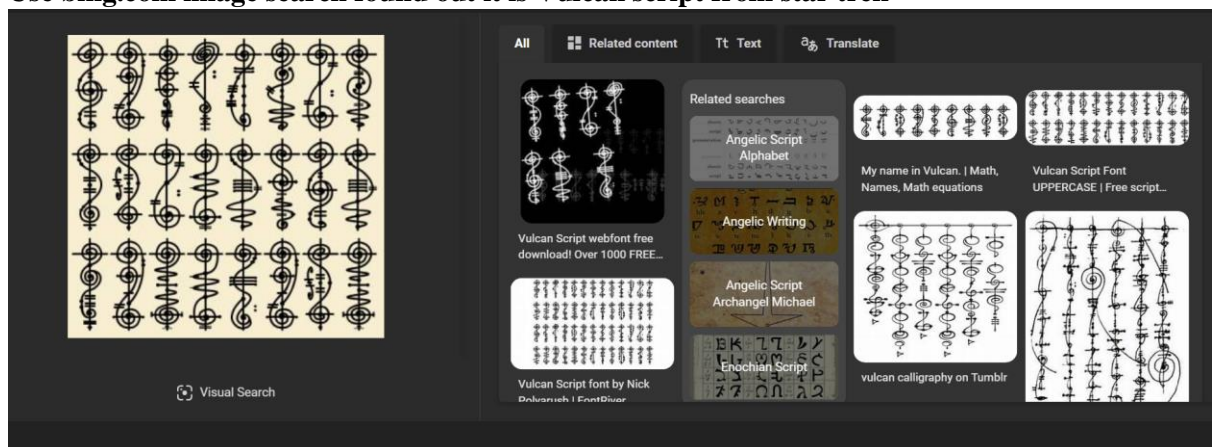
- 4) Go to cyberchef, and use recipe “From Binary” and “From Hex”

The screenshot shows the CyberChef web interface. On the left, the 'Recipe' panel has two recipes added: 'From Binary' and 'From Hex'. The 'From Binary' recipe has a 'Delimiter' of 'Space' and a 'Byte Length' of '8'. The 'From Hex' recipe has a 'Delimiter' of 'Space'. The 'Input' panel on the right contains the binary data from the previous step. The 'Output' panel at the bottom shows the result of applying these recipes: `apuCTF{b3_mY_ST4R_5tud3nt!}`.

- 5) The flag is apuCTF{b3_mY_ST4R_5tud3nt!}

Question 1.2**1) Go to Microsoft teams Download the images**

Mohd Hanis Jenalis 11:02 AM Edited

Puzzle challenges [CTF-122024-APU/D2406CS\(CYB/DF\)](#)**2) Use bing.com image search found out it is Vulcan script from star trek**

- 3) Go to <https://www.dcode.fr/vulcan-language>, click followed by the images. Then Click decrypt

APUCTFLIVELONGANDPROSPER

Vulcan Language (Star Trek) - dCode
Tag(s) : Symbol Substitution

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? Write to dCode!

VULCAN SCRIPT DECODER

Vulcan calligraphy is complex and the 26 symbols below (the source of which is unknown) are theoretically inaccurate (yet circulating on the Internet).

★ VULCAN SYMBOLS/ALPHABET (CLICK TO ADD)

★ VULCAN CIPHERTEXT

▶ DECRYPT

- 4) apuCTF{LIVELONGANDPROSPER}

Question 2.1

- 1) Connect to the instance and try some random value

```

siowhanbin_AyamMan@kali: ~
File Actions Edit View Help
(siowhanbin_AyamMan@kali)-[~]
$ nc saturn.picoctf.net 51279
n1 > n1 + n2 OR n2 > n1 + n2
What two positive numbers can make this possible:
2147483999
11
You entered -2147483297 and 11
No overflow

(siowhanbin_AyamMan@kali)-[~]
$ nc saturn.picoctf.net 51279
n1 > n1 + n2 OR n2 > n1 + n2
What two positive numbers can make this possible:
2147483297
1
You entered 2147483297 and 1
No overflow

```

- 2) Read the code and google integer overflow

```

#include <stdio.h>
#include <stdlib.h>

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

int main() {
    int num1, num2, sum;
    FILE *flag;
    char c;

    printf("n1 > n1 + n2 OR n2 > n1 + n2 \n");
    fflush(stdout);
    printf("What two positive numbers can make this possible: \n");
    fflush(stdout);

    if (scanf("%d", &num1) && scanf("%d", &num2)) {
        printf("You entered %d and %d\n", num1, num2);
        fflush(stdout);
        sum = num1 + num2;
        if (addIntOvf(sum, num1, num2) == 0) {
            printf("No overflow\n");
            fflush(stdout);
            exit(0);
        } else if (addIntOvf(sum, num1, num2) == -1) {

```

```

        printf("You have an integer overflow\n");
        fflush(stdout);
    }

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

return 0;
}

```

- 3) Maximum value can be inserted after executing the code is 4,294,967,295. Which is range between -2,147,483,648 and 2,147,483,647. [reference: <https://www.twingate.com/blog/glossary/integer%20overflow>]
- 4) Go to Chatgpt(unlogin version), paste the code with a prompt “How to make integer overflow”

```

tgets(buf, 59, flag);
printf("YOUR FLAG IS: %s\n", buf);
fflush(stdout);
exit(0);
}
}
return 0;
}

```

How to make integer overflow

In the provided C code, the key part is in the `addInt0vf` function, which checks for integer overflow

5) Read text given by chatgpt

For an integer overflow to occur, it must exceed the maximum value that can be represented by an `int`. On most systems with a 32-bit `int`, the maximum value is `INT_MAX` (2,147,483,647). If the sum of two positive integers exceeds this value, an overflow will occur, and the `addInt0vf` function will return `-1`.

Let's break down the conditions for causing overflow:

- **Overflow Condition:** If both `num1` and `num2` are positive integers, and their sum exceeds `INT_MAX` (the maximum positive value an `int` can hold).

6) Connect to instance again and input 2147483647 as first input, 1 as second input

```
(siowhanbin_AyamMan@kali)-[~]  
$ nc saturn.picoctf.net 51279  
n1 > n1 + n2 OR n2 > n1 + n2  
What two positive numbers can make this possible:  
2147483647  
1  
You entered 2147483647 and 1  
You have an integer overflow  
YOUR FLAG IS: picoCTF{Tw0_Sum_Integer_Bu773R_0v3rfl0w_e06700c0}
```

7) The flag is: apuCTF{Tw0_Sum_Integer_Bu773R_0v3rfl0w_e06700c0}**Question 3.1****1) Connect to instance**JAuth 

Medium

Web Exploitation

picoGym Exclusive

AUTHOR: GEOFFREY NJOGU

Description

Most web application developers use third party components without testing their security. Some of the past affected companies are:

- Equifax (a US credit bureau organization) - breach due to unpatched Apache Struts web framework CVE-2017-5638
- Mossack Fonesca (Panama Papers law firm) breach - unpatched version of Drupal CMS used
- VerticalScope (internet media company) - outdated version of vBulletin forum software used

This challenge launches an instance on demand.

Its current status is:

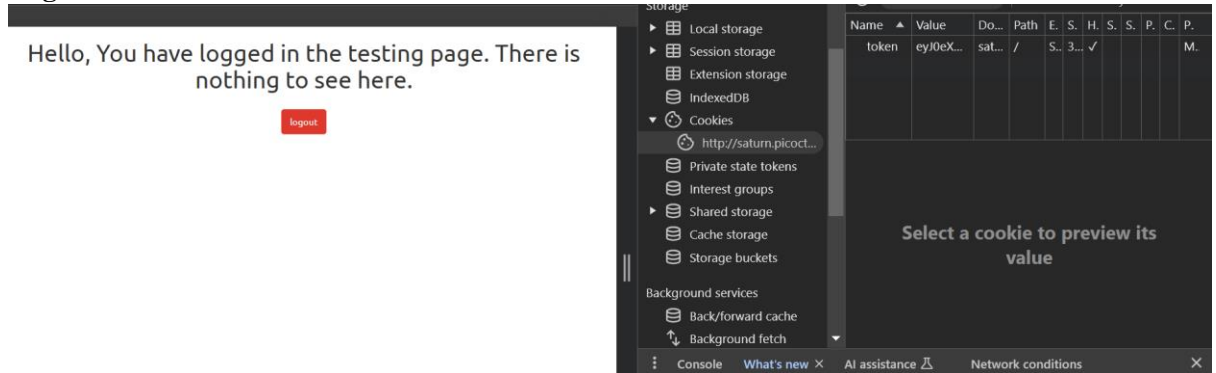
RUNNING

Instance Time Remaining:

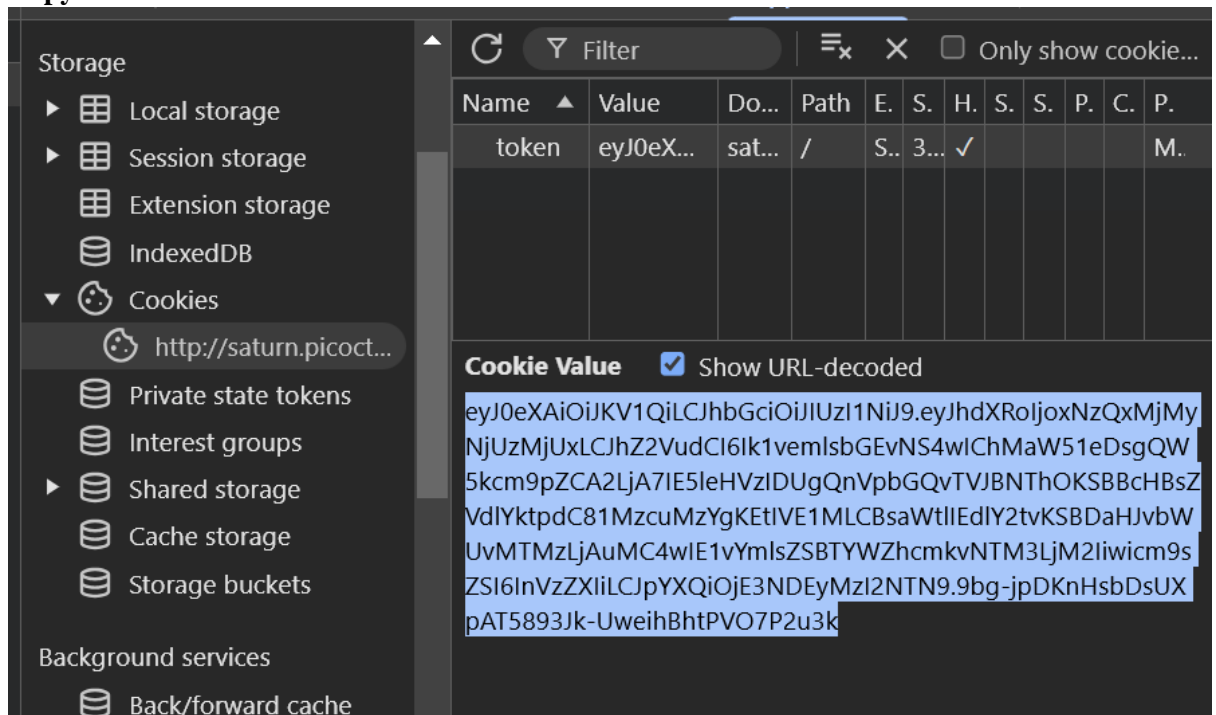
6:07**Restart
Instance****Hints ?****1****2**

The JWT should always have two (2) . separators.

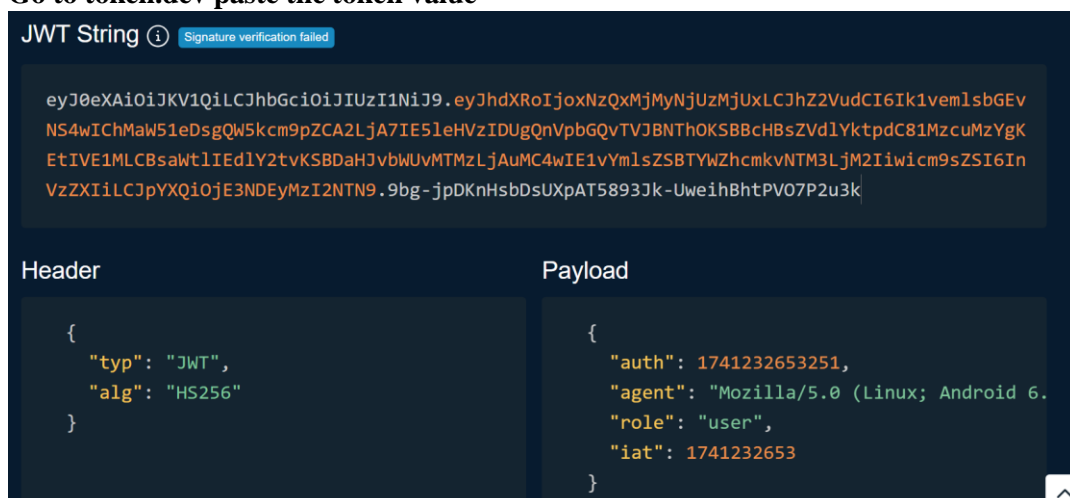
2) Login with test Test123!



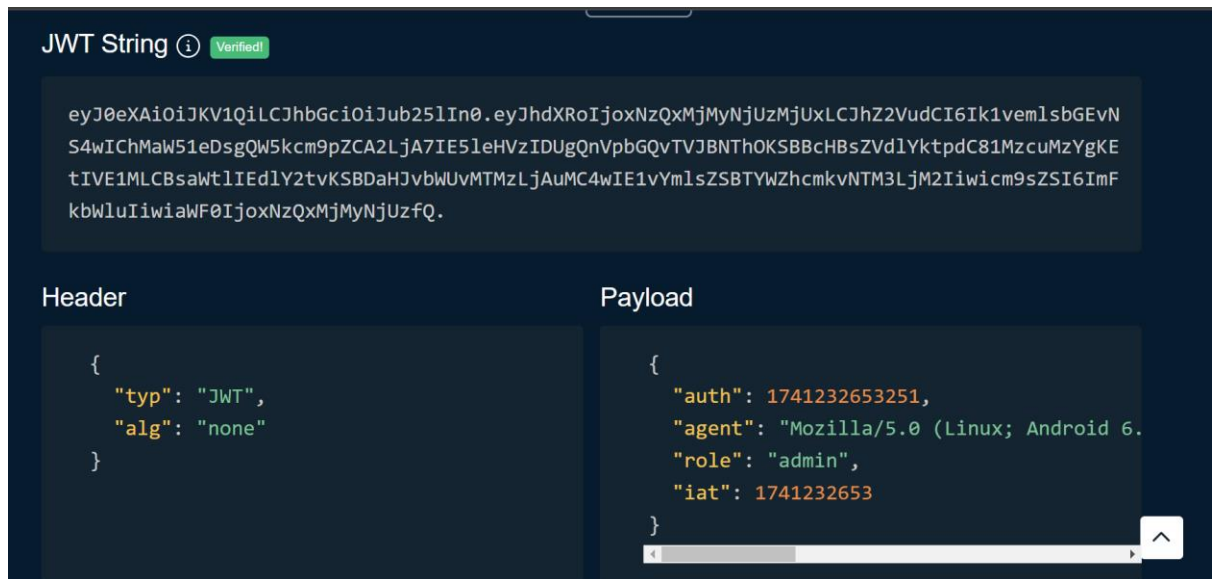
3) Copy the token value



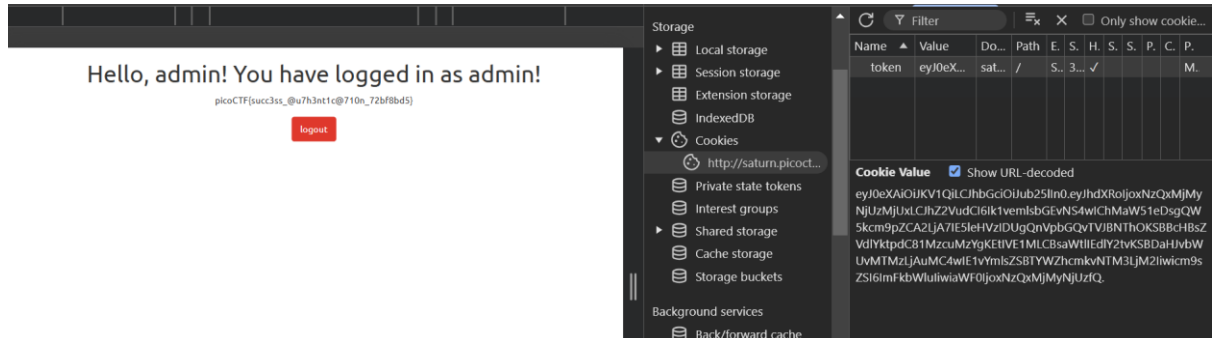
4) Go to token.dev paste the token value



5) change “alg” from HS256 to none, change “role” from user to admin, add a separator . at the end of token



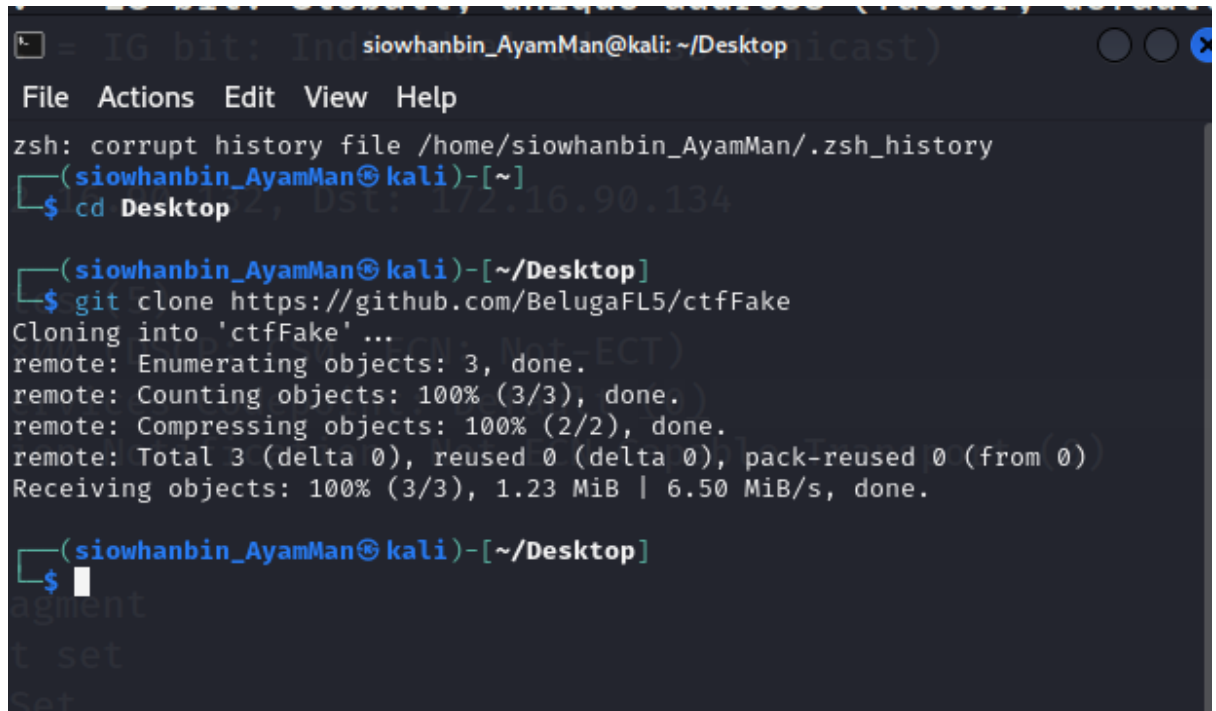
6) **Paste the token and refresh**



7) **The flag is apuCTF{succ3ss_@u7h3nt1c@710n_72bf8bd5}**

Question 3.2

- 1) First download the file



```
siowhanbin_AyamMan@kali: ~/Desktop
File Actions Edit View Help
zsh: corrupt history file /home/siowhanbin_AyamMan/.zsh_history
(siowhanbin_AyamMan@kali)-[~]
$ cd Desktop
(siowhanbin_AyamMan@kali)-[~/Desktop]
$ git clone https://github.com/BelugaFL5/ctfFake
Cloning into 'ctfFake' ...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (3/3), 1.23 MiB | 6.50 MiB/s, done.
(siowhanbin_AyamMan@kali)-[~/Desktop]
$
```

- 2) Then read the question, dits and dahs refer to morse code. Sending message on internet is http or https protocol

Question 3.2 - Network Forensic (15 marks)

Title: dits and dahs

Description:

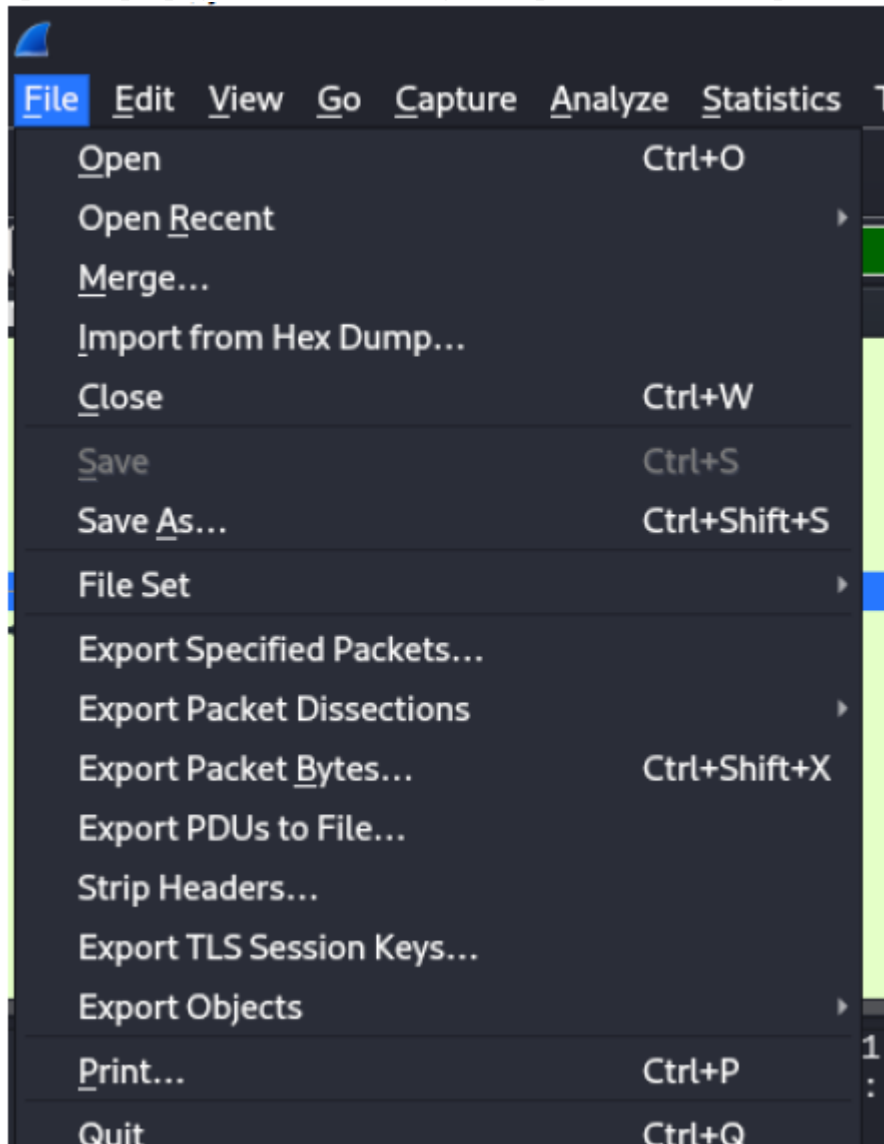
Somebody is asking for help by sending a message on the internet. We manage to intercept the traffic in the network. Discover the flag and help this person.

Attached file: [dits-and-dahs.pcapng](#)

Hint: *There are three (3) part of the flag.*

Flag Format: **apuCTF{flag}**

- 3) Open the pcapng file in wireshark, go to exports objects -> http -> save all



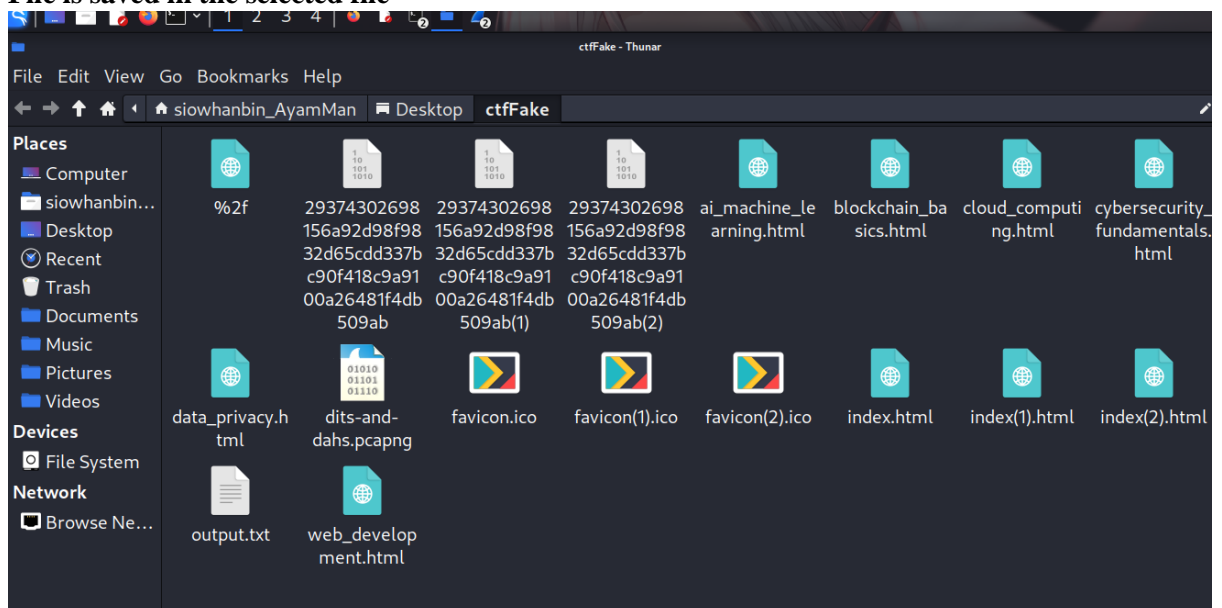
Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

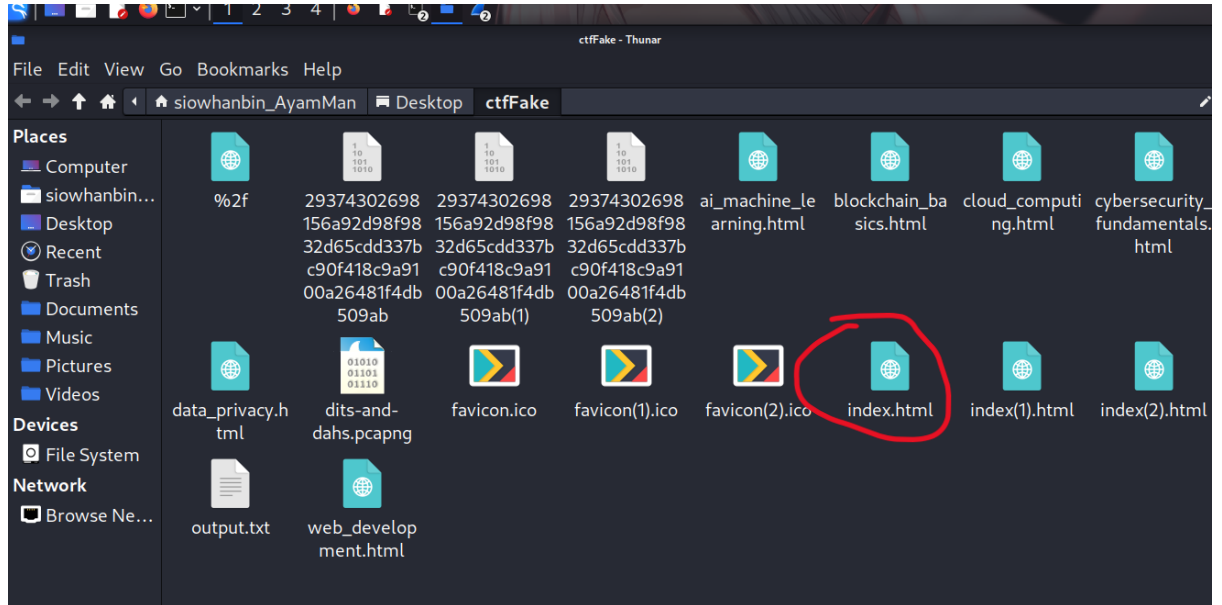
| Packet | Hostname | Content Type | Size | Filename |
|--------|--------------------|--------------------------|-------------|---------------------------------|
| 1471 | 172.16.90.134 | text/html | 1,163 bytes | / |
| 1478 | 172.16.90.134 | text/html | 335 bytes | favicon.ico |
| 1491 | 172.16.90.134 | text/html | 719 bytes | web_development.html |
| 1567 | edgedl.me.gvt1.com | application/octet-stream | 1,120 bytes | 29374302698156a92d98f9832d65cdc |
| 1572 | 172.16.90.134 | text/html | 1,163 bytes | index.html |
| 1585 | 172.16.90.134 | text/html | 669 bytes | blockchain_basics.html |
| 1594 | edgedl.me.gvt1.com | application/octet-stream | 2,016 bytes | 29374302698156a92d98f9832d65cdc |
| 1602 | edgedl.me.gvt1.com | application/octet-stream | 2,355 bytes | 29374302698156a92d98f9832d65cdc |
| 1607 | 172.16.90.134 | text/html | 727 bytes | cybersecurity_fundamentals.html |
| 1620 | 172.16.90.134 | text/html | 624 bytes | ai_machine_learning.html |
| 1663 | 172.16.90.134 | text/html | 582 bytes | data_privacy.html |
| 1688 | 172.16.90.134 | text/html | 671 bytes | cloud_computing.html |
| 1698 | 172.16.90.134 | text/html | 1,163 bytes | index.html |
| 1705 | 172.16.90.134 | text/html | 335 bytes | favicon.ico |
| 1715 | 172.16.90.134 | text/html | 1,163 bytes | index.html |
| 1728 | 172.16.90.134 | text/html | 335 bytes | favicon.ico |

Save Save All Preview Close Help

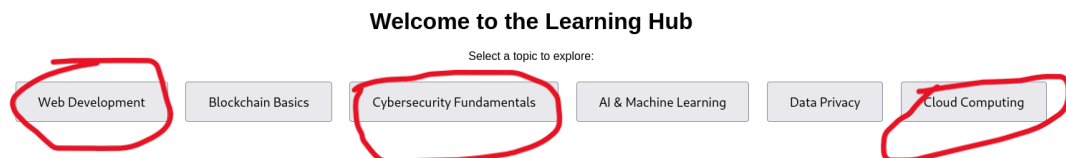
- 4)
- 5) File is saved in the selected file



6) Access index.html at firefox



7) Click Web Development, Cybersecurity Fundamentals and Cloud Computing

**Web Development (1)**

Web development involves building and maintaining websites. It includes aspects like web design, web publishing, web programming, and database management. Web developers use HTML, CSS, JavaScript, and frameworks like React and Angular to create websites and web applications.

11 0010 1011 0000 101 1101 00111 001 00 1100 00000 011 11 11 100 11 10 010 1001 0001 111 1001

[Go Back to Main Page](#)

8)

Cybersecurity Fundamentals (2)

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are typically aimed at accessing, changing, or destroying sensitive information; extorting money; or interrupting normal business processes.

00011 001 10 01 1100 0001 10000 10 0100 001 111 00 1100 1 00 00011 101 11000 0 1100 0110 1001 000

[Go Back to Main Page](#)

Cloud Computing (3)

Cloud computing is the delivery of computing services, including servers, storage, databases, networking, software, and intelligence, over the Internet (the cloud) to offer faster innovation, flexible resources, and economies of scale.

11 100 0001 0100 00000 0100 011 000 00011 100 11 0100 00000 1100 1 110 11 00011 00000

[Go Back to Main Page](#)

9)

10) Paste all the binary code into dcode.fr/morse-code

The screenshot shows the dcode.fr Morse Code Translator interface. On the left, a search bar is present with the text 'F4UTAB0' and 'Q9GENJ0' in the results. The main area is titled 'MORSE CODE TRANSLATOR' and features a 'MORSE CIPHERTEXT TO CONVERT' section with a long binary string. Below this, there are settings for 'MORSECODE CHARACTERS' and 'MORSE SPACE MANAGEMENT'. A 'TRANSLATE AUTOMATICALLY' button is visible. The right sidebar contains a 'Summary' section with links to various Morse code resources.

11) Try everything in cyberchef

The screenshot shows the CyberChef web application. The 'Recipe' panel on the left shows a 'From Base32' step. The 'Input' panel on the right contains the text 'MFYHKQ2UIZ5WMMDMNRXVOX3UNAZV6NLU0IZTI3K7EZXPSMDVL5LWS3DML5ZTGM35'. The 'Output' panel on the right shows the result 'apuCTF{f0ll0w_th3_5tr34m_&_y0u_Will_s33}'.

12) The flag is: apuCTF{f0ll0w_th3_5tr34m_&_y0u_Will_s33}

13) Learnt from: https://github.com/BelugaFL5/ctf_Writeups/