

Challenge Security (CTFlearn)

Name: Rimas Alharbi

Months: June-July

Supervised: Eng. Fahad Alsadda And Ms. Reeman Alharbi

1. Overall Summary

This document provides a comprehensive summary of the cybersecurity challenges I am working on as part of my learning and skill development in the field of security. These challenges cover a wide range of attack and defense techniques that are essential. The primary goal is to strengthen my practical knowledge in identifying vulnerabilities, exploiting them responsibly in a controlled environment, and applying appropriate defensive measures. Each challenge is designed to simulate real-world scenarios using a safe and isolated lab environment, ensuring ethical practice. The outcomes of these exercises will enhance my ability to conduct security assessments and respond effectively to potential threats.

2. Study Progress

2.1 Forensics 101 Challenge (easy Level)

1. First, visit this site. "https://mega.nz/#!OHohCbTa!wbg60PARf4u6E6juuvK9-aDRe_bgEL937VO01EImM7c"
2. Download the image, create a file named CTF and rename for ex:
3. Write in terminal "cd CTF" Go into the folder named CTF that exists in the current directory.
4. Write in terminal "exiftool Forensics\ 101.jpeg" Use exiftool to extract metadata from the file named Forensics 101.jpeg
5. Write in terminal "strings Forensics\ 101.jpeg" Use strings Extract readable text (ASCII strings) from inside the image file Forensics 101.jpeg
6. Well done we have found the flag.

Screenshot:

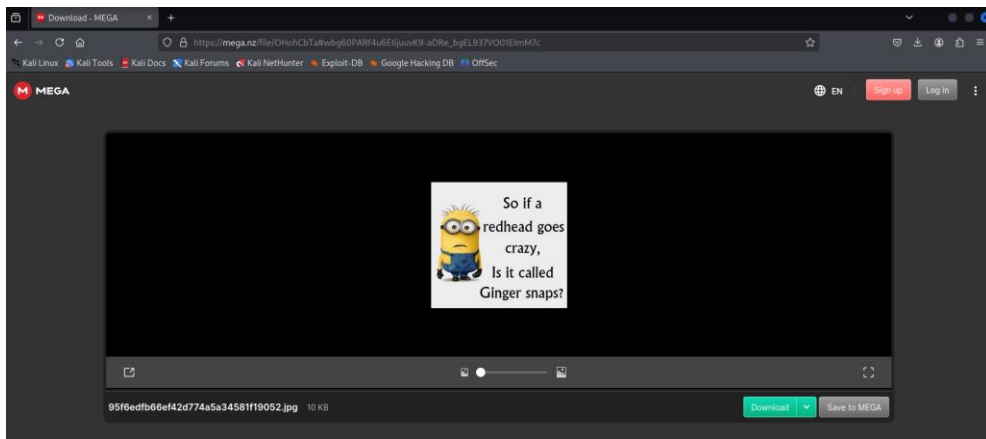


Figure 1



Figure 2

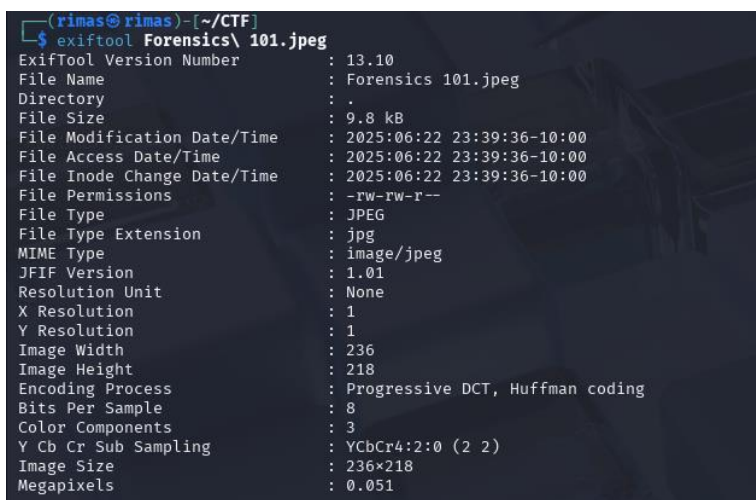


Figure 3



Figure 4

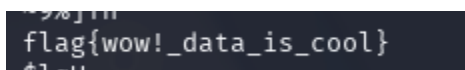


Figure 5

2.2 Taking LS Challenge (easy Level)

1. First, visit this site. https://mega.nz/#!mCgBjZgB!FtmAm8s_mpsHr7KWv8GyUzhhbThNn0l8cHMBi4fjQp8
2. Download the ZIP File.
3. Write in Terminal “unzip The\ Flag.zip” To open the ZIP file.
4. Write in Terminal “cd The\ Flag” Go into the folder named The Flag that exists in the current directory.
5. Write in Terminal “ls -la” to lists all files and folders, including hidden ones, with detailed information.
6. Take the file highlighted in a different color because it is the hidden file.
7. Repeat step 2 in ThePassword' file
8. Repeat step 2
9. Write in Terminal “cat ThePassword.txt” to Display the contents of a file in the terminal.
10. Well done we have found the password and go to The flag PDF and write the password.

Screenshot:

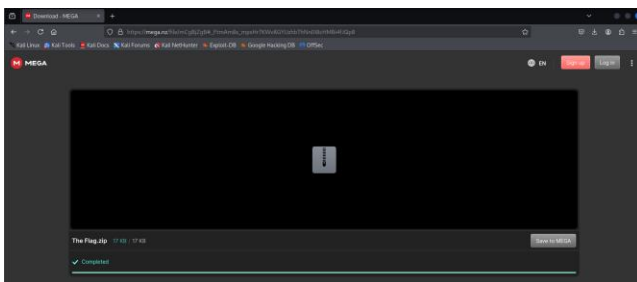


Figure 1

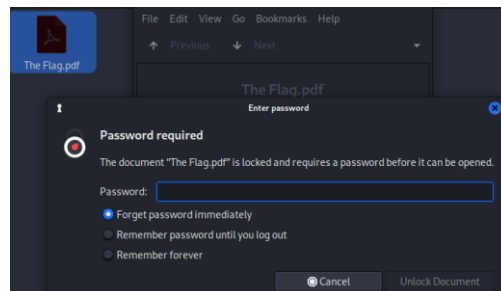


Figure 2

```
(rimas@rimas) ~/Challenges/Taking_LS
$ unzip The Flag.zip
Archive: The Flag.zip
  creating: The Flag/
  inflating: The Flag/.DS_Store
  creating: __MACOSX/
  creating: __MACOSX/The Flag/
  inflating: __MACOSX/The Flag/._.DS_Store
  creating: The Flag/.ThePassword/
  inflating: The Flag/.ThePassword/ThePassword.txt
  inflating: The Flag/The Flag.pdf
  inflating: __MACOSX/The Flag/._The Flag.pdf

(rimas@rimas) ~/Challenges/Taking_LS
$ cd The Flag
(rimas@rimas) ~/Challenges/Taking_LS/The Flag
$ ls
The Flag.pdf
(rimas@rimas) ~/Challenges/Taking_LS/The Flag
$ ls -la
total 40
drwxr-xr-x 3 rimas rimas 4096 Oct 30 2016 .
drwxrwxr-x 4 rimas rimas 4096 Jun 24 22:48 ..
-rw-r--r-- 1 rimas rimas 6148 Oct 30 2016 .DS_Store
-rw-r--r-- 1 rimas rimas 16647 Oct 30 2016 'The Flag.pdf'
drwxr-xr-x 2 rimas rimas 4096 Oct 30 2016 '.ThePassword'
```

Figure 3

```
(rimas@rimas) ~/Challenges/Taking_LS/The Flag
$ cd .ThePassword
(rimas@rimas) ~/Challenges/Taking_LS/The Flag/.ThePassword
$ ls
ThePassword.txt
(rimas@rimas) ~/Challenges/Taking_LS/The Flag/.ThePassword
$ cat ThePassword.txt
Nice Job! The Password is "Im The Flag".
```

Figure 4

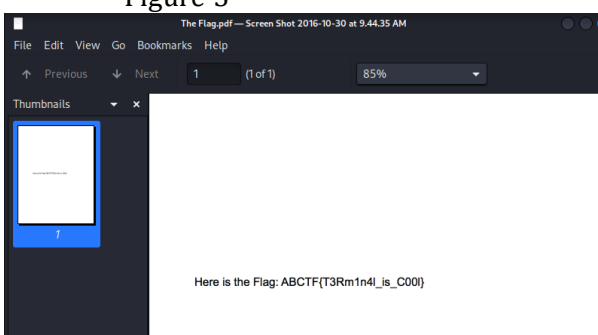


Figure 5

2.3 What could this be? (Medium Level)

1. First, visit this site. https://mega.nz/#!SDQkUYQZ!b1Fu7iZ_wGiNX0aOjez95_74TYDCnLb3YSQfRzs0J-o
2. Download the what_can_this_be .txt.
3. So you can see it is a JSfuck
4. Go to <https://jsfuck.com/>
5. Copy and paste and run the text to the site to find out the flag.
6. The flag (flag{5uch_j4v4_5crip7_much_w0w})

Screenshot:



Figure 1

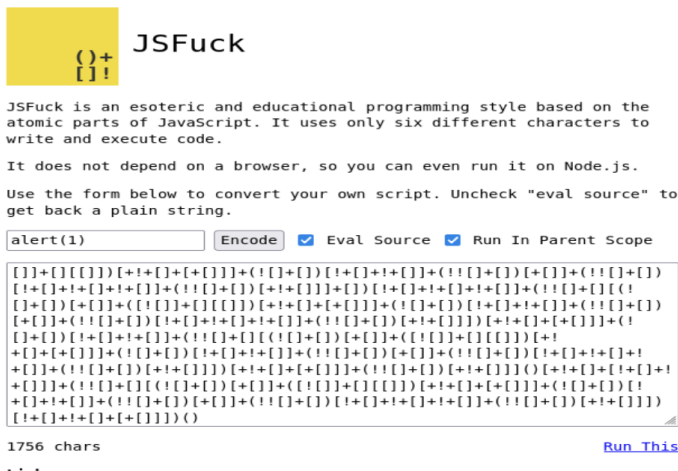


Figure 2

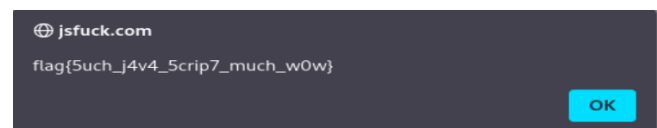


Figure 3

2.4 Substitution Cipher (Medium Level)

1. First, visit this site. https://mega.nz/#!iCBz2IIL!B7292dISx1PGXoWhd9oFLk2g0NFqGApBaltI_2Gsp9w
[Figure it out for me, will ya?](#)
2. Download the Substitution .txt.
3. You can go to this site to Analyze the speech and solve the problem yourself. I solved it myself, then I used a site to solve the codes because of the time like <https://legacy.cryptool.org/en/cto/frequency-analysis>.
4. The site that solves <https://www.guballa.de/substitution-solver>
5. Copy and paste and run the text to the site to find out the flag.
6. The flag it is {flag{IFONLYMODERNCRYPTOWASLIKETHIS}}

Screenshot:

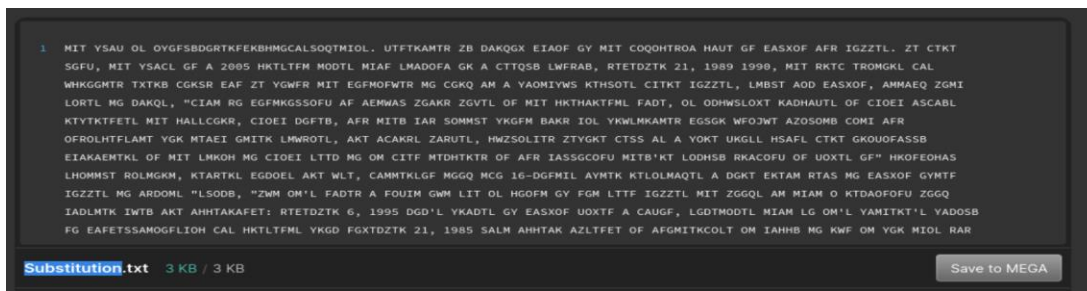


Figure 1

Substitution Solver

This tool solves monoalphabetic substitution ciphers, also known as cryptograms. These are ciphers where each letter of the clear text is replaced by a corresponding letter of the cipher alphabet.

As an example here is an English cryptogram this tool can solve:

```
Rbo rpkktgo vcrb buwcja wj kloj hcjd, km sktpgo, cq rbwr loklgo  
vcgg cjqr kj skhcja wqkja wjd rpycja rk ltr rbcjaq cj cr.  
-- Roppy Lpwsborr
```

A Python implementation of this breaker is provided on [GitLab](#).

If you want to break a polyalphabetic cipher instead try the [Vigenère Solver](#).

Input

Cipher Text *

Ciph Please fill out this field.

Result

Key	abcdefghijklmnopqrstuvwxyz	This clear text ...
	aywmcnophqrstjizkdlegxuvfb	... maps to this cipher text

THE FLAG IS IFONLYMODERNCRYPTOWASLIKETHIS. GENERATED BY MARKOV CHAIN OF THE WIKIPEDIA PAGE ON CALVIN AND HOBBS. BE WERE LONG, THE FLAWS ON A 2005 PRESENT TIMES THAN STAMINA OR A WEEKLY SUNDAY, DECEMBER 21, 1989 1990, THE DREW EDITORS WAS UPROOTED EVERY WORLD CAN BE FOUND THE CONTINUED TO WORK AT A FAITHFUL REPLIES WHERE HOBBS, STYLE AIM CALVIN, ATTACK BOTH SIDES TO MARKS, "WHAT DO CONTROLLING AN ACTUAL BOARD BOXES IN THE PREPARENTS NAME, IS IMPULSIVE RAMPAGES IN WHICH ALWAYS

► Details

Runtime: 0.017 seconds

Figure 2

Figure 3

2.5 The adventures of Boris Ivanov. Part 1. (Medium Level)

1. First, visit this site. https://mega.nz/#!HfAHmKQb!zg6EPqfwes1bBDCjx7-ZFR_000-GtGg2Mrn56l5LCkE
2. Download the Boris_Ivanov_1.jpg.
3. Write in Terminal “sudo -s” starts a new shell with root privileges, allowing you to run commands as the root user without switching users completely.
4. Write in Terminal “cd Downloads” Change into the Downloads directory from the current location.
5. Write in Terminal “ls” List the files and folders in the current directory.
6. Write in Terminal “file Boris_Ivanov_1.jpg” tell me the type of the file.
7. Write in Terminal “java -jar stegsolve.jar” To Run the StegSolve tool using Java.
8. Open the Image Boris_Ivanov_1.jpg from File.
9. And go to analyse and go to stereogram solver and change the offset to 102.

Screenshot:

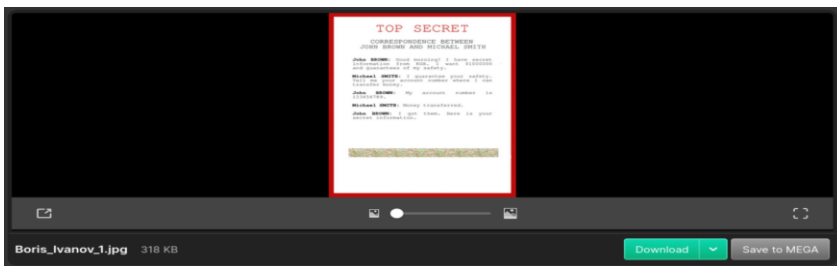


Figure 1

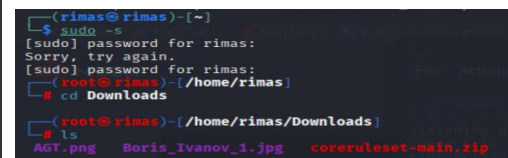


Figure 2

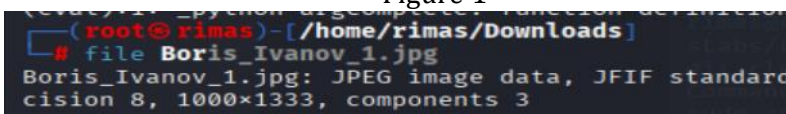


Figure 3

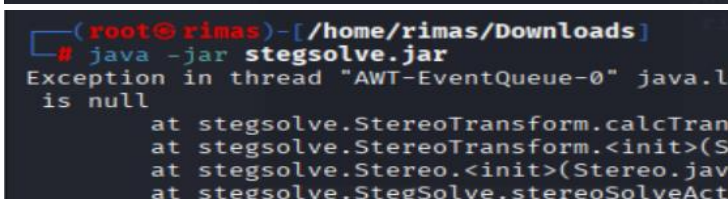


Figure 4

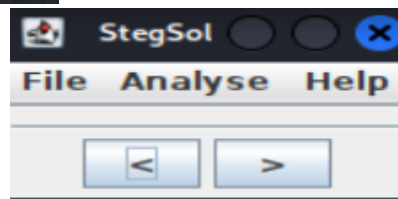


Figure 5

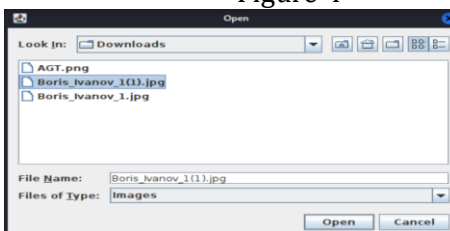


Figure 6



Figure 7

2.6 PIN (Medium Level)

1. First, visit this site. <https://mega.nz/file/PXYjCKCY#F2gcs83XD6RxjOR-FNWGQZpyvUFvDbuT-PTnqRhBPGQ>
2. Download the rev1 file.
3. Write in Terminal “cd Downloads” Change into the Downloads directory from the current location.
4. Write in Terminal “ls” List the files and folders in the current directory.
5. Write in Terminal “chmod +x rev1” is used in Linux to make the file rev1 executable, so you can run it like a program or script.
6. Write in Terminal “./rev1” try to run a file and write the PIN.
7. Write in Terminal “r2 -AA rev1” This command opens the file rev1 in Radare2 (r2) and performs deep automatic analysis.
8. In Radare2, write ood This reopens the file in debug mode, allowing you to step through the program during execution.
9. Write pdf @main This command disassembles and displays the instructions inside the main function.
10. Write pdf @sym.cek This shows the disassembly of the cek function, which contains the logic used to check the correct PIN.
11. From analyzing the function, identify the correct PIN value (e.g., 333333) and use it to run the file successfully.

Screenshot:

```
(rimas@rimas)~[~]
$ cd Downloads
(rimas@rimas)~[~/Downloads]
$ ls
AGT.png          rev1              what_can_this_be.txt
'Boris_Ivanov_1(1).jpg' stegsolve.jar    windowsandroid-4-0-3.exe
'Boris_Ivanov_1.jpg' Substitution.txt
coreruleaset-main.zip 'The Flag.zip'
```

Figure 1

```
(rimas@rimas)~[~/Downloads]
$ chmod +x rev1
(rimas@rimas)~[~/Downloads]
$ ./rev1
Masukan PIN = 123123123
PIN salah !
```

Figure 2

```
(rimas@rimas)~[~/Downloads]
$ r2 -AA rev1
WARN: Relocs has not been applied. Please use '-e bin.relocs.apply=true' or '-e bin.cache=true' next time
INFO: Analyze all flags starting with sym. and entry (aa)
INFO: Analyze imports (af0001)
INFO: Analyze entrypoint (af0000)
INFO: Analyze symbols (af0005)
INFO: Analyze all functions arguments/locals (afva000f)
INFO: Analyze function calls (aac)
INFO: Analyze len bytes of instructions for references (aar)
INFO: Finding and parsing C++ vtables (aavr)
INFO: Analyzing methods (af aa method+)
INFO: Recovering local variables (afv0000f)
INFO: Type matching analysis for all functions (aadt)
INFO: Propagate nonreturn information (aanr)
INFO: Scanning for strings constructed in code (/aaz)
INFO: Finding function preludes (aap)
INFO: Enable anal.types.constraint for experimental type propagation
[Q=00400000] ood
INFO: File dbg:///home/rimas/downloads/rev1 reopened in read-write mode
WARN: Relocs has not been applied. Please use '-e bin.relocs.apply=true' or '-e bin.cache=true' next time
00000000
[Q=7F1B17F93440] pdf @main
961 int main(int argc, char *argv, char **envp){
  afv: vars(1:sp[0xc..0xc])
  00000000 55          push rbp
  00000001 4889e5      mov rbp, rsp
  00000002 48b1e0      sub rsp, 0x10
  00000003 48bd0f08    lea rdi, str.Masukan_PIN ; 0x08
  00000004 48b50005    ; const char *format
  00000005 48b50005    ; 0x00000005
  00000006 48b50005    ; 0x00000005
  00000007 48b50005    ; 0x00000005
  00000008 48b50005    ; 0x00000005
  00000009 48b50005    ; 0x00000005
  0000000a 48b50005    ; 0x00000005
  0000000b 48b50005    ; 0x00000005
  0000000c 48b50005    ; 0x00000005
  0000000d 48b50005    ; 0x00000005
  0000000e 48b50005    ; 0x00000005
  0000000f 48b50005    ; 0x00000005
  00000010 48b50005    ; 0x00000005
  00000011 48b50005    ; 0x00000005
  00000012 48b50005    ; 0x00000005
  00000013 48b50005    ; 0x00000005
  00000014 48b50005    ; 0x00000005
  00000015 48b50005    ; 0x00000005
  00000016 48b50005    ; 0x00000005
  00000017 48b50005    ; 0x00000005
  00000018 48b50005    ; 0x00000005
  00000019 48b50005    ; 0x00000005
  0000001a 48b50005    ; 0x00000005
  0000001b 48b50005    ; 0x00000005
  0000001c 48b50005    ; 0x00000005
  0000001d 48b50005    ; 0x00000005
  0000001e 48b50005    ; 0x00000005
  0000001f 48b50005    ; 0x00000005
  00000020 48b50005    ; 0x00000005
  00000021 48b50005    ; 0x00000005
  00000022 48b50005    ; 0x00000005
  00000023 48b50005    ; 0x00000005
  00000024 48b50005    ; 0x00000005
  00000025 48b50005    ; 0x00000005
  00000026 48b50005    ; 0x00000005
  00000027 48b50005    ; 0x00000005
  00000028 48b50005    ; 0x00000005
  00000029 48b50005    ; 0x00000005
  0000002a 48b50005    ; 0x00000005
  0000002b 48b50005    ; 0x00000005
  0000002c 48b50005    ; 0x00000005
  0000002d 48b50005    ; 0x00000005
  0000002e 48b50005    ; 0x00000005
  0000002f 48b50005    ; 0x00000005
  00000030 48b50005    ; 0x00000005
  00000031 48b50005    ; 0x00000005
  00000032 48b50005    ; 0x00000005
  00000033 48b50005    ; 0x00000005
  00000034 48b50005    ; 0x00000005
  00000035 48b50005    ; 0x00000005
  00000036 48b50005    ; 0x00000005
  00000037 48b50005    ; 0x00000005
  00000038 48b50005    ; 0x00000005
  00000039 48b50005    ; 0x00000005
  0000003a 48b50005    ; 0x00000005
  0000003b 48b50005    ; 0x00000005
  0000003c 48b50005    ; 0x00000005
  0000003d 48b50005    ; 0x00000005
  0000003e 48b50005    ; 0x00000005
  0000003f 48b50005    ; 0x00000005
  00000040 48b50005    ; 0x00000005
  00000041 48b50005    ; 0x00000005
  00000042 48b50005    ; 0x00000005
  00000043 48b50005    ; 0x00000005
  00000044 48b50005    ; 0x00000005
  00000045 48b50005    ; 0x00000005
  00000046 48b50005    ; 0x00000005
  00000047 48b50005    ; 0x00000005
  00000048 48b50005    ; 0x00000005
  00000049 48b50005    ; 0x00000005
  0000004a 48b50005    ; 0x00000005
  0000004b 48b50005    ; 0x00000005
  0000004c 48b50005    ; 0x00000005
  0000004d 48b50005    ; 0x00000005
  0000004e 48b50005    ; 0x00000005
  0000004f 48b50005    ; 0x00000005
  00000050 48b50005    ; 0x00000005
  00000051 48b50005    ; 0x00000005
  00000052 48b50005    ; 0x00000005
  00000053 48b50005    ; 0x00000005
  00000054 48b50005    ; 0x00000005
  00000055 48b50005    ; 0x00000005
  00000056 48b50005    ; 0x00000005
  00000057 48b50005    ; 0x00000005
  00000058 48b50005    ; 0x00000005
  00000059 48b50005    ; 0x00000005
  0000005a 48b50005    ; 0x00000005
  0000005b 48b50005    ; 0x00000005
  0000005c 48b50005    ; 0x00000005
  0000005d 48b50005    ; 0x00000005
  0000005e 48b50005    ; 0x00000005
  0000005f 48b50005    ; 0x00000005
  00000060 48b50005    ; 0x00000005
  00000061 48b50005    ; 0x00000005
  00000062 48b50005    ; 0x00000005
  00000063 48b50005    ; 0x00000005
  00000064 48b50005    ; 0x00000005
  00000065 48b50005    ; 0x00000005
  00000066 48b50005    ; 0x00000005
  00000067 48b50005    ; 0x00000005
  00000068 48b50005    ; 0x00000005
  00000069 48b50005    ; 0x00000005
  0000006a 48b50005    ; 0x00000005
  0000006b 48b50005    ; 0x00000005
  0000006c 48b50005    ; 0x00000005
  0000006d 48b50005    ; 0x00000005
  0000006e 48b50005    ; 0x00000005
  0000006f 48b50005    ; 0x00000005
  00000070 48b50005    ; 0x00000005
  00000071 48b50005    ; 0x00000005
  00000072 48b50005    ; 0x00000005
  00000073 48b50005    ; 0x00000005
  00000074 48b50005    ; 0x00000005
  00000075 48b50005    ; 0x00000005
  00000076 48b50005    ; 0x00000005
  00000077 48b50005    ; 0x00000005
  00000078 48b50005    ; 0x00000005
  00000079 48b50005    ; 0x00000005
  0000007a 48b50005    ; 0x00000005
  0000007b 48b50005    ; 0x00000005
  0000007c 48b50005    ; 0x00000005
  0000007d 48b50005    ; 0x00000005
  0000007e 48b50005    ; 0x00000005
  0000007f 48b50005    ; 0x00000005
  00000080 48b50005    ; 0x00000005
  00000081 48b50005    ; 0x00000005
  00000082 48b50005    ; 0x00000005
  00000083 48b50005    ; 0x00000005
  00000084 48b50005    ; 0x00000005
  00000085 48b50005    ; 0x00000005
  00000086 48b50005    ; 0x00000005
  00000087 48b50005    ; 0x00000005
  00000088 48b50005    ; 0x00000005
  00000089 48b50005    ; 0x00000005
  0000008a 48b50005    ; 0x00000005
  0000008b 48b50005    ; 0x00000005
  0000008c 48b50005    ; 0x00000005
  0000008d 48b50005    ; 0x00000005
  0000008e 48b50005    ; 0x00000005
  0000008f 48b50005    ; 0x00000005
  00000090 48b50005    ; 0x00000005
  00000091 48b50005    ; 0x00000005
  00000092 48b50005    ; 0x00000005
  00000093 48b50005    ; 0x00000005
  00000094 48b50005    ; 0x00000005
  00000095 48b50005    ; 0x00000005
  00000096 48b50005    ; 0x00000005
  00000097 48b50005    ; 0x00000005
  00000098 48b50005    ; 0x00000005
  00000099 48b50005    ; 0x00000005
  0000009a 48b50005    ; 0x00000005
  0000009b 48b50005    ; 0x00000005
  0000009c 48b50005    ; 0x00000005
  0000009d 48b50005    ; 0x00000005
  0000009e 48b50005    ; 0x00000005
  0000009f 48b50005    ; 0x00000005
  000000a0 48b50005    ; 0x00000005
  000000a1 48b50005    ; 0x00000005
  000000a2 48b50005    ; 0x00000005
  000000a3 48b50005    ; 0x00000005
  000000a4 48b50005    ; 0x00000005
  000000a5 48b50005    ; 0x00000005
  000000a6 48b50005    ; 0x00000005
  000000a7 48b50005    ; 0x00000005
  000000a8 48b50005    ; 0x00000005
  000000a9 48b50005    ; 0x00000005
  000000aa 48b50005    ; 0x00000005
  000000ab 48b50005    ; 0x00000005
  000000ac 48b50005    ; 0x00000005
  000000ad 48b50005    ; 0x00000005
  000000ae 48b50005    ; 0x00000005
  000000af 48b50005    ; 0x00000005
  000000b0 48b50005    ; 0x00000005
  000000b1 48b50005    ; 0x00000005
  000000b2 48b50005    ; 0x00000005
  000000b3 48b50005    ; 0x00000005
  000000b4 48b50005    ; 0x00000005
  000000b5 48b50005    ; 0x00000005
  000000b6 48b50005    ; 0x00000005
  000000b7 48b50005    ; 0x00000005
  000000b8 48b50005    ; 0x00000005
  000000b9 48b50005    ; 0x00000005
  000000ba 48b50005    ; 0x00000005
  000000bb 48b50005    ; 0x00000005
  000000bc 48b50005    ; 0x00000005
  000000bd 48b50005    ; 0x00000005
  000000be 48b50005    ; 0x00000005
  000000bf 48b50005    ; 0x00000005
  000000c0 48b50005    ; 0x00000005
  000000c1 48b50005    ; 0x00000005
  000000c2 48b50005    ; 0x00000005
  000000c3 48b50005    ; 0x00000005
  000000c4 48b50005    ; 0x00000005
  000000c5 48b50005    ; 0x00000005
  000000c6 48b50005    ; 0x00000005
  000000c7 48b50005    ; 0x00000005
  000000c8 48b50005    ; 0x00000005
  000000c9 48b50005    ; 0x00000005
  000000ca 48b50005    ; 0x00000005
  000000cb 48b50005    ; 0x00000005
  000000cc 48b50005    ; 0x00000005
  000000cd 48b50005    ; 0x00000005
  000000ce 48b50005    ; 0x00000005
  000000cf 48b50005    ; 0x00000005
  000000d0 48b50005    ; 0x00000005
  000000d1 48b50005    ; 0x00000005
  000000d2 48b50005    ; 0x00000005
  000000d3 48b50005    ; 0x00000005
  000000d4 48b50005    ; 0x00000005
  000000d5 48b50005    ; 0x00000005
  000000d6 48b50005    ; 0x00000005
  000000d7 48b50005    ; 0x00000005
  000000d8 48b50005    ; 0x00000005
  000000d9 48b50005    ; 0x00000005
  000000da 48b50005    ; 0x00000005
  000000db 48b50005    ; 0x00000005
  000000dc 48b50005    ; 0x00000005
  000000dd 48b50005    ; 0x00000005
  000000de 48b50005    ; 0x00000005
  000000df 48b50005    ; 0x00000005
  000000e0 48b50005    ; 0x00000005
  000000e1 48b50005    ; 0x00000005
  000000e2 48b50005    ; 0x00000005
  000000e3 48b50005    ; 0x00000005
  000000e4 48b50005    ; 0x00000005
  000000e5 48b50005    ; 0x00000005
  000000e6 48b50005    ; 0x00000005
  000000e7 48b50005    ; 0x00000005
  000000e8 48b50005    ; 0x00000005
  000000e9 48b50005    ; 0x00000005
  000000ea 48b50005    ; 0x00000005
  000000eb 48b50005    ; 0x00000005
  000000ec 48b50005    ; 0x00000005
  000000ed 48b50005    ; 0x00000005
  000000ee 48b50005    ; 0x00000005
  000000ef 48b50005    ; 0x00000005
  000000f0 48b50005    ; 0x00000005
  000000f1 48b50005    ; 0x00000005
  000000f2 48b50005    ; 0x00000005
  000000f3 48b50005    ; 0x00000005
  000000f4 48b50005    ; 0x00000005
  000000f5 48b50005    ; 0x00000005
  000000f6 48b50005    ; 0x00000005
  000000f7 48b50005    ; 0x00000005
  000000f8 48b50005    ; 0x00000005
  000000f9 48b50005    ; 0x00000005
  000000fa 48b50005    ; 0x00000005
  000000fb 48b50005    ; 0x00000005
  000000fc 48b50005    ; 0x00000005
  000000fd 48b50005    ; 0x00000005
  000000fe 48b50005    ; 0x00000005
  000000ff 48b50005    ; 0x00000005
  00000100 48b50005    ; 0x00000005
  00000101 48b50005    ; 0x00000005
  00000102 48b50005    ; 0x00000005
  00000103 48b50005    ; 0x00000005
  00000104 48b50005    ; 0x00000005
  00000105 48b50005    ; 0x00000005
  00000106 48b50005    ; 0x00000005
  00000107 48b50005    ; 0x00000005
  00000108 48b50005    ; 0x00000005
  00000109 48b50005    ; 0x00000005
  0000010a 48b50005    ; 0x00000005
  0000010b 48b50005    ; 0x00000005
  0000010c 48b50005    ; 0x00000005
  0000010d 48b50005    ; 0x00000005
  0000010e 48b50005    ; 0x00000005
  0000010f 48b50005    ; 0x00000005
  00000110 48b50005    ; 0x00000005
  00000111 48b50005    ; 0x00000005
  00000112 48b50005    ; 0x00000005
  00000113 48b50005    ; 0x00000005
  00000114 48b50005    ; 0x00000005
  00000115 48b50005    ; 0x00000005
  00000116 48b50005    ; 0x00000005
  00000117 48b50005    ; 0x00000005
  00000118 48b50005    ; 0x00000005
  00000119 48b50005    ; 0x00000005
  0000011a 48b50005    ; 0x00000005
  0000011b 48b50005    ; 0x00000005
  0000011c 48b50005    ; 0x00000005
  0000011d 48b50005    ; 0x00000005
  0000011e 48b50005    ; 0x00000005
  0000011f 48b50005    ; 0x00000005
  00000120 48b50005    ; 0x00000005
  00000121 48b50005    ; 0x00000005
  00000122 48b50005    ; 0x00000005
  00000123 48b50005    ; 0x00000005
  00000124 48b50005    ; 0x00000005
  00000125 48b50005    ; 0x00000005
  00000126 48b50005    ; 0x00000005
  00000127 48b50005    ; 0x00000005
  00000128 48b50005    ; 0x00000005
  00000129 48b50005    ; 0x00000005
  0000012a 48b50005    ; 0x00000005
  0000012b 48b50005    ; 0x00000005
  0000012c 48b50005    ; 0x00000005
  0000012d 48b50005    ; 0x00000005
  0000012e 48b50005    ; 0x00000005
  0000012f 48b50005    ; 0x00000005
  00000130 48b50005    ; 0x00000005
  00000131 48b50005    ; 0x00000005
  00000132 48b50005    ; 0x00000005
  00000133 48b50005    ; 0x00000005
  00000134 48b50005    ; 0x00000005
  00000135 48b50005    ; 0x00000005
  00000136 48b50005    ; 0x00000005
  00000137 48b50005    ; 0x00000005
  00000138 48b50005    ; 0x00000005
  00000139 48b50005    ; 0x00000005
  0000013a 48b50005    ; 0x00000005
  0000013b 48b50005    ; 0x00000005
  0000013c 48b50005    ; 0x00000005
  0000013d 48b50005    ; 0x00000005
  0000013e 48b50005    ; 0x00000005
  0000013f 48b50005    ; 0x00000005
  00000140 48b50005    ; 0x00000005
  00000141 48b50005    ; 0x00000005
  00000142 48b50005    ; 0x00000005
  00000143 48b50005    ; 0x00000005
  00000144 48b50005    ; 0x00000005
  00000145 48b50005    ; 0x00000005
  00000146 48b50005    ; 0x00000005
  00000147 48b50005    ; 0x00000005
  00000148 48b50005    ; 0x00000005
  00000149 48b50005    ; 0x00000005
  0000014a 48b50005    ; 0x00000005
  0000014b 48b50005    ; 0x00000005
  0000014c 48b50005    ; 0x00000005
  0000014d 48b50005    ; 0x00000005
  0000014e 48b50005    ; 0x00000005
  0000014f 48b50005    ; 0x00000005
  00000150 48b50005    ; 0x00000005
  00000151 48b50005    ; 0x00000005
  00000152 48b50005    ; 0x00000005
  00000153 48b50005    ; 0x00000005
  00000154 48b50005    ; 0x00000005
  0000015
```

2.7 Calculat3 M3. (Hard Level)

1. First, visit this site. <http://web.ctflearn.com/web7/>.
2. I right-clicked anywhere on the page and chose Inspect to open Developer Tools.
3. I entered a basic expression in the calculator, for example: 9 * 9, then clicked the "=" button to calculate.
4. I went to the Network tab to monitor requests sent by the calculator.
5. I looked at the first network request that appeared in the list after I clicked "="
6. I clicked on that request to see the expression, then go to header then resend and go to the body.
7. I modified the expression to: expression=;ls — trying to test for command injection.
8. I clicked on send the expression and clicked the new state and go to the response and see the flag.

Screenshot:

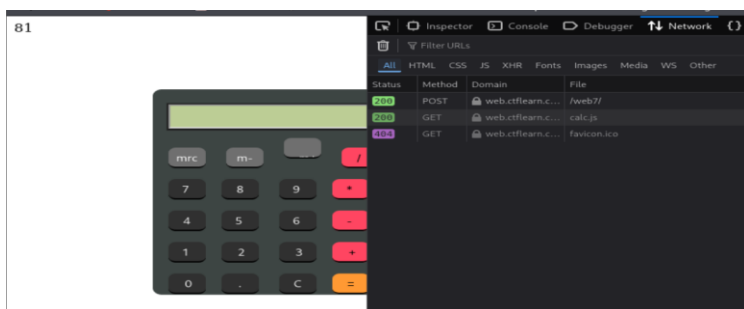


Figure 1

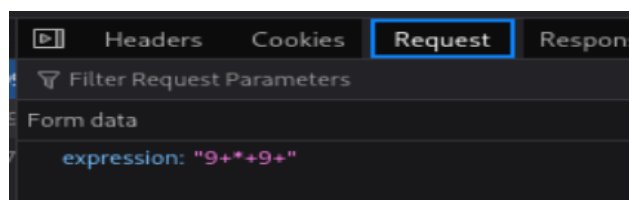


Figure 2

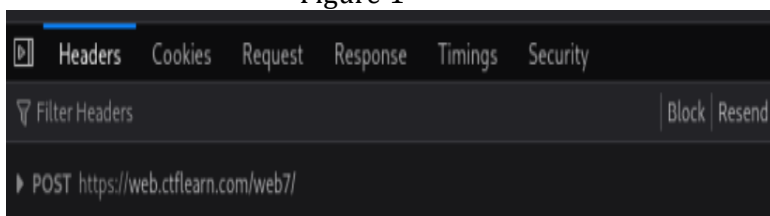


Figure 3

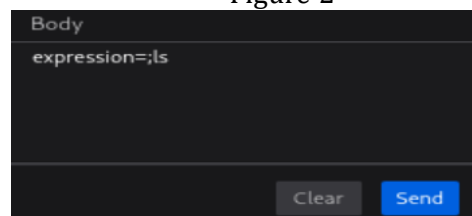


Figure 4



Figure 5

2.8 Corrupted File. (Hard Level)

1. First, visit this site. https://mega.nz/#!OKxByZyT!vaabCjRG5D9zAU7drTekcA5pszu67r_TbQMtxEzqGE
2. Download the unopenable .gif.
3. Write in Terminal “file unopenable.gif” tell me the type of the file.
4. Write in Terminal “hexdump -C unopenable.gif | head -n 5” This shows the first few lines of the file in hex. The first 6 bytes of a real .gif file.
5. Write in Terminal “echo -ne '\x47\x49\x46\x38\x39\x61' > fixed.gif” This creates a new file called fixed.gif and writes the correct .gif header to it.
6. Write in Terminal “tail -c +2 unopenable.gif >> fixed.gif” corrupted file starting from the second byte and appends it to the new file fixed.gif.
7. Write in Terminal “identify fixed.gif” uses ImageMagick to show detailed information about the image.
8. Write in Terminal “convert fixed.gif frames_%02d.png” split the animated GIF into separate PNG images.
9. Go to Downloads file and see the image, see the text in image, go to the <https://www.base64decode.org/>
10. Decode the text “ZmxhZ3tnMWZfb3JfajFmfq==”
11. See the flag.

Screenshot:

```
(rimas@rimas)-[~/Downloads]
$ file unopenable.gif
unopenable.gif: data

(rimas@rimas)-[~/Downloads]
$ hexdump -C unopenable.gif | head -n 5
00000000  39 61 f4 01 f4 01 f4 00 00 00 00 00 3a 00 00 00 |9a.....:..|
00000010  00 3a 3a 00 3a 66 00 00 66 00 3a 00 00 66 90 3a |.:.:f..f.:.f.:|
00000020  00 90 3a 3a b6 66 00 b6 66 3a 90 90 3a db 90 3a |..:..f..f.:.f.:|
00000030  ff b6 66 00 3a 90 66 3a 90 00 66 90 00 66 b6 3a |..f.:.f.:.f.:|
00000040  66 b6 90 66 90 3a 90 db 66 b6 ff b6 ff b6 ff db |f..f.:.f.....|

(rimas@rimas)-[~/Downloads]
$ echo -ne '\x47\x49\x46\x38\x39\x61' > fixed.gif

(rimas@rimas)-[~/Downloads]
$ tail -c +2 unopenable.gif >> fixed.gif

(rimas@rimas)-[~/Downloads]
$ identify fixed.gif
fixed.gif[0] GIF 500x500 62561x62465+0+0 8-bit sRGB 4c 0.000u 0:00.001
fixed.gif[1] GIF 500x500 62561x62465+0+0 8-bit sRGB 32c 0.000u 0:00.002
fixed.gif[2] GIF 500x500 62561x62465+0+0 8-bit sRGB 64c 0.000u 0:00.002
fixed.gif[3] GIF 500x500 62561x62465+0+0 8-bit sRGB 32c 0.000u 0:00.002
fixed.gif[4] GIF 500x500 62561x62465+0+0 8-bit sRGB 32c 10175B 0:00.002

(rimas@rimas)-[~/Downloads]
$ convert +adjoin fixed.gif frames_%02d.png
convert: invalid colormap index `fixed.gif' @ error/colormap-private.h/ConstrainColormapIndex/35.
```

Figure 1

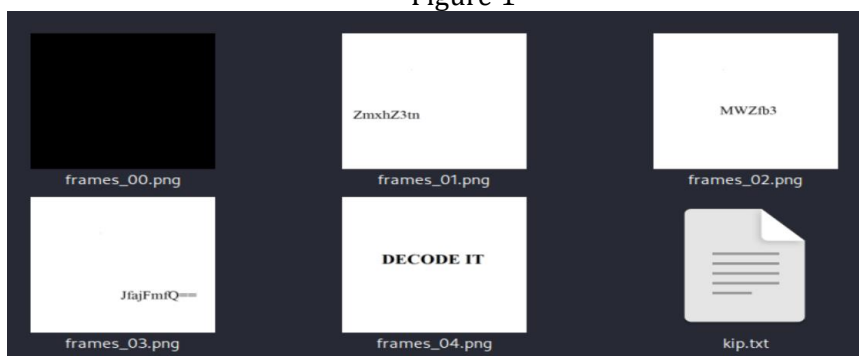


Figure 2

Decode from Base64 format

Simply enter your data then push the decode button.

ZmxhZ3tnMWZfb3JfajFmfq==

Figure 3

< DECODE >

Decodes your data into the area below.

flag{g1f_or_j1f~

Figure 4