Story of image

1. I used “strings” command to get the file.
2. And grep “flag”

Push and regret

1. I have cloned the git repository

```
┌──(kali㉿kali)-[~/codefest25/Stegno]
└─$ git clone https://github.com/ktscyberlk/ironbank-api-ctf.git
Cloning into 'ironbank-api-ctf'...
remote: Enumerating objects: 218, done.
remote: Counting objects: 100% (218/218), done.
remote: Compressing objects: 100% (111/111), done.
remote: Total 218 (delta 95), reused 175 (delta 74), pack-reused 0 (from 0)
Receiving objects: 100% (218/218), 29.96 KiB | 59.00 KiB/s, done.
Resolving deltas: 100% (95/95), done.
```

2. Checked for git log and used different key words to find the flag.
3. When I tried word “key” in log file, found an base64 encrypted string.

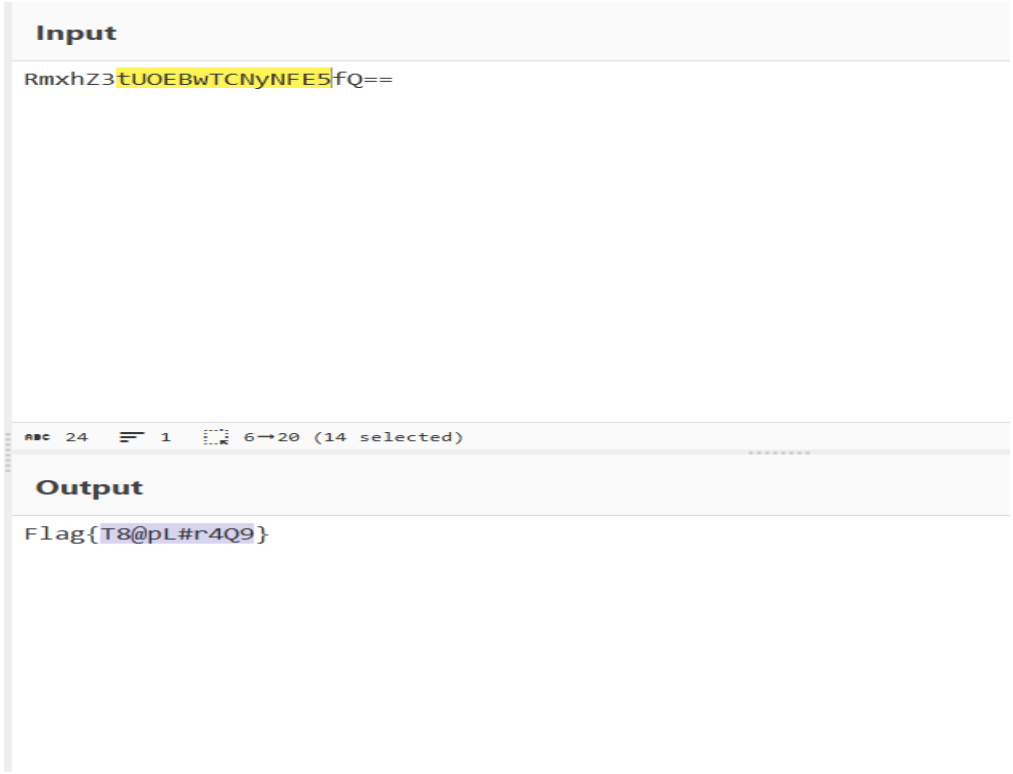
```
┌──(kali㉿kali)-[~/codefest25/Stegno/ironbank-api-ctf]
└─$ git log -p | grep -i "flag"

┌──(kali㉿kali)-[~/codefest25/Stegno/ironbank-api-ctf]
└─$ git log -p | grep -i "secret"
 JWT_SECRET=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
 JWT_SECRET=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
+JWT_SECRET=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
+Your mission is to investigate the repository history and uncover the exposed secret.

┌──(kali㉿kali)-[~/codefest25/Stegno/ironbank-api-ctf]
└─$ git log -p | grep -i "secret"key

┌──(kali㉿kali)-[~/codefest25/Stegno/ironbank-api-ctf]
└─$ git log -p | grep -i "key"
+API_KEY=##########
    Update .env (Removed API key)
-API_KEY=RmxhZ3tUOEBwTCNyNFE5fQ==
+API_KEY=RmxhZ3tUOEBwTCNyNFE5fQ==
+STRIPE_KEY=sk_test_51Hxxxxxxxxxxxxxxxxxxxxxxx
```

4. And then I decrypted the strings. And got the flag.



Trail of Access

1. First I searched the log file for name “greenwilliams”.
2. I got 2 lines with same name with different password, trying that password before the transaction helped me to solve the challenge.

```
217.244.19.166 - - [06/Aug/2025:15:39:14 +0000] "POST /transfer HTTP/1.1" 404 3918 "Mozilla/5.0 (compatible; MSIE 5.0; Windows NT 6.2; Trident/4.1)"
179.120.71.20 - - [06/Aug/2025:15:39:22 +0000] "GET /transfer HTTP/1.1" 403 4125 "Mozilla/5.0 (compatible; MSIE 9.0; Windows 98; Trident/5.0)"
128.82.40.243 - - [06/Aug/2025:15:39:31 +0000] "POST /transfer HTTP/1.1" 301 559 "Mozilla/5.0 (X11; Linux i686) AppleWebKit/531.1 (KHTML, like Gecko) Chrome/30.0.865.0 Safari/531.1"
111.77.67.214 - - [06/Aug/2025:15:39:38 +0000] "GET /profile HTTP/1.1" 404 3293 "Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 4.0; Trident/5.0)"
157.19.229.95 - - [06/Aug/2025:15:39:43 +0000] "POST /dashboard HTTP/1.1" 404 2912 "Opera/8.80.(Windows NT 5.1; ce-RU) Presto/2.9.189 Version/12.00"
80.16.3.250 - - [06/Aug/2025:15:39:52 +0000] "POST /transfer HTTP/1.1" 500 1368 "Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 5.0; Trident/3.1)"
139.35.44.255 - - [06/Aug/2025:15:40:01 +0000] "POST /dashboard HTTP/1.1" 404 2999 "Mozilla/5.0 (compatible; MSIE 8.0; Windows 95; Trident/5.1)"
49.73.219.195 - - [06/Aug/2025:15:40:09 +0000] "GET /settings HTTP/1.1" 500 940 "Mozilla/5.0 (Windows; U; Windows NT 5.0) AppleWebKit/533.5.7 (KHTML, like Gecko) Version/4.1 Safari/533.5.7"
67.12.243.182 - - [06/Aug/2025:15:40:18 +0000] "POST /login?user=greenwilliam&pass=+2U5ZGcUI6 HTTP/1.1" 301 4200 "Opera/8.68.(Windows NT 10.0; mag-IN) Presto/2.9.170 Version/10.00"
194.217.75.128 - - [06/Aug/2025:15:40:21 +0000] "POST /transfer HTTP/1.1" 404 3139 "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5; rv:1.9.2.20) Gecko/2494-10-16 09:23:33 Firefox/3.8"
107.219.17.214 - - [06/Aug/2025:15:40:29 +0000] "POST /login HTTP/1.1" 404 3006 "Mozilla/5.0 (iPod; U; CPU iPhone OS 3_3 like Mac OS X; ia-FR) AppleWebKit/534.35.4 (KHTML, like Gecko) Versi
200.139.3.192 - - [06/Aug/2025:15:40:35 +0000] "POST /profile HTTP/1.1" 500 4113 "Mozilla/5.0 (Macintosh; PPC Mac OS X 10_7_8 rv:3.0; sv-FI) AppleWebKit/533.37.2 (KHTML, like Gecko) Version
33.5.216.48 - - [06/Aug/2025:15:40:45 +0000] "GET /profile HTTP/1.1" 404 3091 "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_9_7; rv:1.9.4.20) Gecko/8729-01-12 18:55:57 Firefox/3.6.12"
106.222.133.117 - - [06/Aug/2025:15:40:48 +0000] "POST /profile HTTP/1.1" 500 4020 "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 10.0; Trident/3.1)"
164.74.7.236 - - [06/Aug/2025:15:40:50 +0000] "POST /dashboard HTTP/1.1" 301 2787 "Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.01; Trident/3.0)"
111.91.16.242 - - [06/Aug/2025:15:40:51 +0000] "GET /transfer HTTP/1.1" 301 1578 "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 11 9 rv:2.0; lt-LT) AppleWebKit/534.43.7 (KHTML, like Gecko) Ver
```

Secret in the file

1. In the given python code I've changed the file name to my downloaed file name. "trythis.png".
2. And got the flag.

```
from stegano import lsb

# Extract from the image
extracted = lsb.reveal("trythis.png")

print("🔓 Hidden message:", extracted)
```

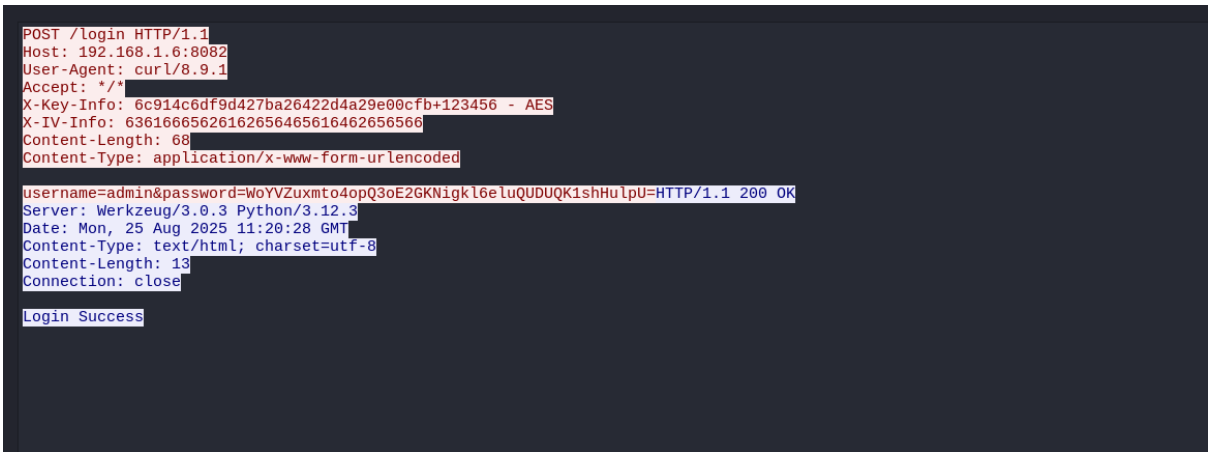
```
E:\download>python Python_Code_Extract.py
🔓 Hidden message: flag{stegano-!*}

E:\download>
```

Pcap Madness

1. I used wireshark to analyse the pcap file.
2. And got the password with AES encrypted.
3. By unhashing the given key and adding 123456, I got the key.

4. And then changed the hex to ascii, and got the IV num.



```
POST /login HTTP/1.1
Host: 192.168.1.6:8082
User-Agent: curl/8.9.1
Accept: */*
X-Key-Info: 6c914c6df9d427ba26422d4a29e00cfb+123456 - AES
X-IV-Info: 6361666562616265646561646256566
Content-Length: 68
Content-Type: application/x-www-form-urlencoded

username=admin&password=WoYVZuxmto4opQ3oE2GKNigkl6eluQUDUQK1shHulpU=HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.12.3
Date: Mon, 25 Aug 2025 11:20:28 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 13
Connection: close

Login Success
```

AES Encrypted Text

WoYVZuxmto4opQ3oE2GKNigkl6eluQUDUQK1shHulpU=

Select Cipher Mode of Decryption

CBC

Select Padding

PKCS5Padding

Enter IV Used During Encryption(Optional)

cafebabedeadbeef

Key Size in Bits

128

Enter Secret Key used for Encryption

dulcemaria123456

Output Text Format (•) Plain-Text ( ) Base64

Decrypt

AES Decrypted Output

{wEaK_3nC_w34K_H45H_Xi08JK}

Stop watch

```
┌──(kali㉿kali)-[~/codefest25/IOS/StopWatch.app]
└─$ strings SLIIT_CTFStopWatch | grep "{*}"
h"}9ab6
Rj}`
STOPWATCH_CTF{A1F9-3D7B-92CE-44E0}
}#;#d
3s}bm
$}Lsc
`7}h
+:zD}O
```

```
┌──(kali㉿kali)-[~/codefest25/IOS]
└─$ unzip SLIIT_CTFStopwatch.ipa
Archive:  SLIIT_CTFStopwatch.ipa
   creating: StopWatch.app/
   creating: StopWatch.app/_CodeSignature/
  inflating: StopWatch.app/_CodeSignature/CodeResources
  inflating: StopWatch.app/SLIIT_CTFStopWatch
  inflating: StopWatch.app/Info.plist
 extracting: StopWatch.app/PkgInfo
```