

*Security is everywhere*[Home](#) [Linux](#) [News](#) [Security](#) [About](#) 

## FOLLOW:


SECURITY &gt; WRITEUPS

 OLDER  
FIT-HACK CTF 2017 - Write-ups

## RECENTS

[SECURITY](#) > [WRITEUPS](#)  
YUBITSEC CTF 2017 - WRITE-UPS  
TUESDAY 25 APRIL 2017 (2017-04-25)[SECURITY](#) > [WRITEUPS](#)  
FIT-HACK CTF 2017 - WRITE-UPS  
SATURDAY 15 APRIL 2017 (2017-04-15)[SECURITY](#) > [WRITEUPS](#)  
EGYPT & UAE NATIONAL CYBER  
SECURITY CTF QUALS 2017 -  
WRITE-UPS  
MONDAY 10 APRIL 2017 (2017-04-10)[SECURITY](#) > [WRITEUPS](#)  
ASIS CTF QUALS 2017 - WRITE-UPS  
MONDAY 10 APRIL 2017 (2017-04-10)[SECURITY](#) > [WRITEUPS](#)  
INS'HACK 2017 - WRITE-UPS  
MONDAY 10 APRIL 2017 (2017-04-10)

# YUBITSEC CTF 2017 - Write-ups

TUESDAY 25 APRIL 2017 (2017-04-25)  
 #CRYPTO #CTF #FORENSICS #MISC  
#SECURITY #STEGANO #WEB  
#WRITEUPS

## Informations

### Version

By	Version	Comment
noraj	1.0	Creation

### CTF

- **Name** : YUBITSEC CTF 2017
- **Website** : [ctf.yubitsec.org](http://ctf.yubitsec.org)
- **Type** : Online
- **Format** : Jeopardy
- **CTF Time** : [link](#)

## 1 - Flag Format - Warmup

## CATEGORIES

- linux (30)
  - archlinux (8)
  - debian (1)
  - opensuse (7)
  - ubuntu (1)

---

- misc (4)

---

- news (7)
  - security (4)
  - warez (1)

---

- programming (3)
  - python (2)
  - ruby (1)

---

- security (118)
  - centos (2)
  - windows (4)
  - writeups (106)

---

- windows (3)

---

## TAG CLOUD

anonymity apache archlinux backdoor bsd  
 centos **crypto** **ctf** debian firefox **forensics**  
 git graphic guessing hyper-v install joy kvm lfi  
**linux** misc netbios network news  
 opensuse pentest php piracy privacy  
 programming proxy pwn python qemu recon  
 reverse reversing ruby **security** ssh stegano  
**system** tor trivia ubuntu update usenet  
 virtualbox virtualization vulnerability warez  
**web** webshell windows **writeups**



*Hello, Welcome to YUBITSEC CTF!*

*We hope you will have a good time.*

*Flag Format is;*

*YUBITSEC{}*

## 5 - Bash - Warmup



*BFYRGHVX{ZGYZHS\_MLG\_DL*

*Bash for **ATBASH**.*

*YUBITSEC{ATBASH\_NOT\_WELCOME\_HERE*

## 10 - A fine cipher - Warmup



*a:9*

*b:13*

*Encrypted:*

*VLWHCTXF{N\_GHAX\_FHSYXk*

*A fine cipher for **Affine cipher**.*

*YUBITSEC{A\_FINE\_CIPHER}*

## 10 - Rome - Warmup

## ARCHIVES

- ▶ April 2017 (7)
- ▶ March 2017 (7)
- ▶ February 2017 (8)
- ▶ January 2017 (2)
- ▶ December 2016 (12)
- ▶ November 2016 (28)
- ▶ October 2016 (4)
- ▶ September 2016 (11)
- ▶ August 2016 (26)
- ▶ July 2016 (26)
- ▶ June 2016 (6)
- ▶ May 2016 (5)
- ▶ April 2016 (8)
- ▶ March 2016 (2)
- ▶ December 2015 (2)
- ▶ October 2015 (1)
- ▶ September 2015 (1)
- ▶ November 2014 (1)
- ▶ October 2014 (1)
- ▶ September 2014 (1)
- ▶ August 2014 (5)
- ▶ December 2012 (1)

## LINKS



*Encrypted:*

*PLSZKJVT{TRVJRI\_WFLEU\_KY*

*Rome for Caesar.*

*YUBITSEC{CAESAR\_FOUND\_THIS\_ACTU/*

## 10 - Telegram - Warmup



*Join our telegram group to get the flag*

*<https://t.me/joinchat/AAAAAEtLHCynDnIjg>*

*YUBITSEC{Abi\_n4sil\_uy3\_0luy0ruz:*

## 5 - Disambiguation - Trivia



*A well known bug in OpenSSL cryptography library.*

*There is no flag format, enter the answer in lowercase.*

*heartbleed*

## 10 - Execution - Trivia



*A well known privilege escalation vulnerability.*

▸ Hexo

---

▸ FOSS

---

▸ Torrent is not a crime

---

*There is no flag format, enter the answer in lowercase.*

shellshock

## 10 - Talk dirty to me - Trivia

“ A linux kernel bug that has been around for at least 11 years.

*There is no flag format, enter the answer in lowercase.*

dirtycow

## 10 - Ümit Besen - Trivia

“ A well known computer worm that spreads with emails.

*There is no flag format, enter the answer in "uppercase".*

ILOVEYOU

## 15 - Global Surveillance - Trivia

“ Intercept the communications!

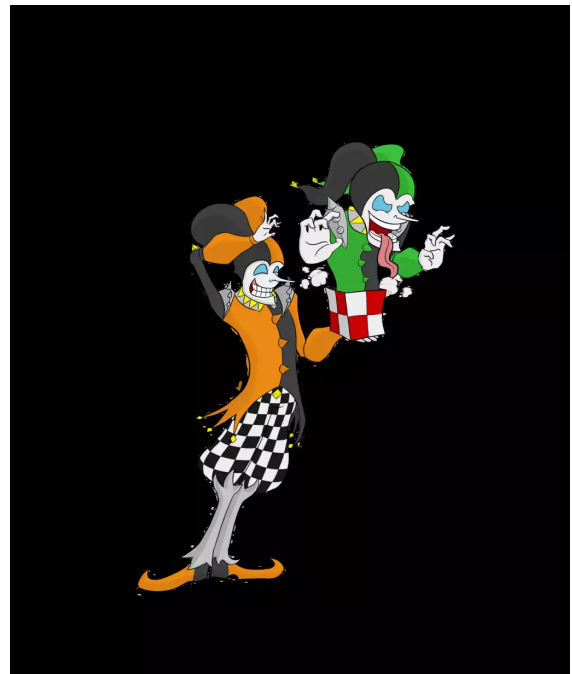
*There is no flag format, enter the answer in lowercase.*

echelon

## 150 - Text into image - Steganography

“ Shaco is hiding something!

*lsb.png*



Orga did a mistake, this is not a LSB challenge, name of the challenge was changed.

Pure guessing. I simply wrote **steganography Text into image** into google and used the first online tool:

<http://manytools.org/hacker-tools/steganography-encode-text-into-image/>

Flag is **YUBITSEC{now\_you\_see\_me}** .

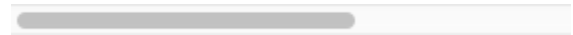
## 30 - Robots Are Cool 1 - Web

“ *I think robots are cool. What you think?* ”

*http://138.197.41.168/fiuuu/robots.txt*

Considering the title, I tried to access the `robots.txt` :

```
1 $ curl http://138.197.41.168/fiuuu/robots.txt
2 User-agent: *
3 Disallow: /pewpewpew.html
4
5 YUBITSEC{c0me_w1th_m3_If_y0u_w4r3}
```



PS:

*http://138.197.41.168/fiuuu/pewpewpew.html*  
also contains the flag.

Flag is

*YUBITSEC{c0me\_w1th\_m3\_If\_y0u\_w4r3}*

## 75 - Simple Sql Injection - Web

“ *http://138.197.41.168/ctf3/login* ”

I tried the following payload:

- Login: `admin`
- Password: `' or 1-- -'`

I succesfully bypassed the authentication and got redirected to <http://138.197.41.168/ctf3/fl0g.html>.

```
1  <!DOCTYPE html>
2  <html>
3  <head>
4      <title>fl0g</title>
5  </head>
6  <body>
7  <p>FLAG IS AROUND HERE SOME
8  </body>
9  </html>
10
11  <!--YUBITSEC{w0w_such_h4ck}
```

## 175 - Coming Soon!! - Web

“ Hello I am Zafer. Beşir puts Izzettin in to a coma and I need help to get Avatar 2 DVD. Can you help me to get it?

<http://138.197.41.168/ctf1/log>

Note: For none Turkish players; if you have any issue with language contact hatMadder on irc

hint: take carefull look at names ;)

I tried the following payload:

- Login: `admin`
- Password: `' or 1-- -'`

I successfully bypassed the authentication and got redirected to <http://138.197.41.168/ctf1/avatar.html>

There is some links:

```
1  Avatar 2
2  Avatar 2 720p Full izle Türk
3  Avatar 2 720p Full izle Türk
4  Avatar 2 720p Full izle Türk
5  Avatar 2 720p Full izle Türk
6  Avatar 2 720p Full izle Türk
7  Avatar 2 720p Full izle Türk
```

They looks to be a base64 image splitted into 6 parts.

[illegible]

So I extracted the base64 parts manually and save them into a file. And then retrieve the image:

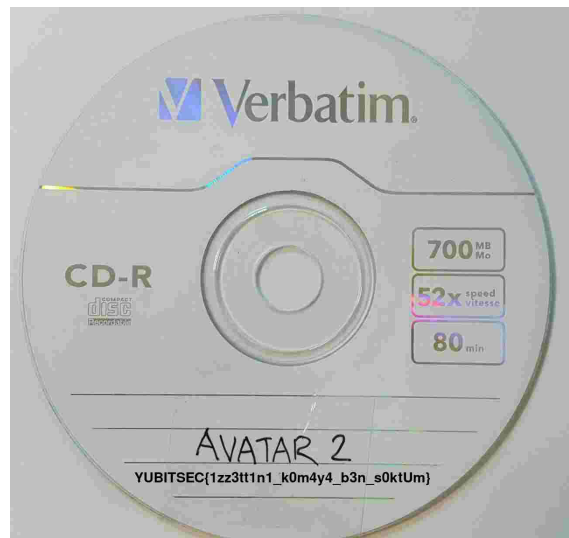
```
1 $ cat test.txt| tr -d '\n'
```

```
2
```

```
3 $ file image
```

```
4 image: JPEG image data, JFIF
```





And then I can see a AVATAR 2 CD  
RIP with

`YUBITSEC{1zz3tt1n1_k0m4y4_b3n_s0ktUm}`

## 50 - Location - OSINT

“ Can you find location ?

*We are looking for city name ?*

*All chars are lowercase and  
close.*

*Flag format:  
YUBITSEC{losangeles}*

*location.jpg*



We are looking for GPS metadata:

```
1 $ exiftool location.jpg | g
```

- 2 GPS Version ID
- 3 GPS Latitude Ref
- 4 GPS Longitude Ref
- 5 GPS Altitude Ref
- 6 GPS Altitude
- 7 GPS Latitude
- 8 GPS Longitude
- 9 GPS Position

I used [indlatitudeandlongitude.com](http://indlatitudeandlongitude.com) (again) to get the location: *Ameghino 400-466, Z9400JEJ Río Gallegos, Santa Cruz, Argentina.*

Flag is `YUBITSEC{riogallegos}` .

**Note:** it's more forensics than OSINT

## 75 - Mobile Number - OSINT

“ *Who took this photo ?*

*Can you find photographer's mobile number ?*

*Show me, How stalker are you!*

*Note: Flag format will be YUBITSEC{+1234567890}*

This time no metadata.

I made a reverse image search with Google image (uploading the picture),

and I found that this picture was taken by *Isaac Kasamani*.

I see his Facebook but nothing there, so I went to **his blog** and found his phone number: **+256 (0) 752166288** .

Flag is **YUBITSEC{+2560752166288}** .

## 15 - Social Media - OSINT

Nothing on Twitter.

Facebook or Instagram profile are not referenced nor with normal search engine search nor with dorks like **yubitsec inurl:instagram.com** .

I looked that there is no local/national Turkish social media.

So I asked an admin that redirect me to instagram.

But there is nothing referenced.

So I surfed on StackExchange and found a topic: **I don't have an Instagram account. Can I still look at users' Instagram photos?** .

The answer was to go to

[instagram.com/profile\\_name](https://www.instagram.com/profile_name) . I

looked for yubitsec and found

<https://www.instagram.com/yubitsec>

There is 1 picture, a QR code.



The original picture may be still available on the [CDN](#).

So I used <https://webqr.com/> (drag'n'drop) and found:

`YUBITSEC{W3LC0M3}` .

This is not really open source information or publicly available data so we can't really talk about OSINT. But you know CTF organizers often don't care to make challenge about true security, well categorize them or even ban guessing.

## 25 - Find me - Misc



*Find me in source code.*

Let's try [yubitssec.org](https://yubitssec.org) :

\_\_\_\_\_

## 25 - Strings - Misc

Strings.jpg



13/19

```
1 $ strings Strings.jpg | tai
2 YUBITSEC{H4CK3R_M4N35}
```

## 35 - Weird symbols - Misc

“ *What is this?*

*weird\_txt*

That is some JavaScript Brainfuck (not original Brainfuck).

You can eval some part in a javascript console, for example `!+[]+!+[]+[]+[]` equal `20` .

So I pasted all into an `eval()` and waited until I got a pop-up with `YUBITSEC{WEIRD_JAVASCRIPT_IS_WEIRD}`

## 35 - B64 - Misc

“ *File.txt*

I remove the `b'base64'` around the base64 data and then:

```
1 $ cat file.txt | base64 -di
```

But it seems very recursive.

So I used and adapted a recursive command:

```
1 $ str=`cat file.txt`; for i
```

YUBITSEC{YUBITSEC{YUBITSEC{YUBIT

## 50 - File - Forensics



*Challenge's link*

*[https://drive.google.com/open?id=0B\\_jBF\\_ZqfxnBd0tKcDJMv](https://drive.google.com/open?id=0B_jBF_ZqfxnBd0tKcDJMv)*

*What is this file ? Can you find hidden flag ?*

*Flag format: YUBITSEC{}*

```
1 $ binwalk File
2
3  DECIMAL          HEXADECIMAL
4  -----
5  30               0x1E
6  11905348         0xB5A944
7  11905370         0xB5A95A
8  11925801         0xB5F929
9
10
11 $ unzip File -d here
```

Then there is a lot of recursive zip

File/Flag/op/Hacker/HackerMan/H

At the end we have `flag.png` :  
`{C0MPR3SS10N_1S_G00D}` . So the  
flag is  
`YUBITSEC{C0MPR3SS10N_1S_G00D}` .

## 100 - Easy - Crypto

“ *Seems like there must be  
hiding flag, find it!*

*secret.txt*

This is a list of MD5 hashes.

Crack the hashes with  
<https://crackstation.net/> and a text  
editor *replace all* feature to go faster.

And then:

```
1 $ cat secret.txt | tr -d '\n'
2 MD5?_Hell_Yes!_So_you_know_v
```

## 50 - Gifted - Reverse

“ *gifted*

```
1 $ strings gifted | grep -i y
2 YUBITSEC{MEH_IT_IS_SOMETHING}
```



## 50 - \*blushes\* - Steganography

“ *indir.png*

The image looks transparent and has no metadata.



But *blushes* means *get red*. So using StegSolve, for example, we can see a QR code in red planes:



Then I used <https://webqr.com/> to get the flag:

`YUBITSEC{hello_nothing_here}` .

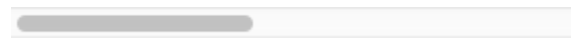
## 75 - Broken - Forensics



*HINT: Compare with normal PNGs. You need to add something? **broken.png***

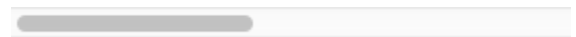
Let's check a correct PNG:

```
1 $ xxd -l50 indir.png
2 00000000: 8950 4e47 0d0a 1a00
3 00000010: 0000 00c8 0000 0000
4 00000020: 9e00 0000 0662 4b00
5 00000030: bda7
```



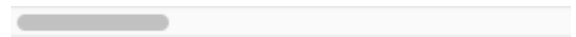
And now the broken one:

```
1 $ xxd -l50 broken.png
2 00000000: 0000 0226 0000 0200
3 00000010: 4600 0000 0662 4b00
4 00000020: bda7 9300 0000 0900
5 00000030: 0000
```



We can see the broken file lack the first *line* with the header (*magic number*) + the first PNG chunk, let's fix this:

```
1 $ printf "\x89\x50\x4e\x47\;
```




Now we have a valid PNG and we can read:

**YUBITSEC{m4g1c\_num3rs\_4r3\_c00l}**

[↪ Share](#)[Comments](#)[Community](#)[Login](#) ▼

1

 [Recommend](#) [Share](#)[Sort by Best](#) ▼

Start the discussion...

Be the first to comment.

---

© 2017 Alexandre ZANNI

Powered by Hexo. Theme by PPOffice