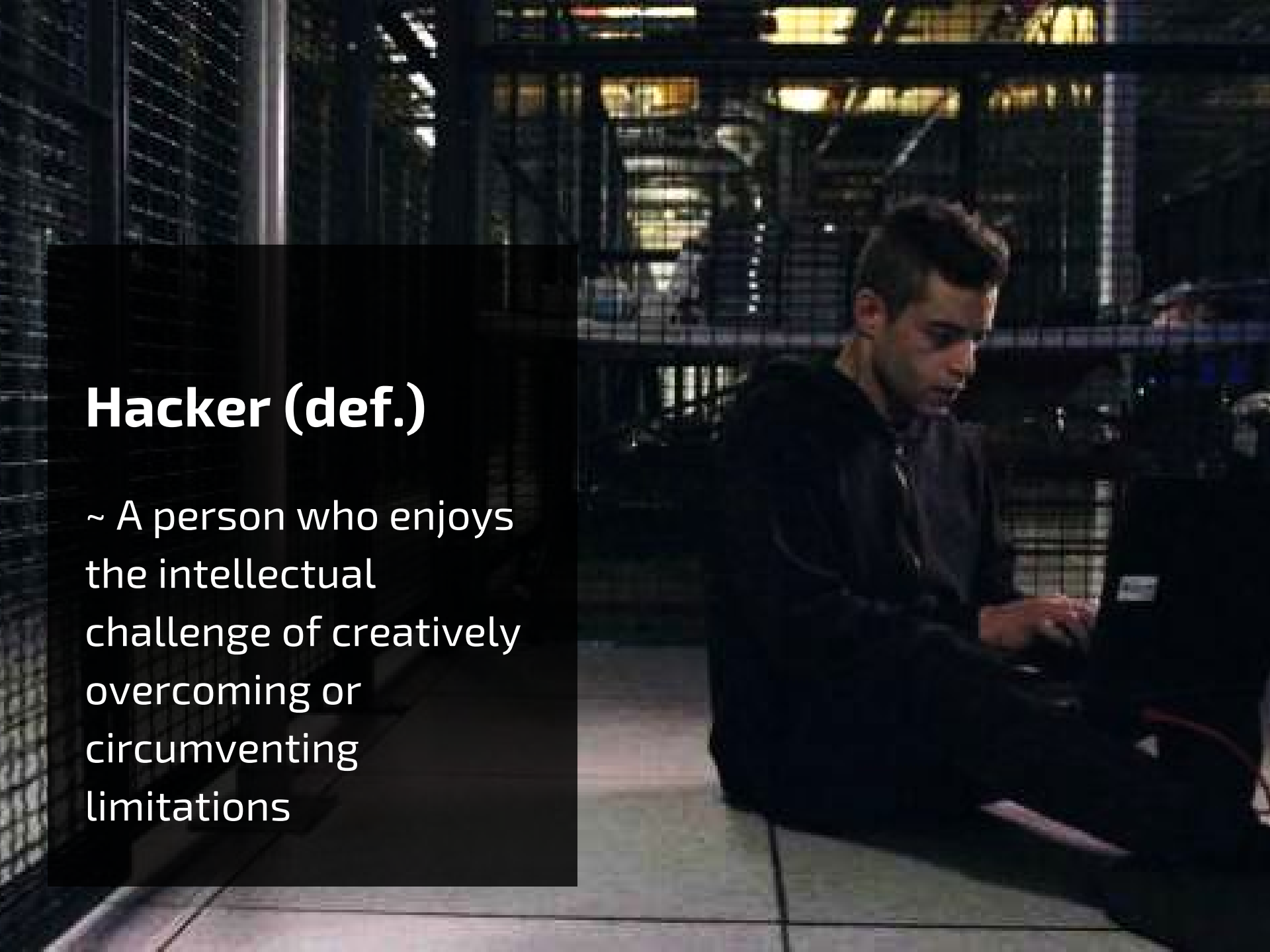

Security Capture the Flag
Enrico Bacis - Università degli Studi di Bergamo



Hacker (def.)

~ A person who enjoys the intellectual challenge of creatively overcoming or circumventing limitations

Cosa è una CTF?

"*gioco*" orientato alla **sicurezza informatica**

si prova a rompere dei sistemi (finti)
"*per divertimento*" e **per imparare**

L'obiettivo è **catturare delle flags**

FLAG{THi5_iS_4_f1aG}

Perché?

- **Divertimento**

- Maturare **esperienza** in Information Security
- Sfide modellate sulla base di **problemi reali**
  - A volte problemi reali modellati sulla base delle CTF?

- **Reputazione** (a volte)

Online o sul posto

Come?

Jeopardy

Attack - Defense

Tipi di challenges

cryptography

reverse engineering

binary exploitation

web application

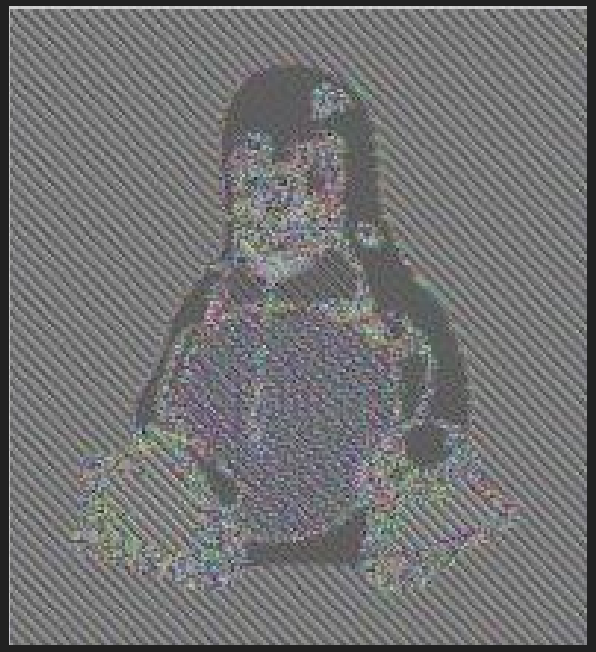
stego / forensics

... e altri

team forti hanno generalmente skills e esperienza in tutte queste aree

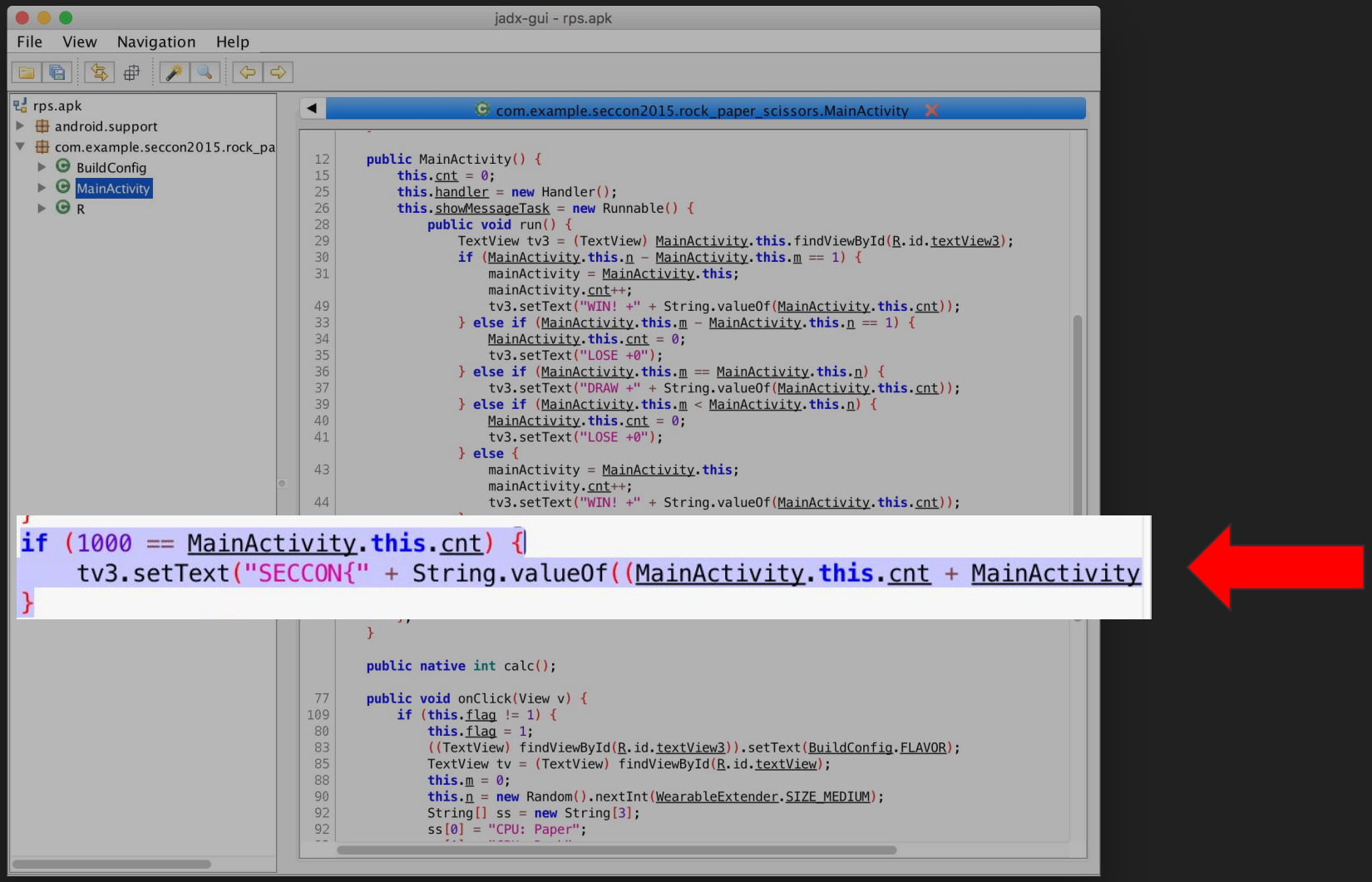
Cryptography

Tux

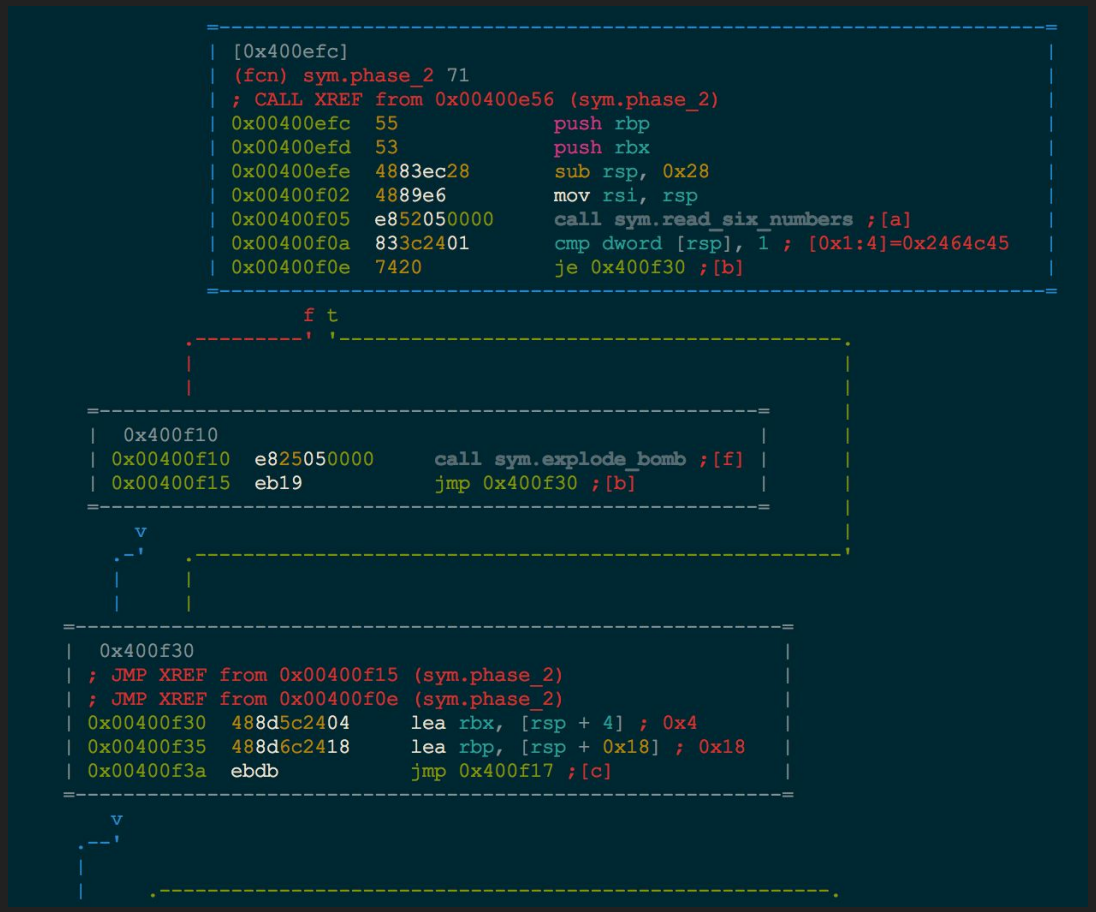


Tux cifrato (male)

Reverse Engineering



Binary Exploitation (pwn)



Exploits:

- Buffer overflow
- String format exploit
- ....

reverse

⬇

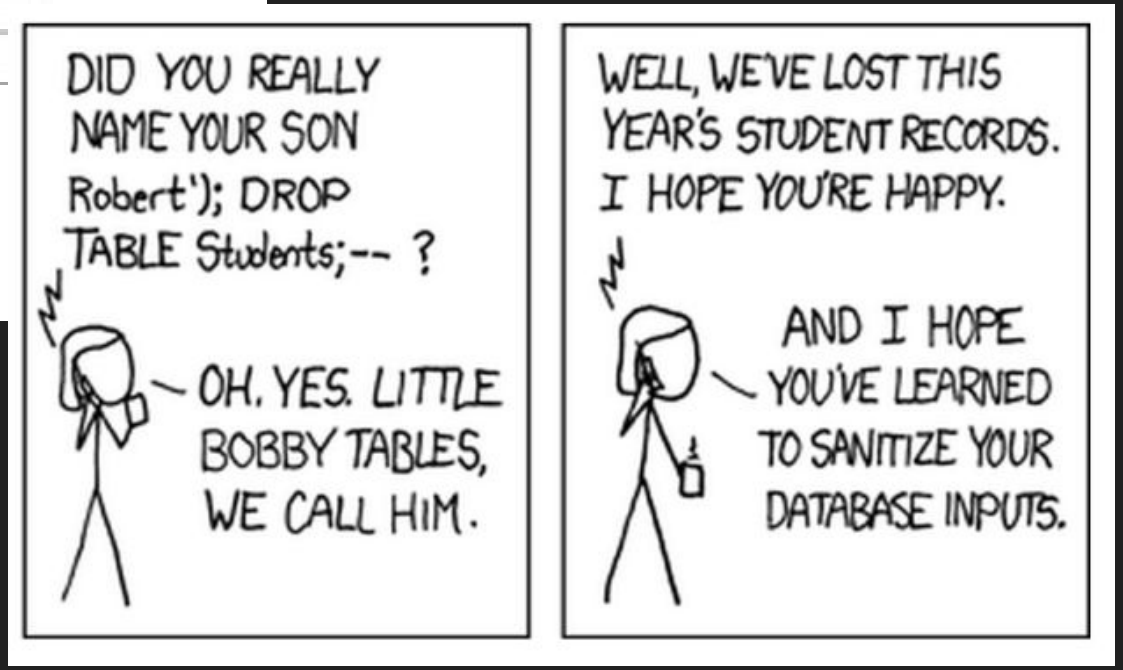
analyse

⬇

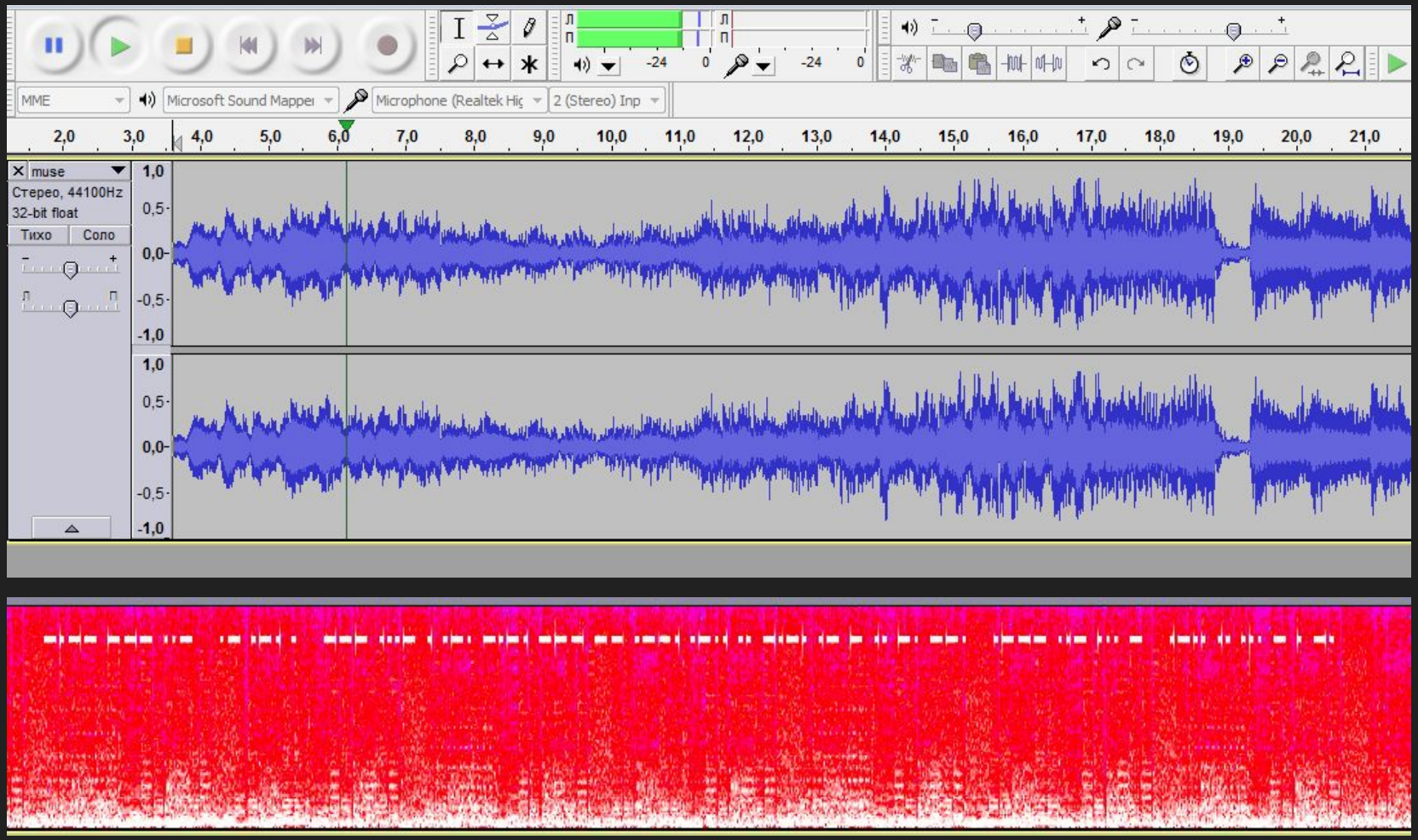
exploit

Web application security

- SQL injection
- Cross Site Scripting
- Local File Inclusion
- ...



Steganography



Forensics


X
ITALIAN SPIES LOST A FILE
250 Points
HEY THESE ARE THE BEST ITALIAN SPIES TALKING. WE SENT OUR COLLEGUE TO DO A LITTLE JOB, HE SHOULD STOLE A SECRET CODE FROM A BAD GUY. BUT THE BAD GUY STILL DOESN'T HAVE A COMPUTER! -> !!!THAT'S CRAZY!!! INSTEAD, HE HAS A VERY GOOD STYLOGRAPHIC PEN. BUT OUR COLLEGUE WAS SO SMART THAT HE DID IT! HE STOLE THE SECRET FROM THAT BAD GUY! HE TOLD US "HEY GUYS, I STOLE THAT!" AAANDDD... WE KILLED HIM BECAUSE HE KNOWS TOO MUCH AHAHAHAHAHAHAHAHAHAHAHAH! NOW WE CAN'T FIGURE OUT HOW TO OPEN THE FILE THAT HE SENT US. PLZ HELP US :)
Download

Forensics

```
$ cat italian-spies-lost-a-file
```

Forensics

```
In [1]: import struct

In [2]: data = open('italian-spies-lost-a-file').read()

In [3]: data[:48]
Out[3]: '\x00\x00\x00\x00k\xa3\xbe\xc0\xa0\xccK\xc2y"\x1dA\x14\x00\x00\x00\x
ae\xbdI@\x96\x8e\x00B\xe9c\x1fA(\x00\x00\x00v<->;0L@\x99\xe1\x1cA'

In [4]: struct.unpack('f'*12, data[:48])
Out[4]:
(0.0,
 -5.957448482513428,
 -50.9498291015625,
 9.820916175842285,
 2.8025969286496 34e-44,
 3.1522021293640137,
 32.1392440795898 44,
 9.961892127990723,
 5.6051938572992 68e-44,
 0.1691759526729 5837,
 3.190443754196167,
 9.80507755279541)
```

g?

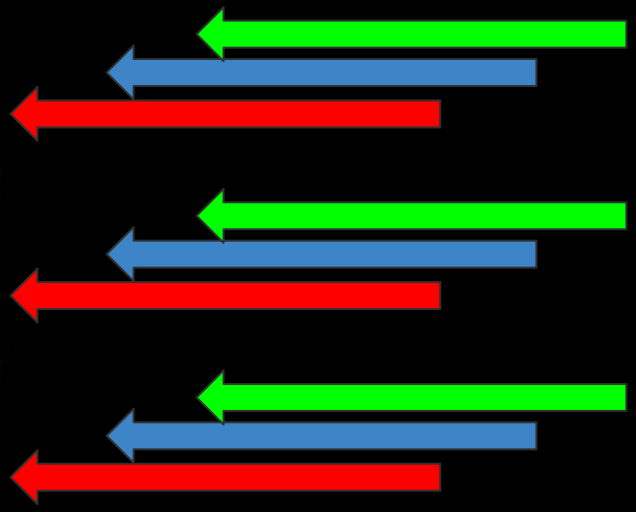
Forensics

```
In [1]: import struct

In [2]: data = open('italian-spies-lost-a-file').read()

In [3]: data[:48]
Out[3]: '\x00\x00\x00\x00k\xa3\xbe\xc0\xa0\xccK\xc2y"\x1dA\x14\x00\x00\x00\x
ae\xbdI@\x96\x8e\x00B\xe9c\x1fA(\x00\x00\x00v<->;0L@\x99\xe1\x1cA'

In [4]: struct.unpack('f'*12, data[:48])
Out[4]:
(0.0,
 -5.957448482513428,
 -50.9498291015625,
 9.820916175842285,
 2.8025969286496 34e-44,
 3.1522021293640137,
 32.1392440795898 44,
 9.961892127990723,
 5.6051938572992 68e-44,
 0.1691759526729 5837,
 3.1904437541961 67,
 9.8050775527954 1)
```

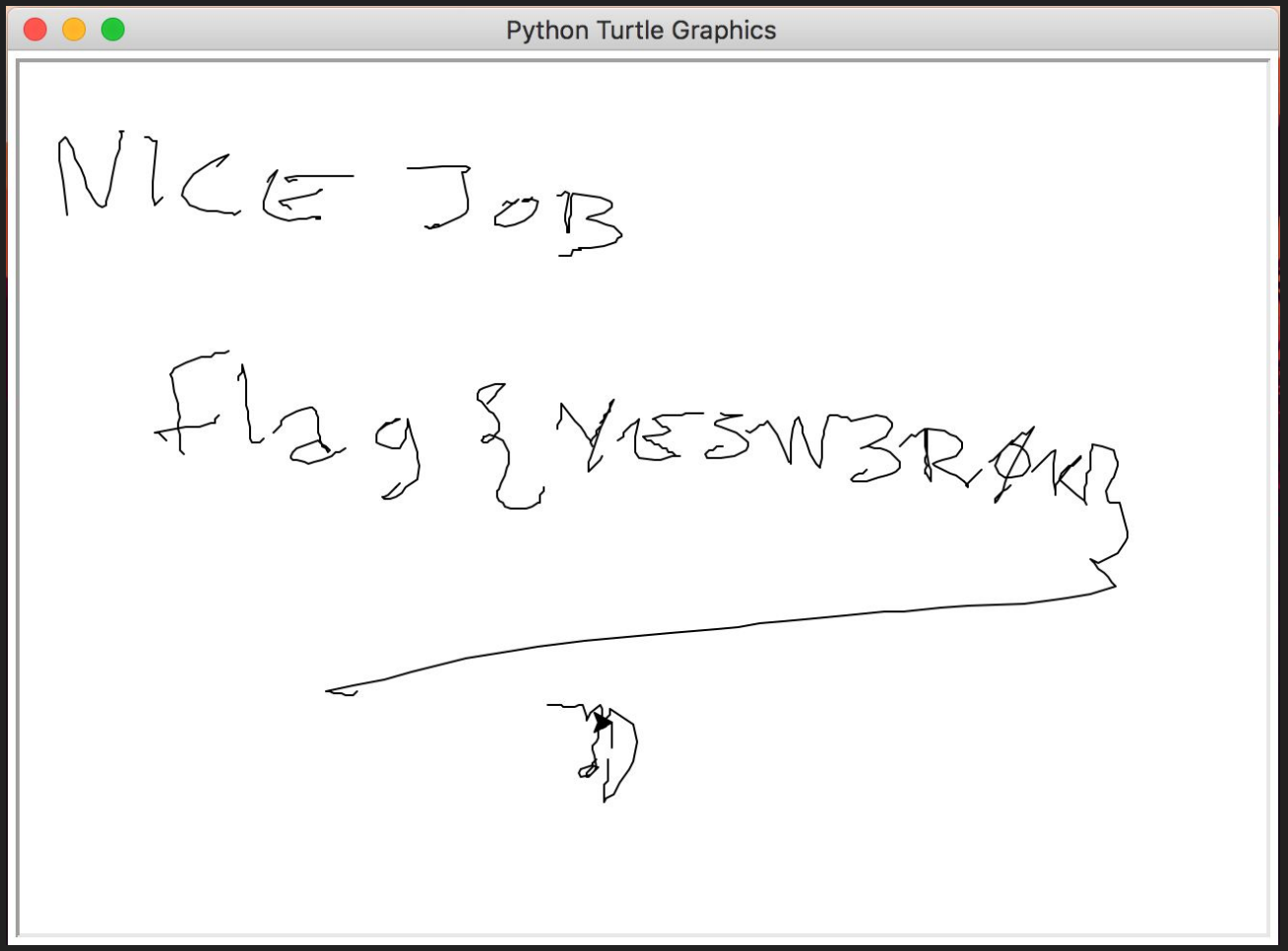


X

Y

Z

Forensics

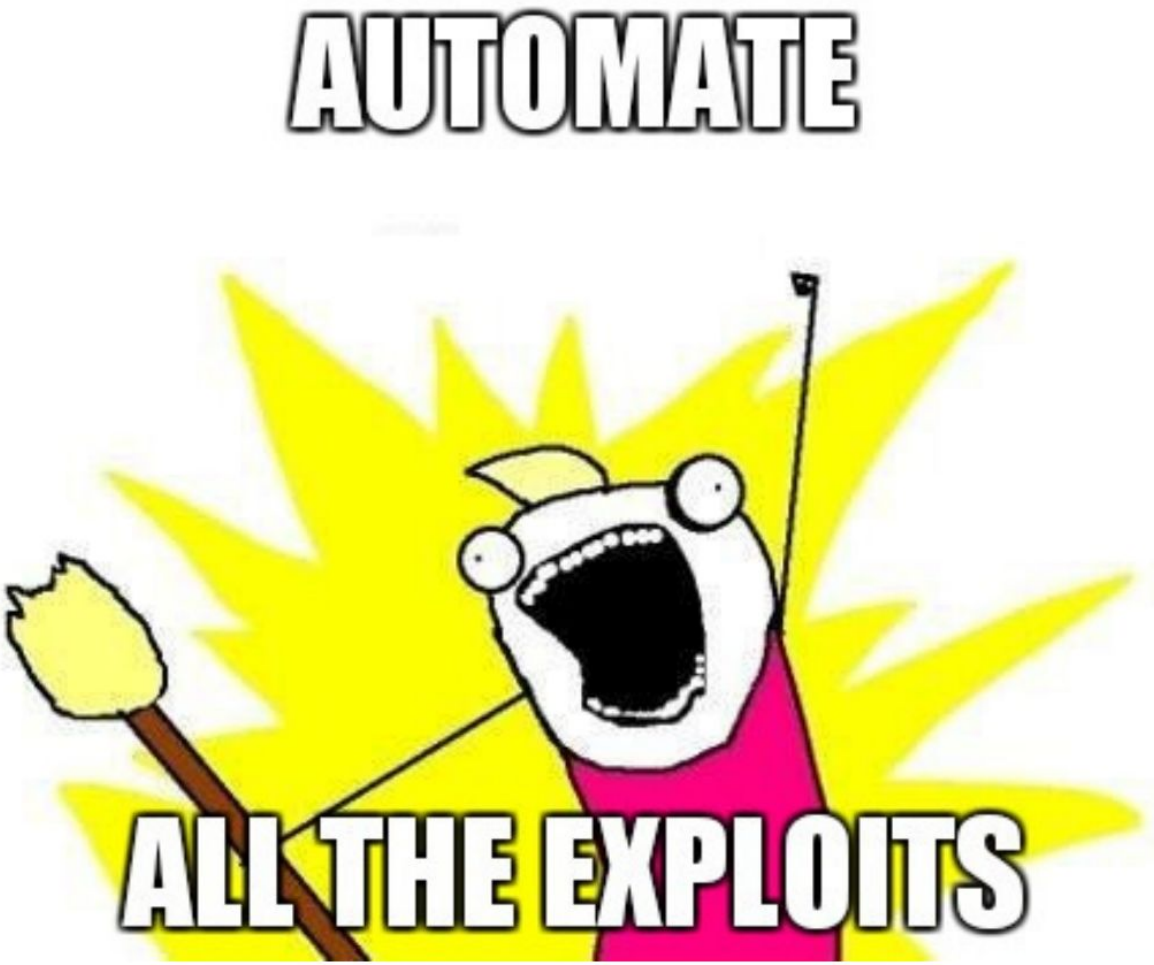


Good challenges = fun

- No **guessing**
  - Non si deve tirare ad indovinare
- No **bruteforcing**
  - sfida le persone, non i loro processori
- No **standard challenges**
  - Google non deve saper risolvere le challenges
- Se ha il formato di una flag e sembra una flag, **è una flag**!

Gli scripts sono tuoi amici

- Sii a tuo agio ad automatizzare
- Usa lo strumento più comodo:
  - Bash, zsh, ...
  - **Python**



Livello automazione: **OVER 9000!**

command-line-fu

- GNU/Linux utilities: `grep, sed, awk, sort, cut, uniq`
- Network utilities: `nc, dig, nmap`
- HTTP: `curl, wget`
- `...`

Usa le UNIX pipes
per concatenare
i comandi tra loro

È solo un gioco?

- **Google**
  - CTF https://capturetheflag.withgoogle.com
- **Facebook**
  - Piattaforma per CTF open source https://github.com/facebook/fbctf
- **Stripe**
  - CTF su web application security e sistemi distribuiti
- MOLTI altri

“ a fool with a tool is still a fool ”

CTF Time (prossimi eventi)

Upcoming events

Format	Name	Date	Duration
	Hack.lu CTF 2016 On-line	Wed, Oct. 19, 10:00 — Thu, Oct. 20, 10:00 UTC 82 teams	1d 0h
	EKOPARTY CTF 2016 On-line	Thu, Oct. 27, 01:00 — Sat, Oct. 29, 01:00 UTC 55 teams	2d 0h
	Hack The Vote 2016 On-line	Fri, Nov. 04, 23:00 — Sun, Nov. 06, 23:00 UTC 52 teams	2d 0h

https://ctftime.org/event/list/upcoming

CTF Time（write-ups）

New writeups

Team	Event	Task	Action
pony7	Hackover CTF 2016	are_you_serialz [22]	read writeup
CInsects	TUM CTF 2016	hiecss [150]	read writeup
CInsects	TUM CTF 2016	zwiebel [50]	read writeup
GoN	HITCON CTF 2016 Quals	ROP [250]	read writeup
NUSGreyhats	CSAW CTF Qualification Round 2016	Warmup [50]	read writeup
Bits For Everyone	HITCON CTF 2016 Quals	Flame [150]	read writeup
NUSGreyhats	HITCON CTF 2016 Quals	Beelzemon [150]	read writeup
PiggyBird	HITCON CTF 2016 Quals	Angry Seam [500]	read writeup
GNUConn	UConn CyberSEED 2016	Missing Flag #2 [300]	read writeup
GNUConn	UConn CyberSEED 2016	Missing Flag #1 [100]	read writeup

https://ctftime.org/writeups

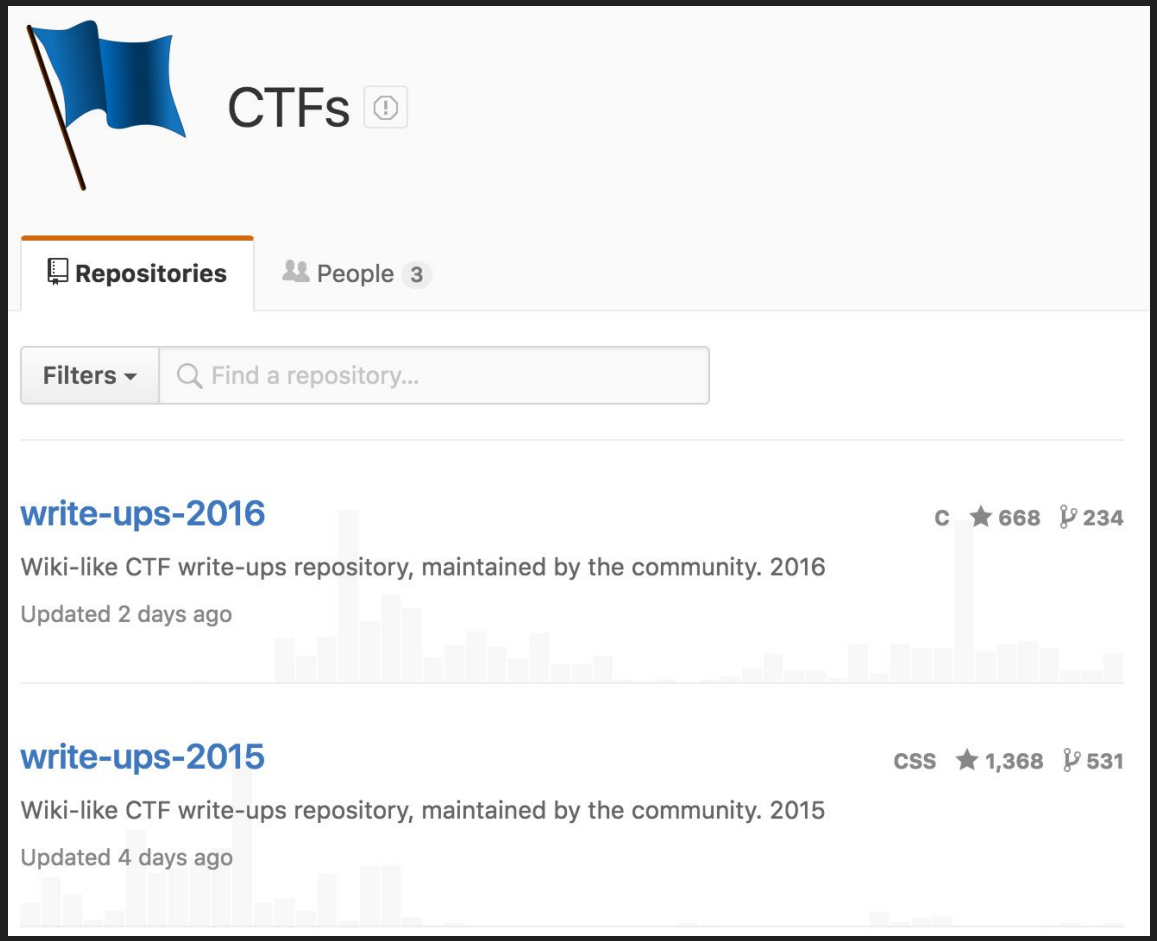
CTF Time (classifica)

2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	dcua		1231.332
2	Plaid Parliament of Pwning		1048.410
3	Dragon Sector		869.926
4	p4		848.341
5	217		846.303
6	LC↯BC		840.375
7	Tasteless		720.011
8	Shellphish		641.266
9	TokyoWesterns		572.156
10	Bushwhackers		472.713

https://ctftime.org/stats

GitHub - CTF Write-ups



https://github.com/ctfs

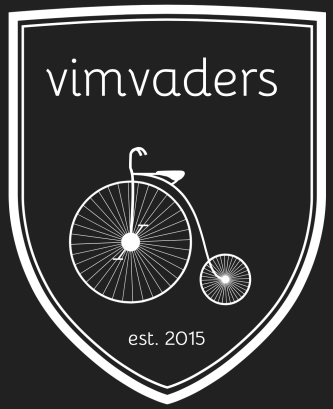
vimvaders: unibg-seclab CTF team

- Gruppo di persone interessate a temi di sicurezza informatica

- Principalmente studenti/ricercatori **UniBG**
  - ma siamo aperti a proposte esterne
  - magari anche tu!

vimvaders: http://vimvaders.github.io

UniBG seclab: http://seclab.unibg.it



domande ?


UNIVERSITATIS
STUDIUM
BERGOMENSIS


Unibg Seclab


vimvaders
est. 2015