



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?

HOME SCOREBOARD CONTEST LOGOUT RULES CONTACT

FLAG: PointsUp

#98 0/150pts	LOL 0/50pts	Crunch 0/250pts	Hidden01 0/30pts	Hidden02 0/250pts	Noelular 0/200pts
dafuq? 0/50pts	AudioMixing 0/100pts	Pair 0/150pts	mentOrpun 0/400pts	T08 0/600pts	invisible 0/150pts
rendeeuous 0/150pts	WTF 0/500pts	Geek 0/600pts	smelf 0/200pts	Eduard 0/300pts	old 0/50pts
Cry 0/100pts	IMAFREAK 0/400pts	#95 0/350pts	mentOrpun2 0/450pts	fantastic 75/75pts	#94 250/250pts
#93 350/350pts					

Copyright © 1337-31337 ForbiddenBITS.

Jeopardy



Attack - Defense

Tipi di challenges

cryptography

reverse engineering

binary exploitation

web application

stego / forensics

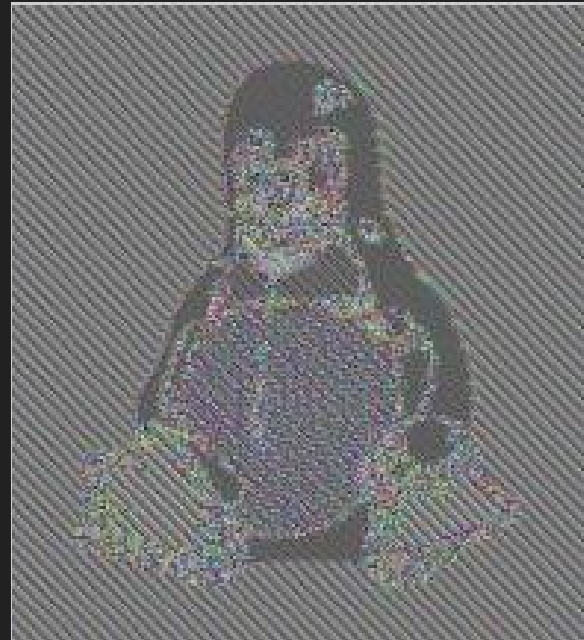
... e altri

team forti hanno
generalmente
skills e
esperienza in
tutte queste
aree

Cryptography

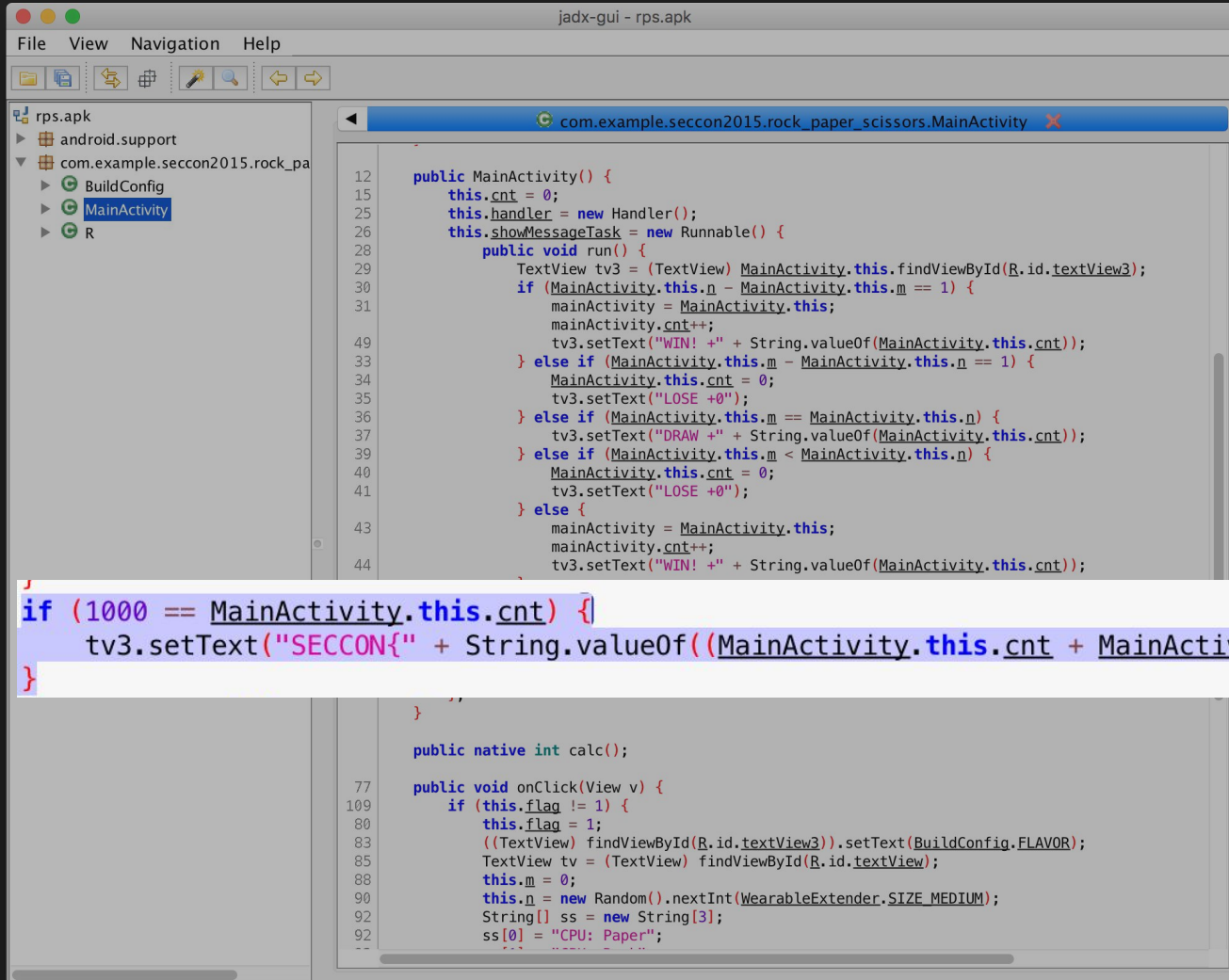


Tux



Tux cifrato (male)

Reverse Engineering




```
jadx-gui - rps.apk
File View Navigation Help
rps.apk
  android.support
  com.example.seccon2015.rock_pa
    BuildConfig
    MainActivity
    R

12 public MainActivity() {
15     this.cnt = 0;
25     this.handler = new Handler();
26     this.showMessageTask = new Runnable() {
28         public void run() {
29             TextView tv3 = (TextView) MainActivity.this.findViewById(R.id.textView3);
30             if (MainActivity.this.n - MainActivity.this.m == 1) {
31                 mainActivity = MainActivity.this;
32                 mainActivity.cnt++;
49                 tv3.setText("WIN! +" + String.valueOf(MainActivity.this.cnt));
33             } else if (MainActivity.this.m - MainActivity.this.n == 1) {
34                 MainActivity.this.cnt = 0;
35                 tv3.setText("LOSE +0");
36             } else if (MainActivity.this.m == MainActivity.this.n) {
37                 tv3.setText("DRAW +" + String.valueOf(MainActivity.this.cnt));
39             } else if (MainActivity.this.m < MainActivity.this.n) {
40                 MainActivity.this.cnt = 0;
41                 tv3.setText("LOSE +0");
43             } else {
44                 mainActivity = MainActivity.this;
45                 mainActivity.cnt++;
46                 tv3.setText("WIN! +" + String.valueOf(MainActivity.this.cnt));
47             }
48         }
49     }
50 }

51 public native int calc();

77 public void onClick(View v) {
109     if (this.flag != 1) {
110         this.flag = 1;
111         ((TextView) findViewById(R.id.textView3)).setText(BuildConfig.FLAVOR);
112         TextView tv = (TextView) findViewById(R.id.textView);
113         this.m = 0;
114         this.n = new Random().nextInt(WearableExtender.SIZE_MEDIUM);
115         String[] ss = new String[3];
116         ss[0] = "CPU: Paper";
117     }
118 }
```

**if (1000 == MainActivity.this.cnt) {
tv3.setText("SECCON{" + String.valueOf((MainActivity.this.cnt + MainActivity**



Binary Exploitation (pwn)

```
[0x400efc]
| (fcn) sym.phase_2 71
| ; CALL XREF from 0x00400e56 (sym.phase_2)
| 0x00400efc 55          push rbp
| 0x00400efd 53          push rbx
| 0x00400efe 4883ec28    sub rsp, 0x28
| 0x00400f02 4889e6      mov rsi, rsp
| 0x00400f05 e852050000  call sym.read_six_numbers ;[a]
| 0x00400f0a 833c2401    cmp dword [rsp], 1 ; [0x1:4]=0x2464c45
| 0x00400f0e 7420        je 0x400f30 ;[b]
```

f t

```
0x400f10
| 0x00400f10 e825050000  call sym.explode_bomb ;[f]
| 0x00400f15 eb19        jmp 0x400f30 ;[b]
```

v

```
0x400f30
| ; JMP XREF from 0x00400f15 (sym.phase_2)
| ; JMP XREF from 0x00400f0e (sym.phase_2)
| 0x00400f30 488d5c2404  lea rbx, [rsp + 4] ; 0x4
| 0x00400f35 488d6c2418  lea rbp, [rsp + 0x18] ; 0x18
| 0x00400f3a ebdb        jmp 0x400f17 ;[c]
```

v

Exploits:

- Buffer overflow
- String format exploit
-

reverse



analyse



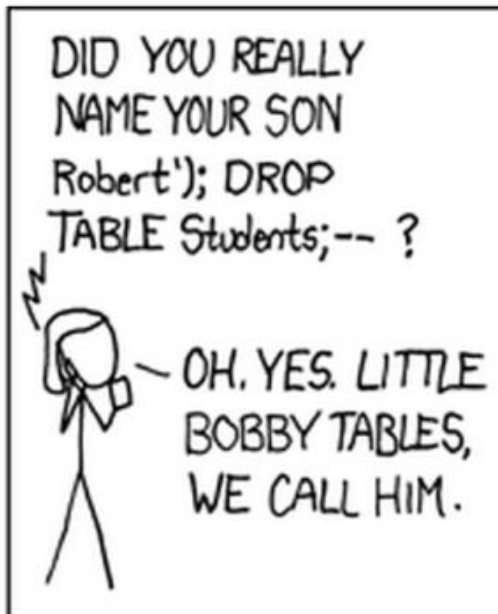
exploit

Web application security

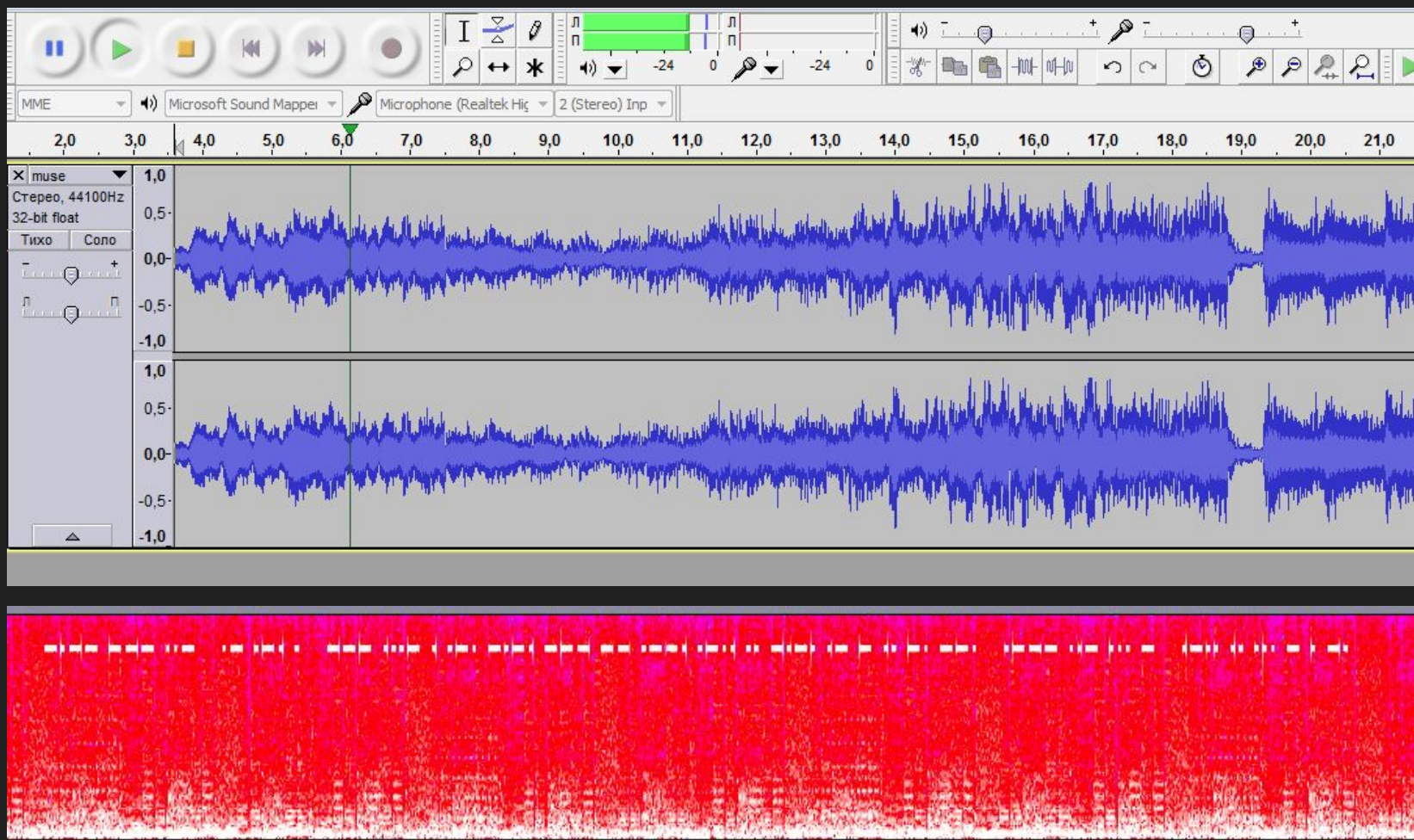
Login Here

Source file : [Here](#)

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



Steganography



Forensics

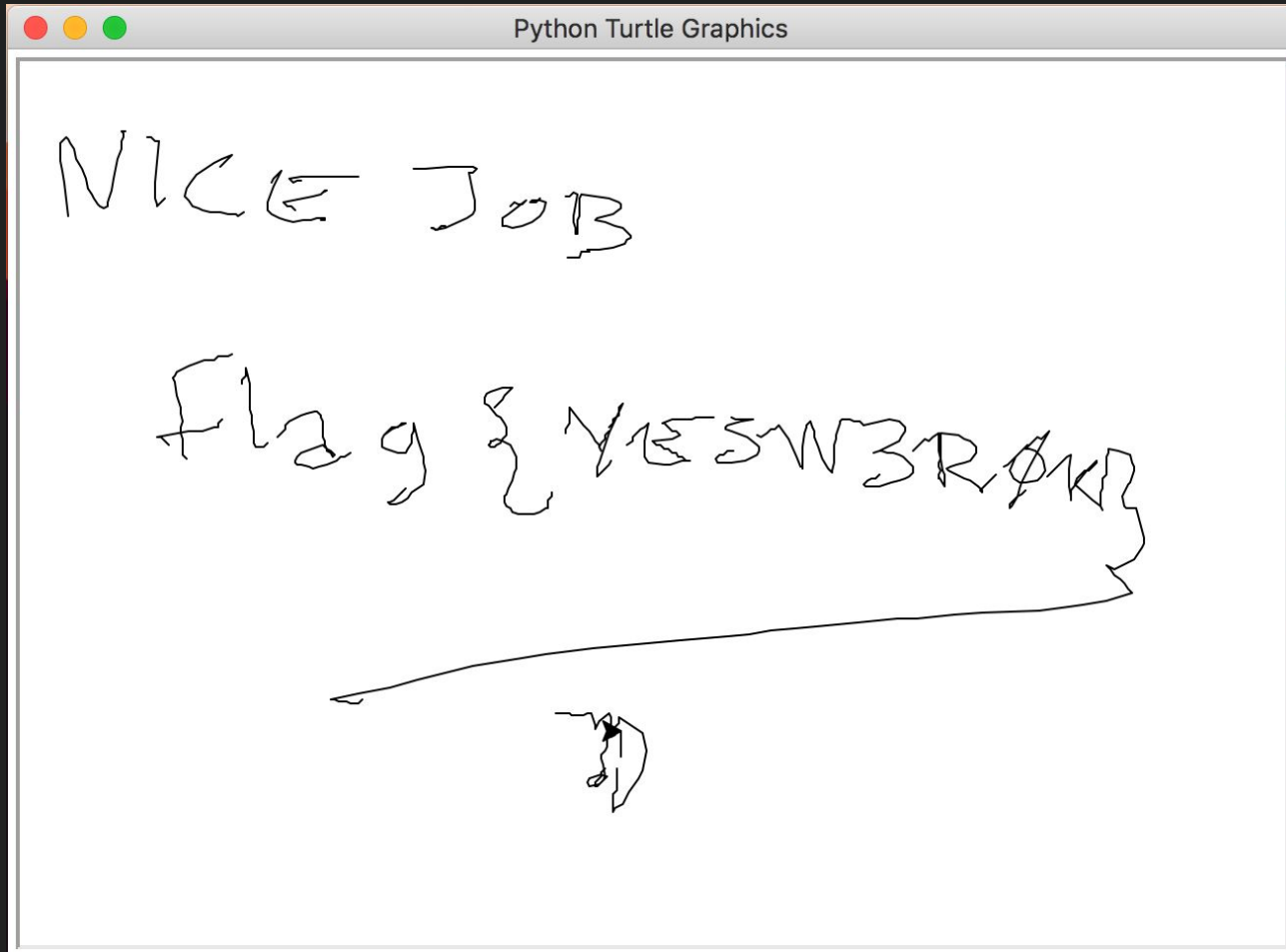


Forensics

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

```
A\¥^[A,^A^@^@é<97><8f>¿©²FÀëû^YA@^A^@^@è<98><80>?7
=À<95>*^]AT^A^@^@éf^H>AP^0>Iº^_Ah^A^@^@¹ é¿9ªuÀå^Y^\A|^A^@^@<93><91>^G@`sj¿
u<9e>À<9d>Y^]Aô^A^@^@à^R<95>?â8^P>^L<9e>^_A^H^B^@^@.Xê¿R<9d>P¿Gc^\A^\^B^@^@
^@í^D^B@9^SA@é^T^]A<94>^B^@^@MâÄ@ot^Q>=^RGA" ^B^@^@ì^S@>^D=4>ÖxZA¼^B^@^@é^Y.
^C^@^@qñ^0>^^e»À<8c>Ý
AH^C^@^@<95>ü<Á»»xB±Â^[A\^C^@^@ªÊ¢@^U<92>;ÁÄè^YAp^C^@^@m±p?À| ÀîX^]A<84>^C^@
v³RAü^C^@^@Mcö=z;½ÀºcXA^P^D^@^@B<9b>$½Ïñ<8c>¼Ïk]A$^D^@^@,^\ü½®8^M¾ÈêYA8^D
^@^@¹^Bú=^^û¼A\¶0@º^D^@^@ìäM½Â¾^B½<98><99>Ä@Ä^D^@^@gÙ+¾6{,¾·:¿@Ø^D^@^@T^D:¾
^@"!¿¼çUp?^Hé^\Ad^E^@^@î^QX?yìW?><98>^_Ax^E^@^@¬<9b>Q?Í<8c><98>¿ÁÁ^\A<8c>^E
9a>^]A^D^F^@^@C6^H¾]<8f>^HÀL²^_A^X^F^@^@fi3@^<84>(¾lÉ^\A,^F^@^@70:@Í(É½_:^Z
@`ë^S¾É+^0¾#<9a>[A,^F^@^@çw$¾-N6¾<95><85>ZAI^F^@^@^@ØÂÀ]<87>Ä½ ^ZXAà^F^@^@c
>^B&A^H^G^@^@ÀòE>¾#/>ç^Yù@^\^G^@^@7P^F>^PÊ÷=¿EÁ@0^G^@^@#<8a>/¼@Ë0½^R
¾@D^G^@^@è^EÁÀ¹ì^\¾¼uÁ@X^G^@^@Áªº@^RIK¾<8d>,Ü@l^G^@^@?ªÆ½N'+½^^\^MA<80>^G^@
^@^@j)^¾<9d>^0HÀ<96><9a>^_Aø^G^@^@<9b>dR?±Z<98>¿l^\A^L^H^@^@ÀRh?^T-¢Àç#^ZA
<84>^H^@^@ª^MÄÀ0^^)¾ü>@A<98>^H^@^@ÚçF¾¾¿ÁÀ}ÆTA¬^H^@^@Z»î½¹y½@¥^ZZAA^H^@^@"Ñ
^L!\¾è^NÁÀ<93>ªÀ@8»^@^@^@Kl5¾ì º@^G,Õ@L»^@^@<8f>Ý»½ÜîÁÀ1¹^CA`» ^@^@x^HhBì4
```


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**

AUTOMATE



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)

CTF TIME

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)

CTF TIME










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>

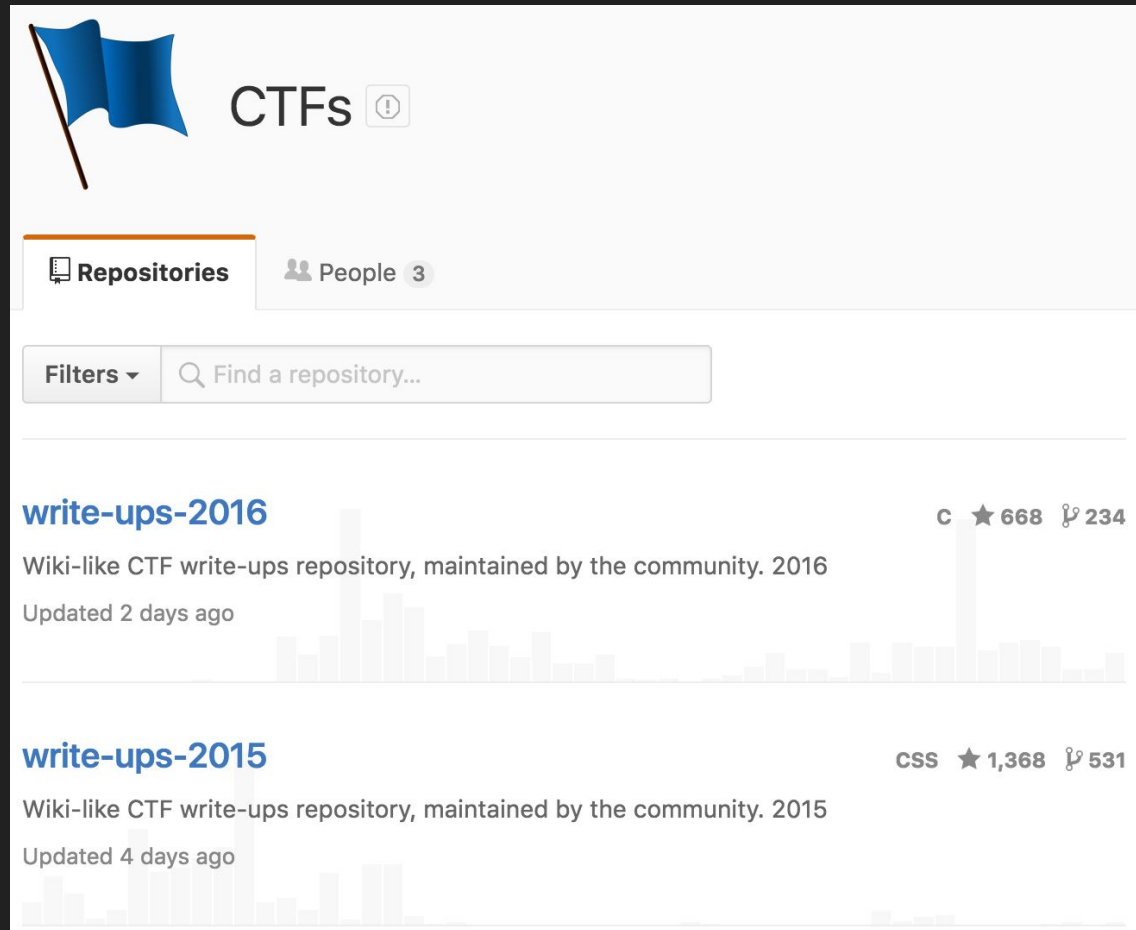
CTF Time (classifica)

CTF TIME

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



The screenshot shows the GitHub interface for the 'CTFs' organization. At the top left is a blue flag icon. To its right is the text 'CTFs' with a small information icon. Below this is a navigation bar with 'Repositories' (selected) and 'People 3'. A search bar contains the text 'Find a repository...'. The main content area lists two repositories:

- write-ups-2016**: Wiki-like CTF write-ups repository, maintained by the community. 2016. Updated 2 days ago. 668 stars, 234 forks.
- write-ups-2015**: Wiki-like CTF write-ups repository, maintained by the community. 2015. Updated 4 days ago. 1,368 stars, 531 forks.

Each repository entry includes a small bar chart showing activity over time.

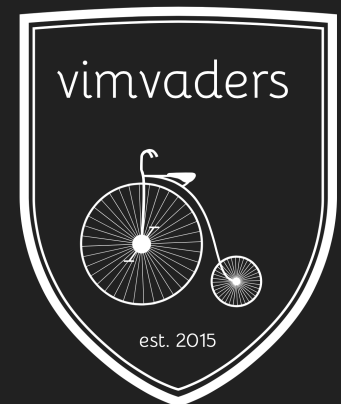
<https://github.com/ctfs>

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 ?

