

Summer School 2025

Introducción a CTFs

Pablo & No one



CTF 101: ¿Qué es un CTF?

- CTF o Capture the Flag



```
CHTB{th1s_1s_my_bug_r3p0rt}.
```

Flag → String



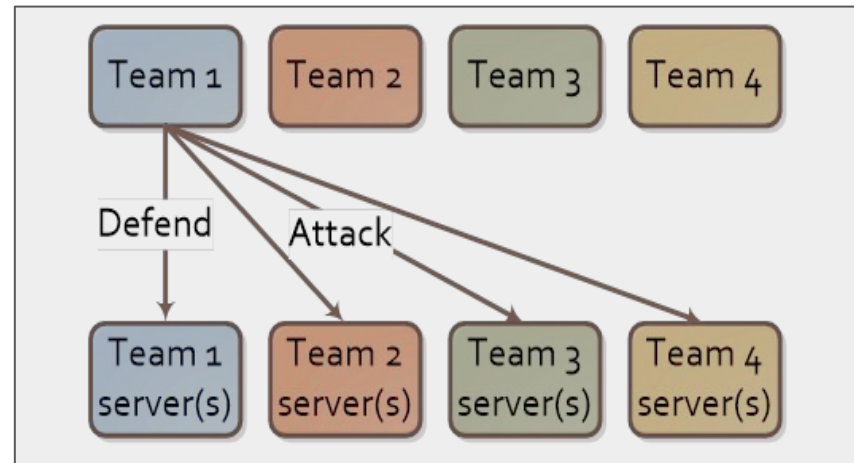
CTF 101: Tipos de CTF



Jeopardy

Web	Crypto	Forensics	Reverse	Misc
1	165	100	50	50
150	150	150	100	100
204	150	150	150	165
203	200	200	200	150

Attack Defense





CTF 101: Categoría de retos de CTF

Retos individuales divididos en categorías.

- **PWN / Exploiting**
- **Reversing (Rev)**
- **Web Security (Web)**
- **Crypto**
- **Misc**
- (Forense)
- (Hardware)
- (Steganography)

Web	Crypto	Forensics	Reverse	Misc
1	165	100	50	50
150	150	150	100	100
204	150	150	150	165
203	200	200	200	150

- DEFCON CTF quals: the only thing that gets a room of professional research staff looking through 10,000 photos of antique furniture for a weekend



Capture-The-Flag (CTF) competition

Jeopardy - Web Security

- Explotación de una página.
 - Bot admin que visita la página dada por el atacante con el objetivo de exfiltrar su Cookie.
 - Remote-Command-Execution (RCE)

```
Ⓢ ~ /E/CT/H/Web/WtldGooseHunt > 5s python3 solve.py
Found one more char : CHTB{1
Found one more char : CHTB{1_
Found one more char : CHTB{1_t
Found one more char : CHTB{1_th
Found one more char : CHTB{1_th1
Found one more char : CHTB{1_th1n
Found one more char : CHTB{1_th1nk
Found one more char : CHTB{1_th1nk_
Found one more char : CHTB{1_th1nk_t
Found one more char : CHTB{1_th1nk_th
Found one more char : CHTB{1_th1nk_the
Found one more char : CHTB{1_th1nk_the
```



BurpSuite

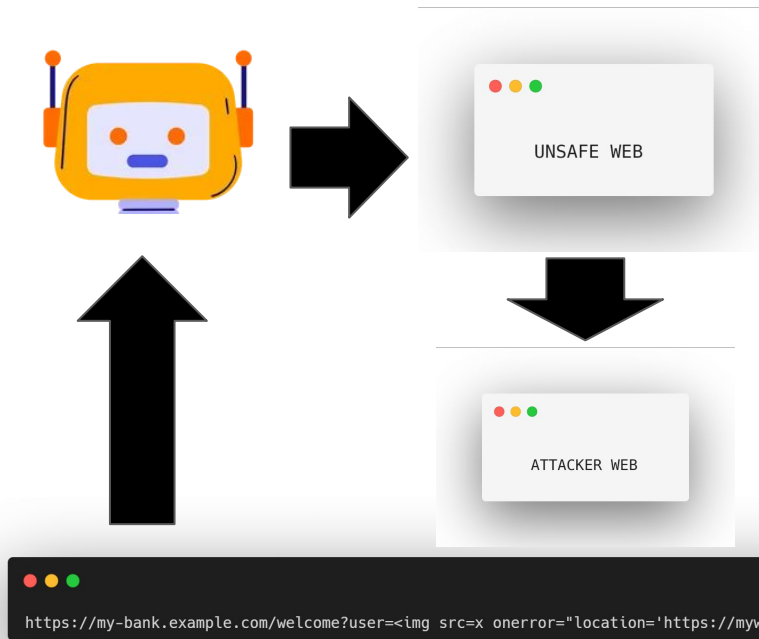


Capture-The-Flag (CTF) competition

Jeopardy - Web Security

- Ejemplo de bot (XSS)

```
const params = new URLSearchParams(window.location.search);  
const user = params.get("user");  
const welcome = document.querySelector("#welcome");  
welcome.innerHTML = `Welcome back, ${user}!`;
```






Capture-The-Flag (CTF) competition

Jeopardy - Web Security

- Ejemplo SQL Injection

user = 105 OR 1=1



```
txtUserId = getRequestString("UserId")  
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId
```

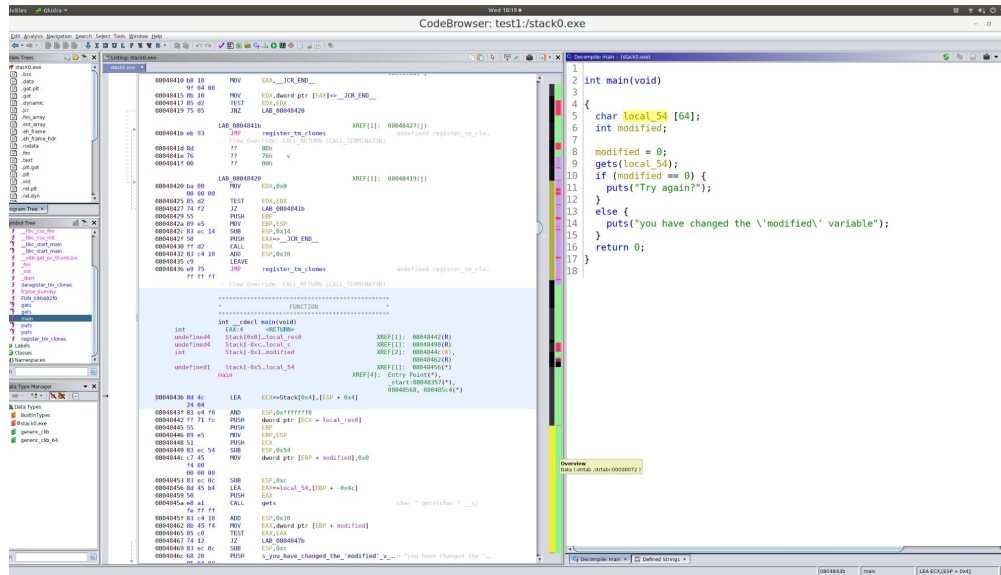
```
https://my-bank.example.com/welcome?user=105%20OR%201=1
```



Capture-The-Flag (CTF) competition

Jeopardy - Reversing

- Hacer ingeniería inversa (reversing) de binarios.
- Reconocer algoritmos.
- Buscar cómo se forma la password con la que nos dan la flag.
- Herramientas como Binary Ninja, IDA, r2, Ghidra o Cutter



```
> python3 exploit.py
=====
SOLUTION:98304

> nc chall.polygl0ts.ch 3600
What's your your number:98304
EPFL{4ft3r_th15_h0w_h4rD_caN_r3V_8e?}
```

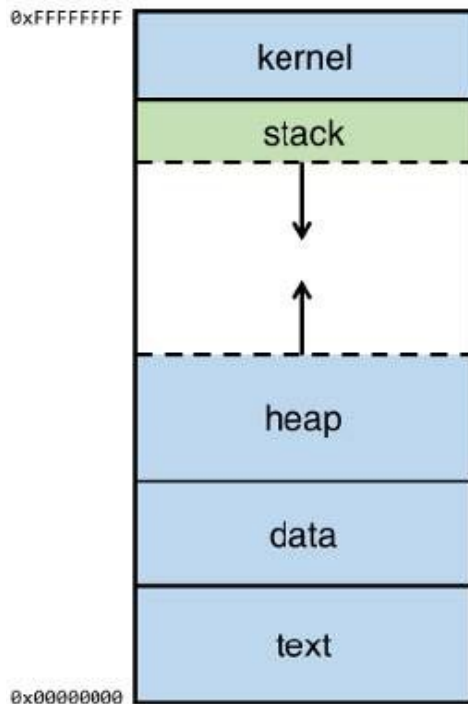
Ghidra



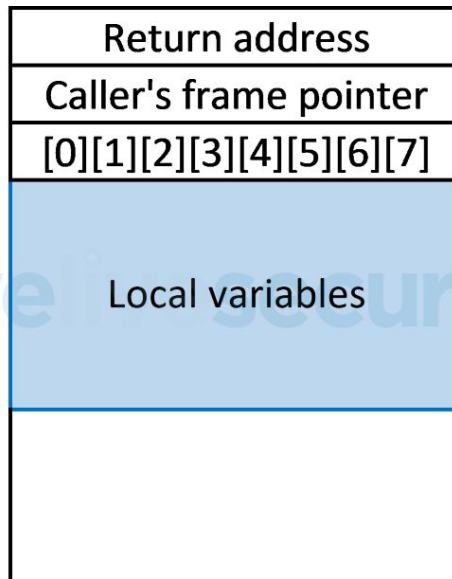
Capture-The-Flag (CTF) competition

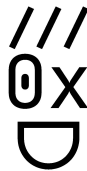
Jeopardy - PWN/Exploiting

- Exploiting de binarios
 - ELF (Linux)
- Encontrar inputs del atacante (nosotros) con los que ejecutar comandos.



Buffer overflow





Capture-The-Flag (CTF) competition

Jeopardy - PWN/Exploiting

- Format string vulnerability

```
printf("%s", input);
```

```
input: %p %p %p  
resultado: %p %p %p
```

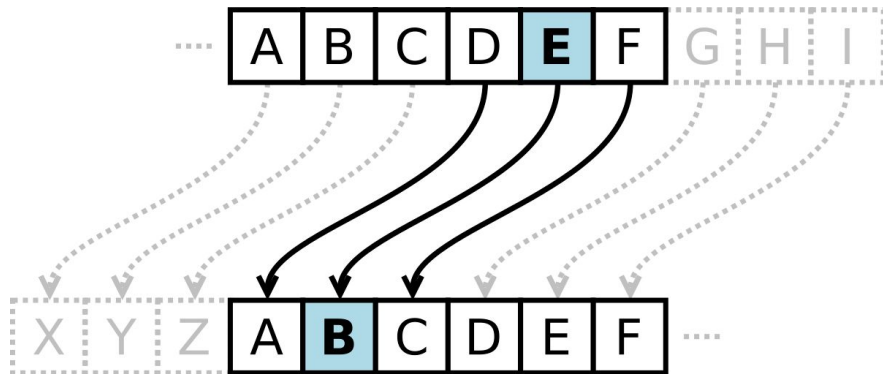
```
printf(input);
```

```
input: %p %p %p  
resultado:  
0x0  
0xdeadbeef  
0x7ffff7a33450
```

Capture-The-Flag (CTF) competition

Jeopardy - Crypto

- Técnicas de cifrado mediante conceptos matemáticos.
- Buscar fallas en la implementación.
- Herramientas:
 - Scripts de python o páginas como CyberChef.

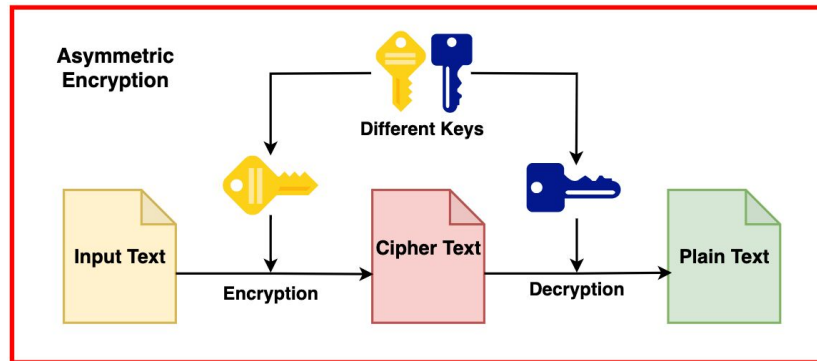
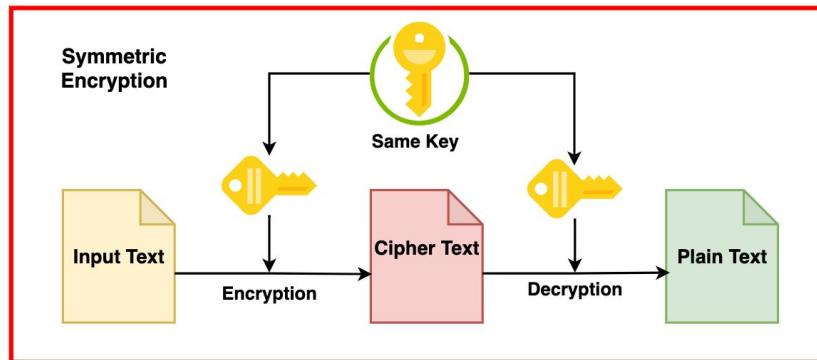


Capture-The-Flag (CTF) competition



Jeopardy - Crypto

- Base64
- Cifrado simétrico
- Cifrado asimétrico
- Hash





Capture-The-Flag (CTF) competition

Misc

- Retos variados y creativos.

El usuario jmartinez olvidó su contraseña. Tu objetivo es acceder a su cuenta en el sistema de recuperación:

<https://www.microsoft.com/login>

Al intentar resetear, te pide responder correctamente tres preguntas de seguridad.

Sabemos que el usuario es muy activo en foros y redes sociales.

Equipo CTF 0xD3C0D3

Para aprender y entrenar

- Plataformas con retos:
 - PWN college
- Entornos preparados y seguros.



Lectures and Reading

(review) Computer Architecture

(review) Assembly

Challenges





set-register

set-multiple-registers



Equipo CTF 0xD3C0D3

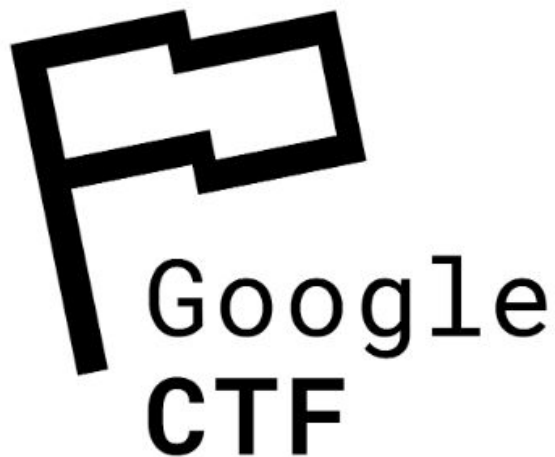
- Participación: CTF time
 - CTFs organizados por universidades, comunidades e instituciones de todo el mundo.
 - 2º en España.
 - Sistema de rating: posición, número de equipos y dificultad del CTF
- Resultados:
 - Top 10-15% de cientos o miles de participantes.

Worldwide position	Name	Country	Points	Events
👑 1	r3kapig		781.772	22
2	kalmarunionen		775.236	24
3	Infobahn		722.339	20
4	The Flat Network Society		692.903	30
5	L3ak		682.295	18
6	Project Sekai		642.865	12

Experiencia final Midnight

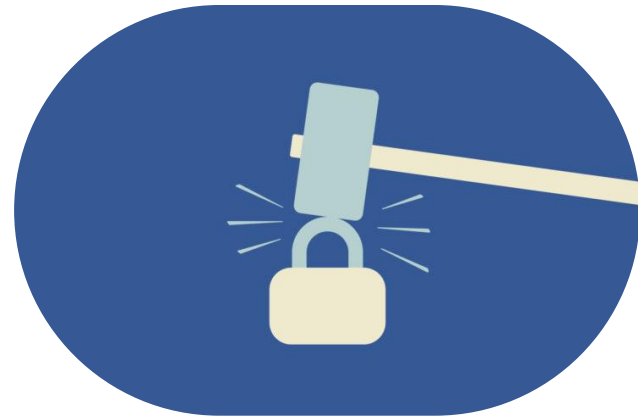
- Clasificación online:
 - 25 primeros clasificados.
- Finales presenciales en Rennes (Francia).





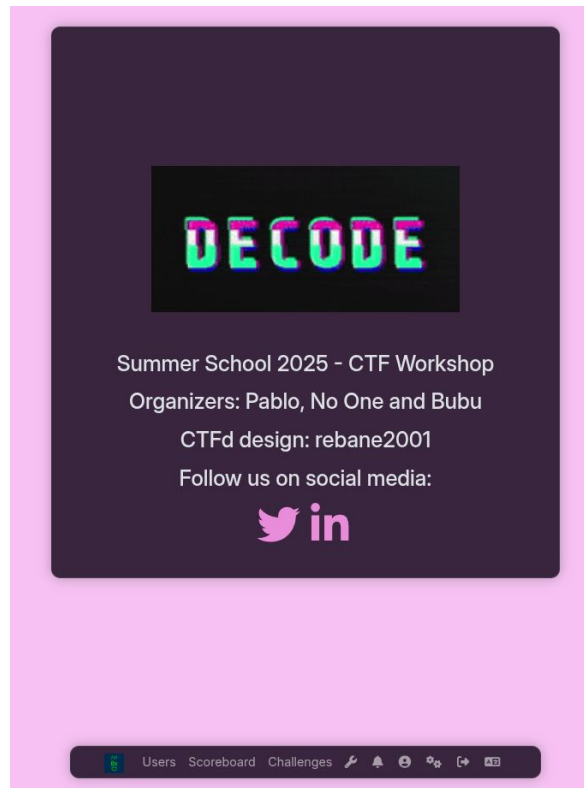
Reglas de etiqueta

- Nada de bruteforce
- No atacar la infraestructura
- No compartir flags
- No holdear flags

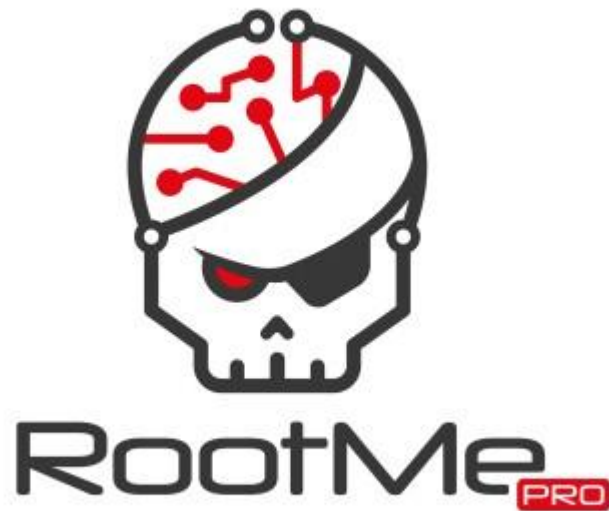


About CTF Workshop

- Duración: Ahora - 13:15
- No habrá pistas adicionales
- Equipos de dos

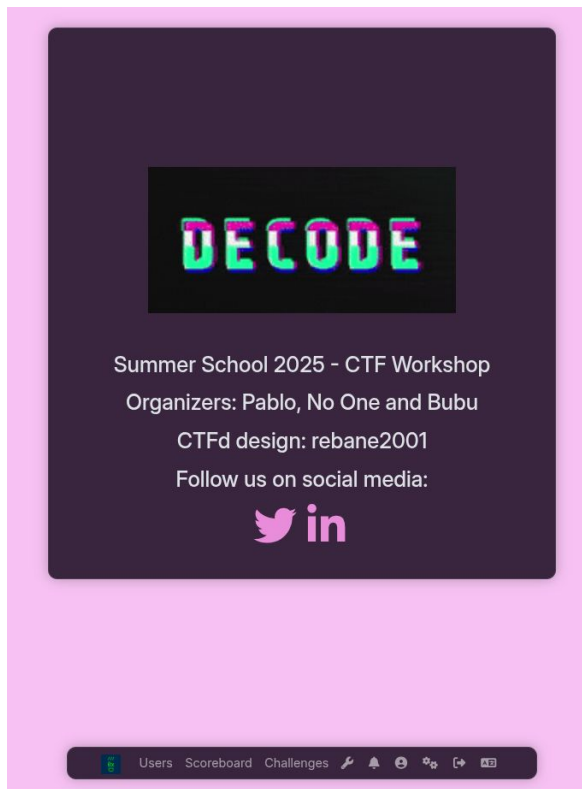


Root-me



<https://www.root-me.org/?lang=es>

CTF Workshop



<https://ctf.0xdecode.apps.deustotech.eu/>