Intro to CTFs

⚠ WARNING ⚠

CTFs are highly addictive

Table of contents

$ whoami

user

sam @bluealder

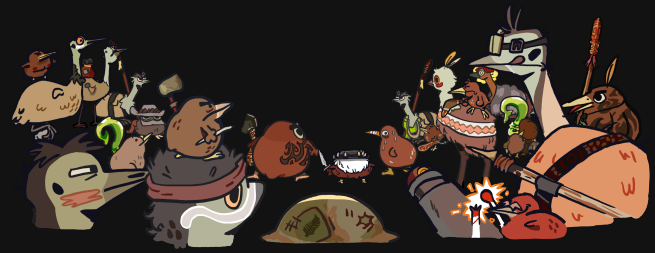
tom @dot

jordan @delta

group

DownUnderCTF

The biggest CTF Competition in the southern hemisphere



WTF is a CTF?


3
38
22
LANFEST
2019

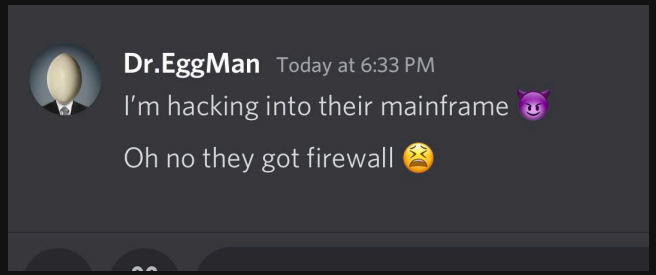
What is a CTF?

CTFs are competitions where teams (or teams of one) use cyber skills across the spectrum computer security to solve challenges by retrieving flags □□□

You will

- Break servers
- Write an exploit
- Discover a vulnerability
- Reverse engineer
- Perform a forensic analysis

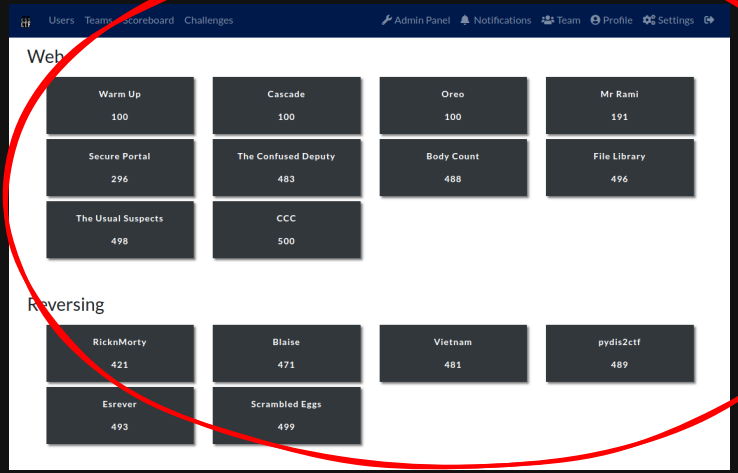
Essentially you have *almost* full permissions to put your hacker hat on and think like an attacker



Flavours of CTFs

There are two main flavours of CTFs

Jeopardy Style



Attack/Defense Style

What does a CTF Challenge Look like?

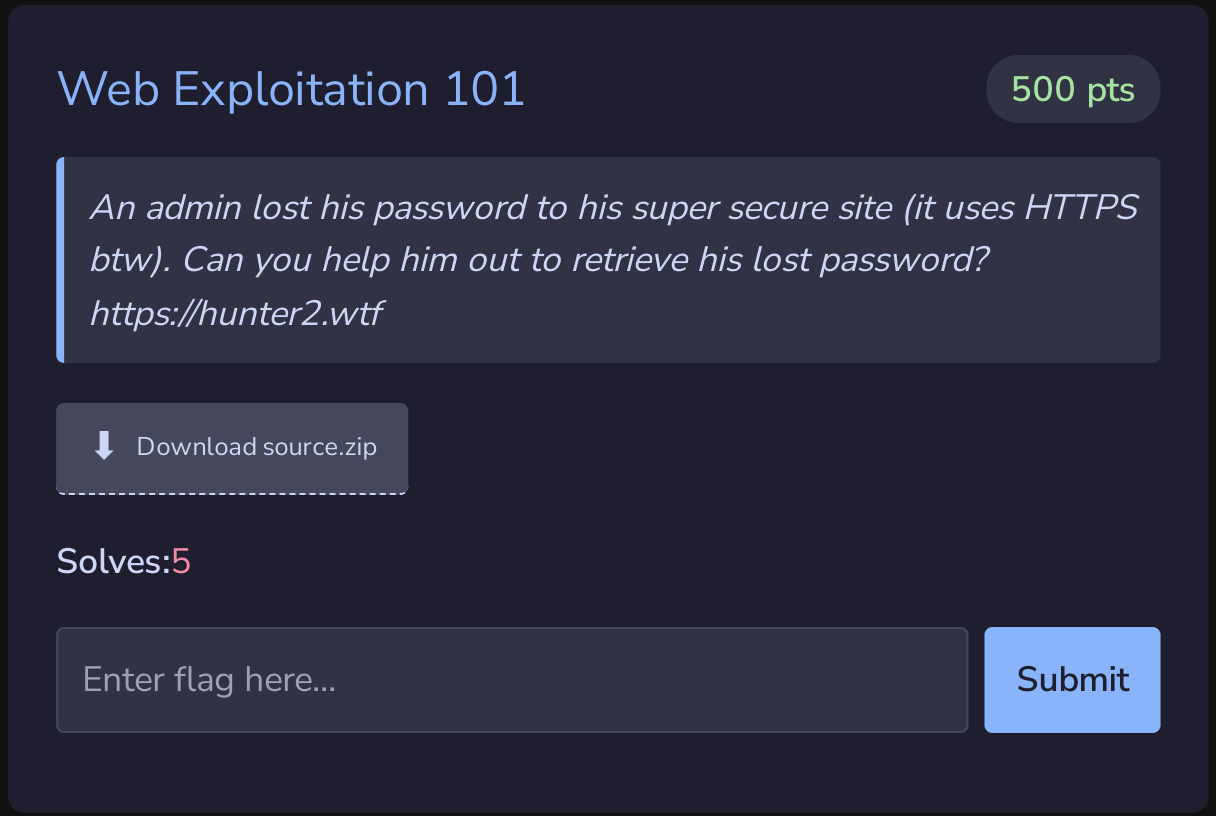
Title: The name of the challenge

Flavour Text: Provides some context about the challenge, likely will include hints on how to get the flag (the intended way)

Files: You might get some source code, or an encrypted output, or literally any kind of file that you will need to analyse which will be required to solve the challenge

Server Details: If the challenge is hosted you will need to connect to it!

Here’s what a super simple challenge might look like



Flags

Here's an example flag `` `DUCTF{ay0_th15_fl4g_b3_bUssing}` ``

They are a short unique string which proved you solved the challenge

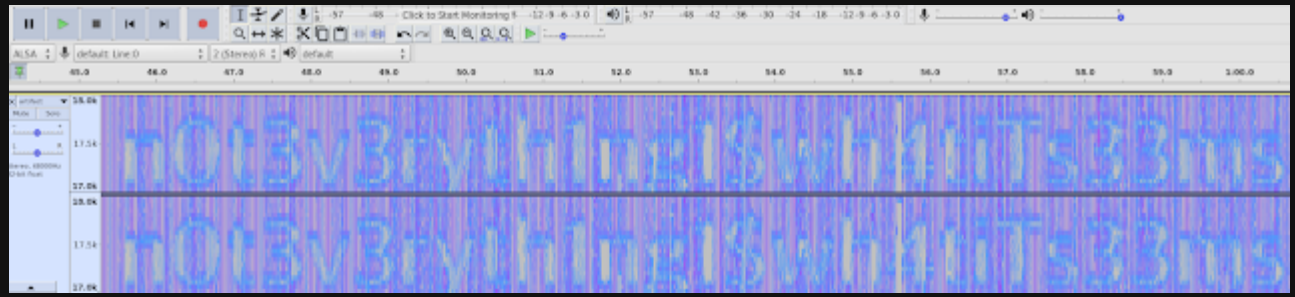
- gives you points
- gives you bragging rights

they will give you an immense dopamine hit

Where can I find flags?

They come in many forms:

- might just be a file on a server
- could be hidden in plain sight
- hidden behind admin privileges
- hidden behind a crypto protocol
- literally could be anything



Solving a Challenge

Web Exploitation 101

500 pts

> *An admin lost his password to his super secure site (it uses HTTPS btw). Can you help him out to retrieve his lost password? https://hunter2.wtf*

⬇ Download source.zip

Solves:5

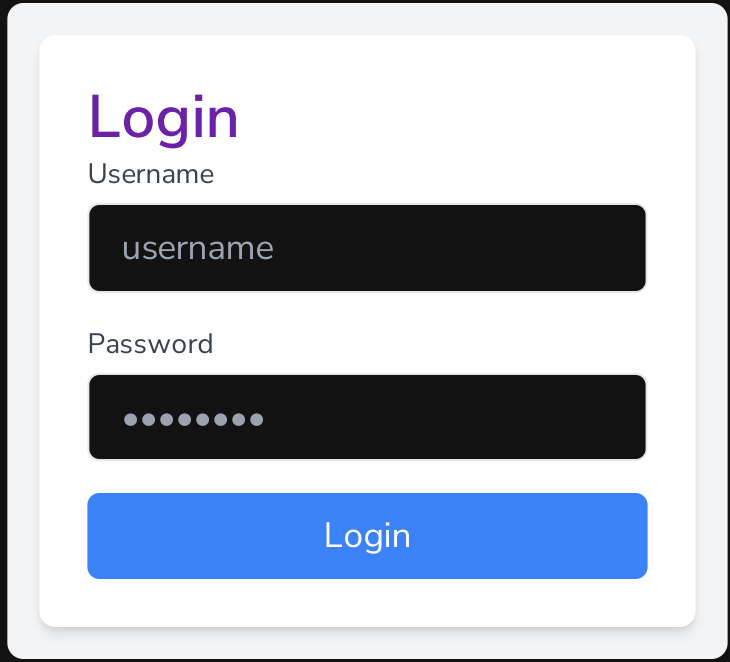
Enter flag here...

Submit

Analyse the files

Here's a super simple example

```
const handleLogin = async () => {
    if (formData.username === 'admin' &&
      formData.password === atob('RFVDVEZ7bXlfZmlyc3RfZmxhZyF
      formData.error = 'Success!'
      formData.isSuccess = true
    } else {
      formData.error = 'Invalid username or password'
      formData.isSuccess = false
    }
}
```



What do we know?

- Some login form, but I don't know where the flag
- User is admin
- Password looks looks very weird and uses an `atob()` function
- Uses JavaScript, no server side code

What can we do?

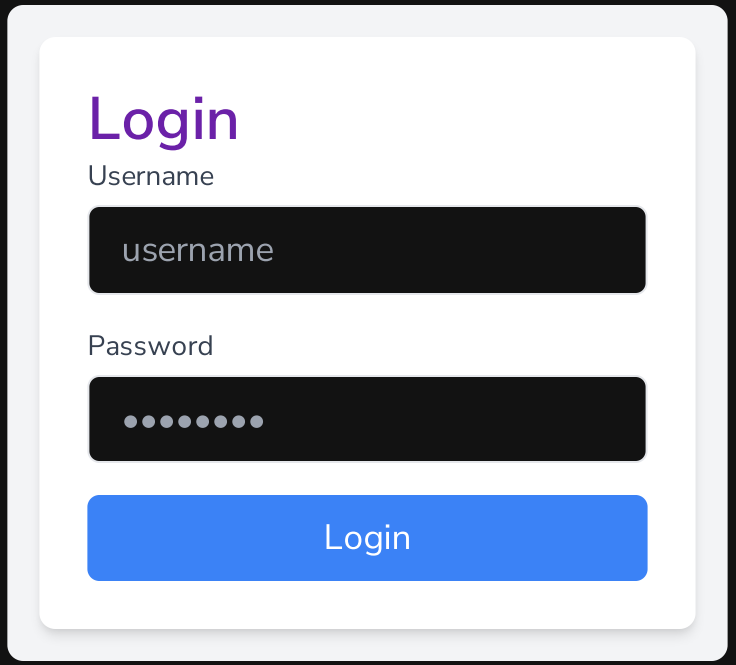
- Hypothesize
- Research Research Research
  - Google unknown concepts
  - Ask AI explain code
- Run the challenge locally
- Analyse your results and try again (scientific method)

Test our hypothesis

```
const handleLogin = async () => {
    if (formData.username === 'admin' &&
      formData.password === atob('RFVDVEZ7bXlfZmlyc3RfZmxhZyF
      formData.error = 'Success!'
      formData.isSuccess = true
    } else {
      formData.error = 'Invalid username or password'
      formData.isSuccess = false
    }
}
```

```
const flag = atob('RFVDVEZ7bXlfZmlyc3RfZmxhZyF9');
console.log(flag);
```

```
DUCTF{my_first_flag!}
```



Submitting the flag

Writeups

Writing down your solution and explaining how you solved the challenge is called a **writeup**.

- Usually published online after the CTF
- Great way to learn how other people approach challenges you struggled with
- Organise and tidy your notes
- Solidify your learning and share it with others

CTF Challenge Categories

There are a bunch of categories for challenges. It varies from CTF to CTF

web	pwn
crypto	rev
osint	misc

We will cover these today, but the list goes on...

- cloud
- mobile
- networking
- stegonography
- forensics
- DFIRs
- hardware
- IOT

CTF Categories

web	pwn
crypto	rev
osint	misc

web

Web challenges focus on exploiting vulns in web apps

You might:

- Perform Injection (SQL, Command) and take over an admin console
- Use an IDOR to read secret blog content
- Steal an admin cookie by getting them to access an XXSd page

CTF Categories

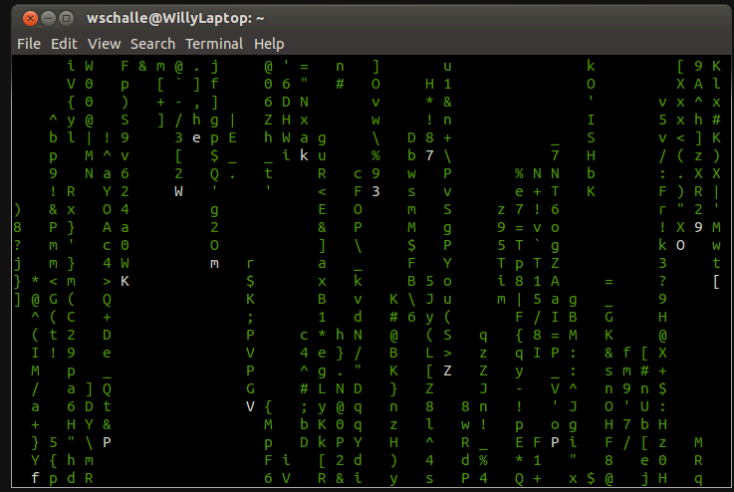
web	pwn
crypto	rev
osint	misc

pwn

Pwn challenges involve some kind of binary exploitation, where the goal is to find vulnerabilities in compiled programs.

Common solving methods include:

- Buffer overflows
- Return Oriented Programming (ROP)
- return to lib c



CTF Categories

web	pwn
crypto	rev
osint	misc

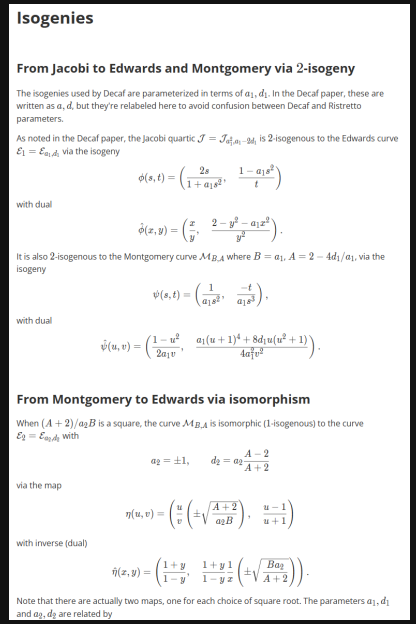
crypto

Cryptography challenges focus on breaking or exploiting cryptographic algorithms and systems. boomer not zoomer crypto

You might:

- decode a secret a message
- do some crazy math to break a crypto protocol
- backdoor a messaging app

this one gets hella mathy



Isogenies

From Jacobi to Edwards and Montgomery via 2-isogeny

The isogenies used by Decaf are parameterized in terms of a_1, d_1. In the Decaf paper, these are written as a, d, but they're relabeled here to avoid confusion between Decaf and Ristretto parameters.

As noted in the Decaf paper, the Jacobi quartic $\mathcal{J} = \mathcal{J}_{\eta_1^2 a_1 - 4d_1}$ is 2-isogenous to the Edwards curve $\mathcal{E}_1 = \mathcal{E}_{a_1,d_1}$ via the isogeny

$$\phi(s,t) = \left(\frac{2s}{1+a_1 s^2}, \quad \frac{1-a_1 s^2}{t}\right)$$

with dual

$$\hat{\phi}(x,y) = \left(\frac{x}{y}, \quad \frac{2-y^2-a_1 x^2}{y^2}\right).$$

It is also 2-isogenous to the Montgomery curve $\mathcal{M}_{B,A}$ where $B = a_1$, $A = 2 - 4d_1/a_1$, via the isogeny

$$\psi(s,t) = \left(\frac{1}{a_1 s^2}, \quad \frac{-t}{a_1 s^3}\right),$$

with dual

$$\hat{\psi}(u,v) = \left(\frac{1-u^2}{2a_1 v}, \quad \frac{a_1(u+1)^4 + 8d_1 u(u^2+1)}{4a_1^2 v^2}\right).$$

From Montgomery to Edwards via isomorphism

When $(A+2)/a_2 B$ is a square, the curve $\mathcal{M}_{B,A}$ is isomorphic (1-isogenous) to the curve $\mathcal{E}_2 = \mathcal{E}_{a_2,d_2}$ with

$$a_2 = \pm 1, \qquad d_2 = a_2 \frac{A-2}{A+2}$$

via the map

$$\eta(u,v) = \left(\frac{u}{v}\left(\pm\sqrt{\frac{A+2}{a_2 B}}\right), \quad \frac{u-1}{u+1}\right)$$

with inverse (dual)

$$\hat{\eta}(x,y) = \left(\frac{1+y}{1-y}, \quad \frac{1+y}{1-y}\frac{1}{x}\left(\pm\sqrt{\frac{B a_2}{A+2}}\right)\right).$$

Note that there are actually two maps, one for each choice of square root. The parameters a_1, d_1 and a_2, d_2 are related by

CTF Categories

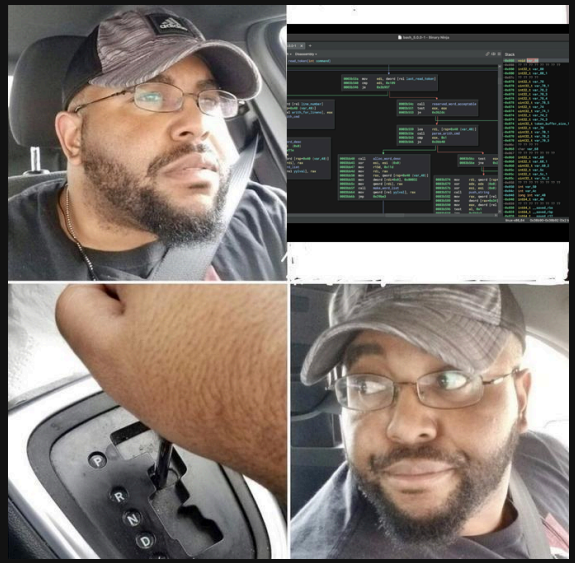
web
pwn
crypto
rev◀
osint
misc

rev◀

Reverse Engineering challenges involve analysing compiled programs and processed outputs to understand their functionality to exploit them

You might:

- find a bug in a game to get the highscore
- dive through assembly
- reconstruct encryption keys



CTF Categories

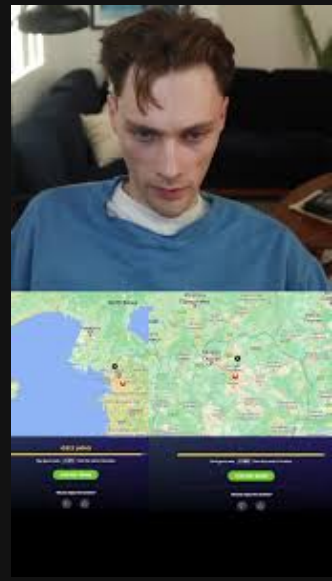
web	pwn
crypto	rev
osint	misc

OSINT

Open-Source Intelligence (OSINT) challenges involve gathering information from publicly available sources.

You might:

- Find some cool bridges
- "research" an online presence to find out personal information
- Become slightly better at geo guesser
- Get really good at google dorking



CTF Categories

web	pwn
crypto	rev
osint	**misc**

misc

Literally anything else that might not fit into a category

You might:

- Listen to some sick beats (mc fat monke)
- Convince an AI that you are an orc from Lord of the Rings
- Program in some esoteric language that only uses the *h* character
- Make some great recipes to take home to your family

Why play CTFs?

- Super interesting
- Fun
- You accidently learn
- You can win prizes

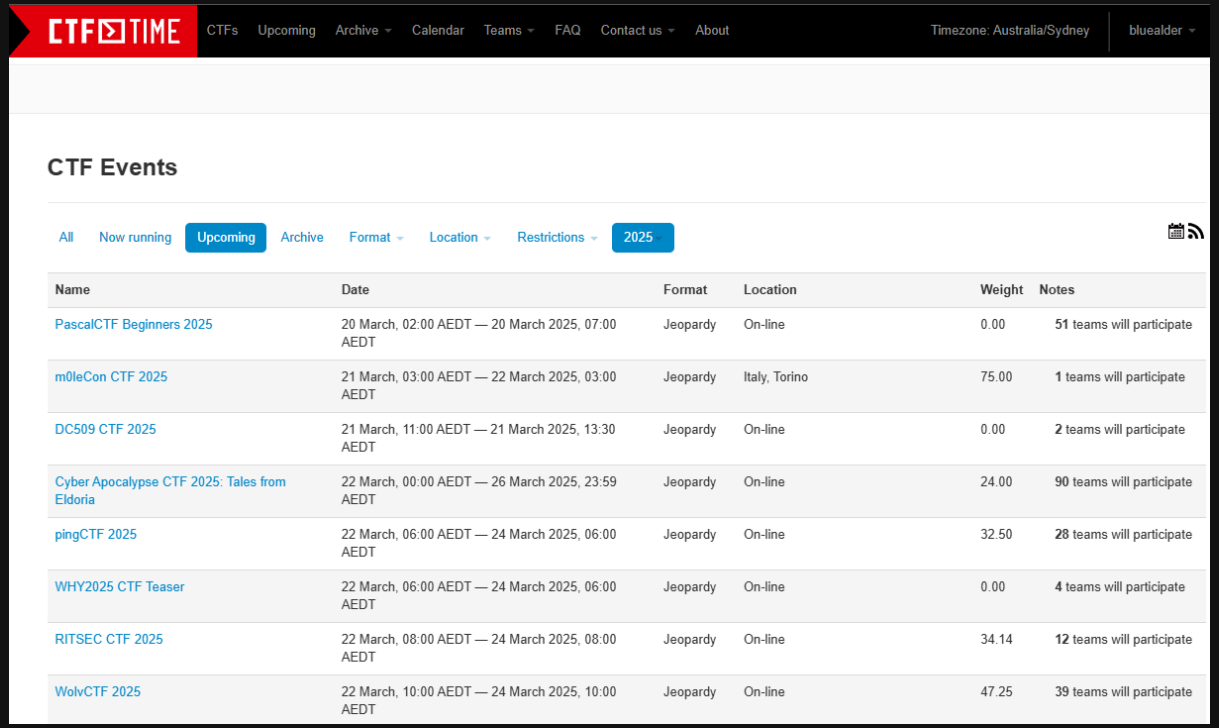
Who plays CTFs?

- School students
- People interested in Cyber Security
- People in the security industry
- Professional Teams

How did I get into CTFs?

How do I find CTFs to play in?

ctftime.org is the primary aggregator of CTFs



Name	Date	Format	Location	Weight	Notes
PascalCTF Beginners 2025	20 March, 02:00 AEDT — 20 March 2025, 07:00 AEDT	Jeopardy	On-line	0.00	**51** teams will participate
m0leCon CTF 2025	21 March, 03:00 AEDT — 22 March 2025, 03:00 AEDT	Jeopardy	Italy, Torino	75.00	**1** teams will participate
DC509 CTF 2025	21 March, 11:00 AEDT — 21 March 2025, 13:30 AEDT	Jeopardy	On-line	0.00	**2** teams will participate
Cyber Apocalypse CTF 2025: Tales from Eldoria	22 March, 00:00 AEDT — 26 March 2025, 23:59 AEDT	Jeopardy	On-line	24.00	**90** teams will participate
pingCTF 2025	22 March, 06:00 AEDT — 24 March 2025, 06:00 AEDT	Jeopardy	On-line	32.50	**28** teams will participate
WHY2025 CTF Teaser	22 March, 06:00 AEDT — 24 March 2025, 06:00 AEDT	Jeopardy	On-line	0.00	**4** teams will participate
RITSEC CTF 2025	22 March, 08:00 AEDT — 24 March 2025, 08:00 AEDT	Jeopardy	On-line	34.14	**12** teams will participate
WolvCTF 2025	22 March, 10:00 AEDT — 24 March 2025, 10:00 AEDT	Jeopardy	On-line	47.25	**39** teams will participate

DownUnderCTF 2025

The biggest CTF in the southern hemisphere

- ~5000 players
- Aimed at students and upskilling YOU
- Cash prizes (students only)
- Spot Prizes
- The best challenges
- Amazing support team
- Good vibes 😎
- Completey Free!

downunderctf.com

You have 116d 0h 6m 15s to prepare

Other CTF Resources

CTFs / Wargames

- picoCTF
- OverTheWire
- DUCTF
- pwnable.kr
- CTFTime

Learning Platforms

- hackthebox.eu (free/paid)
- BurpSuite Academy (free)
- Vulnhub (free)
- TryHackMe (free/paid)
- cryptohack.org - (free)
- Pentester Lab (paid)

YouTube Channels

- LiveOverFlow
- John Hammond
- Ippsec

Useful Tools

- BurpSuite
- PayloadAllTheThings
- CTFKatana
- Ghidra
- gdb
- python
- WireShark

We’ve got some challenges for you!

uni.duc.tf

Questions?

Workshop CTF Link: uni.duc.tf

These slides are available at intro-to-ctf.duc.tf