

Intro to CTFs



⚠ WARNING ⚠

CTFs are highly addictive

Table of contents

- 1. Intro to CTF
- 2. △ WARNING △
- 3. Table of contents
- 4. What is a CTF?
- 5. Flavours of CTFs
- 6. What does a CTF Challenge Look like?
- 7. Flags
- 8. Solving a Challenge
 - 1. Analyse the files
 - 2. What do we know?
 - 3. Test our hypothesis
 - 4. Submitting the flag
- 9. Writeups
- 10. CTF Challenge Categories
 - 1. web
 - 2. pwn
 - 3. crypto
 - 4. rev
 - 5. osint
 - 6. misc
- 11. Why play CTFs?
- 12. How did I get into CTFs?
- 13. How do I find CTFs to play in?
- 14. DownUnderCTF 2025
- 15. Other CTF Resources
- 16. We've got some challenges for you!
- 17. Questions?



\$ whoami

user

sam
@bluealder



tom
@dot



jordan
@delta



group

DownUnderCTF



The biggest CTF Competition in the southern hemisphere



WTF is a CTF?







What is a CTF?

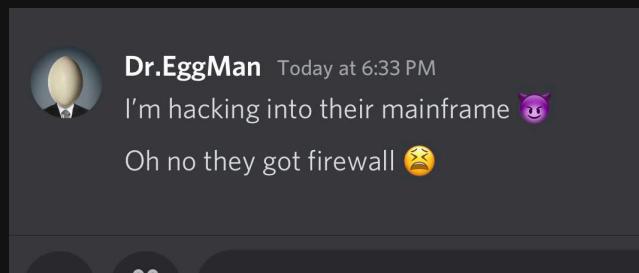
CTFs are competitions where teams (or teams of one) use cyber skills across the spectrum computer security to solve challenges by retrieving flags ☺☺☺



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

A screenshot of a Jeopardy-style CTF scoreboard. The interface includes a navigation bar with 'Users', 'Team', 'Scoreboard', 'Challenges', 'Admin Panel', 'Notifications', 'Team', 'Profile', and 'Settings'. Below this, there are two sections: 'Web' and 'Reversing'. The 'Web' section contains challenges like 'Warm Up' (100), 'Secure Portal' (296), 'The Usual Suspects' (498), 'Cascade' (100), 'The Confused Deputy' (483), 'Body Count' (488), 'Oreo' (100), 'File Library' (496), and 'Mr Rami' (191). The 'Reversing' section contains challenges like 'RicknMorty' (421), 'Blaise' (471), 'Scrambled Eggs' (499), 'Esrever' (493), 'Vietnam' (481), and 'pydis2ctf' (489).

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

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



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

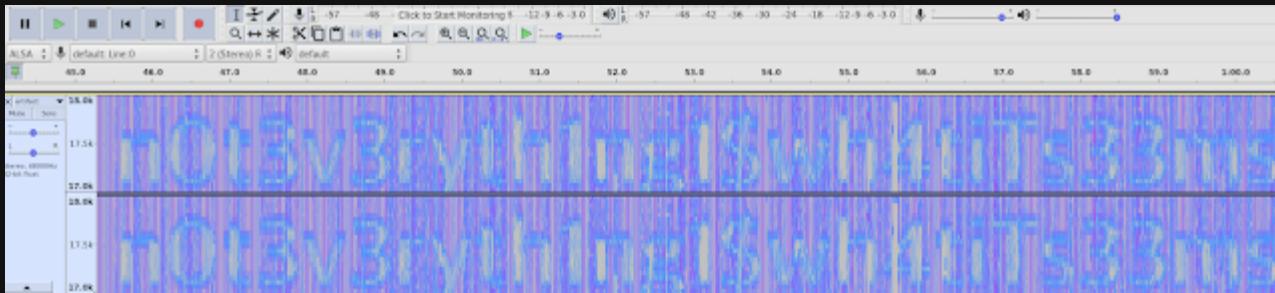
they will give you an **immense** dopamine hit



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...

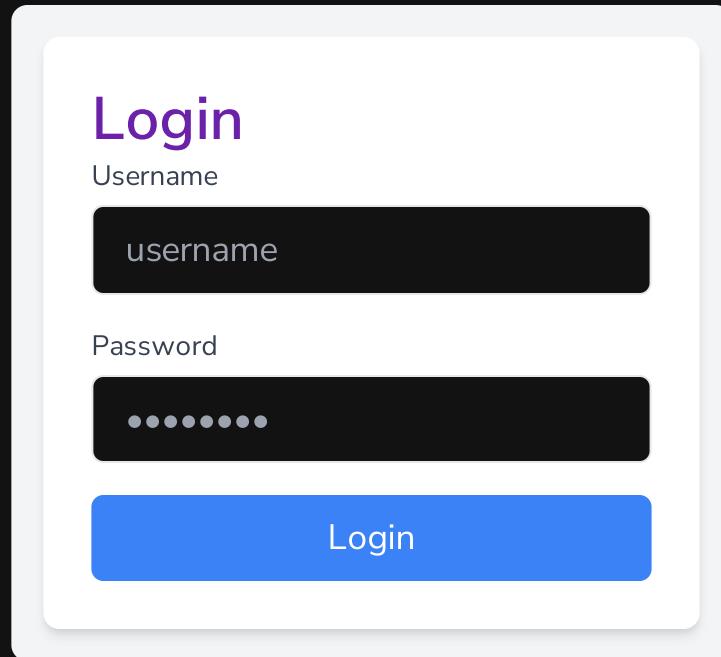
Submit



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
  }
}
```



The image shows a stylized login interface. At the top center, the word "Login" is written in a large, purple, sans-serif font. Below it, the word "Username" is displayed in a smaller, gray font. A dark gray rectangular input field contains the word "username". Below this, the word "Password" is shown in a smaller, gray font. An input field below it contains six black dots, representing a password. At the bottom center is a large, blue rectangular button with the word "Login" in white.



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!}

Login

Username

Password

Login



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
- steganography
- forensics
- DFIRs
- hardware
- IOT



CTF Categories

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



()

SUBSCRIBE



CTF Categories

web

pwn

crypto

rev

osint[

misc

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

```
i W F & m @ . j @ ' = n ] o h u k [ 9
V o p 0 6 " # v w * & o x ^ 
{ @ ) + - , ] 6 D N v * & o x ^ 
{ @ ) + - , ] 6 D N v w * & o x ^ 
^ y @ S ] / h g | Z H x w * & o x ^ 
b l | ! 9 3 e p E h W a g % b 7 \ 7 H b K 
p M ^ v [ $ - i k u r c 9 w s v % N N 
9 N a 6 2 Q - t M g g 9 = v o 
! R Y 2 W ' < F 3 s v e + T K 
) & x 0 4 g E O m m z 7 ! 6 
8 P ) A a 2 & P M g g 9 = v o 
? m ' c 0 0 ] \ $ T 5 T 
j m } 4 W m r a - F Y T p T Z 
] * < m > K $ x - k B 5 o 
] @ G ( Q K B v K \ J u m | 5 a g _ G 
^ ( C + ; 1 d # 6 y ( F / I B 
( t 2 D P c * h n @ ( s q { 8 = M K @ 
I I 9 e V 4 e ) / B L > z q I P : & f [ X 
M p _ P ^ g . " K [ Z J y - ^ v 
/ a ] Q G # L N D ) Z J J 
a 6 D t V { ; y @ q n 8 n ! p o g H 7 b 
+ H Y & M b k o q n 8 n ! p o g H 7 b 
} 5 " \ P p D k p Y H L R _ E F P i 
Y h m F i [ 2 d ) 4 d % * 1 
f p d R 6 V R & i v s P 4 o + x S @ i H 
[ 9 h 
v x ^ 
v x ^ 
/ ( z 
F ) R 
r ! X 9 
K K 
3 ? 
= ? 
9 
- G 
K @ 
s m # + 
s m n 9 n 
u : 
o g H 7 b 
F / [ z 
B 
M
```



CTF Categories

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

web

pwn

crypto

rev

osint

misc

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 $\mathcal{J} = \mathcal{J}_{a_1^2, a_1 - 2d_1}$ is 2-isogenous to the Edwards curve $\mathcal{E}_1 = \mathcal{E}_{a_1, d_1}$ via the isogeny

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

with dual

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

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

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

with dual

$$\hat{\psi}(u, v) = \left(\frac{1 - u^2}{2a_1 v}, \frac{a_1(u+1)^4 + 8d_1 u(u^2+1)}{4a_1^2 v^3} \right).$$

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

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

via the map

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

with inverse (dual)

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

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

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



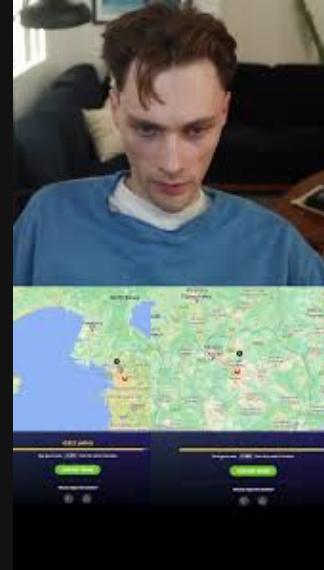
CTF Categories

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

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



web[] pwn[]

crypto[] rev◀

osint[] misc[]



Why play CTFs?

- Super interesting
- Fun
- You accidentally 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

The screenshot shows the ctftime.org website's 'CTF Events' page for March 2025. The page has a header with navigation links for 'CTFs', 'Upcoming', 'Archive', 'Calendar', 'Teams', 'FAQ', 'Contact us', and 'About'. It also shows the current 'Timezone: Australia/Sydney' and a user 'bluealder'. Below the header, there's a search bar and a 'CTF Events' section with a table of upcoming competitions.

| 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



downunderctf.com

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

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!



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

