



# /WHY DO WE PLAY BY CTF?

Black Bauhinia -  
Byron Wai (GonJK)





# \$ blackb6a -help

Black Bauhinia (blackb6a)

- Best CTF team in Hong Kong (self-proclaimed)
- Top 30 CTF Team in CTFTIME

<https://b6a.black>



@blackb6a



@blackb6a



/team/83678





## Black Bauhinia

### Also known as

- blackb6a
- BlackBauhinia

Website: <https://b6a.black>

Twitter: blackb6a

[Sign in](#) to join the team.

# CTFTime (20 Nov 2022)



A team based in Hong Kong.  
(We are NOT affiliated with any associations.)

### Participated in CTF events

[2022](#)[2021](#)[2020](#)[2019](#)

Overall rating place: **30** with **394.451** pts in 2022

Country place: **1**

Place	Event	CTF points	Rating points
45	<a href="#">SECCON CTF 2022 Quals</a>	1029.0000	25.076
26	<a href="#">Hack.lu CTF 2022</a>	1692.0000	24.301
19	<a href="#">ASIS CTF Quals 2022</a>	1327.0000	35.714
6	<a href="#">SekaiCTF 2022</a>	8243.0000	22.689
11	<a href="#">Balsn CTF 2022</a>	1987.0000	26.774





# \$ byronwai -help

- ~~Snacks Provider of BlackB6a~~
- Founding Member of BlackB6a
- Founding Member of HKUST Firebird CTF Team
- System Engineer -> Security Analyst
- HITCON 2020 Speaker
- CISSP





# /TABLE OF CONTENTS



**/01** /About CTF

**/02** /Learn from Playing CTF

**/03** /Learn from Hosting CTF





**/01**

**/About CTF**







# \$ ctf -help



Is CTF a kind of sport?



CTF competitions could be considered a type of sport, as they involve players competing against each other in a structured way. However, CTF competitions are typically focused on cybersecurity and involve solving challenges related to computer systems and networks, rather than physical activities. Some people might consider CTF competitions to be more of a mental or intellectual sport, rather than a physical one. Ultimately, whether or not CTF is considered a sport may depend on how you define the term "sport".







i'm now writing slides on CTF. Do you know what a CTF competition is?



Yes, a CTF competition is a type of cybersecurity competition where participants are tasked with finding and exploiting vulnerabilities in computer systems, applications, and networks. The goal is to find and flag hidden pieces of information, known as "flags," which are usually represented as strings of text. These competitions can be educational and help participants learn more about cybersecurity, as well as provide a fun and competitive environment for participants to showcase their skills.



# \$ ctf -help



CSAW CTF, a Jeopardy CTF, has some of the best collegiate hackers in the nation



DEFCON CTF Finals, an Attack & Defense CTF, is widely considered the world cup of hacking



**/02**

# **/Learn from Playing CTF**





# /What can be achieved from playing CTF



**/01** Improved knowledge and skills in cyber security

**/02** Enhanced problem-solving abilities

**/03** Increased teamwork and collaboration

**/04** Opportunities to network and learn from others

**/05** Fun and engaging way to learn



# Improved knowledge & skills in cyber security

- Require players to use a wide range of cyber security skills
  - Reverse engineering
  - Cryptography
  - Exploitation (pwn)
  - Web
  - Forensic
  - ...
- Become more knowledgeable and proficient in cyber security



# Enhanced problem-solving abilities

- Require creative thinking to solve
- Think outside the box and come up with creative solutions





# Advertisement - Best write-up Awards

- Received numbers of “Creative” (unintended) solutions
- Good Job!



# Increased teamwork and collaboration

- Team-based, requiring players to work together to solve challenges
- Develop strong teamwork and collaboration skills
- Essential in the cyber security field (but not limited)





# Opportunities to network and learn from others

- CTF competitions often attract a wide range of participants
- Network with others in the field
- Learn from others experiences, and potentially even find job opportunities





# Fun and engaging way to learn

- Fun and engaging way to learn about cyber security
- Rewarding and enjoyable way to spend their time
- Challenges can be a great way to stay motivated and engaged in learning



# But wait, CTF can be ...

- Time-consuming and require a significant amount of effort and dedication
- Challenging and frustrating, especially for beginners
- Require specialized knowledge and skills that may not be applicable outside of the competition



**/03**

# **/Learn from Hosting CTF**



# Why do we want to host a CTF?



地盤佬江湖



係愛定係責任呀？



# Back in the old days (2017-2019)

- Cyber security was not “that” common in Hong Kong
- Coding, development is always included in STEM, but not cyber security



# Engage in CTF





# Team up



BOCCHI THE ROCK! OPENING SONG



青春カンプレックス

結束バンド





# What could go wrong?



**/01** Finding sponsors and funding

**/02** Developing challenges and setting up the infrastructure

**/03** Managing participants and ensuring fair play

**/04** Providing adequate support and assistance



# Finding sponsors and funding





# Finding sponsors and funding

- Hosting a CTF competition can be expensive
  - rent space
  - provide refreshments, prizes
  - cover other costs.
- Reach out to businesses and organizations for help





# Develop challenges & Set up infrastructure

- Creating engaging and challenging CTF is difficult
- Develop tasks that will test participants' skills
- Set up the infrastructure
  - Servers
  - Networks
  - Challenges environment





# Developing challenges



wwkenwong 2022/11/12 13:24

Me now

<https://i.kym-cdn.com/photos/images/newsfeed/001/373/328/b>



**babyUXSS return**

富康街寵物公園

300 points · 0 solves · a month ago

pwn

★★★★☆





# Setting up the infrastructure





# Setting up the infrastructure

CTF 2022 challenge

Challenges

Information

Scoreboard

Manage Challenges

Manage Announcem...

DIVISION SCOREBOARD

Project Sekai  
5826 points

no rev/pwn no lfe  
3250 points

Shellphish  
2590 points

#4 PLUS  
2535 points

#5 Colorful Stage  
865 points

#6 MOCSCTF-B  
825 points

#7 MOCSCTF-A  
365 points

#8 AbyssalCrualty  
285 points

#9 HKCERT  
125 points

OAO

< ALL CRYPTO PWN REVERSE WEB FORENSICS MISC >

☆☆☆☆ ☆☆☆☆ ★★★★★ ★★★★★

Show map view

## 必去之處

如果你沒去過以下景點，你還是不要跟其他人說你去過香港...

黑繞環山訊號站  
Zooni Recording  
55 points · 198 solves · a month ago  
misc ★★★★★

珍寶海鮮舫  
SD Card  
50 points · 215 solves · a month ago  
forensics ★★★★★

海山樓  
Flawed ElGamal  
50 points · 127 solves · a month ago  
crypto ★★★★★

歷史檔案館  
Back to the Past  
50 points · 178 solves · a month ago  
web misc ★★★★★

九龍灣綜合回收中心  
UAF  
100 points · 18 solves · a month ago

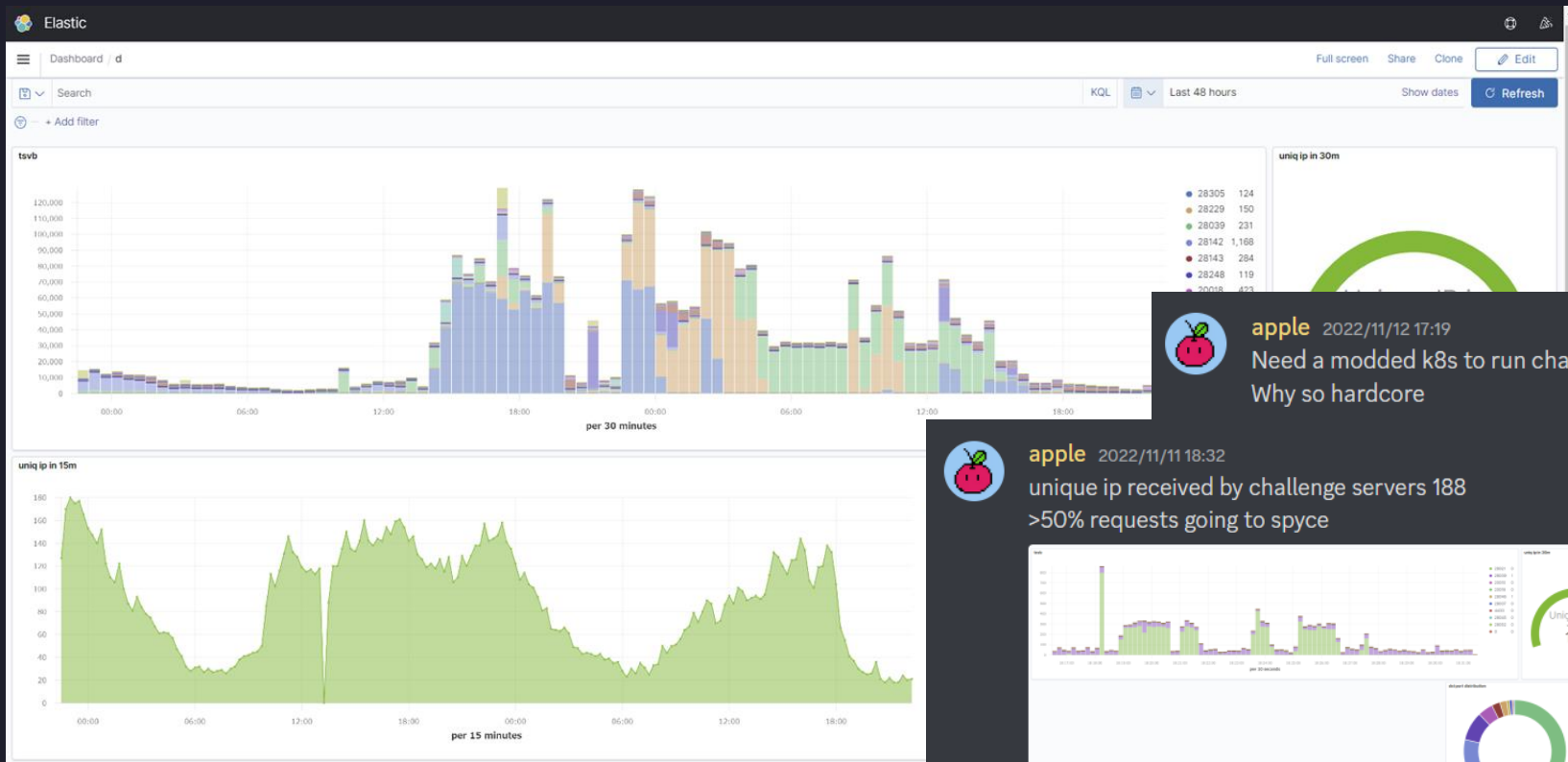
沙田大會堂  
Echo  
100 points · 20 solves · a month ago

美麗都大廈  
Spyce  
50 points · 278 solves · a month ago

米埔自然護理區  
fiddler-crab  
100 points · 22 solves · a month ago



# Setting up the infrastructure







# Managing participants and ensuring fair play

- Managing and organizing a large amount of participants can be challenging
- Require to ensure participants are following the rules of the competition and not cheating
  - difficult to monitor and enforce



# Providing adequate support and assistance

- Need help and support during the event
  - require team of volunteers or staff on hand to provide assistance
- Need to ensure that support team is knowledgeable and able to help participants



## (Recall) But wait, CTF can be ...

- Time-consuming and require a significant amount of effort and dedication
- Challenging and frustrating, especially for beginners
- Require specialized knowledge and skills that may not be applicable outside of the competition





# What could go wrong?



what is a bad CTF?



A "bad" CTF, or Capture the Flag competition, is one that is poorly designed or executed. This could include challenges that are too easy or too difficult, lack of clear instructions or rules, technical problems or errors, and other issues that make the competition less enjoyable or fair for participants. In general, a well-designed and well-run CTF competition should be challenging but fair, engaging, and provide a positive learning experience for participants.






# Bad CTF Bingo

## Bad CTF BINGO!!!!!!

Drama in the the Discord server	Solution dependent on raw manpower	>30% downtime	Prizes are delayed >1month	No source code
Solution requires \$\$\$ cloud cluster	<20 CTFtime rating	Every admin asleep	>1 OSINT challenge	Solution uses author's tool
Forgot to upload files	Fake flags	<b>FREE</b> Waste of time	Guessing	Stolen/ recycled challenges
Challenge retracted after solved	Stego	Registration closed after CTF starts	Broken reversing challenge	"Scoreboard is frozen"
Releasing hints after first solve	Blind pwn challenge	No flag format	Flags/ chals get leaked	CTF infrastructure gets hacked

### BONUS

Twitter drama after CTF 	+1
"Cyber league"	+1
Admins ban over criticism	+5





# Our Solution?

**Hand-over-hand**  
**手把手**





# Hand-over-hand (手把手)

## Must-go Scenic Spots

If you have never been to those spots, you are not allowed to tell others that you visited Hong Kong.



### Zoonn Recording

照鏡環山訊號站

55 points · 198 solves · a month ago

misc

★★★★☆



### SD Card

珍寶海鮮舫

50 points · 215 solves · a month ago

forensics

★★★★☆



### Flawed ElGamal

海山樓

50 points · 127 solves · a month ago

crypto

★★★★☆



### Back to the Past

歷史檔案館

50 points · 178 solves · a month ago

web

misc

★★★★☆



### UAF

九龍灣綜合回收中心

100 points · 18 solves · a month ago

pwn

★★★★☆



### Echo

沙田大會堂

100 points · 20 solves · a month ago

pwn

★★★★☆



### Spyce

美麗都大廈

50 points · 278 solves · a month ago

web

★★★★☆



### fiddler-crab

米埔自然護理區

100 points · 22 solves · a month ago

reverse

★★★★☆





# Hand-over-hand (手把手)

## Solution

**Note.** Copying the cookies from the write-up would not work. The encryption keys are different when I compile the write-up and for the actual challenge.

### Interacting with the browser 🍪s

If you are using Google Chrome (probably the same for the common browsers), you can press F12 to open the developer tools and switch to the "Console" tab. You can read the cookies by typing the below snippet, and execute it by pressing Enter:

```
document.cookie
```

To set a cookie (for example, setting the value of the `game-token` to `bar`), type the below snippet and press Enter:

```
document.cookie="game-token=bar"
```

That's it! You can manipulate cookies easily from your browser.

Encrypting messages of arbitrary length for block ciphers







# 手把手 (?)



harrier 2022/11/07 23:41

手把手都驚唔多人 solve 🤖



一星題唔係真係一星題㗎  
唔好信佢啊 😭😭  
有 writeup 都唔識做 😭😭😭

[Translate Tweet](#)

Nov 11

仲有幾分鐘 hkcertctf 就要開始啦!

1:30 AM · Nov 12, 2022





# One more thing...





# Surprise?



**ozeTWYta** 2022/11/12 11:04

🎉 S0080 - Lok Sin Tong Ku Chiu Man Secondary School solved 油街實現 Oi! Auction with Blockchain! - FIRST BLOOD! 🩸



1

竟然中學組做先



**Mystiz** ✓✓



2022/11/12 16:59



S0162 - CCC Kei Yuen College solved CGA 香港電競館 Minecraft Geoguessr! - FIRST BLOOD!



2

哇

癲到

