



Capture-the-Flag : an introduction

Muiz Kadir

5/11/2022

What is a Capture-the-Flag(CTF) Competition



Information Security Capture the flag (CTF) Competition

Alternative & Fun ways to learn Cybersecurity

Team-based or Individuals competition attract a diverse range of participants, including students, enthusiasts and professionals.

Aimed at helping in capacity development in the fields of Cybersecurity especially during this Post-Covid Era.

Highlights real cyber security concepts, real vulnerabilities, real techniques etc.

CYBERBATTLE; CTF in Brunei



Why participate in CTFs



IT SECURITY ANALYST

Responsibilities:

- Perform vulnerability assessment for our clients and produce the relevant reports in a timely manner.
- Assist Senior IT Security Analyst to manage assessment projects
- Keep up with the latest security and technology developments
- Research/evaluate cyber security threats and manage them
- Evaluate cyber security related products and services
- Conduct training/talks on IT Security related matters
- Provide subject matter expert assistance to relevant teams within the organization
- Assist with creation, updating and delivery of cyber security awareness training and materials
- Mentor Junior IT Security Analyst

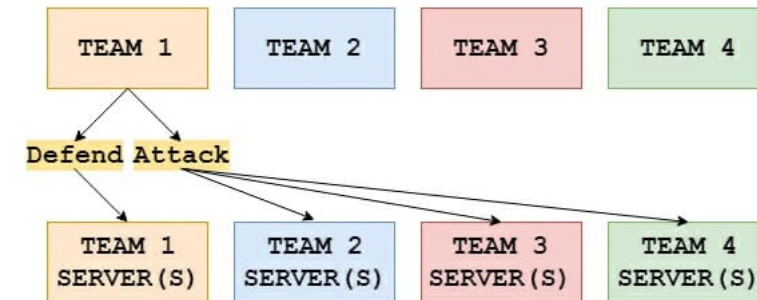
Requirements:

- Professional qualification/certifications would be an advantage
- Minimum 3 years working experience in I.T. or any experience related to I.T. security auditing would be an advantage
- Previous participation in Capture The Flag (CTF) or similar competitions would be preferred
- Experience in mobile/cellular communication protocols would be an advantage i.e. SS7 technologies
- Experience in mobile application development (Android or iOS) would be an advantage
- Experience in Internet of Things (IoT) would be advantage
- Strong interpersonal leadership and communication skills

Types of CTFs

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

Jeopardy Style



Attack and Defense

Jeopardy Style – Challenge Prompt

Challenge

0 Solves

×

Soalan - this sometimes
leaves hints
900000

This describes the challenge.

Flag

Submit

Flag Format

Flag{iamtheflag}

This is where you'd put the answer, i think...

CBCTF{Pr0Gr355N0tP3rF3C710N}

General Rules

- Do not attack other player's workstation/laptop.
- Do not share flag (answers) with other contestants during competition.
- Do not attack Score Server i.e. Denial of Service , Bruteforcing challenges.

* different CTF organizers have different set of rules



Categories

Web

Digital Forensics

Cryptography

Programming

What is Cryptography

-- --- .- .-.-. --- -.. = morsecode

F9d08276bc85d30d578e8883f3c7e843 = md5 hash

OTVhMTQ0NmE3MTIwZTRhZjVjMGM4ODc4YWJiN2U2ZDI= = base64

- Involves “breaking” or reversing encryption, ciphers or encoding
- Can either be really simple reversing base64 or something that needs some coding/scripting and deep understanding of encryption algorithms
- Few examples: XOR, Caesar’s Cipher, Substitution Cipher, Vigenere Cipher, Hashing Functions(MD5, SHA256), Block Ciphers, Stream Ciphers, RSA, Base64, Base32
- Tools of the trade: Cyberchef, dcode.fr, python or any scripting languages
- For this CTF Cyberchef would be the ultimate tool
- <https://gchq.github.io/CyberChef/>

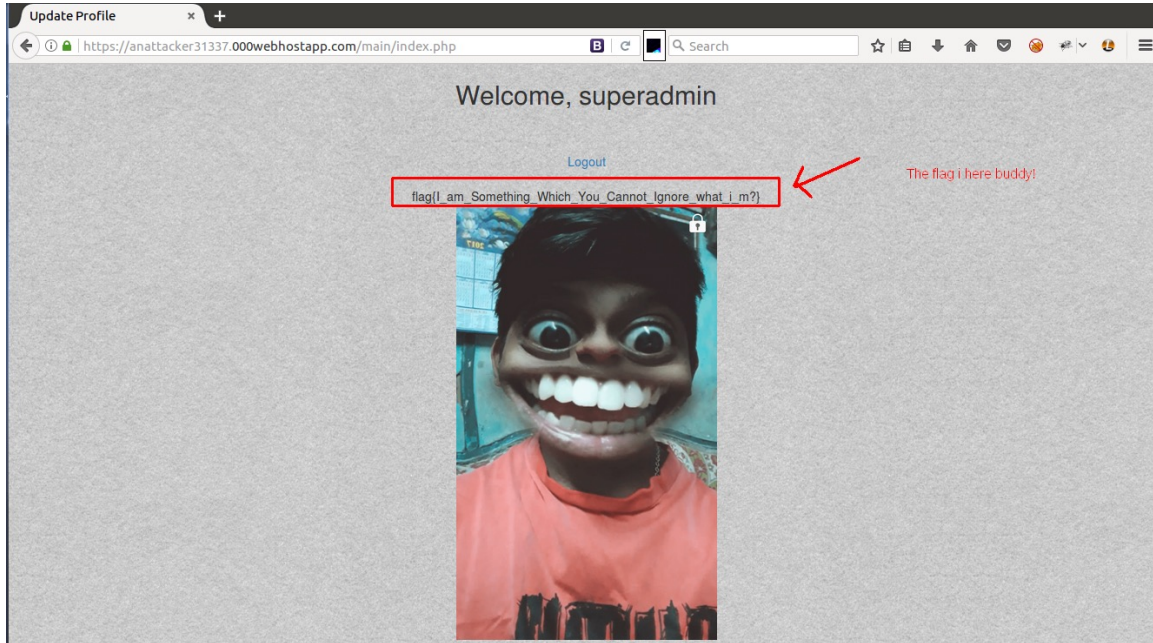


What is Digital Forensics

- Involves file format analysis, steganography, memory dump analysis, or analyzing metadata
- Varies from real life scenarios and game like challenges
- Any challenge to examine and process a hidden piece of information out of static data files
- Tools of the trade: online exif tools, autopsy, binwalk, pic2map(for location of photo), volatility, stegsolve, steghide and many more
- For this CTF we're focusing on using things we can google, online tools

```
root@kali2:/mnt/hgfs/VM_FileShare# volatility -f mem.data --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)      Name      PID      PPID     Thds     Hnds     Sess     Wow64     Start
-----
0xffffffff80003a5040 System    4         0       108      373      ----- 0 2018-11-07 08:12:31 UTC+0000
0xffffffff80010729d0 smss.exe  276        4         2        32      ----- 0 2018-11-07 08:12:31 UTC+0000
0xffffffff8001ee7060 csrss.exe 364       344        9       462      0 0 2018-11-07 08:12:33 UTC+0000
0xffffffff8001fe2060 wininit.exe 416       344        3        81      0 0 2018-11-07 08:12:33 UTC+0000
0xffffffff8001fe1060 csrss.exe 424       408       11       197      1 0 2018-11-07 08:12:33 UTC+0000
0xffffffff800261eb30 services.exe 472       416        9       230      0 0 2018-11-07 08:12:33 UTC+0000
0xffffffff8002638670 winlogon.exe 504       408        3       114      1 0 2018-11-07 08:12:33 UTC+0000
0xffffffff800263cb30 lsass.exe 516       416        8       560      0 0 2018-11-07 08:12:33 UTC+0000
0xffffffff8002640880 lsm.exe 524       416        9       145      0 0 2018-11-07 08:12:33 UTC+0000
0xffffffff80026fdb30 svchost.exe 648       472       11       366      0 0 2018-11-07 08:12:35 UTC+0000
0xffffffff800272ab30 vmacthlp.exe 704       472        3        60      0 0 2018-11-07 08:12:35 UTC+0000
0xffffffff8002725b30 svchost.exe 748       472        7       279      0 0 2018-11-07 08:12:35 UTC+0000
0xffffffff8002780b30 svchost.exe 844       472       22       505      0 0 2018-11-07 08:12:35 UTC+0000
0xffffffff80026deb30 svchost.exe 884       472       11       298      0 0 2018-11-07 08:12:36 UTC+0000
0xffffffff80027cab30 svchost.exe 912       472       33       909      0 0 2018-11-07 08:12:36 UTC+0000
0xffffffff8002c02b30 audiodg.exe 1000      844        8       143      0 0 2018-11-07 08:12:36 UTC+0000
0xffffffff8002c169e0 svchost.exe 288       472       20       776      0 0 2018-11-07 08:12:36 UTC+0000
0xffffffff8002c3eb30 svchost.exe 520       472       17       374      0 0 2018-11-07 08:12:37 UTC+0000
0xffffffff80026f8340 spoolsv.exe 1096      472       13       320      0 0 2018-11-07 08:12:37 UTC+0000
0xffffffff8002760060 svchost.exe 1124      472       18       306      0 0 2018-11-07 08:12:37 UTC+0000
0xffffffff800271e060 VGAuthService.exe 1300      472        3        91      0 0 2018-11-07 08:12:37 UTC+0000
0xffffffff8002c62060 vmtoolsd.exe 1356      472        9       225      0 0 2018-11-07 08:12:37 UTC+0000
0xffffffff8001cabb30 taskhost.exe 1452      472       10       208      1 0 2018-11-07 08:12:37 UTC+0000
0xffffffff8001d21b30 dwm.exe 1628      884        3        84      1 0 2018-11-07 08:12:38 UTC+0000
0xffffffff8001d64b30 explorer.exe 1696     1548       20       661      1 0 2018-11-07 08:12:38 UTC+0000
0xffffffff8002d0cb30 vmtoolsd.exe 2028     1696        9       199      1 0 2018-11-07 08:12:39 UTC+0000
0xffffffff8002d42570 WmiPrvSE.exe 1392      648       10       218      0 0 2018-11-07 08:12:40 UTC+0000
0xffffffff8002d53630 dllhost.exe 1716      472       13       204      0 0 2018-11-07 08:12:40 UTC+0000
0xffffffff8002775b30 msdtc.exe 2236      472       12       150      0 0 2018-11-07 08:12:42 UTC+0000
0xffffffff8002de3b30 SearchIndexer.exe 2476      472       13       538      0 0 2018-11-07 08:12:46 UTC+0000
0xffffffff8003297b30 svchost.exe 2568      472       15       260      0 0 2018-11-07 08:12:46 UTC+0000
0xffffffff8003303630 wmpnetwk.exe 2724      472       10       212      0 0 2018-11-07 08:12:47 UTC+0000
0xffffffff8002cab800 WmiPrvSE.exe 3052      648        8       281      0 0 2018-11-07 08:12:59 UTC+0000
0xffffffff8001cfab30 WmiApSrv.exe 1228      472        4       115      0 0 2018-11-07 08:13:05 UTC+0000
0xffffffff8003303060 sppsvc.exe 1040      472        4       150      0 0 2018-11-07 08:14:39 UTC+0000
0xffffffff8003323060 svchost.exe 1376      472       13       365      0 0 2018-11-07 08:14:39 UTC+0000
0xffffffff8003344390 wordpad.exe 1804     1696        3       120      1 0 2018-11-07 08:15:35 UTC+0000
0xffffffff8000d9ab30 Minesweeper.exe 312      1696        9       208      1 0 2018-11-07 08:15:39 UTC+0000
0xffffffff8002de1560 mspaint.exe 2768     1696        6       122      1 0 2018-11-07 08:16:05 UTC+0000
0xffffffff8000e07470 svchost.exe 2472      472        6       104      0 0 2018-11-07 08:16:06 UTC+0000
0xffffffff8000cfab30 cmd.exe 2824     1356        0       ----- 0 0 2018-11-07 08:26:51 UTC+0000
0xffffffff8002d68060 conhost.exe 2932      364        0        28      0 0 2018-11-07 08:26:51 UTC+0000
```

What is Web



- Involves interpreting, finding vulnerabilities and exploiting a web application
- By exploiting the web application it will reveal the flag
- Common vulnerabilities include, SQL Injection, SSRF, XSS, Cookie Tampering, and others on the OWASP Top 10
- Tools of the Trade: Burp Suite, browser's built in web developer tools, BeeF, SQLMap
- FOR THIS CTF WE'RE ONLY USING BROWSER'S BUILT IN WEB DEVELOPER TOOLS
- Important link: <https://nira.com/chrome-developer-tools/>
- With web developer tools; you can manipulate cookies, read source code, and manipulate javascript
 - CTRL-U to open source code view
 - Right-Click > Inspect tools to open developer tools

What is Programming



The image shows a screenshot of a Python 3.8.5 Shell window. The window has a title bar that says "Python 3.8.5 Shell" and standard window controls (minimize, maximize, close). Below the title bar is a menu bar with options: File, Edit, Shell, Debug, Options, Window, and Help. The main area of the window is a text editor with a light gray background. It contains the following text: "Type 'help', 'copyright', 'credits' or 'license()' for more information." followed by a prompt ">>>" and the command "print('Hello, World!')". The output "Hello, World!" is displayed below the command. The prompt ">>>" is followed by a vertical cursor. At the bottom right of the window, the status bar shows "Ln: 5 Col: 4".

```
Python 3.8.5 Shell
File Edit Shell Debug Options Window Help
Type "help", "copyright", "credits" or "license()" for more information.
>>> print('Hello, World!')
Hello, World!
>>> |
```

Ln: 5 Col: 4

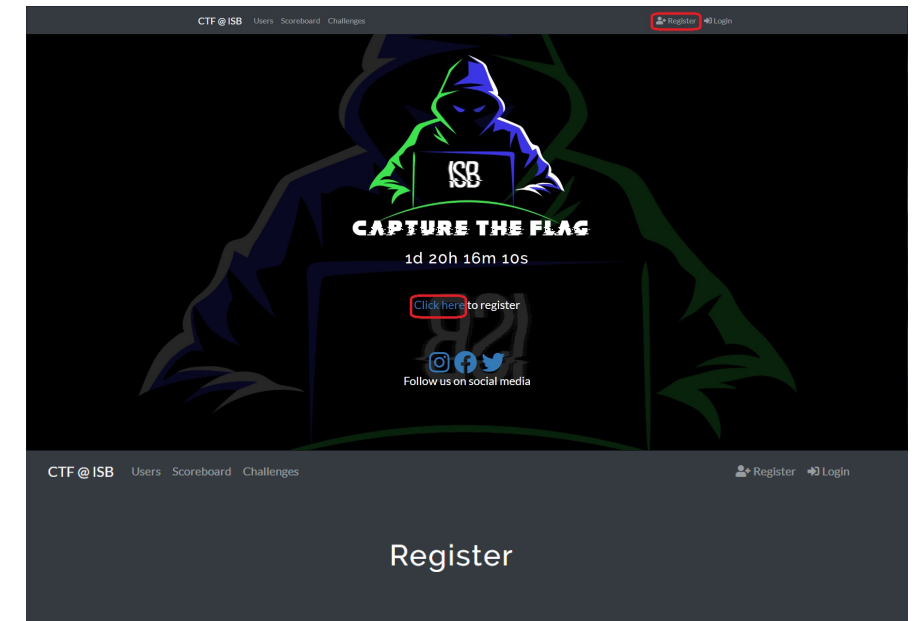
- Solving challenges by coding
- <https://www.codingrooms.com/compiler/python3>

Other Categories – not covered here

- Network
- Reverse Engineering
- Binary Exploitation
- Open-Source Intelligence

How to register yourself

- Go to <http://isb.cyberbattlefinals.xyz>
- Then click on register or click here button. Fill in all form and click submit
- FYI, You can pick any pseudonym u want. As long as it does not contain any vulgar words.



User Name

Your username on the site

Email

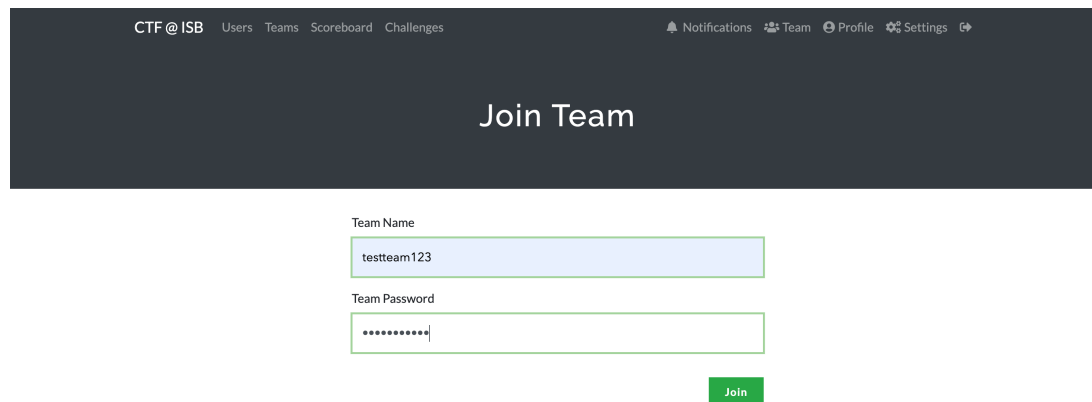
Never shown to the public

Password

Password used to log into your account

How to create teams

- Only one person in the team will need to do this
- Click the "Create teams" button
- Fill in the details, make sure the password is easily sharable with your teammates



The screenshot shows the 'Join Team' page of the CTF@ISB application. The page has a dark header with navigation links: CTF@ISB, Users, Teams, Scoreboard, Challenges, Notifications, Team, Profile, Settings, and a help icon. The main heading is 'Join Team'. Below it, there are two input fields: 'Team Name' with the value 'testteam123' and 'Team Password' with masked characters. A green 'Join' button is at the bottom right.

CTF@ISB Users Teams Scoreboard Challenges Notifications Team Profile Settings

Join Team

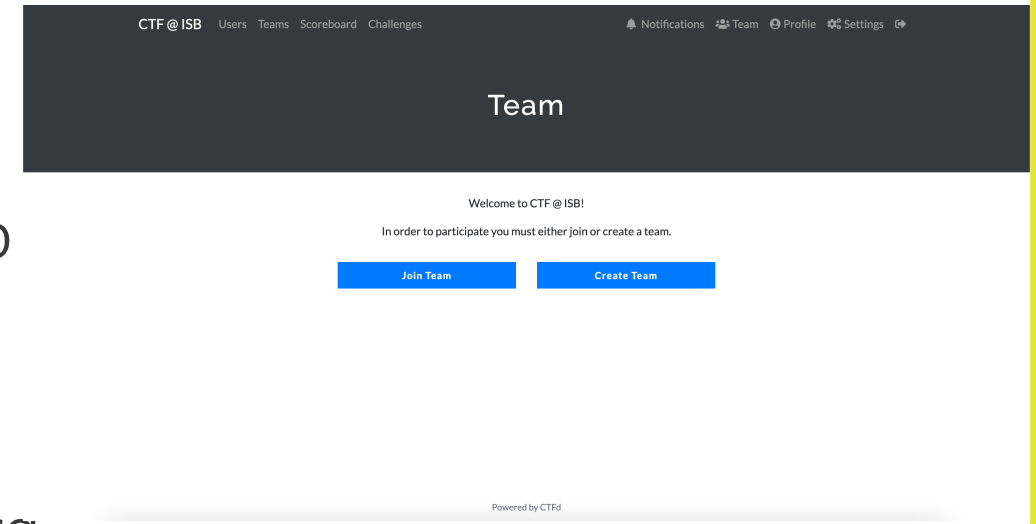
Team Name

testteam123

Team Password

.....

Join



The screenshot shows the 'Team' page of the CTF@ISB application. The page has a dark header with navigation links: CTF@ISB, Users, Teams, Scoreboard, Challenges, Notifications, Team, Profile, Settings, and a help icon. The main heading is 'Team'. Below it, there is a welcome message: 'Welcome to CTF@ISB! In order to participate you must either join or create a team.' There are two blue buttons: 'Join Team' and 'Create Team'. At the bottom, there is a footer: 'Powered by CTFd'.

CTF@ISB Users Teams Scoreboard Challenges Notifications Team Profile Settings

Team

Welcome to CTF@ISB!

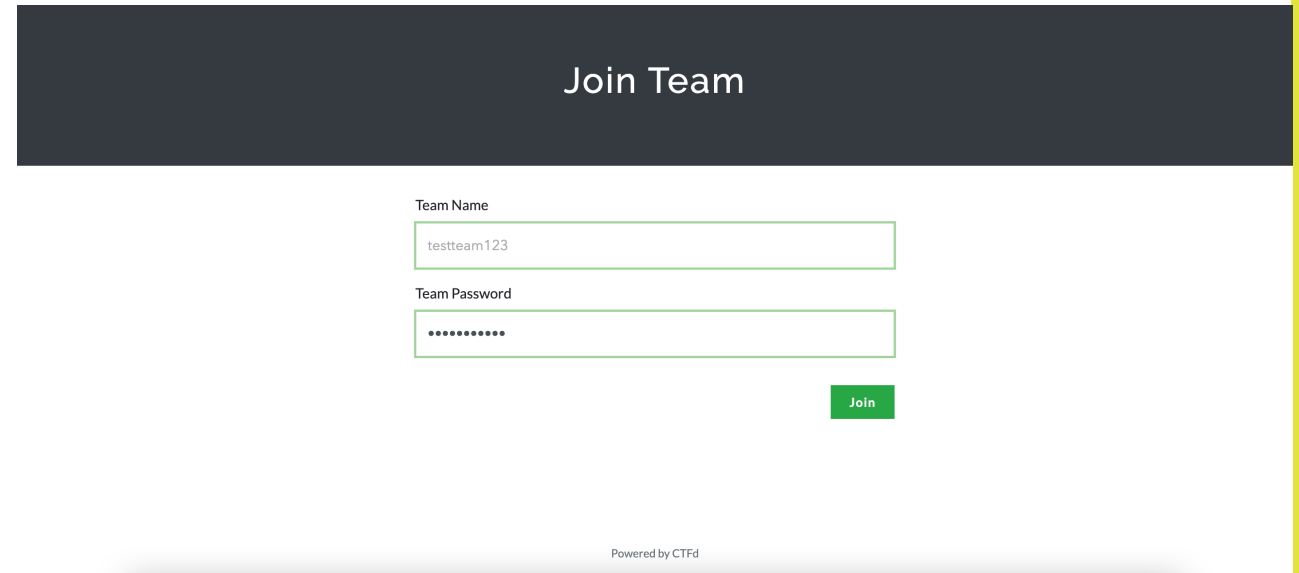
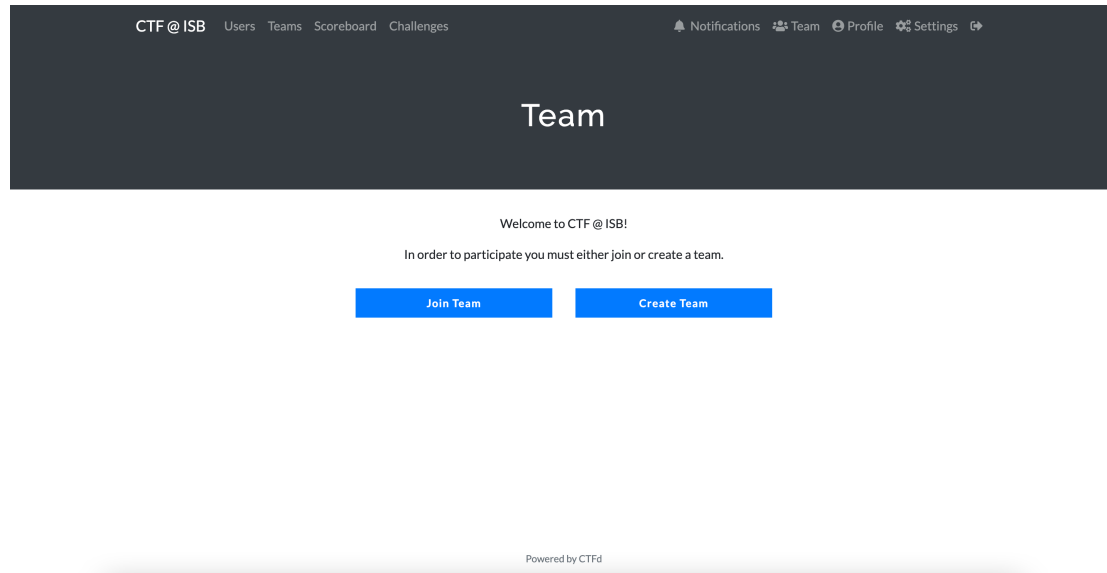
In order to participate you must either join or create a team.

Join Team Create Team

Powered by CTFd



How to create teams



How to submit flags

Challenge

1 Solves

×

saucy
50

[link](#)

Find the flag

Flag

Submit

Correct

Challenge

0 Solves

×

saucy
50

[link](#)

Find the flag

CBCTF{WrongFlag}

Submit

Incorrect

How to do well in CTF competition

- Google is always your friend
- Pay attention to the challenge prompt and challenge names, they always leave clues
- Time-boxing, if you're stuck move on to other challenges

... More online practice for CTFs

CTFTime, general CTF site, can see upcoming CTFs

Cryptopals, for cryptography

Exploit.education, for binary and reversing challenges

Crackmes

Burp suite academy

PicoCTF

HackTheBox

TryHackMe

Vulnhub

Google Beginner's Quest

Read writeups on github/online

And many more

Thanks & GLHF



IT Protective Security Services Sdn Bhd

Simpang 69, Jalan E-Kerajaan

Gadong BE1110, Brunei Darussalam

T (673) 245 8000

F (673) 245 6211

E gen.inquiries@itpss.com

www.itpss.com