BEGINNER'S GUIDE TO

Hardware in Capture The Flag

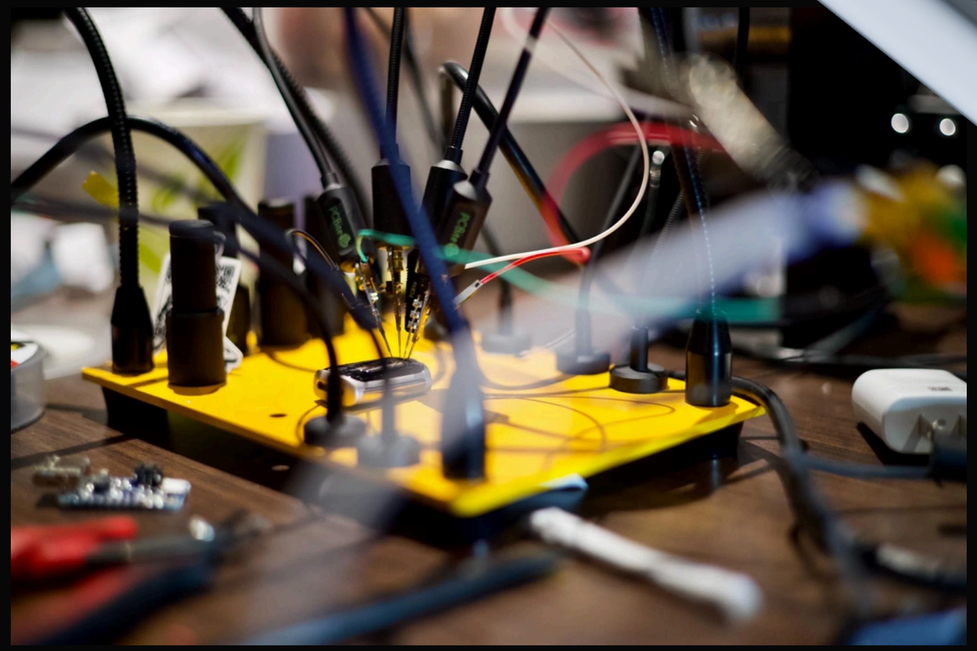
Cyber Skills Level-Up! @ UPM

Overview

Key topics covered
in this presentation

- Introduction to Hardware CTF
- Learn how to interact with ESP32
- Solve practical challenges using ESP32
- Win a prize :)

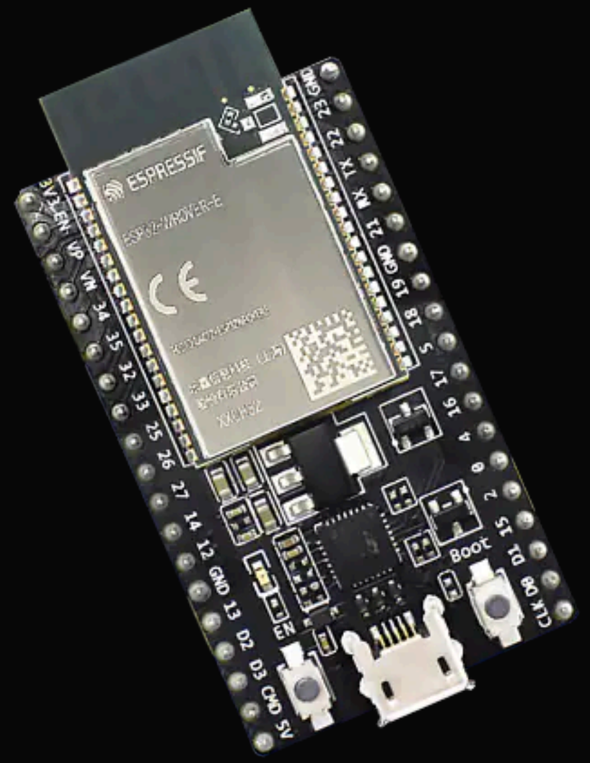
What is Hardware CTF?



Hardware CTF focuses on devices like microcontrollers, embedded systems, and IoT devices.

Introduction to ESP32

Powerful, low-cost microcontroller with Wi-Fi and Bluetooth capabilities.



It is widely used in IoT projects and hardware hacking.

Features: Dual-core processor, built-in Wi-Fi, Bluetooth (classic & BLE).

How the CTF challenge work?

STEP 1

Work with 3 participants.

Share and take turns to use them

STEP 2

Interact with ESP32 devices to solve challenges

STEP 3

Each challenge will involve different concepts.

STEP 4

Write the code in your Arduino IDE

Get them from my Github

STEP 5

Retrieve the flag from each challenge

#1 Wi-Fi Setup and Scan

- Objective: Configure ESP32 as a Wi-Fi access point and scan for nearby networks.
- Instructions: Participants will find hidden flags by scanning the network.
- Key Learning: Basic Wi-Fi interaction and ESP32 networking capabilities.

Code Example

```
WiFi.softAP("CTF_AP", "password123");

WiFi.scanNetworks();
```

#2 Serial Communication

- Objective: Interact with the ESP32 using UART to retrieve the flag.
- Instructions: Connect to the ESP32 via USB and use a terminal program to communicate.
- Key Learning: Understanding UART communication and how to send/receive data.

Code Example

```
Serial.begin(115200);
while (!Serial) { delay(10); }
Serial.println("Send the correct command to receive
the flag!");
if (Serial.available()) {
  String input = Serial.readString();
  if (input == "give_flag") {
    Serial.println("Congrats! Your flag is:
CTF{uart_flag}");
  }
}
```

#3 Hidden Files in SPIFFS

- Objective: Retrieve a hidden file from the ESP32’s file system (SPIFFS).
- Instructions: Participants will explore the ESP32 file system to find a flag hidden in a text file.
- Key Learning: File handling on embedded devices.

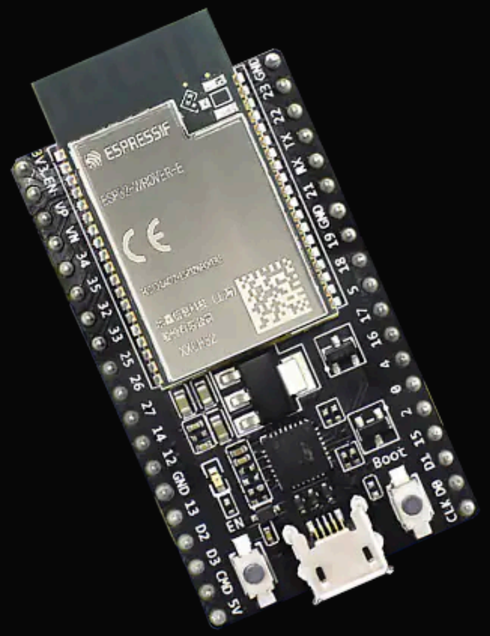
Code Example

```
File file = SPIFFS.open("/flag.txt", FILE_WRITE);

file.println("Congrats! Your flag is:

CTF{SPIFFS_is_awesome}");
```

Summary and Closing Remarks

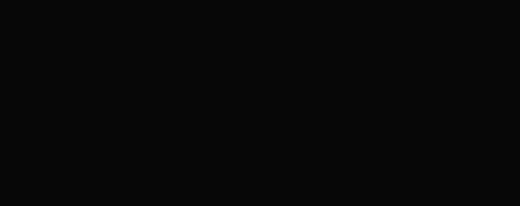


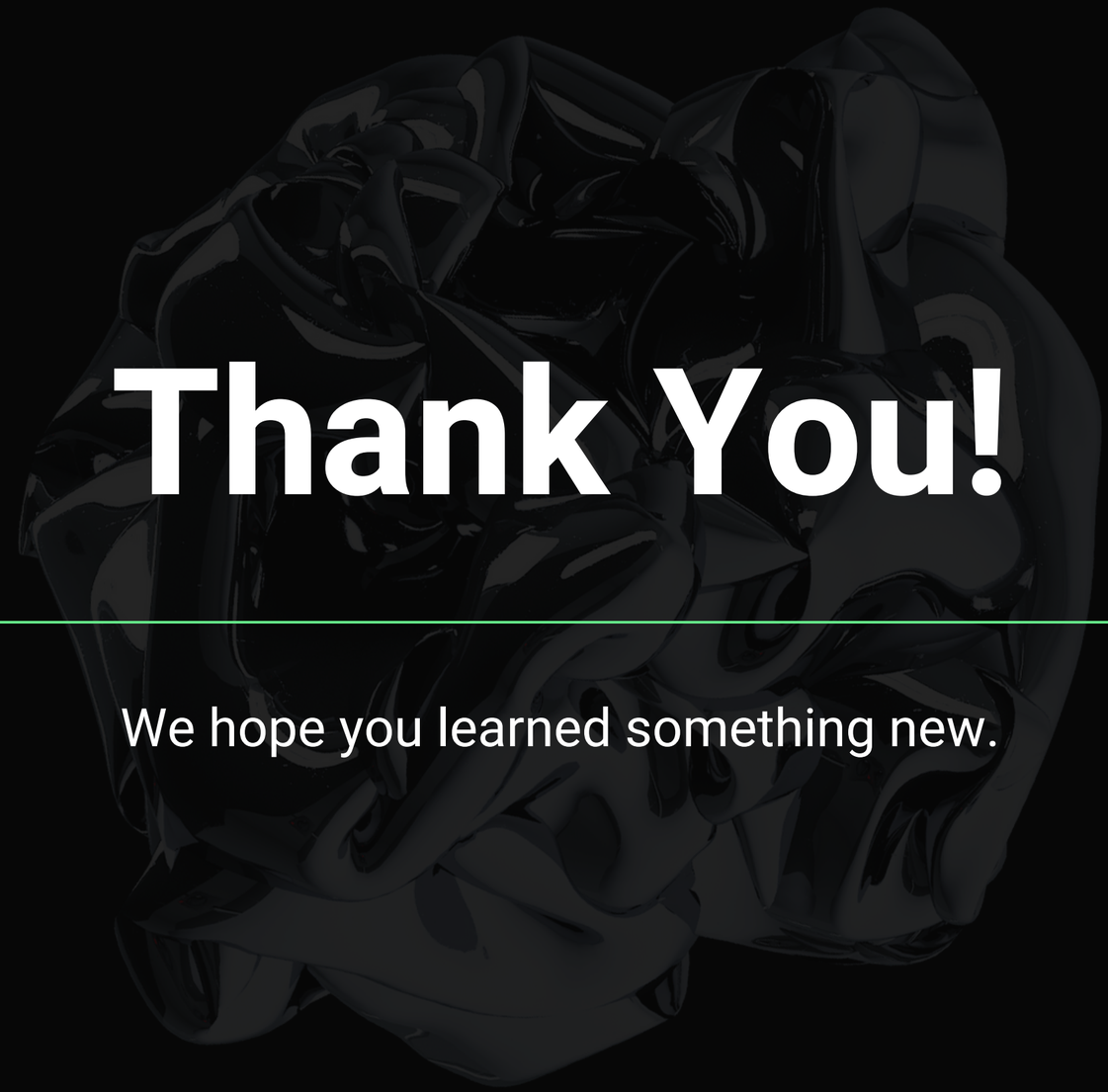
CHECKLIST	
✓	Understanding ESP32
✓	Arduino IDE
✓	Wi-Fi Setup and Scan
✓	UART Communication
✓	Hidden Files in SPIFFS

Are you ready for the challenge?

First 2 participant to successfully retrieve the flag wins a prize!

Connect to CTF_ESP32_Challenge with password123 and look for the flag!





Thank You!

We hope you learned something new.