ACES TECHFEST 5.0

CAPTURE THE FLAG RULEBOOK

OVERVIEW

CTF is a competition in which participants need to find Flags which are secretly hidden in purposefully-vulnerable programs or websites.
Each Challenge will have Points based on their complexity. The participant having the maximum number of Points at the end of competition will be declared as the winner.

EVENT INFO

Event Schedule

- Poush 5

ENTRY FEE

Rs. 20 per participants(non-refundable)
Entry fee payment must be done through our payment partner *(MyPay)*:
Link : **ACES Techfest 5.0 – Registration Form (mypay.com.np)**

Scan to visit our website

EVENT DESCRIPTION

FLAG FORMAT

- Every flag will be in the format ACESCtf{xxxxxxxxxxxxxxx} if not specified otherwise.

CTF FLAGS TYPES

- **Web Exploitation**: In this category, competitors will try to exploit vulnerabilities in web based applications to get access to the flag.
- **Forensics:** Forensics is the art of recovering the digital trail left on a computer. Competitors will have to find data which is hidden, not stored, or covertly recorded.
- **Reverse Engineering:** Reverse Engineering in a CTF is typically the process of taking a compiled program and converting it back into a human readable format to get a flag.
- **Cryptography:** In this category, competitors will try to break widely used encryption schemes which are improperly implemented.
- **OSINT:** OSINT, also known as Open Source Intelligence, refers to gathering of information from publicly available resources, such as social media. Competitors will collect and exploit publicly available information to access the flag.

Note: Any technical difficulties faced by the participants is not a liability of the organizers and no refund shall be made. The committee has the right to ban any participant in case of any suspicious activity or malicious intent.