RULES AND REGULATIONS

PRAYAG'25

CAPTURE THE FLAG

General Information

- Event Name: Prayag CTF 2025
- Format: Jeopardy-Style, On-site
- Team Size: 1-3 members.
- Eligibility: Open to all ASIET students.
- Communication: All official announcements will be made by the organizers at the event venue and through the Official Whatsapp Group

Code of Conduct & Ethics

1. Respect for All: All participants, organizers, and volunteers are expected to treat each other with respect. Harassment, discrimination, or any form of disruptive behaviour will not be tolerated and will result in immediate disqualification.
2. Spirit of the Game: The primary goal is to learn and have fun. Compete ethically and with integrity.
3. Organizer's Authority: The decisions of the CTF organizers are final. This includes rule interpretations, scoring, and disqualifications.

Scoring & Flags

1. Static Scoring: Each challenge has a fixed, predetermined point value. Points are awarded upon the successful submission of the correct flag. The team with the most points at the end of the competition wins.
2. Flag Format: All flags are case-sensitive and must be submitted in the following format: flag{content}. For example: flag{th1s_1s_a_s4mpl3_fl4g}. Any other format will be rejected.
3. Submission: Flags must be submitted on the official CTF platform to earn points.

Rules of Engagement: What is NOT Allowed

Violation of any of these rules is a serious offense and will lead to immediate disqualification of the entire team. We have a zero-tolerance policy for cheating.

1. No Attacking the Infrastructure: You are forbidden from attacking the scoring server, the submission platform, or any other infrastructure not explicitly designated as a target for a challenge. This includes, but is not limited to:
    - Denial of Service (DoS / DDoS) attacks.
    - Scanning the competition infrastructure for vulnerabilities.
    - Attempting to gain unauthorized access to the scoreboard or other teams' accounts.
2. Attack Targets Only: Only perform attacks on the machines, applications, or services specified in the challenge descriptions. Attacking any other IP address or domain is strictly prohibited.
3. No Sharing Flags or Hints: Sharing flags, hints, or detailed write-ups with other teams is strictly forbidden. All work must be your team's own.
4. No Sabotage: Intentionally disrupting a challenge to prevent other teams from solving it is considered sabotage and is grounds for immediate disqualification. This includes altering flags, deleting files, or crashing services on a shared challenge instance.
5. No Brute-Forcing Submissions: Do not use automated tools to brute-force the flag submission form on the platform. This generates unnecessary traffic and may be flagged as an attack on the infrastructure.
6. No Inter-Team Collaboration: Each team must work independently. Collaboration between different teams is not allowed

Systems & Allowed Tools

- Provided Systems: Each team will be provided with a system running Ubuntu. These systems come pre-loaded with a variety of common open-source tools to help you get started immediately.
- Use of Tools: You are free to use the pre-installed tools. You also have permission to install any additional software or tools you require to solve the challenges. The use of any tool (e.g., Wireshark, Burp Suite, Ghidra) is permitted, provided it does not violate any of the rules outlined in Section 4.
- Internet Access: Using the internet for research and reference is encouraged.Scripting: Writing your own scripts to solve challenges is permitted and encouraged.

Challenge Categories

The competition will feature challenges from the following domains. Be prepared for a wide range of difficulties.

- Web Exploitation: Find and exploit vulnerabilities in web applications.
- Cryptography: Decrypt messages and break ciphers.
- Reverse Engineering: Analyze compiled binaries to understand their functionality and find hidden flags.
- Open-Source Intelligence (OSINT): Gather information from publicly available sources to uncover flags.
- Steganography: Find information hidden within other files, such as images or audio tracks.
- Networking: Analyze network traffic and protocols to extract information.
- And More...

(OPEN TO ADISHANKARA STUDENTS ONLY)

COORDINATORS:
MAHESWAR : 7736903562
RODIC : 81295 37717