CYBER SECURITY CLUB

PRESENTS

ROOTBREACH

CAPTURE THE FLAG

28th - 29th March, 2026
9 AM Onwards

PRIZE POOL WORTH

RS. 10,00,000+

REGISTRATION FEE
RS. 300 PER
TEAM ONLY

Venue: Central Seminar Hall (Opening)
IT Building (Competition)

Contact for any query:
Vikash Kushwah (Coordinator): 9644919251
Mohit Gangwar (PR Head): 9068171368

EVENT DESCRIPTION

OVERVIEW

ROOTBREACH: Capture The Flag is a nationwide Capture The Flag (CTF) competition designed to challenge and enhance cybersecurity skills among students across India. Organized by the Cyber Security Club, this event aims to bring together aspiring ethical hackers, developers, and security enthusiasts to compete in a dynamic and intellectually stimulating environment.

The competition covers multiple domains including:

- **Cryptography:** Crack encryption and uncover hidden messages.
- **Reverse Engineering:** Analyze binaries to reveal concealed logic.
- **Digital Forensics:** Extract crucial evidence from digital artifacts.
- **Binary Exploitation (Pwn):** Exploit low-level program vulnerabilities.
- **OSINT:** Gather intelligence from publicly available sources.
- **Miscellaneous:** Logic, scripting, and unconventional security challenges.

Participants will compete in a controlled environment under strict ethical guidelines. The scoring system is designed to reward accuracy, strategic thinking, efficiency, and effective time management.

This competition is structured to test not just technical knowledge, but also analytical thinking, teamwork, and problem-solving under pressure.

EVENT DESCRIPTION

STRUCTURE

ROOTBREACH features five competitive stages divided into two phases, conducted in a hybrid format—online (for external participants) and offline. Each stage contributes to the final cumulative score, ensuring a comprehensive evaluation of both technical and practical cybersecurity skills.

Phase 1: Infiltration Phase

Stage 1: CodeIgnite

Participants solve problem-solving and security-based challenges, testing logical reasoning and coding fundamentals.

Stage 2: FlagForge

A fixed-scoring challenge round across multiple cybersecurity domains, focusing on technical accuracy and understanding.

Phase 2: Domination Phase

Stage 3: SpeedBreach

A fast-paced round with dynamic scoring that rewards speed and effective problem-solving.

Stage 4: VulnHunt

Teams analyze a deliberately vulnerable application to identify and document security flaws, simulating real-world penetration testing scenarios.

Stage 5: SecureShield

Participants patch and secure identified vulnerabilities, demonstrating defensive expertise, secure coding practices, and effective remediation strategies.

EVENT RULES AND GUIDELINES

THE RULES OF ENGAGEMENT

Team Formation

- Maximum 5 participants per team (individual entry is allowed).
- Each participant can only belong to one team.

Flag Format

- All flags follow the standard format: CSC{flag_h3r3} unless stated otherwise.

Zero Tolerance (Instant DQ)

- No Attacking Infrastructure: Attacking the scoring server or the CTF platform is strictly prohibited.
- No Brute Forcing: Do not use automated tools on submission boxes.
- No Collaboration: Sharing flags, hints, or write-ups between teams is forbidden.
- No DoS: Any attempt to crash a challenge or deny service to others will result in immediate disqualification.

Scoring Logic

- Points are awarded based on challenge difficulty and performance.
- In case of a tie, the team that reaches the final score earlier will be ranked higher.
- At least two of the top three teams must be from the offline mode.

EVENT RULES AND GUIDELINES

PARTICIPANT CHECKLIST

Hardware Requirements

- Laptop: Minimum 8GB RAM & 50GB Free Space
- Power: Bring your own laptop charger (and a power strip if possible).

Software Toolkit

- Operating System: Kali Linux or Parrot OS (running on VirtualBox/VMware).
- Misc: Python 3 (with pwntools).

Essentials

- Valid College ID: Required for entry and prize claiming.
- Registration ID: Keep your confirmation email or receipt handy.