- ❖ Event: ShellSeekers

  A Capture the Flag (CTF) event in cybersecurity is a professional and engaging competition designed to assess and enhance participants' skills in various aspects of information security. This gamified exercise typically involves participants solving a series of challenges that mimic real-world security scenarios to demonstrate their proficiency in offensive and defensive techniques.

- ❖ Participants: Solo
- ❖ Venue: D-Block
- ❖ Fees: ₹30/-
- ❖ Main Co-ordinator: Meet Katarmal, Karan Bharda
- ❖ Faculty: Dr Leena Patel
- ❖ Rules & Regulations:

  - All attendees must maintain respectful and professional behavior throughout the duration of the event.
  - Organizers retain the authority to disqualify any attendee found in breach of event rules or engaging in disruptive conduct.
  - Time constraints: Participants must adhere to strict time limits for responses.
  - Students are permitted to bring their laptops.
  - Utilization of only the official channels provided by the organizers is mandatory for submitting flags or engaging with the competition infrastructure.
  - Unauthorized interaction with challenges, including attempts to disrupt or exploit them beyond defined parameters, is strictly prohibited.
  - Participants are prohibited from sharing flags or solutions with teams that have not yet solved a specific challenge.

- Any participant found cheating will face immediate disqualification from the competition.
- The use of automation tools like nuclei is strictly prohibited. Violators will be disqualified immediately upon detection.
- The scoring system and criteria for ranking participants or teams are typically clearly outlined by the organizers.
- **Judges' decisions are considered final.**

❖ Rounds:

- ROUND 1 (Qualifier Round):

  Participants are required to solve all the given problems within the designated time to qualify for the next round.

- ROUND 2 (Final Round):

  Qualified participants will receive a vulnerable machine and must identify bugs within it, providing proof of concept (POC) for each. Duplicates are not allowed; if another participant discovers a bug or vulnerability before you, credit will be given to them.

  Scoring System:

  - P1: 500 points
  - P2: 250 points
  - P3: 100 points
  - P4: 50 points
  - P5: No points awarded