RULE BOOK version 1.0

CONTENT

1. Event Overview

About Breach Point CTF

Breach Point is a **24-Hour National Level Capture The Flag (CTF) competition** designed to assess participants' practical knowledge and hands-on skills in cybersecurity. The event simulates real-world security scenarios where participants are required to analyze systems, identify vulnerabilities, and extract flags within defined ethical and technical boundaries.

The competition focuses on **problem-solving, analytical thinking, and time-bound decision making** across multiple domains of cybersecurity. Participants will be challenged to think like attackers while maintaining professional and ethical standards expected in real-world security environments.

Breach Point CTF is organized by the **Department of Cyber Security, School of Engineering, Malla Reddy University**, with the objective of providing students a national-level platform to apply theoretical concepts to practical cybersecurity challenges

Objectives of the Competition

The key objectives of Breach Point CTF are to:

- Promote hands-on learning through practical cybersecurity challenges
- Enhance analytical and critical thinking skills
- Encourage ethical hacking practices
- Provide national-level exposure to cybersecurity enthusiasts
- Foster teamwork, adaptability, and strategic thinking under pressure

Target Audience

Breach Point CTF is open to:

- Undergraduate and postgraduate students from all institutions
- Cybersecurity enthusiasts seeking real-world CTF experience
- Beginners and intermediate participants interested in competitive cybersecurity

Participation is subject to the eligibility and team formation rules defined in this rule book.

2. Theme Philosophy – Siege of Troy

Concept Behind the Theme

The theme ***Siege of Troy*** is inspired by one of history's most well-known examples of strategic deception and exploitation of trust. The fall of Troy was not the result of direct force alone, but of careful planning, psychological manipulation, and the successful concealment of an attack within something perceived as safe.

In cybersecurity, many successful breaches follow the same pattern. Systems are rarely compromised by brute-force attacks alone; instead, attackers exploit **assumptions, overlooked vulnerabilities, and misplaced trust**.

Relevance to Cybersecurity

The Trojan Horse symbolizes how trust can become a vulnerability when not properly verified. Modern cyber-attacks such as malware delivery, social engineering, and logic-based exploits often rely on similar principles.

By adopting the ***Siege of Troy*** theme, Breach Point CTF emphasizes the importance of:

- Thinking beyond surface-level defenses
- Questioning assumptions within systems
- Understanding attacker mindset
- Identifying hidden or non-obvious vulnerabilities

Theme Message

"Trust Was the Vulnerability."

This message reflects the core philosophy of the competition: strong systems fail not only because of weak defenses, but because of unverified trust.

Participants are encouraged to approach every challenge with curiosity, caution, and critical reasoning skills that are essential for cybersecurity professionals.

3. Eligibility & Team Formation

Eligibility

- The competition is **open to all**
- Participants must be currently enrolled in a recognized educational institution.
- Students from all academic disciplines are eligible to participate.

Team Formation Rules

- Participants must register as a **team consisting of 1 to 3 members**.
- Each participant may be part of **only one team** throughout the competition.
- Teams may consist of members from the same institution or different institutions.
- Team composition cannot be changed after successful registration.

Team Identification

- Each team must choose a **unique team name** at the time of registration.
- The **same team name must be used consistently** across all platforms, including **HackCulture** and the **CTF platform**.

4. Registration & Fees

Registration Process

- All participants must complete the registration through the **official registration portal**.
- Registration shall be considered **valid only after successful payment**.
- Each team must ensure that all registration details provided are accurate and complete.

Registration Fee

- The **registration fee is ₹250 per team**, irrespective of whether the team consists of 1, 2, or 3 members.
- The registration fee is **non-refundable under any circumstances**.

Platform Consistency

- Teams are required to use the **same team name** across all competition platforms, including **HackCulture** and the **Only CTF platform**.
- Any mismatch in team names across platforms may lead to disqualification or restricted access to the competition.

Confirmation of Registration

- A team will be considered successfully registered **only after payment confirmation**.
- Further event-related communications will be shared with registered teams through official channels.

5. Event Structure & Format

Breach Point CTF will be conducted in **two stages**: an **Online Round** followed by an **Offline Round**.

Online Round

- The online round will be conducted on **14th and 15th February**.
- The competition will follow a **Jeopardy-style Capture The Flag (CTF) format**, where teams solve independent challenges across multiple cybersecurity domains.
- Teams may attempt challenges in any order unless specified otherwise.
- Based on the online round leaderboard, the **top 70 teams** will be shortlisted for the next stage.
- Shortlisted teams must submit **detailed write-ups** for the challenges they have solved.

Offline Round

- From the submitted write-ups, the **top 50 teams** will qualify for the offline round.
- The offline round will be conducted on **6th and 7th March**.
- This round will be **theme-based**, inspired by the *Siege of Troy* theme.
- Challenges in the offline round will be **narrative-driven and scenario-based**, designed to test advanced problem-solving and analytical skills.
- Further instructions regarding the offline round, including venue and challenge format, will be communicated to the qualified teams.

6. Domains Covered

The challenges in Breach Point CTF are designed to assess participants' skills across multiple areas of cybersecurity. The competition will include challenges from the following domains:

- **Web Security**
- **Digital Forensics**
- **Cryptography**
- **Reverse Engineering**
- **Open-Source Intelligence (OSINT)**
- **API Security**
- **Mobile Security ….more**

Each domain will feature challenges of varying difficulty levels, encouraging participants to apply both foundational knowledge and advanced techniques.

Participants are expected to approach challenges ethically and within the scope defined by the competition rules.

7. Write-up Submission Guidelines

Write-up submissions are a mandatory requirement for teams shortlisted from the online round. These write-ups will be evaluated to determine qualification for the offline round.

Write-up Requirements

- Write-ups must clearly explain the **approach**, **tools**, and **methodology** used to solve each challenge.
- Submissions should demonstrate the participant's understanding of the problem and the solution process.
- Each team is responsible for ensuring the originality of their submission.

Submission Policy

- Write-ups must be submitted **within the deadline** specified by the organizers.
- **Copied, plagiarized, or shared write-ups** will result in **immediate disqualification**.
- Failure to submit the required write-up within the given timeframe will lead to disqualification from the offline round.

8. Challenge Format (BPCTF{….})

- All challenges will be presented in a **Jeopardy-style CTF format**, unless explicitly stated otherwise.
- Challenges may be attempted in **any order**.
- Each challenge will require participants to identify and submit a **valid flag** to receive points.
- Flags must be submitted in the **prescribed format** as specified on the competition platform.
- Hints, if provided, may carry a **point penalty** (if applicable).

9. Scoring System

- Each challenge carries a **predefined point value**, based on its difficulty level.
- Points will be awarded **only for correct flag submissions**.
- Incorrect submissions may result in **penalties**, if enabled on the platform.
- In case of a tie on the leaderboard, the **earliest completion time** will be used as the tie-breaker.
- The organizers reserve the right to **adjust scoring parameters** if required to maintain fairness.

10. Certificates & Prizes

Certificates

- **Participation Certificates** will be issued to all registered participants who actively take part in the competition and comply with the event rules.
- **Merit Certificates** will be awarded to teams securing top positions on the final leaderboard.
- Certificates will be provided in **digital format**, unless stated otherwise.

Digital Credentials (Credly Badges)

- Eligible participants will receive **digital skill badges** issued through the **Credly** platform.
- These badges serve as **verifiable digital credentials** that can be shared on professional platforms such as LinkedIn and personal portfolios.
- Issuance of Credly badges is subject to:
    - Successful participation in the event
    - Fulfillment of eligibility criteria defined by the organizers
- Detailed information regarding badge criteria and distribution will be communicated through official channels.

Prizes

- Prizes will be awarded to **top-performing teams** based on the final results.
- Prize details and distribution mechanisms will be announced separately.
- The organizing committee reserves the right to modify prize structures if required.

11. Important Dates

- **Registration Deadline: 12th February**
- **Online Round: 14th – 15th February** (24 Hours)
- **Write-up Submission Deadline: 17th February**
- **Offline Round: 6th – 7th March** (24 Hours)
- **Result Announcement: 7th March**

Participants are advised to regularly check official communication channels for updates related to dates and timelines.

General Rules

All participants must adhere strictly to the rules outlined in this rule book.

The decision of the organizers and judges shall be **final and binding** in all matters related to the competition.

Participants are responsible for ensuring compliance with platform guidelines and event instructions.

Any violation of rules may result in penalties, disqualification, or removal from the competition.

Disclaimer

The organizing committee reserves the right to modify, amend, or update the rules, event structure, challenge format, scoring system, or schedule at any time, if required.

Any such changes will be communicated through official channels. Participation in the competition implies full acceptance of all rules, decisions, and modifications stated by the organizers.

Final Note to Participants

- Breach Point CTF is designed to challenge how you think, how you analyze, and how you respond under pressure. Every challenge is an opportunity to learn, adapt, and push beyond your current limits.
- If you have not registered yet, this is your moment.
  Prepare your team, sharpen your skills, and step into the arena.
- If you are already registered, stay tuned for further updates and announcements.
  The battlefield is being prepared.

We'll See You at Breach Point

Breaking systems is only the beginning.
What you build from the breach defines you.

Organized by
Department of Cyber Security
School of Engineering
Malla Reddy University

breachpointctf@mallareddyuniversity.ac.in

breachpoint.live