

## **Cybersecurity Challenge: CryptoXcape – Decode to Escape**

**Participants:** Open to students of all semesters

**Date:** 26 February 2026

### **Brief Description of the Event**

On 26 February 2026, the Department of Information Science and Engineering organised CryptoXcape – “Decode to Escape” as part of the Silver Jubilee celebrations. The event was conducted at the ISE Department, Chhatrapathi Shivaji Block – 5th Floor. The competition was designed as a two-phase technical challenge that tested participants’ logical reasoning, analytical thinking, teamwork, and cybersecurity skills. Inspired by the theme “*Now You See Me*”, the event combined a scavenger hunt with a Capture-The-Flag (CTF) cybersecurity challenge. The primary objective was to decode and unlock a 4-digit security code by solving strategically designed clues and identifying hidden flags within a web-based environment. The event created an intense and engaging competitive atmosphere where participants were required to think under pressure and act strategically. The event had a prize pool of ₹10,000. Registration was free, with a maximum of 40 teams allowed to participate. Each team consisted of four members, and three winning teams were awarded prizes.

### **Key Points Covered**

1. Participants were required to determine and input the correct 4-digit security code to unlock the CryptoXcape system.

### **Phase 1 – Clue Collection (Scavenger Hunt):**

2. Teams had to solve four strategically hidden clues within the room. Each solved clue provided:
  - One numerical digit required for the final code.
  - A hint directing the team to the next clue location.
3. **Goal of Phase 1:**  
To collect four distinct numerical digits in the minimum possible time through logical reasoning and teamwork.

### **Phase 2 – Hill Capture (Attack & Defence):**

4. In this web-based CTF round, 12 flags were hidden across a website based on common web vulnerabilities. Teams were required to discover and decode these hidden answers.
5. **Application of Web Security Concepts:**  
Participants utilised principles of web exploitation and red teaming to identify vulnerabilities and capture flags.
6. **Flag Submission Format:**  
Flags were to be submitted in the format CTF{...} or FLAG{...}, exactly as shown and case-sensitive.
7. **Scoring System:**  
Each flag carried 100 points, with points reducing gradually after the first team captured it. Winners were decided based on the highest score, number of flags captured, and earliest submission time in case of ties.

## **Outcome**

The event successfully enhanced students' problem-solving abilities, strategic thinking, and technical understanding of cybersecurity concepts. Participants improved their teamwork and coordination skills while working under time constraints. The scavenger hunt phase strengthened logical reasoning and observation skills, while the CTF round provided practical exposure to web vulnerabilities and ethical hacking concepts. Overall, CryptoXcape provided an engaging platform for experiential learning and competitive technical growth.

## **Activities Conducted**

1. **Phase 1:** Clue Collection (Scavenger Hunt)
2. **Phase 2:** Hill Capture (CTF – Attack & Defence Round)

**Number of Participants:** 160

## **Winners**

### **1st Place:**

Kishore H (1NH23EC084 – ECE)  
Senthil Kumar S (1NH23IS149 – ISE)  
Prathik H (1NH23EC120 – ECE)  
Rithesh Venkatesh Kulkarni (1NH23AI131 – AIML)

### **2nd Place:**

Shreya R C (1NH23CS244 – CSE-2)  
Vanshika Sharma (1NH23CS327 – CSE-2)  
Preethi Yadav (1NH23CS193 – CSE-2)  
Srilekha M (1NH23CS257 – CSE-2)

### **3rd Place:**

Naveen M (1NH23CS165 – CSE-1)  
Shari Priya (1NH23CS210 – CSE-2)  
Harshitha Hegde (1NH23IS058 – ISE)  
Bharath Kishore L (1NH22CE006 – CSE-2)