MADANAPALLE INSTITUTE OF TECHNOLOGY & SCIENCE
(Deemed to be University)
Affiliated to JNTUA, Ananthapuramu & Approved by AICTE, New Delhi
NAAC Accredited with A+ Grade, NIRF India Rankings 2024 - Band: 201-300 (Engg.)
NBA Accredited - B.Tech. (CIVIL, CSE, ECE, EEE, MECH, CST), MBA & MCA

A Report on
"Defend the Digital Frontier Hackathon on capture the Flag"
Organized by
Department of Computer Science & Engineering - Cyber Security
on 07.01.2026

Report Submitted by: Mrs. M. Srilakshmi Preethi, Assistant Professor, Department of CSE-Cyber Security.
Mode of Conduct: Offline
No of Participants: 70
Date & Time: 07/01/2026 09.00 AM - 5.00 PM
Report Received on 10.01.2026.
Objectives:
The primary objectives of the MITS Cybersecurity Hackathon 2026 were:

- To provide hands-on exposure to real-world cybersecurity challenges through a CTF-based competitive environment.
- To strengthen students' understanding of core cybersecurity concepts, including networking, cryptography, web security, forensics, and reverse engineering.
- To encourage innovative thinking and creative problem-solving in the field of cybersecurity.
- To bridge the gap between theoretical knowledge and practical implementation.
- To promote ethical hacking practices and awareness of cyber laws and digital responsibility.
- To enhance analytical, logical, and critical thinking skills among participants.
- To identify and nurture young talent in cybersecurity for future academic and professional opportunities.

The Department of Computer Science & Engineering (Cyber Security), Madanapalle Institute of Technology & Science (MITS), successfully organized the MITS Cyber Security Hackathon 2026, a CTF-based offline event, on 7th January 2026 at Seminar Hall – C & D. The hackathon was conducted for a duration of 8 hours, starting from 9:30 AM onwards, with the objective of enhancing students' technical skills, problem-solving abilities, and teamwork in the domain of cyber security.

The event was inaugurated by the Dr. P. Ramanathan (principal), the Dr. Chandra Prakash Gupta (Dean of the School of Computing), and the Dr. S. V. S. Ganga Devi (Head of the Department), who motivated the participants and emphasized the importance of cyber security in the modern digital era. Their inaugural address inspired the students to actively participate and explore real-world security challenges.

The hackathon followed a structured multi-level format:

Level 1: Basic MCQs
Level 2: Basic CTF Challenges
Level 3: Intermediate CTF Challenges

Participants were tested in areas such as cryptography, forensics, web security, reverse engineering, and general cyber security concepts. The competition encouraged innovation, collaboration, and hands-on learning through real-time problem-solving.

The event witnessed enthusiastic participation from students, who showcased their technical competence and competitive spirit. Throughout the 8-hour session, teams worked rigorously on challenges, demonstrating strong analytical and debugging skills.

At the conclusion of the hackathon, the winners were announced, and prizes were awarded First, Second, Third, Consolation Prizes.

The event concluded with a valedictory session, where the organizers appreciated the efforts of all participants and congratulated the winners for their outstanding performance. The hackathon was a great success and provided a valuable platform for students to gain practical exposure to cyber security concepts in a competitive and engaging environment.

Outcome:

The hackathon successfully enhanced participants' practical exposure to real-world cybersecurity challenges through CTF activities, leading to improved technical skills in cryptography, digital forensics, web security, and reverse engineering. It boosted students' confidence in applying theoretical knowledge, strengthened their analytical and problem-solving abilities, and increased awareness of ethical hacking practices and responsible tool usage. The event promoted active learning and engagement, helped identify talented students in cybersecurity, strengthened the institutional cybersecurity culture, and motivated participants to pursue certifications, internships, and research, thereby contributing significantly to their academic and professional development.