Sarvajanik Education Society

Sarvajanik College of Engineering & Technology

Dr. R. K. Desai Marg, Opp.Mission Hospital, Athwalines, Surat-395001

Report for a Workshop on

CyberForge AI

"Finding Security Vulnerabilities in AI-Generated Websites"

Organized by

Artificial Intelligence Club
under Department of Information Technology/
Department of Artificial Intelligence and Data Science in
collaboration with IEEE SCET SB

Date: 7th February 2026

Venue: EC AV Room, SCET

Faculty Co-ordinator:
Prof. (Dr.) Ketki Pathak
Prof. (Dr.) Krishna Delvadia

Faculty Advisor:
Prof. (Dr.) Dhruti Sharma
Prof. Mukesh Patel

Prof. (Dr.) Vivaksha Jariwala
HoD, IT Department

Student Co-ordinators:

Mr. Bhavya Bavisi

Mr. Het Salmawala

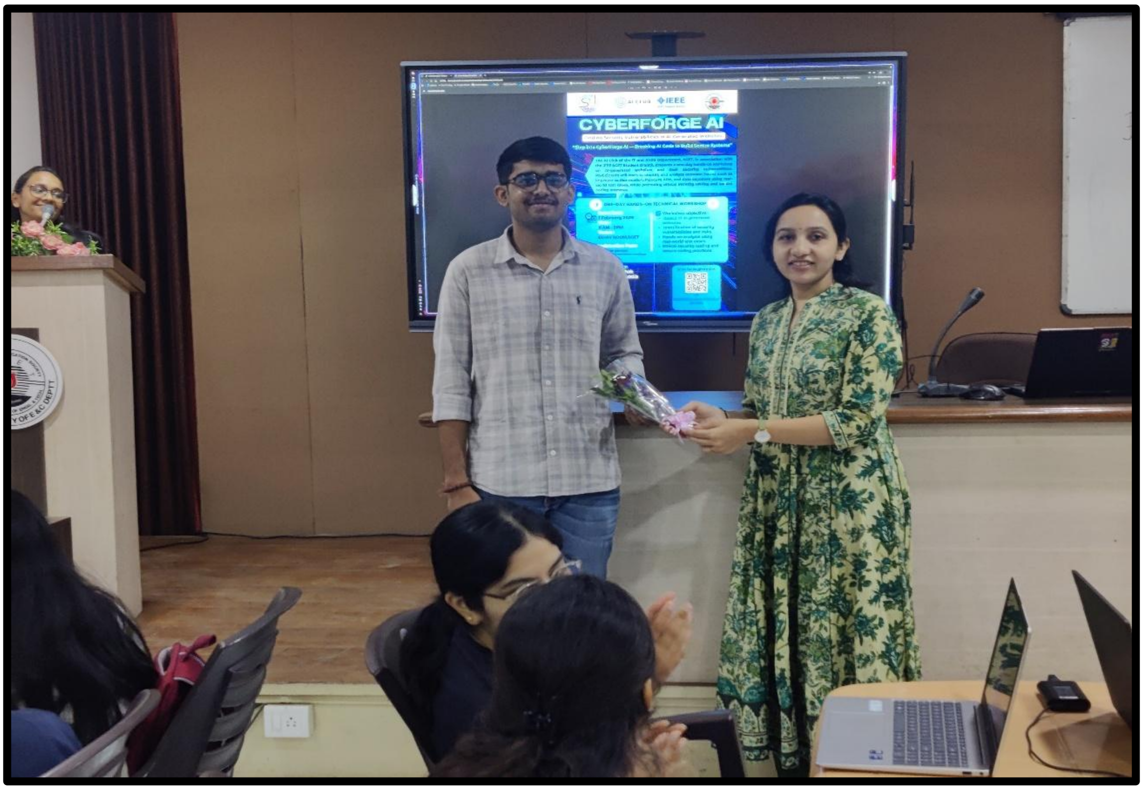
Ms. Tanisha Agarwal

Mr. Dhwanil Doshi

Ms. Chharvvi Batra

Resource person:

Mr. Bhavya Ladumor, IEEE SCET SB, TechLead



About the Event :

The Artificial Intelligence Club, in collaboration with the IEEE SCET Student Branch, organized a one-day hands-on technical workshop titled “CyberForge AI: Finding Security Vulnerabilities in AI-Generated Websites.” The workshop was designed to create awareness among engineering students about the security risks that can arise when AI tools are used for rapid web development without proper validation and enforcement.

With the increasing use of AI for generating websites and applications, developers often focus on functionality and speed while overlooking security considerations. This workshop aimed to address this gap by helping students understand how AI-generated code can unintentionally introduce vulnerabilities and why it is essential to critically analyze such systems from a security perspective.

Participation Details:

The workshop received active participation from around 60 students belonging to various engineering branches from institutes of surat district. The diverse audience contributed to interactive discussions and collaborative learning throughout the workshop.

Session Details:

The workshop began with an initial address by the AI Club, followed by a technical session conducted by Bhavya Ladumor, Technical Lead of IEEE SCET Student Branch and a member of the Technical Committee of the AI Club. The session focused on explaining the importance of identifying vulnerabilities in AI-generated websites and understanding the responsibility of developers while working with AI-assisted code.

An introductory theoretical overview was provided to establish key concepts related to web security, trust boundaries, and ethical security analysis. This was followed by a series of structured, simulation-based demonstrations where participants actively analyzed web applications designed to reflect real-world security flaws.

Event Highlights:

The workshop was designed to bridge the gap between theoretical knowledge and real-world applications, focusing on identifying and mitigating security vulnerabilities in AI-driven systems. Through expert-led sessions, live demonstrations, and interactive discussions, participants gained practical insights into modern cyber threats, AI-powered attack surfaces, and defensive strategies. The event fostered critical thinking, technical skill development, and awareness of secure AI practices, making it a highly impactful and enriching learning experience for all attendees. It can be categorized under following different session heads:

Simulation-Based Learning:

The core workflow of workshop consisted three hands-on simulations:

- Simulation 1: Analysis of frontend-only web applications to demonstrate the risks of clientside trust.

- Simulation 2: Examination of AI-generated web applications using backend APIs to highlight business logic flaws and improper server- side validation.
- Simulation 3: Focus on authorization and access control issues, helping students understand the difference between authentication and authorization.

Participants were encouraged to explore the simulations independently before guided explanations were provided, fostering critical thinking and practical understanding.

Ethical Security Awareness:

Throughout the workshop, emphasis was placed on ethical and responsible security practices. Participants were clearly informed that all simulations were authorized for testing, and that similar activities on real-world systems must only be conducted with explicit permission.

IEEE Membership Development Session:

A short IEEE Membership Development session was conducted by Dhwanil Doshi and Ved Kapadia, members of the IEEE SCET Student Branch ExCom. This session introduced students to IEEE membership benefits, professional opportunities, and the importance of involvement in technical communities.

CTF Challenge:

The workshop concluded with a Capture The Flag (CTF) challenge based on the concepts covered during the simulations. The challenge combined practical implementation with a competitive learning environment. The top three performers were awarded physical certificates, and notably, all three winners were female students, highlighting strong female participation in technical security activities.

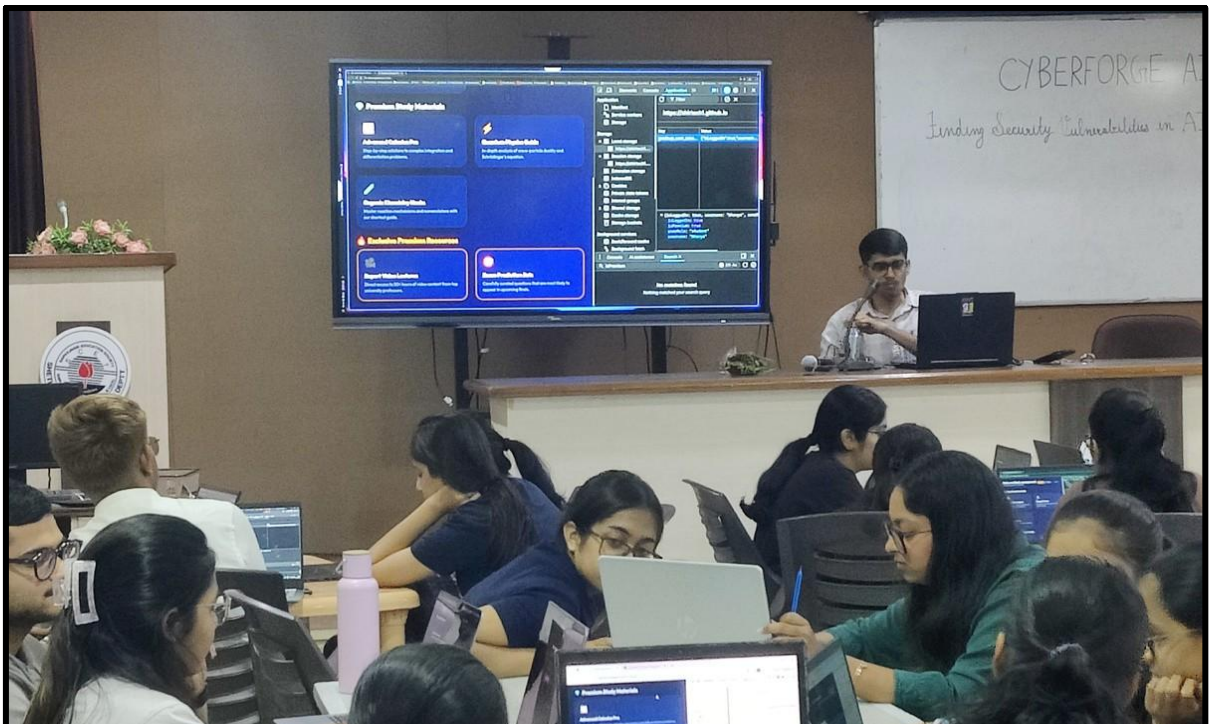
Rank	**Name**	**Email-ID**	**Levels Solved**	**Time Taken**
1	Tamanna Patel	tamanna2010patel@gmail.com	3	00:18:35
2	Aesha Patel	aeshashiv81@gmail.com	3	00:21:56
3	Darshana Patil	dspatil2965@gmail.com	3	00:27:37

Outcomes:

- Participants identified and classified common security vulnerabilities in AI-generated websites.
- Participants analyzed AI-generated source code to detect insecure coding practices.
- Participants applied vulnerability assessment techniques on AI-built web applications.
- Participants implemented secure coding and validation measures to mitigate identified vulnerabilities.
- The workshop has offered skill-based knowledge on evaluation of AI-generated web solutions from a cybersecurity and ethical perspective.

Event Highlights:

Workshop Flow Overview
Simulation 1
Simulation 2
Simulation 3
Final Challenge
CYBERFORGE
Finding Security Vulnerabilities


CYBERFORGE AI
Finding Security Vulnerabilities in AI
Premium Study Materials
Exclusive Premium Resources

CYBERFORGE AI
CYBERFORGE AI
Finding Security Vulnerabilities in AI-Generated Websites
Username - ECC_ubiquiti
Password - ECCUb1234

Conclusion:

The CyberForge AI workshop proved to be a technically enriching and engaging session that successfully combined artificial intelligence concepts with real-world web security practices. By focusing on hands- on simulations and ethical awareness, the event helped students build a strong foundation in analyzing AI-generated systems responsibly. The collaboration between the AI Club and IEEE SCET Student Branch played a key role in delivering a meaningful learning experience and set a strong precedent for future technical initiatives.

---****---