A Report on **Online Hands-on workshop on**
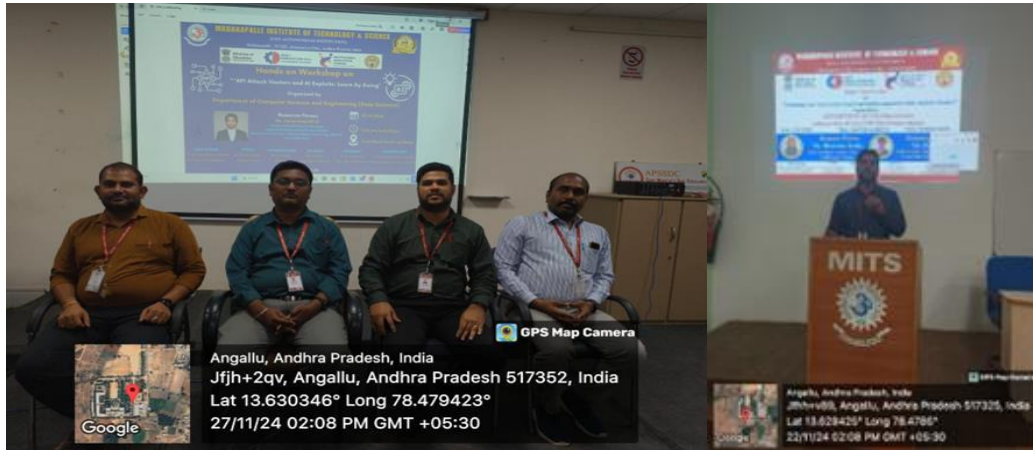**"API Attack Vectors and AI Exploits: Learn by Doing"**
Organised by Department of CSE-Data Science
in association with **IIC, MITS**
Date: 27.11.2024

Report Submitted by: Mr. G. Rajkumar, Assistant Professor, Department of CSE-Data Science.
Resource Person Details: Mr. Hariprasanth.R, Former Assistant Security Manager, National E-Governance Division (NeGD), Ministry of Electronics and Information Technology (MeitY). New Delhi, India.
Attendance: 52 participants from II CSE (Data Science) Department.
Venue: East Block Scaleup Room.
Mode of Conduct: Online
Report Received on 13.12.2024

Introduction:

The online Hands-on workshop on **"API Attack Vectors and AI Exploits: Learn by Doing"** was organized on 27nd November 2024 from 1:30 PM to 5:00 PM. The session featured by Mr. Hariprasaanth.R, Former Assistant Security Manager, National E-Governance Division (NeGD), Ministry of Electronics and Information Technology (MeitY). New Delhi, India.

Welcome Speech:
The session commenced with a **welcome speech** delivered by **Dr. N. Komal Kumar**, who warmly welcomed the guest speaker, faculty members, and students. He expressed the significance of the topic in today's fast-evolving tech landscape and highlighted how such sessions help bridge the gap between academia and industry. Dr. Komal Kumar emphasized the importance of gaining hands-on experience and practical knowledge to succeed in the tech field.

Address by Academic Coordinator:

Next, **Dr. K. Lokeshwaran**, the Academic Coordinator of the Department, addressed the audience. He spoke about the ever-changing nature of the tech industry, stressing the growing demand for professionals skilled in both front-end development and data analytics. Dr. K. Lokeshwaran encouraged the students to take full advantage of the learning opportunities provided through this lecture to enhance their technical capabilities and career prospects.

Address by IIC Coordinator:

Following Dr. K. Lokeshwaran, **Dr. S. Gopalakrishnan**, the IIC Coordinator, addressed the gathering. He discussed the role of industry-academia collaborations in shaping the future of students. Dr. Gopalakrishnan highlighted how the institution continually strives to connect students with industry experts through such lectures and workshops.

Agenda
- Introduction to cyber security
- Ethical hacking and Penetration Testing
- API Security
- Real world cyber-attacks
- OWASP

Hands On
- LLM
- NPL
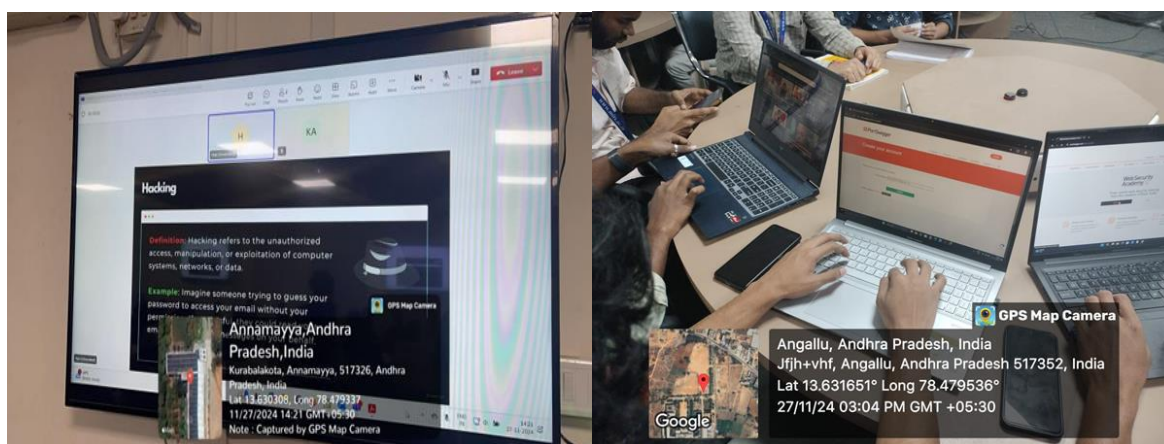
Conclusion and Q&A Session:

The workshop concluded with an **interactive Q&A session**, where students had the opportunity to ask questions and clarify doubts with both speakers. The students actively participated, asking insightful questions about front-end technologies, data analytics, and career opportunities in the tech industry.

Dr. N. Komal Kumar thanked Mr. Hariprasaanth.R for his valuable contributions to the session and expressed his appreciation for their time and expertise. He also encouraged the students to apply the knowledge gained during the session in their academic and professional journeys.

Feedback:

The event was well received by the students, who appreciated the practical approach and real-time examples shared by the speakers. The hands-on sessions on Microsoft Visual Studio and Splunk were particularly noted as being highly beneficial for their future endeavors. The students left with a better understanding of how to build a strong foundation in tech careers, whether in front-end development or data analytics.

Outcomes:

- **Practical Knowledge**: Students acquire hands-on experience with cybersecurity tools and techniques.
- **Problem-Solving Abilities**: Improved ability to tackle real-world cybersecurity challenges.
- **Enhanced Awareness**: Better understanding of the risks associated with digital systems and the importance of implementing robust security measures.
- **Career Opportunities**: Exposure to potential careers in cybersecurity, ethical hacking, API security, and related fields.
- **Proactive Thinking**: Encourages students to adopt a proactive mindset toward cybersecurity, fostering innovation and responsibility.

These topics not only provide theoretical knowledge but also prepare students for real-world applications, enhancing their employability and readiness for the cybersecurity industry.