LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING
(An Autonomous Institution since 2010)
Accredited by NAAC with 'A' Grade & NBA (Under Tier - I),
An ISO 21001:2018, 14001:2015, 50001:2018 Certified Institution
Approved by AICTE, New Delhi and Affiliated to JNTUK, Kakinada
L.B. REDDY NAGAR, MYLAVARAM, NTR DIST., A.P.-521 230.
hodcse@lbrce.ac.in, cseoffice@lbrce.ac.in, Phone: 08659-222 933, Fax: 08659-222931
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Date: 28-03-2025

Report on One-Day Guest lecture
On
Web Application Hacking

Event Type : One Day Guest lecture
Date : 28-03-2025
Time : 6:30 PM to 8:30PM
Mode : Online
Organized By : Dept. of CSE, LBRCE, Mylavaram, India
Resource person: Mr. Sai Satish, CEO, Indian Servers.
Convener : Dr.D.Veeraiah, Professor and HOD of CSE
Coordinators : T N V S Praveen, Ch. Srinivasa Rao, M. Swathi
Target : VI-Sem Students (CSE)]
Total Number of students: 210

1. Objective:

The objective of this guest lecture was to provide participants with an in-depth understanding of cryptographic vulnerabilities in web applications. The session focused on real-world security flaws, cryptographic weaknesses, and best practices for securing web applications against cryptographic attacks. Attendees were introduced to key concepts such as encryption algorithms, cryptanalysis techniques, and security misconfigurations that could lead to cyber threats.

Goal:

The goal of this lecture was to equip attendees with practical knowledge on:

- Identifying cryptographic flaws in web applications.
- Understanding attacks such as padding oracle attacks, broken encryption, and weak hash functions.
- Implementing secure cryptographic practices to prevent exploitation.
- Learning about modern cryptographic standards and secure coding practices.
- Analyzing real-world case studies on cryptographic vulnerabilities.

2. Outcome of the Event:

By the end of the lecture, participants were able to:

- Gain knowledge about cryptographic protocols and their weaknesses.
- Identify cryptographic attacks such as hash collision attacks, key leakage, and SSL/TLS vulnerabilities.
- Understand the role of cryptanalysis in breaking insecure cryptographic implementations.
- Learn best practices for implementing strong encryption in web applications.
- Analyze case studies of security breaches due to cryptographic failures.

3. Description of the event:

On 28-03-2025, the CSE department at LBRCE hosted an informative guest lecture on "Web Application Hacking in Cryptography." The session covered critical aspects of cryptographic security in web applications and explored how attackers exploit cryptographic flaws.

Key Highlights of the Lecture:

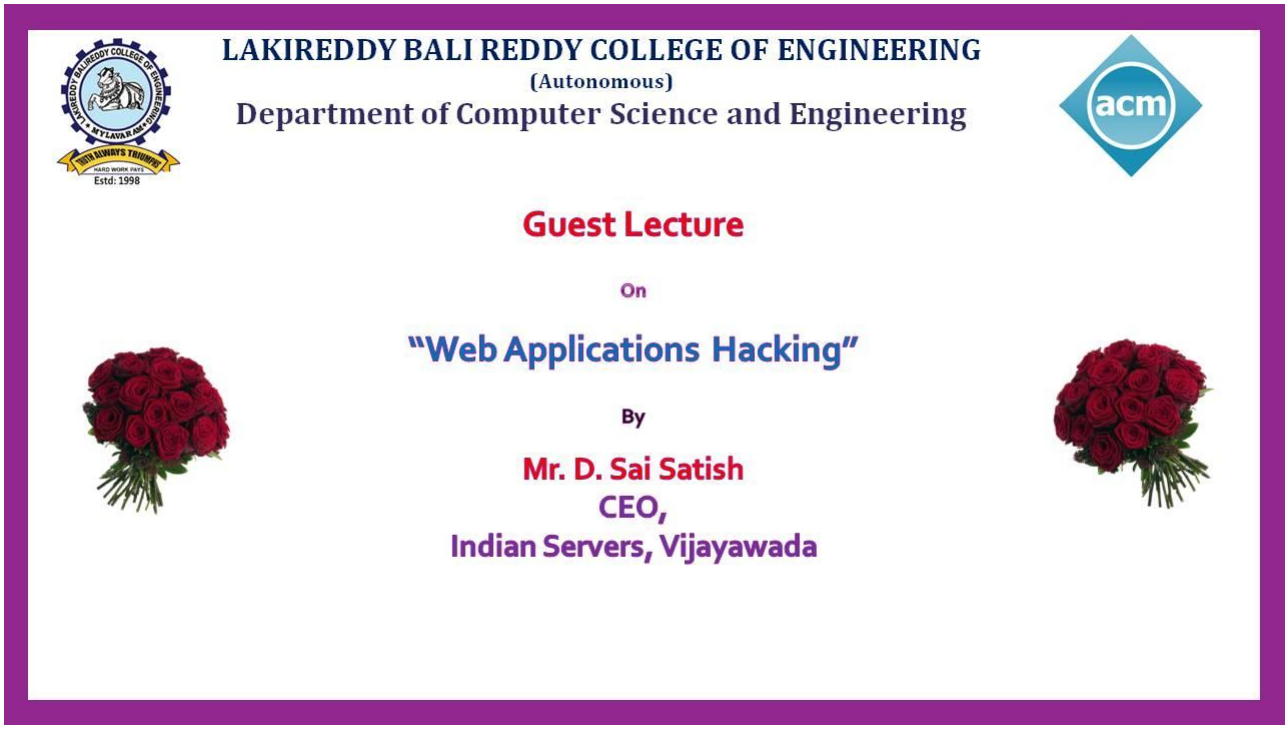
1. **Introduction to Cryptography in Web Applications:**
    - Overview of encryption techniques used in web security (AES, RSA, SHA, TLS, etc.).
    - Importance of cryptographic integrity and confidentiality.
2. **Common Cryptographic Vulnerabilities:**
    - Weak encryption algorithms and their risks.
    - Improper key management and its consequences.
    - SSL/TLS misconfigurations leading to security breaches.
3. **Cryptographic Attacks on Web Applications:**
    - **Padding Oracle Attacks** – Exploiting padding scheme weaknesses in encryption.
    - **Man-in-the-Middle (MITM) Attacks** – Intercepting encrypted communication.
    - **Hash Collision Attacks** – Breaking weak hash functions like MD5 and SHA-1.
    - **Key Leakage & Side-Channel Attacks** – Extracting encryption keys using various attack vectors.
4. **Best Practices for Secure Cryptography in Web Applications:**
    - Using strong encryption standards (AES-256, RSA-4096, SHA-3, etc.).
    - Proper implementation of SSL/TLS to prevent MITM attacks.
    - Implementing secure key storage and management techniques.
    - Regular security audits and cryptographic key rotation.
5. **Real-World Case Studies:**
    - Analysis of high-profile cryptographic failures in web applications.
    - Lessons learned from cyber attacks exploiting weak cryptographic implementations.
6. **Future Trends in Cryptographic Security:**
    - Quantum cryptography and its impact on modern encryption.
    - Advancements in homomorphism encryption and zero-knowledge proofs.

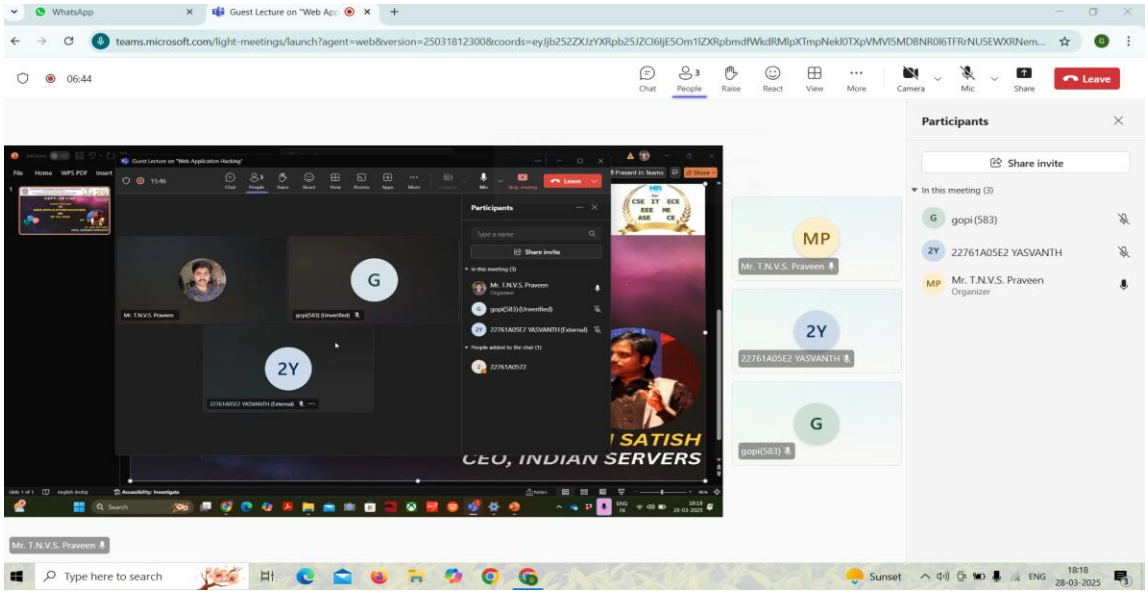
4. Impact Analysis

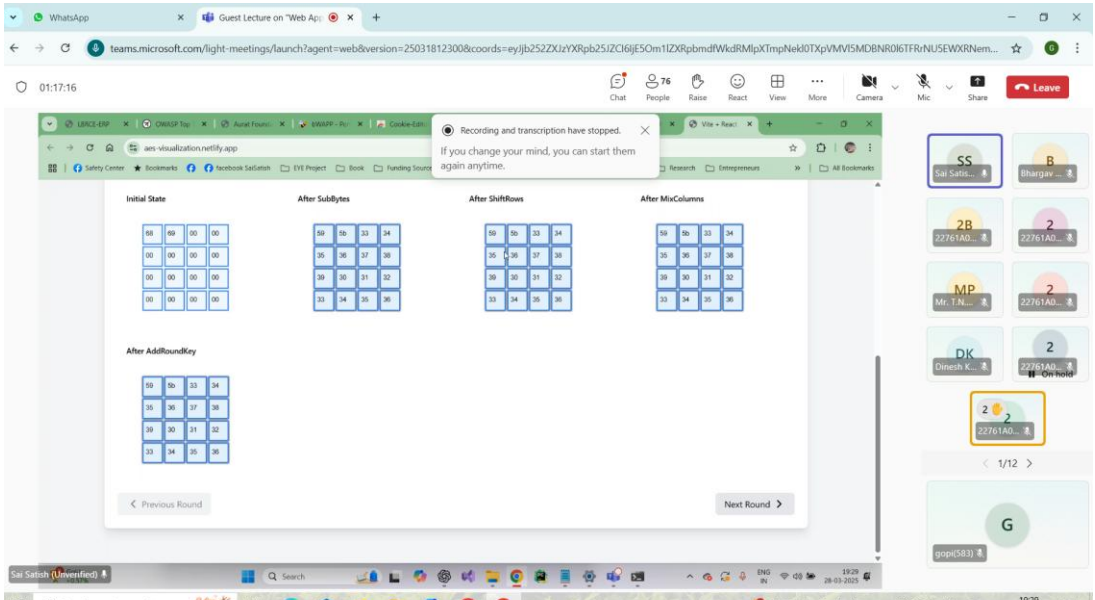
The lecture significantly enhanced participants' understanding of cryptographic security in web applications. Students gained hands-on knowledge about cryptographic weaknesses and the importance of secure implementation practices. The discussion on real-world cryptographic failures provided insights into industry practices for securing web applications. Additionally, the session inspired students to explore cyber security and cryptography as potential research and career paths.

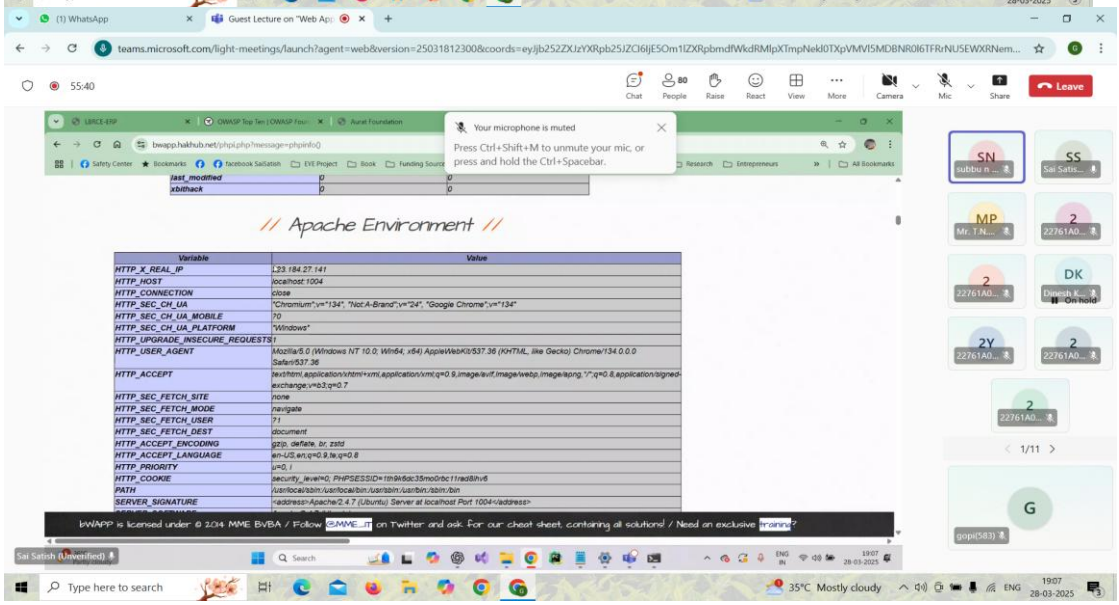
5. Feedback and Suggestions

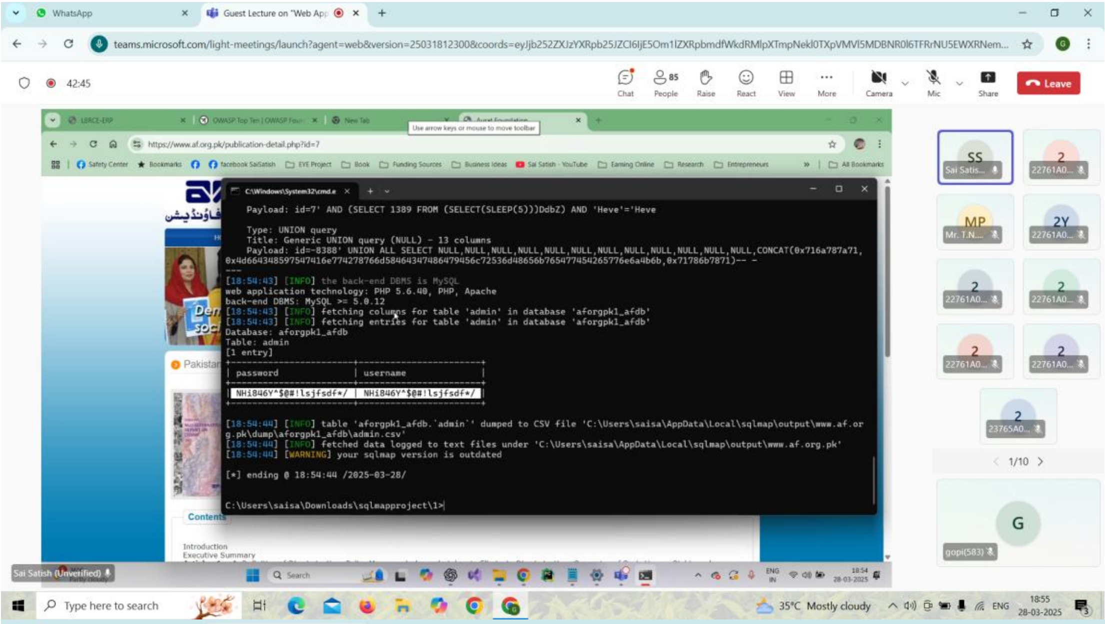
The lecture received positive feedback from attendees, who found the session highly insightful and engaging. Participants appreciated the detailed explanations and practical examples provided by the speaker. Many students expressed interest in attending further workshops on cryptography and ethical hacking. The Q&A session was particularly engaging, allowing students to clarify doubts on cryptographic security, modern encryption standards, and real-world hacking incidents.

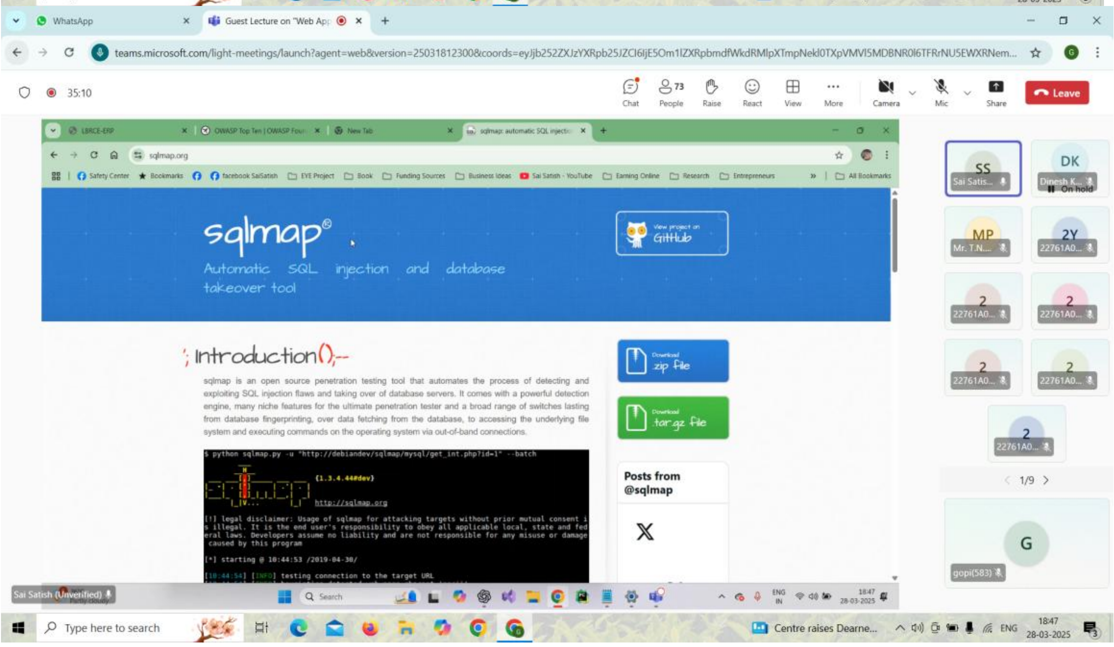


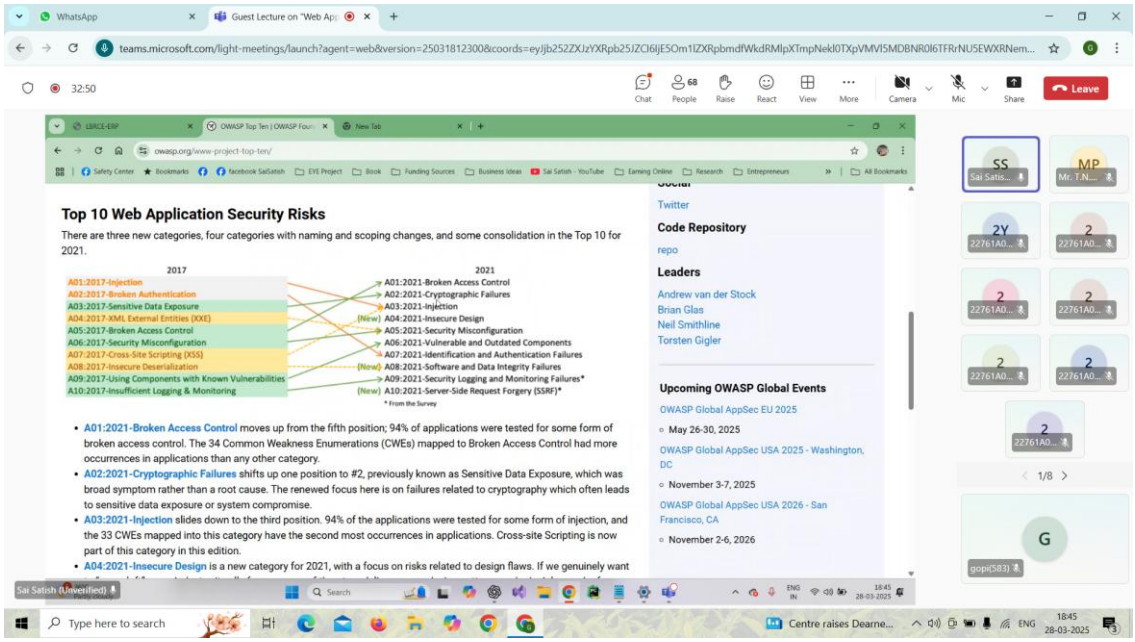

Participants
Share invite
In this meeting (3)
gopi (583)
22761A05E2 YASVANTH
Mr. T.N.V.S. Praveen
Organizer
Leave
SATISH
CEO, INDIAN SERVERS


Recording and transcription have stopped.
If you change your mind, you can start them again anytime.
Initial State
After SubBytes
After ShiftRows
After MixColumns
After AddRoundKey
Previous Round
Next Round
Leave


Your microphone is muted
Press Ctrl+Shift+M to unmute your mic, or press and hold the Ctrl+Spacebar.
// Apache Environment //
Variable
Value
HTTP_X_REAL_IP
HTTP_HOST
HTTP_CONNECTION
HTTP_SEC_CH_UA
HTTP_SEC_CH_UA_MOBILE
HTTP_SEC_CH_UA_PLATFORM
HTTP_UPGRADE_INSECURE_REQUESTS
HTTP_USER_AGENT
HTTP_ACCEPT
HTTP_SEC_FETCH_SITE
HTTP_SEC_FETCH_MODE
HTTP_SEC_FETCH_USER
HTTP_SEC_FETCH_DEST
HTTP_ACCEPT_ENCODING
HTTP_ACCEPT_LANGUAGE
HTTP_PRIORITY
HTTP_COOKIE
PATH
SERVER_SIGNATURE
Leave


Guest Lecture on "Web App
teams.microsoft.com/light-meetings/launch?agent=web&version=25031812300&coords=
42:45
Leave
https://www.af.org.pk/publication-detail.php?id=7
C:\Windows\System32\cmd.e
Type: UNION query
Title: Generic UNION query (NULL) - 13 columns
[18:54:43] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, PHP, Apache
back-end DBMS: MySQL >= 5.0.12
[18:54:43] [INFO] fetching columns for table 'admin' in database 'aforgpk1_afdb'
[18:54:43] [INFO] fetching entries for table 'admin' in database 'aforgpk1_afdb'
Database: aforgpk1_afdb
Table: admin
[1 entry]
password
username
[18:54:44] [WARNING] your sqlmap version is outdated
[*] ending @ 18:54:44 /2025-03-28/
C:\Users\saisa\Downloads\sqlmapproject\1>
Type here to search
35°C Mostly cloudy
18:55
28-03-2025


Guest Lecture on "Web App
35:10
Leave
sqlmap.org
sqlmap
Automatic SQL injection and database takeover tool
View project on GitHub
Introduction
sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.
zip file
tar.gz file
Posts from @sqlmap
Type here to search
18:47
28-03-2025



Conclusion:

The guest lecture on "**Web Application Hacking in Cryptography**" successfully provided participants with an in-depth understanding of cryptographic vulnerabilities and security best practices in web applications. The session bridged the gap between theoretical knowledge and real-world cyber security applications, encouraging students to explore the domain of cryptographic security further.

Coordinator	HOD
(T N V S Praveen)	(Dr.D.Veeraiah)