

Course File Contents

S.No	Name of the Topic	Page No
1.	Cover page	
2.	Vision and Mission of the department	
3.	PEOs, POs and PSOs	
4.	Syllabus copy and Academic calendar	
5.	Brief notes on the importance of the course	
6.	Prerequisites if any	
7.	Course objectives and outcomes	
8.	CO-PO, CO-PSO mapping and Justification	
9.	Class Time table and Individual time table	
10	Method of teaching, Chalk and talk/ppts/NPTEL lectures/cds, etc.	
11	Lecture schedule(without faculty name)	
12	Detailed notes	
13	Additional topics	
14	Mid exam question Papers- Theory and quiz	
15	University Question papers of previous years	
16	Unit-wise quiz questions	
17	Tutorial problems with blooms mapping	
18	Assignment questions with blooms mapping	
19	List of students.	
20	Scheme and solution of internal tests.	
21	Sample answer papers.	
22	Marks sheet.	
23	Result analysis for internal exams (tests) with respect to COs-POs.	
24	Result analysis for external exams (university)	
25	CO and PO attainment sheet	
26	References, Journals, websites and E-links if any	

I.COVER PAGE

BALAJI INSTITUTE OF TECHNOLOGY & SCIENCE (AUTONOMOUS) DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING (AI&ML)	
Name of the Subject : WEB SECURITY	
BITS CODE : 21CS8116PE:	Programme : UG
Branch : CSE(AI&ML)	Version No :
Year : III	Document Number : BITS/AI&ML
Semester : II	Number of Pages :
Classification status (Unrestricted/Restricted) : Unrestricted	
Distribution List: Dept. Library, Dept. Office, Concerned Faculty	
Prepared by : 1. Name : 2. Sign : 3. Design: 4. 4) Date:	Updated by : 1. Name : 2. Sign : 3. Design : 4. Date :
<u>Verified by : *For Q.C only</u>	
1. Name : 2. Sign : 3. Design : 4. Date :	1. Name : 2. Sign : 3. Design : 4. Date :
Approved by (HOD) :	
1. Name : 2. Sign : 3. Date :	

CSE (Artificial Intelligence & Machine Learning)

II. VISION AND MISSION OF THE DEPARTMENT

VISION

To be a global leader in Artificial Intelligence and Machine Learning research, innovation, and education, driving transformative advancements that empower industries, enhance human capabilities, and contribute to a smarter, more sustainable world.

MISSION

M1: Innovative Research & Quality Education – To Conduct research on cutting-edge Technologies to address complex real-world problems across diverse domains and provide world-class education and training to equip students with technical expertise, ethical responsibility, and problem-solving skills.

M2: Industry Collaboration & Ethical AI Development –To Foster strong partnerships with industries, academia, and government organizations to develop impactful AI solutions and promote responsible and ethical AI practices that align with societal values and global sustainability.

M3: Entrepreneurship & Innovation – Encourage entrepreneurship and the development of AI-driven start-ups and products that contribute to economic growth.

M4: Community Engagement – Engage with communities to spread AI awareness, inclusivity, and accessibility for societal benefit.

III. PEOs, POs and PSOs

Program Educational Objectives

PEO1: Graduates shall apply the analytical, decision making and prediction skills in AI & ML to formulate and solve complex intelligent computing and multidisciplinary problems.

PEO2: Graduates will be able to take up higher studies, research & development by acquiring in-depth knowledge in Artificial Intelligence & Machine Learning.

PEO3: Graduates will be able to exhibit their employability skills and practice the ethics of their profession with a sense of social responsibility.

Programs Outcomes

PO1: graduate of the Artificial Intelligence & Machine Learning Program will demonstrate:

PO1:Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO3:Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO4:Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO5:Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO6:Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO7:The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO8:Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

Program Specific Outcomes (PSOs)

PSO1: Apply a set of Artificial Intelligence principles, tools, and techniques to model various real-world business problems, analyze them, and suggest a suitable solution by communicating relevant findings and effectively presenting results using appropriate techniques.

PSO2: Apply the skills of Artificial Intelligence and Machine Learning in the areas of Health Care, Education, Agriculture, e-commerce, financial sector, Smart Systems, and Multi-disciplinary areas of AI.

PSO3: Cultivate the ability to work in teams and learn by participating in Technical Events and Social Welfare Programs and develop the attitude for working productively as an individual and in cross- disciplinary teams to become better citizens in multicultural world.

IV. Syllabus copy and Academic calendar

21CS8116PE: WEB SECURITY (Professional Elective-V)

B.Tech. IV Year II Sem.

L	T	P	C
3	0	0	3

Course Objectives:

- Give an Overview of information security
- Give an overview of Access control of relational databases

Course Outcomes: Students should be able to

- Understand the Web architecture and applications
- Understand client side and service side programming
- Understand how common mistakes can be bypassed and exploit the application
- Identify common application vulnerabilities

UNIT - I

The Web Security, The Web Security Problem, Risk Analysis and Best Practices. Cryptography and the Web: Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification.

UNIT - II

The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Antitheft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications.

UNIT - III

Database Security: Recent Advances in Access Control, Access Control Models for XML, Database Issues in Trust Management and Trust Negotiation, Security in Data Warehouses and OLAP Systems.

UNIT - IV

Security Re-engineering for Databases: Concepts and Techniques, Database Watermarking for Copyright Protection, Trustworthy Records



ACADEMIC CALENDAR FOR B.TECH. IV-YEAR FOR THE ACADEMIC YEAR 2024-25

B.Tech-IV-YEAR I Semester

S.No	Description	Date		Duration
		From	To	
1	1 st Spell of instructions	30-07-2024	28-09-2024	9 Weeks
2	First Unit Test Examinations	29-08-2024	31-08-2024	3 days
3	First Mid Term Examinations	30-09-2024	03-10-2024	3 days
4	2 nd Spell of Instructions (Including Dussera Recess)	04-10-2024	14-12-2024	10 Weeks
5	Dussehra Recess	07-10-2024	12-10-2024	1 week
6	Second Unit Test Examinations	21-11-2024	23-11-2024	3 days
7	Second Mid Term Examinations	16-12-2024	18-12-2024	3 days
8	Preparation Holidays & Practical Examinations	19-12-2024	30-12-2024	1 week
9	End Semester Examinations	31-12-2024	11-01-2025	2 Weeks

B.Tech - IV-YEAR II Semester

S.No	Description	Date		Duration
		From	To	
1	Commencement of II Semester class work	16-01-2025		
2	1st Spell of Instructions	16-01-2025	19-03-2025	9 Weeks
3	First Unit Test Examinations	20-02-2025	22-02-2025	3 days
4	First Mid Term Examinations	20-03-2025	22-03-2025	3 days
5	2 nd Spell of instructions	24-03-2025	10-05-2025	7 Weeks
6	Second Unit Test Examinations	21-04-2025	23-04-2025	3 days
7	Summer Vacation	12-05-2025	24-05-2025	2 Weeks
8	2 nd Spell of instructions Continuation	26-05-2025	31-05-2025	1 week
9	Second Mid Term Examinations	02-06-2025	04-06-2025	3 days
10	Preparation Holidays and Practical Examination	05-06-2025	14-06-2025	1 week
11	End Semester Examinations	16-06-2025	28-06-2025	2 Weeks

V. P. Nallabelli
 PRINCIPAL 24/7/24

Copy to:

1. Dean-Academics
2. All Head of the Departments
3. Examination branch

V. BRIEF NOTES ON THE IMPORTANCE OF THE COURSE

What Is Web Security?

Web security aims to safeguard data and network resources from online threats. This comprehensive field employs a combination of monitoring tools, user training, and other strategies to keep data, infrastructure, and people safe from cyber-attacks. Web security encompasses a wide range of practices, technologies, and protocols designed to protect websites, web applications, and web services from unauthorized access, data breaches, and other malicious activities. Advanced web security provides a proxy between users and their browsers to block malware and advanced persistent threats.

With the mounting persistence of cyber threats, web security has become a continuous cycle of assessment, implementation, and adaptation to new risks and vulnerabilities. Organizations must remain vigilant and proactive in their approach to web security to protect their assets, reputation, and people.

How Web Security Works

Today's web security solutions employ a multi-layered approach to protect websites and applications from cyber-attacks. Here's a simplified overview of how it works:

Authentication and access control

Data encryption

Vulnerability management and testing

Network security

Monitoring and incident response

Challenges in Web Security

- Malicious websites
- Credential theft
- Social engineering and phishing emails
- Ransomware
- Website vulnerabilities
- Malware

- Advanced persistent threats (APTs)
- Distributed denial-of-service (DDoS) attacks
- SQL injection and cross-site scripting (XSS)

VI. PREREQUISITES

Here's a breakdown of key prerequisites for web security

Networking: Understand TCP/IP, DNS, HTTP, HTTPS, and other relevant protocols.

Operating Systems: Familiarity with how operating systems work, including security aspects of Linux and Windows.

Security Principles: Grasp fundamental security concepts like confidentiality, integrity, and availability (CIA triad).

Cryptography: Basic understanding of encryption, hashing, and key management.

Basic Programming: Familiarity with scripting languages like Python or basic knowledge of programming languages used in web development (e.g., HTML, CSS, JavaScript, PHP, Python, etc.).

VII. COURSE OBJECTIVES & OUTCOMES

COURSE OBJECTIVES:

Course Objectives:

- Give an Overview of information security
- Give an overview of Access control of relational databases

COURSE OUTCOMES (COs):

- Understand the Web architecture and applications
- Understand client side and service side programming
- Understand how common mistakes can be bypassed and exploit the application
- Identify common application vulnerabilities.
- Demonstrate the use of penetration testing tools and perform security audits.

By the end of this course, Students should be able to:

CO Number	Statement
CO1	Understand and analyze the Web architecture and applications
CO2	Understand and analyze client side and service side programming
CO3	Understand how common mistakes can be bypassed and exploit the application
CO4	Identify common application vulnerabilities
CO5	Demonstrate the use of penetration testing tools and perform security audits.

VIII. CO-PO, CO-PSO MAPPING & JUSTIFICATION

CO-PO and CO-PSO Mapping table

Course Outcome	Program Outcomes(POs)												Program Specific Outcomes (PSOs)		
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	3	2	1	2	1	-	-	-	-	-	-	1	3	2	1
CO2	3	3	2	3	2	-	-	-	-	-	-	2	2	3	2
CO3	3	2	3	3	2	-	-	-	-	-	-	2	3	3	2
CO4	3	3	2	3	2	-	-	-	-	-	-	3	2	3	3
CO5	2	2	3	3	3	-	-	-	-	-	-	3	3	2	3
Average	2.8	2.4	2.2	2.8	2.0	-	-	-	-	-	-	2.2	2.6	2.6	2.2

JUSTIFICATION FOR COURSE OUTCOMES MAPPING WITH POs AND PSOs

Justification:

- **PO1 (Engineering Knowledge):** Apply knowledge of computing fundamentals to analyze web security concepts.
- **PO2 (Problem Analysis):** Identify, analyze, and mitigate security vulnerabilities and threats.
- **PO3 (Design/Development):** Design and develop secure web applications and implement secure coding practices.
- **PO4 (Investigations of Complex Problems):** Investigate and address real-world web application security challenges.
- **PO5 (Modern Tool Usage):** Use modern penetration testing and security tools to enhance web security.
- **PO12 (Life-long Learning):** Encourage continuous learning to stay updated with emerging web security threats.

Justification of CO-PSO Mapping

1. **CO1 → PSO1, PSO2, PSO3:**
 - Understanding web vulnerabilities enhances the ability to design secure solutions (PSO1).
 - Identifying web security threats improves threat analysis skills (PSO2).
 - Familiarity with web security frameworks supports the application of security measures (PSO3).
2. **CO2 → PSO1, PSO2, PSO3:**
 - Applying cryptographic techniques ensures secure software design (PSO1).
 - Securing data transmission aligns with mitigating cyber threats (PSO2).
 - Knowledge of encryption contributes to securing data in transit (PSO3).
3. **CO3 → PSO1, PSO2, PSO3:**

- Implementing secure coding practices contributes to developing secure software (PSO1).
 - Addressing common vulnerabilities mitigates security threats (PSO2).
 - Applying frameworks enhances the security of applications (PSO3).
4. **CO4 → PSO1, PSO2, PSO3:**
- Performing penetration testing aids in developing secure systems (PSO1).
 - Identifying security flaws improves threat assessment skills (PSO2).
 - Applying assessment tools enhances technical competence (PSO3).
5. **CO5 → PSO1, PSO2, PSO3:**
- Implementing web security protocols ensures secure communication (PSO1).
 - Configuring secure protocols mitigates external threats (PSO2).
 - Integrating protocols enhances overall application security (PSO3)

IX. CLASS TIME TABLE AND INDIVIDUAL TIME TABLE



Balaji Institute of Technology & Science
 Laknepally (V), Narsampet (M), Warangal District - 506 331, Telangana State, India
 (AUTONOMOUS)
 Accredited by NBA (UG - CE, ME, ECE & CSE) & NAAC A+ Grade
 (Affiliated to JNT University, Hyderabad and Approved by AICTE, New Delhi)
 www.bitswgl.ac.in, email: principal@bitswgl.ac.in, Ph:98660 50044, Fax: 08718-230521

Dept. of Computer Science & Engineering (AI&ML)

CLASS TIME TABLE

A.Y. (2024-25) (II Sem) Reg (R22)

Class:B.Tech IVCSM					w.e.f. 16.01.25			
DAY	1	2	3	4	1:00-1:40	5	6	7
	9:30 - 10:20	10:20 - 11:10	11:20 - 12:10	12:10 - 01:00	L U N C H B R E A K	1:40 - 02:30	2:30 - 03:20	3:20 - 04:10
MON	WS	SW	CRT-PRACTICE			PROJECTS		
TUE	PROJECTS					WS	SW	EIP
WED	SW	CRT-PRACTICE				WS	EIP	SW
THU	EIP	CRT-PRACTICE				EIP	PROJECTS	
FRI	SW	CRT-TECHNICAL LAB				PROJECTS		
SAT	CRT-PRACTICE					EIP	WS	WS
SUBJECTS:					LABS:			
Semantiv Web (SW) : Mrs.M.Supriya					CRT Technical:Dr.G.Naresh - IIT BOMBAY LAB			
PROFESSIONAL ELECTIVES-VI:								
Web Security(WS) : Mrs.P Srivalli					PROJECTS: K Murali Sagar/Summaiya Zahera			
OPEN ELECTIVES:III								
Entrepreneurship (EIP) : Dr.A.Gopikrishna								

Day	P1	P2	P3	P4	P5	P6	P7
MON	WS						
TUE					WS		
WED					WS		
THU							
FRI							
SAT						WS	WS

METHOD OF TEACHING

Teaching methods for a course on Data analytics should be diverse and interactive to cater to the complexity and depth of the subject matter. Here are some effective methods:

1. LECTURES

TRADITIONAL LECTURES: Using clear explanations, real-world examples, and visual aids like slides and diagrams for explaining key concepts such as Maxwell's equations, wave propagation, and transmission line theory.

GUEST LECTURES: Invited industry experts/researchers for providing insights into current trends and applications of electromagnetic fields and transmission lines.

2. INTERACTIVE LEARNING

PROBLEM-SOLVING SESSIONS: Conducting sessions where students solve problems in real-time, encouraging participation and collaborative learning.

Q&A SESSIONS: Regularly holding sessions where students can ask questions and engage in discussions to clarify doubts and deepen their understanding.

3. LABORATORY EXERCISES

Hands-On EXPERIMENTS: Setting up laboratory experiments where students can observe and measure electromagnetic phenomena, such as wave propagation and impedance matching.

4. PROJECTS AND CASE STUDIES

DESIGN PROJECTS: Assign projects where students design components such as antennas, transmission lines, or RF circuits, applying theoretical knowledge to practical problems.

CASE STUDIES: Analyzing real-world case studies of electromagnetic field applications in various industries, encouraging students to think critically about practical challenges and solutions.

5. FLIPPED CLASSROOM

PRE-CLASS ASSIGNMENTS: Providing reading materials, videos, and online resources for students to study before class. This prepares them for more in-depth discussions and activities during class time.

INTERACTIVE CLASS ACTIVITIES: Using class time for interactive activities such as group discussions, problem-solving, and hands-on experiments, reinforcing the pre-class material.

6. ASSESSMENT AND FEEDBACK

QUIZZES AND TESTS: Regular quizzes and tests to assess understanding and providing feedback on areas needing improvement.

PEER REVIEW: Incorporating peer review sessions for project presentations and reports, fostering collaborative learning and constructive criticism.

7. VISUAL AND MULTIMEDIA AIDS

VIDEOS AND ANIMATIONS: Using videos and animations to illustrate complex electromagnetic phenomena, making abstract concepts more tangible.

8. COLLABORATIVE LEARNING

GROUP PROJECTS: Encouraging teamwork through group projects where students can collaborate on designing and testing electromagnetic systems.

STUDY GROUPS: Forming study groups to promote peer-to-peer learning and discussion outside of formal class hours.

9. SUPPLEMENTARY RESOURCES

ONLINE FORUMS: Creating online forums or discussion boards for students to ask questions, share resources, and discuss course material.

READING MATERIALS: Provide a list of recommended textbooks, research papers, and articles for further reading and exploration of advanced topics.

S.No.	Question	Response (No of students) (%)	No of students (%) Response: b
1.	Preferred the conventional lecture by “Talk and chalk”.	(95%)	20 (5%)
2.	Diagrams should be shown by drawing on board.	(85%)	60 (15%)
3.	Concepts become clearer by “Talk and Chalk”.	(90%)	40 (10%)
4.	Teachers take more time to explain the concept rather than changing the slides fast.	(92%)	32 (8%)
5.	Easier to take down notes when taught by “Talk and chalk” method because power point slides are changed very fast.	(90%)	40 (10%)
6.	Diagrams are easier to follow when drawn on board step by step.	(70%)	120 (30%)
7.	They connect better with the teacher during Talk and chalk lecture.	(80%)	80 (20%)
8.	Lectures should be taken by “chalk and talk”.	(95%)	Response b: 20 (5%) Response c: 60 (15%)

XI. LECTURE SCHEDULE

ISO 9001:2015 Certified Institution Estd.:2001

 **Balaji Institute of Technology & Science**

Laknepally (V), Narsampet (M), Warangal District - 506 331, Telangana State, India

(AUTONOMOUS)

Accredited by NBA (UG - CE, ME, ECE & CSE) & NAAC A+ Grade
(Affiliated to JNT University, Hyderabad and Approved by AICTE, New Delhi)

www.bitswgl.ac.in, email: principal@bitswgl.ac.in, Ph:98660 50044, Fax: 08718-230521

Department of CSE (AI&ML)

LESSON PLAN & DELIVERY REPORT

Subject: **WEB SECURITY**

Class: B.Tech. IV CSE (AI&ML) (II Sem)

Faculty: S. Sravanthi

Academic Year: 2024-25

Regulation: R21

Commencement of Class Work: 16.01.25

UNIT- I					
Topics (as per	Subtopics	Lect. No.	Scheduled Date	Topic Delivered Date	Remarks
	<ul style="list-style-type: none">About Subject & GuidelinesVision, Mission, CO's of subjectText & Reference Books Introduction to the Web Security	L1	18-01-2025		
	<ul style="list-style-type: none">web security threats and How can we achieve web security	L2	20-01-2025		
	<ul style="list-style-type: none">The Web Security Problem	L3	21-01-2025		
	<ul style="list-style-type: none">Risk Analysis and Best Practices	L4	22-01-2025		
	<ul style="list-style-type: none">Cryptography and the Web	L5	25-01-2025		
	<ul style="list-style-type: none">Cryptography and Web Security	L6	25-01-2025		
	<ul style="list-style-type: none">Working Cryptographic Systems	L7	27-01-2025		

	• Protocols	L8	28-01-2025		
	• Legal Restrictions on Cryptography	L9	29-01-2025		
	• Digital Identification	L10	01-02-2025		
	• Overview of Unit-I	L11	03-02-2025		
	• Sliptest-I	L12	04-02-2025		
UNIT II The Web's War on Your Privacy					
	• The Web's War on Your Privacy	L13	05-02-2025		
	• Privacy-Protecting Techniques	L14	08-02-2025		
	• Privacy-Protecting Techniques	L15	10-02-2025		
	• Backups and Antitheft	L16	15-02-2025		
	• Web Server Security	L17	17-02-2025		
	• Physical Security for Servers	L18	24-02-2025		
	• Host Security for Servers	L19	25-02-2025		
	• Securing Web Applications.	L20	01-03-2025		
	• Securing Web Applications	L21	03-03-2025		
	• Overview of unit-II	L22	05-03-2025		
	• Sliptest-II	L23	08-03-2025		
UNIT III					
Topics (as per	Subtopics	Lect . No.	Scheduled Date	Topic Delivered Date	Remarks
	• Database Security	L24	10-03-2025		

	<ul style="list-style-type: none"> • Introduction to database security 	L25	12-03-2025		
	<ul style="list-style-type: none"> • Recent Advances in Access Contro 	L26	17-03-2025		
	<ul style="list-style-type: none"> • Access Control Models for XML 	L27	18-03-2025		
MID-I Exams(20-03-2025 to 22-03-2025)					
	<ul style="list-style-type: none"> • Database Issues in Trust Management 	L28	24-03-2025		
	<ul style="list-style-type: none"> • Trust Negotiation 	L29	26-03-2025		
	<ul style="list-style-type: none"> • Security in Data Warehouses 	L30	29-03-2025		
	<ul style="list-style-type: none"> • OLAP Systems. 	L31	01-04-2025		
	<ul style="list-style-type: none"> • OLAP Systems. 	L32	03-04-2025		
	<ul style="list-style-type: none"> • Overview of unit-III 	L33	05-04-2025		
	<ul style="list-style-type: none"> • Sliptest-III 	L34	07-04-2025		
UNIT IV					
	<ul style="list-style-type: none"> • Security Re-engineering for Databases 	L35	08-04-2025		
	<ul style="list-style-type: none"> • Security Re-engineering for Databases 	L36	09-04-2025		
	<ul style="list-style-type: none"> • Concepts and Techniques 	L37	12-04-2025		
	<ul style="list-style-type: none"> • Database Watermarking for Copyright Protection 	L38	19-04-2025		
	<ul style="list-style-type: none"> • Trustworthy Records Retention 	L39	21-04-2025		
	<ul style="list-style-type: none"> • Damage Quarantine 	L40	22-04-2025		
	<ul style="list-style-type: none"> • Recovery in Data Processing Systems 	L41	26-04-2025		
	<ul style="list-style-type: none"> • Hippocratic Databases 	L42	28-04-2025		

	• Current Capabilities	L43	29-04-2025		
	• Future Trends.	L44	30-05-2025		
	• Overview of unit-IV	L45	03-05-2025		
	• Sliptest-IV	L46	03-05-2025		
UNIT V					
Topics (as per syllabus)	Subtopics	Lect . No.	Scheduled Date	Topic Delivered Date	Remark s
	• Privacy in Database Publishing	L47	05-05-2025		
	• Privacy in Database Publishing	L48	06-05-2025		
	• A Bayesian Perspective	L49	07-05-2025		
	• A Bayesian Perspective	L50	10-05-2025		
	• Privacy-enhanced Location-based Access Control	L51	26-05-2025		
	• Privacy-enhanced Location-based Access Control	L53	28-05-2025		
	• Efficiently Enforcing the Security	L54	29-05-2025		
	• Privacy Policies in a Mobile Environment.	L55	30-05-2025		
	• Privacy Policies in a Mobile Environment	L56	30-05-2025		
	• Overview of unit-V	L57	31-05-2025		
	• Sliptest-V	L58	31-05-2025		
II-Mid Exams-02-06-2025 to 04-06-2025					

TEXT BOOKS:

- 1.Web Security, Privacy and Commerce Simson G Arfinkel, Gene Spafford,O'Reilly
- 2.Handbook on Database security applications and trends Michael Gertz,Sushil Jajodia

Signature of Faculty

HOD

XI. DETAILED NOTES

UNIT - I:

1. Introduction to Web Security

- **Web Security** refers to the protection of online services and user data from various types of threats and malicious activities.
- In today's digital age, securing web applications, systems, and user data is critical as cyber-attacks are increasingly sophisticated.

2. The Web Security Problem

- **Vulnerabilities:** Web applications face numerous vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).
- **Threats:** Hackers, malware, phishing attacks, and data breaches are some of the most common threats.
- **Impact:** Cyber-attacks can lead to financial losses, data theft, loss of reputation, and legal consequences.

3. Risk Analysis and Best Practices

- **Risk Analysis:** This is the process of identifying potential threats, assessing their likelihood, and determining the impact on the organization. The goal is to minimize risks through proper security measures.
 - Steps in Risk Analysis:
 - Identify Assets: What is valuable (data, user accounts, etc.)?
 - Identify Threats: What can go wrong (hackers, software bugs, etc.)?
 - Analyze Vulnerabilities: Where are the weaknesses (code errors, configuration flaws)?
 - Assess Impact: What happens if a breach occurs (financial loss, damage to reputation)?
 - **Tools:** Risk Assessment Matrix, Threat Modelling Tools, and Security Audits.
- **Best Practices for Web Security:**
 - Use **HTTPS** (HyperText Transfer Protocol Secure) for encrypted communication.

- Implement **Two-Factor Authentication (2FA)** to ensure stronger authentication.
- Regularly **patch and update** software to fix vulnerabilities.
- **Data encryption**: Use strong encryption for sensitive data both at rest and in transit.
- Implement **Firewalls and Intrusion Detection Systems (IDS)**.
- Follow the **principle of least privilege**, granting users only the permissions they need.
- Regularly **backup** critical data and store it securely.

Cryptography and the Web

4. Cryptography and Web Security

Cryptography is a fundamental component of web security. It ensures confidentiality, integrity, and authenticity of data.

- **Key Aspects of Cryptography:**
 - **Symmetric Encryption**: The same key is used to encrypt and decrypt data (e.g., AES - Advanced Encryption Standard).
 - **Asymmetric Encryption**: Different keys are used for encryption and decryption (e.g., RSA - Rivest-Shamir-Adleman).
 - **Hashing**: Converts data into a fixed-size value, typically used for password storage and integrity checks (e.g., SHA-256).
 - **Digital Signatures**: Ensures the authenticity of the sender of a message or document.
 - **Public Key Infrastructure (PKI)**: The framework that manages digital keys and certificates for secure communications.

5. Working Cryptographic Systems and Protocols

- **SSL/TLS (Secure Sockets Layer/Transport Layer Security):**
 - Used to encrypt data between a web server and a client (browser).
 - SSL/TLS ensures that the communication between two parties is private and secure.

- This protocol relies on asymmetric encryption for the exchange of keys and symmetric encryption for the actual data transfer.
- **HTTPS (HyperText Transfer Protocol Secure):**
 - HTTPS is the secure version of HTTP, using SSL/TLS for encryption.
 - It ensures that sensitive data, such as login credentials and financial information, is transmitted securely over the web.
- **Digital Certificates:**
 - A digital certificate is issued by a Certificate Authority (CA) to authenticate the identity of a server.
 - It includes the server's public key and is used during the SSL/TLS handshake to establish secure connections.
- **Pretty Good Privacy (PGP):**
 - PGP is used to encrypt emails and files, ensuring confidentiality and authenticity.
 - It uses a combination of asymmetric and symmetric encryption techniques.

6. Legal Restrictions on Cryptography

- **International Cryptography Laws:**
 - Some countries impose restrictions on the use of strong cryptography. For example, the U.S. has had regulations controlling the export of cryptographic software, although these have been relaxed over time.
 - **Export Controls:** In some jurisdictions, there are legal limitations on how encryption tools can be exported to certain countries.
- **Legal and Compliance Issues:**
 - Companies need to be aware of laws related to encryption, such as the **General Data Protection Regulation (GDPR)** in Europe, which mandates the protection of personal data.
 - Organizations must be cautious about using encryption to prevent unauthorized access while ensuring compliance with government regulations.

7. Digital Identification

- **Digital Identity** is the representation of an individual, organization, or system in the digital world.

- Examples include online banking credentials, social media accounts, and digital certificates used in SSL/TLS connections.
- **Techniques for Digital Identification:**
 - **Username/Password Authentication:** The most common method, though prone to phishing and password cracking attacks.
 - **Multi-Factor Authentication (MFA):** A more secure method that requires two or more verification factors (something you know, something you have, something you are).
 - **Biometric Authentication:** Uses physical characteristics such as fingerprints or facial recognition.
 - **Digital Certificates:** Used in public key infrastructure to verify the identity of a server or user.
 - **Single Sign-On (SSO):** Allows users to authenticate once and gain access to multiple systems or applications without re-entering credentials.

8. Key Considerations for Implementing Cryptography

- **Key Management:** Effective key management practices are essential to ensuring that encryption remains secure.
- **Key Length:** Longer keys offer better security but may result in increased computational overhead.
- **Algorithm Selection:** Choosing the right cryptographic algorithm for the task at hand is crucial (e.g., RSA for key exchange, AES for bulk data encryption).
- **Cryptanalysis:** The study of breaking cryptographic algorithms. Ensuring that chosen algorithms are resistant to cryptanalysis is vital.

9. Threats to Web Security from Cryptographic Systems

- **Man-in-the-Middle Attacks (MITM):** An attacker intercepts and potentially alters the communication between two parties.
 - To protect against MITM attacks, SSL/TLS encryption and certificate pinning should be used.
- **Cryptographic Attacks:** Attacks like **brute-force** and **side-channel attacks** can be used to break encryption.

- Proper configuration, key management, and the use of strong cryptographic algorithms can help mitigate these attacks.

UNIT - II: Web's War on Your Privacy

1. The Web's War on Your Privacy

- **Privacy Issues:** In today's digital world, maintaining privacy has become increasingly difficult as personal data is constantly collected and used without consent.
 - **Data Tracking:** Web browsers, social media platforms, and websites track user behavior using cookies, third-party scripts, and trackers.
 - **Data Harvesting:** Companies and online services collect vast amounts of personal information, often without the knowledge or consent of users.
 - **Surveillance:** Government agencies and other entities may also engage in surveillance, monitoring online activity to various extents.
- **Common Privacy Violations:**
 - **Third-party Data Sharing:** Data shared with external entities, sometimes without user knowledge, increases the risk of privacy violations.
 - **Data Breaches:** Sensitive data can be compromised in the event of a security breach or hacking incident.
 - **Tracking & Profiling:** Online activities can be monitored and used for profiling individuals for targeted advertising or other purposes.

2. Privacy-Protecting Techniques

- **Data Encryption:** Encrypting sensitive data ensures that even if data is intercepted, it remains unreadable to unauthorized parties.
 - **SSL/TLS Encryption:** Secure websites use SSL/TLS to encrypt data during transmission.
 - **End-to-End Encryption (E2EE):** Used in messaging apps and email to ensure that only the sender and receiver can decrypt the data.
- **Anonymity Tools:**
 - **VPNs (Virtual Private Networks):** VPNs mask your IP address, making it difficult to track your online activities or determine your geographic location.

- **Tor Network:** A privacy-focused browser that allows anonymous browsing by routing traffic through a decentralized network of servers.
- **Browser Privacy Settings:**
 - Disable third-party cookies and tracking scripts.
 - Use privacy-focused browsers like **Brave** or **Firefox** with additional privacy extensions.
- **Data Minimization:**
 - Avoid sharing unnecessary personal information.
 - Be cautious about giving apps or websites access to your personal data.
- **Privacy Policies:** Always review privacy policies of online services before sharing any personal information. These policies outline how your data is collected, used, and shared.

3. Backups and Anti-theft

- **Data Backup:** Regular backups are essential for protecting data from loss due to accidental deletion, hardware failure, or malicious attacks (like ransomware).
 - **Types of Backup:**
 - **Full Backup:** A complete copy of all files.
 - **Incremental Backup:** Backs up only data that has changed since the last backup.
 - **Differential Backup:** Backs up data that has changed since the last full backup.
- **Backup Strategies:**
 - **Off-site Backups:** Store backups in remote locations or the cloud to protect against physical theft or damage.
 - **Automated Backups:** Use automated systems to perform regular backups to ensure data is always up to date.
- **Anti-theft Measures:**
 - **Encryption:** Encrypt backup data to prevent unauthorized access in case the backup is stolen.
 - **Device Tracking:** Use tools to track stolen devices (e.g., **Find My Device** on Android or **Find My Mac** on Apple devices).

- **Remote Wiping:** Enable remote data wiping features in case devices are lost or stolen, ensuring that sensitive data cannot be accessed by unauthorized individuals.

4. Web Server Security

- **Web Server Overview:** A web server is a system that delivers web pages and content to users. Its security is critical to prevent attacks and breaches.
- **Common Web Server Vulnerabilities:**
 - **Unpatched Software:** Running outdated or unpatched server software can leave vulnerabilities open to exploitation.
 - **Configuration Errors:** Improper server configuration can expose sensitive information or create vulnerabilities.
 - **Exploiting Server-Side Scripts:** Attackers may exploit poorly written server-side scripts (e.g., PHP, Python) to gain unauthorized access.
- **Web Server Security Measures:**
 - **Keep Software Updated:** Ensure that the server software, operating system, and applications are always up-to-date.
 - **Disable Unused Services:** Disable unnecessary services or ports that are not required by the web server.
 - **Web Application Firewall (WAF):** Use a WAF to protect the server from common web application attacks such as SQL injection, XSS, and CSRF.

5. Physical Security for Servers

- **Server Location:** Servers should be physically located in a secure environment to prevent unauthorized physical access.
- **Physical Security Measures:**
 - **Access Control:** Use physical access controls such as locks, biometric scanners, and keycards to restrict access to server rooms.

- **Surveillance:** Install CCTV cameras and motion detectors to monitor access to critical infrastructure.
- **Fire Suppression:** Ensure that server rooms are equipped with fire suppression systems to prevent damage from fires.
- **Temperature and Humidity Control:** Servers generate a lot of heat, and maintaining optimal environmental conditions is crucial to prevent hardware failure.
- **Disaster Recovery:** Implement measures to recover from disasters, such as fire, flood, or other physical damage. This can include geographically dispersed data centers and redundant server hardware.

6. Host Security for Servers

- **Operating System Security:** The security of the server's operating system is crucial for preventing unauthorized access or exploitation.
 - **Hardening:** Minimize the attack surface by removing unnecessary software, services, and users from the server.
 - **Security Patches:** Regularly apply patches and updates to the operating system to fix known vulnerabilities.
- **Access Control:**
 - **Use Strong Passwords:** Ensure that server accounts use strong, unique passwords.
 - **Multi-Factor Authentication (MFA):** Implement MFA for administrative access to the server.
 - **User Permissions:** Follow the principle of least privilege, ensuring that users only have access to the resources necessary for their work.
- **Intrusion Detection and Prevention Systems (IDPS):**
 - Deploy an IDPS to monitor and detect unauthorized access attempts and suspicious activities.
 - **Log Monitoring:** Regularly monitor server logs for signs of unauthorized activity or potential attacks.

7. Securing Web Applications

- **Web Application Security:** The security of web applications is essential to prevent data breaches, hacking, and other malicious activities.
- **Common Web Application Vulnerabilities:**
 - **SQL Injection:** Attackers inject malicious SQL queries into input fields to manipulate the database.
 - **Cross-Site Scripting (XSS):** Attackers inject malicious scripts into web pages, which are then executed in the user's browser.
 - **Cross-Site Request Forgery (CSRF):** Attackers trick users into executing unwanted actions on a website where they are authenticated.
- **Securing Web Applications:**
 - **Input Validation:** Always validate and sanitize user input to prevent SQL injection and XSS attacks.
 - **Use HTTPS:** Ensure all data exchanged between the server and the client is encrypted using HTTPS.
 - **Authentication and Authorization:** Implement strong authentication mechanisms (such as MFA) and ensure proper authorization for accessing resources.
 - **Session Management:** Properly manage sessions to prevent session hijacking or fixation.
 - **Regular Security Audits:** Perform regular security audits and vulnerability assessments of web applications to identify and fix weaknesses.
 - **Use Security Libraries and Frameworks:** Utilize well-established libraries and frameworks that are designed with security in mind to prevent common vulnerabilities.

UNIT - III: Database Security

1. Database Security Overview

- **Database Security** refers to the protection of databases from unauthorized access, misuse, and threats that could compromise the confidentiality, integrity, and availability of stored data.
- Databases are essential to businesses and organizations as they store sensitive data, making them prime targets for cyberattacks, data breaches, and manipulation.
- The focus of database security is to prevent unauthorized access, ensure data privacy, and maintain the integrity of the data.

2. Recent Advances in Access Control

- **Access Control** is the mechanism that determines which users or systems can access which resources and what actions they can perform. In the context of databases, access control regulates who can read, write, update, or delete data.
- **Recent Advances in Access Control** include:
 - **Attribute-Based Access Control (ABAC):** ABAC allows access decisions based on attributes of the user, resource, and environment. This provides more granular control over who can access what data.
 - **Role-Based Access Control (RBAC):** While RBAC has been widely used for years, advancements in its implementation now allow for dynamic roles and permissions, including time-based roles and temporary permissions.
 - **Mandatory Access Control (MAC):** MAC has been enhanced to integrate with advanced data protection techniques and encryption to ensure data confidentiality and privacy.
 - **Discretionary Access Control (DAC):** While DAC has limitations, it is evolving to incorporate better user roles and automated policy enforcement.
 - **Fine-Grained Access Control:** Systems now allow more specific control over database objects (e.g., allowing access to specific columns or rows instead of the whole table).
- **Data Masking and Obfuscation:** These methods allow administrators to restrict access to certain pieces of sensitive data while allowing users to query databases in a way that preserves privacy (e.g., showing only partial credit card numbers or masked phone numbers).

- **Context-Aware Access Control:** This is an advanced form of access control that takes into account the context of the access request (e.g., user location, device, or time of day) before granting or denying access.

3. Access Control Models for XML

- **XML (Extensible Markup Language)** is widely used for storing and transmitting structured data in databases and web services. However, its flexible structure presents unique security challenges.
- **Access Control Models for XML** address the need to secure XML documents and ensure that sensitive information is protected while allowing valid operations.
- **Key Access Control Models for XML:**
 - **Role-Based Access Control (RBAC) for XML:** This approach applies traditional RBAC methods to XML data, controlling access based on roles assigned to users or processes.
 - **Attribute-Based Access Control (ABAC) for XML:** This model assigns access rights based on attributes of the XML data or the user requesting access. ABAC allows more fine-grained control over who can access specific parts of an XML document.
 - **XPath-Based Access Control:** XPath expressions are used to specify the parts of an XML document that a user or process can access. This allows for fine-grained control, such as giving access to specific elements or attributes within the XML data.
 - **XML Encryption and Digital Signatures:** Ensures that sensitive XML data is encrypted and that its authenticity can be verified through digital signatures.
- **Challenges:**
 - Ensuring privacy and security in XML-based systems, especially when data is shared between systems.
 - Managing access control for both structured and unstructured data.
 - Supporting granular control over data without compromising performance or scalability.

4. Database Issues in Trust Management and Trust Negotiation

- **Trust Management** refers to the management of trust relationships between entities (e.g., users, systems) within a database system, ensuring that users or applications can trust the data and services they interact with.
- **Trust Negotiation:** This is the process by which two or more entities exchange information to establish trust before allowing access to data or services. It involves dynamic trust evaluations and negotiations based on attributes, roles, and behavior.
- **Key Issues in Trust Management:**
 - **Trust Model Integration:** Integrating trust models into traditional database systems and access control frameworks.
 - **Trust Policies:** Defining and enforcing trust policies that specify the requirements for granting access to data (e.g., verifying the identity and reputation of users or systems).
 - **Trust Negotiation Protocols:** Developing secure protocols to negotiate and establish trust dynamically (e.g., protocols for mutual authentication, identity verification, and data validation).
 - **Reputation Systems:** Trust management may rely on reputation systems where past behavior or ratings influence trust decisions (common in decentralized or distributed systems like blockchain).
- **Trust in Database Transactions:** Ensuring that transactions are trustworthy and that they are not manipulated or fraudulently altered. This is especially important for online financial databases, healthcare systems, and other sensitive areas.
- **Examples of Trust Negotiation:**
 - **Public Key Infrastructure (PKI):** Used for establishing trust between different parties by verifying digital certificates.
 - **Secure Multi-Party Computation (SMC):** A cryptographic technique where multiple parties can jointly compute a function over their inputs without revealing their inputs to each other.
- **Challenges:**
 - Managing and scaling trust in large, distributed database systems.
 - Ensuring the trust negotiation process is efficient and secure in systems where data ownership and access are decentralized.

5. Security in Data Warehouses and OLAP Systems

- **Data Warehouses** are large repositories of integrated data from multiple sources that are used for analysis and reporting. Security in data warehouses is crucial because they often store vast amounts of sensitive and strategic business data.
- **OLAP (Online Analytical Processing)** systems enable users to perform complex queries and analysis on multidimensional data. Protecting OLAP systems is critical because they support decision-making in organizations and often contain sensitive business data.
- **Security Challenges in Data Warehouses and OLAP:**
 - **Data Integrity:** Ensuring that the data within a data warehouse is accurate, complete, and trustworthy. This is important because analytical results depend heavily on the quality and integrity of the data.
 - **Access Control:** Defining who can access different levels of data within the warehouse, especially when dealing with sensitive business intelligence. Fine-grained access control and role-based security are essential.
 - **Data Masking:** Masking sensitive data within OLAP systems to ensure that only authorized users can view full data. This is particularly important when the warehouse is accessed by analysts or non-administrative users.
 - **Audit Logging:** Tracking access to the data warehouse and logging queries, data modifications, and other relevant activities for security auditing and compliance purposes.
 - **Encryption:** Ensuring that sensitive data is encrypted both at rest (stored in the database) and in transit (when being transferred or queried). This prevents unauthorized users from accessing or intercepting sensitive business intelligence.
- **Advanced Security Techniques in Data Warehouses:**
 - **Federated Security:** In some cases, data warehouses are spread across different organizations or systems, and federated security allows organizations to share data securely while respecting their individual security policies.

- **Multi-Tenant Security:** Ensuring that multiple organizations can share the same data warehouse without compromising the security of each individual tenant's data.
- **Data Anonymization:** Anonymizing certain data fields in OLAP queries to protect privacy while still allowing for meaningful analysis.

Conclusion

- Database security is a complex and evolving field, with significant emphasis on controlling access to data, managing trust relationships, and protecting data during storage and processing.
- Advances in access control models, trust management, and security techniques in data warehouses and OLAP systems are essential to safeguard sensitive business and personal information.
- Implementing effective database security measures helps prevent unauthorized access, data corruption, and leakage, while also ensuring that data integrity and privacy are maintained.

UNIT - IV: Security Re-engineering for Databases

1. Security Re-engineering for Databases: Concepts and Techniques

- **Security Re-engineering** in databases refers to the process of revisiting and improving the security measures in an existing database system to protect it against new vulnerabilities, threats, and compliance requirements.
- This involves a **holistic approach** where database systems are analyzed, reconfigured, and sometimes redesigned to enhance their security posture.
- **Key Concepts:**

- **Database Hardening:** Strengthening a database's security by minimizing unnecessary services, changing default settings, and implementing strict access control policies.
- **Security Auditing:** Constant monitoring of database activity to detect unusual access or changes to sensitive data. Auditing helps in identifying potential security breaches and tracking down the responsible party.
- **Security Patching:** Updating the database system with patches to address vulnerabilities. This is essential for protecting the database from exploits and cyber-attacks.
- **Encryption:** Securing data at rest and in transit using encryption algorithms. This ensures that sensitive data is unreadable by unauthorized users.
- **Access Control Revisions:** Reassessing user roles and privileges to ensure only authorized users have access to critical data. This may involve applying **role-based access control (RBAC)** or **attribute-based access control (ABAC)**.
- **Techniques:**
 - **Data Masking:** Masking sensitive data in non-production environments to protect it from unauthorized access while ensuring that test data is usable.
 - **Database Partitioning:** Dividing a large database into smaller, manageable parts that can be secured separately to reduce the risk of a large-scale breach.
 - **Database Encryption:** Using database encryption tools (e.g., Transparent Data Encryption or TDE) to protect data in databases.

2. Database Watermarking for Copyright Protection

- **Database Watermarking** involves embedding a hidden marker or identifier into the database content to prove ownership and protect intellectual property. This method is used to ensure copyright protection and to track the source of data leaks or unauthorized distribution.
- **Types of Watermarks:**
 - **Visible Watermarking:** Watermarks that are evident to the user but do not interfere with the data itself. These may be used for securing ownership of publicly available databases or datasets.

- **Invisible Watermarking:** Watermarks that are hidden and designed to be undetectable under normal circumstances. These are inserted into the database structure or the actual data.
- **Watermarking Techniques:**
 - **Embedding in Data:** The watermark is inserted into the data itself, either by slightly altering the values or by appending additional data (e.g., adding an identifier to text fields or adding unique keys to database records).
 - **Hash-Based Watermarking:** Watermarks are generated based on hashing algorithms. A unique hash value is created and stored, representing the database content or specific fields.
- **Benefits:**
 - **Copyright Protection:** Watermarks help protect the database from unauthorized copying, distribution, or exploitation.
 - **Tracking:** Watermarking enables tracking the flow of data, making it easier to identify the origin of data leaks.
- **Challenges:**
 - **Data Integrity:** Watermarking must not alter the usability of the data or affect database performance.
 - **Security:** Watermarks must be robust to prevent tampering, such as deliberate attempts to remove or alter the watermark.

3. Trustworthy Records Retention

- **Trustworthy Records Retention** refers to the secure and reliable management of records or data in databases for extended periods of time, ensuring that these records remain intact, authentic, and accessible when required by legal or business needs.
- **Key Aspects:**
 - **Legal Compliance:** Many industries are required by law to retain certain types of records for a specific period (e.g., financial records, healthcare data). Ensuring compliance with data retention policies is critical.
 - **Data Authenticity:** Retained records must remain unchanged and trustworthy. This is particularly important for audit trails, financial transactions, and healthcare information.

- **Data Integrity:** Ensuring that records are not altered or tampered with. Techniques such as cryptographic hashing or digital signatures can verify the integrity of records.
- **Challenges in Trustworthy Records Retention:**
 - **Data Storage:** Storing records securely for long periods without degradation or unauthorized access.
 - **Evolving Legal Requirements:** Navigating the complexity of changing laws and regulations that affect data retention and compliance.
 - **Data Availability:** Ensuring that records remain accessible when needed, even after long retention periods, while balancing security and user access control.

4. Damage Quarantine and Recovery in Data Processing Systems

- **Damage Quarantine** involves isolating and securing compromised or damaged data to prevent it from spreading or contaminating the rest of the system.
- **Data Recovery** is the process of restoring data and services after an incident such as a cyberattack, data corruption, or natural disaster.
- **Key Techniques for Damage Quarantine:**
 - **Isolation:** Suspected compromised data or systems are isolated to prevent further damage, ensuring the rest of the data processing system remains intact.
 - **Forensic Analysis:** Involves examining the compromised data to determine the cause of the damage, who was responsible, and how to prevent further incidents.
- **Recovery Techniques:**
 - **Backup Systems:** Regular backups ensure that data can be restored after an incident. These backups should be stored in secure, geographically separate locations to avoid being affected by the same disaster.
 - **Redundant Systems:** Implementing redundant hardware and systems (e.g., failover systems) ensures that services continue to operate even if one component fails.
 - **Disaster Recovery Plans:** A comprehensive disaster recovery plan (DRP) is essential for data recovery. It defines the steps to be taken in the event of a data breach, corruption, or loss.
- **Challenges:**

- **Speed of Recovery:** Ensuring that recovery times are as short as possible to minimize downtime and data loss.
- **Ensuring Data Integrity:** After quarantine and recovery, it is essential to verify that the restored data is accurate and has not been tampered with.

5. Hippocratic Databases: Current Capabilities and Future Trends

- **Hippocratic Databases** are designed to respect user privacy and data protection principles. The term "Hippocratic" refers to the Hippocratic Oath in medicine, where practitioners promise to do no harm. Similarly, Hippocratic databases aim to limit the collection, processing, and sharing of personal data to the minimum necessary to achieve the desired outcome.
- **Current Capabilities:**
 - **Data Minimization:** Hippocratic databases adhere to the principle of only collecting the minimal amount of personal data needed for a given purpose.
 - **Data Anonymization:** These databases implement strong anonymization techniques to ensure that personal data cannot be traced back to individuals.
 - **User Consent:** A fundamental feature of Hippocratic databases is obtaining explicit consent from users before processing their data. This is especially important in complying with data protection laws like GDPR.
 - **Audit and Transparency:** These databases log every access and modification to sensitive data, ensuring transparency and accountability.
- **Future Trends:**
 - **Decentralized Databases:** In the future, we may see an increase in decentralized databases (e.g., blockchain-based systems) that empower users to control their data and ensure privacy by design.
 - **Smart Contracts for Data Sharing:** Smart contracts could be used to automate and enforce privacy policies, ensuring that personal data is only shared under agreed-upon conditions.
 - **Privacy-Preserving Data Analytics:** Techniques such as **federated learning** and **differential privacy** will enable organizations to conduct data analysis without compromising user privacy.

- **Integration with Legal Frameworks:** Hippocratic databases will likely become more tightly integrated with evolving privacy laws and regulatory frameworks, offering seamless compliance feature.

UNIT - V: Privacy in Database Publishing and Mobile Environment Security

1. Privacy in Database Publishing: A Bayesian Perspective

- **Database Publishing** refers to the process of sharing or publishing data stored in databases, typically for analytical, reporting, or research purposes. This raises concerns about **privacy**, especially when the data includes sensitive or personal information.
- **Privacy in Database Publishing** is about ensuring that when data is shared or published, it does not violate the privacy of individuals or organizations. This involves techniques and policies to prevent **data leakage** while still making the data useful for analysis.
- **Bayesian Perspective:**

- A **Bayesian approach** to privacy focuses on managing the uncertainty and probabilistic nature of information in database publishing.
- In this context, the **Bayesian approach** deals with estimating the likelihood that certain pieces of information can be derived or inferred from the published data. This is particularly useful in cases where some level of data anonymization or generalization is needed.
- The **Bayesian model** helps in quantifying and managing the risk of re-identifying individuals in anonymized datasets by assessing the likelihood of disclosure based on known background information.
- **Differential Privacy** techniques can be incorporated into the Bayesian perspective to ensure that the risk of re-identification is minimized, by adding controlled noise to data queries or releases.
- **Techniques to Protect Privacy:**
 - **K-Anonymity:** A technique where data is generalized or suppressed to ensure that each record is indistinguishable from at least k other records.
 - **L-Diversity:** Ensures that sensitive attributes are well-represented across the dataset, preventing attackers from making inferences about individuals' sensitive information.
 - **T-Closeness:** Ensures that the distribution of sensitive attributes within each group is similar to the distribution in the overall database, reducing the risk of inference attacks.
- **Challenges:**
 - Balancing privacy with the utility of the data. Overly aggressive anonymization can reduce the value of the dataset for analysis.
 - Ensuring that privacy protection techniques do not conflict with regulations, such as GDPR or HIPAA, which demand stricter privacy controls.

2. Privacy-enhanced Location-based Access Control

- **Location-based Access Control (LBAC)** is a type of access control that grants or denies access to information based on the geographical location of the user or device making the request.

- **Privacy-Enhanced Location-based Access Control** focuses on ensuring that location-based policies do not inadvertently leak sensitive information about individuals or compromise privacy. It is especially important in systems like mobile apps, IoT devices, and other services that rely on location data.
- **Key Features:**
 - **Location Privacy:** Ensuring that users' exact locations are not unnecessarily exposed to unauthorized parties. Techniques like **location obfuscation** (randomly altering the precision of location data) are often used to protect users' privacy.
 - **Access Control Based on Zones:** Rather than granting access based on a precise location, access can be granted based on predefined zones (e.g., granting access if the user is within a certain city, region, or even a specific building).
 - **Geo-Fencing:** Setting up virtual boundaries to restrict or grant access when a user enters or exits a specific geographical area. Geo-fencing can trigger specific actions based on location while protecting the user's privacy by limiting the amount of location data shared.
 - **Role-Based Location Access:** Using the roles of users in combination with location information to make access decisions (e.g., allowing an employee to access a particular resource only when they are within a specific geographic boundary).
- **Challenges:**
 - **Accuracy vs. Privacy:** There is often a trade-off between the accuracy of location-based services and the privacy of the user. Higher accuracy can increase privacy risks.
 - **Contextual Access Control:** Enforcing policies based on both location and other contextual information (e.g., time of day, device type, etc.) is complex and may require fine-grained control mechanisms.
 - **Dynamic and Evolving Privacy:** As a user moves, the privacy requirements might change dynamically, creating difficulties in enforcing location-based privacy rules.
- **Techniques:**
 - **K-Anonymity for Location Data:** Ensuring that the location data shared about a user corresponds to multiple users, thus hiding their precise position.

- **Location-based Encryption:** Encrypting location data to protect it from unauthorized access while still enabling authorized users to access services based on location.

3. Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment

- **Mobile Environments** (smartphones, tablets, IoT devices) present unique security and privacy challenges due to their portability, constant internet connectivity, and the collection of personal data.
- **Security and Privacy Policies in Mobile Environments:**
 - Mobile applications and services collect a large amount of personal and sensitive data, such as location, contacts, browsing history, and photos. Enforcing security and privacy policies effectively is essential to protect users from unauthorized access, data breaches, and privacy violations.
- **Key Considerations:**
 - **App Permissions:** Mobile applications require permissions to access various system resources (e.g., camera, microphone, location services). Ensuring that apps only request the minimum necessary permissions is key to enforcing privacy policies.
 - **Data Encryption:** Encrypting sensitive data both at rest (on the device) and in transit (during communication) is essential in protecting users from potential breaches or man-in-the-middle attacks.
 - **Secure Data Storage:** Mobile devices often store data locally (e.g., on the device's file system, cloud storage, or caches). Protecting data locally ensures that even if a device is lost or compromised, the data remains secure.
- **Privacy Policies in Mobile Environments:**
 - **Consent Management:** Implementing clear and transparent consent mechanisms that allow users to choose what data is collected and shared.
 - **Data Minimization:** Limiting the collection and sharing of user data to only what is necessary for the app or service to function.
 - **Anonymization and Pseudonymization:** Anonymizing or pseudonymizing user data so that it cannot be traced back to the individual without additional information, thus enhancing privacy.

- **Context-Aware Policies:** Privacy policies that adjust based on factors such as the user's current location, device type, and network conditions.
- **Efficient Enforcement of Security:**
 - **Mobile Device Management (MDM):** Organizations use MDM solutions to enforce security policies on employees' mobile devices, such as requiring encryption, setting strong passwords, and ensuring compliance with corporate security standards.
 - **Trusted Execution Environments (TEE):** A secure area within the mobile device's processor that ensures sensitive data is processed in a protected environment. This can help in protecting both privacy and security.
 - **App Sandboxing:** Isolating apps within separate containers to ensure that malicious apps cannot access data or resources belonging to other apps.
 - **Behavioral Analysis:** Analyzing the behavior of apps and users to detect anomalous or suspicious activity. If suspicious behavior is detected, the system can enforce privacy and security policies to limit potential damage.
- **Challenges:**
 - **Battery Life and Performance:** Security and privacy enforcement mechanisms must be optimized to ensure they do not excessively drain battery life or degrade performance.
 - **Fragmentation:** The variety of mobile operating systems (e.g., Android, iOS) and devices makes it difficult to enforce uniform security and privacy policies across all devices.
 - **Cross-Platform Security:** Many mobile apps are available across multiple platforms (iOS, Android, etc.), which means security and privacy policies must be enforceable across different operating systems.

XIII. ADDITIONAL TOPICS

- To enhance the depth and breadth of a **Web Security** course or module, incorporating the following advanced and emerging topics can be highly beneficial:

1.Cloud Security in Web Applications

- Securing web applications hosted on cloud platforms (AWS, Azure, GCP).
- Identity and Access Management (IAM) for cloud services.
- Data encryption and key management in the cloud.
- Security compliance and governance for cloud applications.

2. Container Security

- Securing Docker containers and Kubernetes clusters.
- Vulnerability scanning of container images.
- Implementing network policies and access control.
- Monitoring containerized applications for security threats.

3.Secure Authentication and Authorization

- Multi-Factor Authentication (MFA) and Adaptive Authentication.
- Implementing Single Sign-On (SSO) solutions.
- Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).
- Password hashing techniques (bcrypt, Argon2).

4. Web Application Firewalls (WAFs)

- Understanding WAF architecture and functionality.
- Configuring WAFs to prevent SQL injection, XSS, and DDoS attacks.
- Comparing cloud-based and on-premises WAFs.
- Monitoring and analyzing WAF logs

5.Incident Response and Forensics

- Identifying, responding to, and mitigating web-based attacks.
- Digital forensics techniques to analyze compromised web applications.
- Creating an incident response plan for web applications.
- Legal and compliance aspects of incident management.

XIV. MID EXAM QUESTION PAPERS-THEORY AND QUIZ

MULTIPLE CHOICE QUESTIONS

1. Which of the following actions compromise cyber security?
 - a) Vulnerability
 - b) Attack
 - c) Threat
 - d) Exploit

2. Which of the following privacy protection mechanisms helps ensure that data sent over the internet is secure and encrypted?
 - A) HTTPS (SSL/TLS)
 - B) Hashing
 - C) Pseudonymization
 - D) Data Minimization

3. Which of the following is a primary concern of physical security for servers?
 - a) Preventing unauthorized access
 - b) Ensuring data encryption
 - c) Installing antivirus software
 - d) Updating the operating system
4. Which of the following is the most effective way to physically secure a server in a data center?
 - a) Use of firewalls
 - b) Biometric authentication
 - c) Regular software updates
 - d) Password protection on the server OS

5. In a data center, what is the purpose of CCTV cameras?
 - a) To detect server hardware failures
 - b) To monitor and record physical access
 - c) To analyze network traffic
 - d) To ensure proper cooling

6. Which of the following measures helps ensure a server is protected from physical damage due to fire?
 - a) Using firewalls
 - b) Installing fire suppression systems
 - c) Regularly patching the server OS
 - d) Configuring backup power systems

7. Which of the following is a primary objective of data backups?

- a) To reduce data storage size
- b) To protect data from loss or corruption
- c) To increase network traffic
- d) To optimize system performance

8. Which of the following should be considered when choosing a backup medium for important data?

- a) The cost of storage
- b) The ease of retrieving data
- c) The security of data at rest
- d) All of the above

9. Which of the following methods can be used to track stolen devices?

- a) Use of full disk encryption
- b) Installation of a tracking software or hardware
- c) Regular data backups
- d) Use of biometric authentication

10 . Which of the following best describes a “data breach” due to theft?

- a) Unauthorized access and/or theft of sensitive information
- b) Loss of data due to hardware failure
- c) Software vulnerability exploitation
- d) Corruption of data due to network failure

FILL IN THE BLANKS

1. A _____ is a technique that allows users to browse the web anonymously by routing internet traffic through a series of servers to mask their IP address and location
2. IDPS stands for _____
3. **To reduce the potential impact of a security breach, it’s important to regularly back up server data, which is known as _____.**
4. A technique for preventing unauthorized access to a server by requiring two different types of verification is called _____.
5. Servers should be placed in _____ environments that control factors like temperature and humidity to prevent hardware damage.
6. To ensure that only authorized individuals can access the server, administrators should implement _____, which grants access based on user roles.

7. XSS stands for _____
8. Use _____ systems to perform regular backups to ensure data is always up to date.
9. A complete copy of all files is called _____.
10. _____ is the practice of collecting only the minimum amount of personal data necessary to fulfill a specific purpose.

ANSWER ANY TWO OF THE FOLLOWING QUESTIONS

1. What is Web Security? Explain in detail the Risk Analysis and Best Practices.
2. Explain in detail about Backups and Antitheft with examples.
3. Explain the feature of Recent Advances in Access Control

XV. UNIVERSITY QUESTION PAPERS OF PREVIOUS YEARS

Code No: 157EE

R18

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, February/March - 2022

WEB SECURITY
(Information Technology)

Time: 3 Hours

Max. Marks: 75

Answer any five
questions All questions
carry equal marks

- - -

- 1.a) What is meant by web security problem?
b) What are the legal restrictions on cryptography? [7+8]
- 2.a) Explain about digital identification.
b) What is the significance of cryptography in view of web security? [7+8]
3. Explain privacy-protecting techniques. [15]
4. Explain how to secure web applications. [15]
- 5.a) Explain access control models of XML.
b) What are the database issues in trust management? [8+7]
- 6.a) Explain the security in OLAP systems. What
b) are the advantages of watermarking? [8+7]
7. Explain the database watermarking for copyright protection. [15]
- 8.a) What are the privacy policies in mobile environment?
b) Explain about Bayesian perspective. [8+7]

---oo0oo---

Code No: 137JG

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

**B. Tech IV Year I Semester Examinations, March
2021**

WEB AND DATABASE SECURITY

(Information Technology)

Time: 3 Hours

Answer any Five Questions

All Questions Carry Equal Marks

1. What is Web Security? Explain in detail the Risk Analysis and Best Practices. [15]
- 2.a) Write a detailed note on Cryptography and legal restrictions on cryptography.
b) Explain in detail about Backups and Antitheft with examples. [6+9]
- 3.a) How to provide security for web applications? Demonstrate with suitable example.
b) Explain in detail about Web Server Security. [6+9]
4. What is Database Security? Explain in detail about Security in Data Warehouses and OLAP Systems. [15]
5. Explain in detail about various techniques in Security Re-engineering for Databases.
6. Write a detailed note on Damage Quarantine and Recovery in Data Processing Systems. [15]
- 7.a) Explain in detail about Future Trends Privacy in Database Publishing.
b) Write a detailed note on Privacy-Protecting Techniques. [6+9]
8. Write a detailed note on Privacy-enhanced Location-based Access Control. [15]

XVI. UNIT-WISE QUIZ QUESTIONS

UNIT-1

MCQ

1. What does the term "Phishing" refer to in the context of web application security?

- a) Enhancing user interfaces
- b) Sending deceptive emails or messages to trick users into revealing sensitive information
- c) Cross-platform scripting languages
- d) Site-specific scripting languages

2. What is the purpose of encrypting data in transit?

- A. Improving website aesthetics
- B. Optimizing server processing speed
- C. Protecting data from interception during transmission
- D. Enhancing user interfaces

3. How can a Distributed Denial of Service (DDoS) attack impact a web application?

- A. By improving website aesthetics
- B. By increasing server performance
- C. By overwhelming server resources and making the application unavailable
- D. By designing efficient database structures

4. What security measure can help protect against SQL injection attacks?

- A. Input validation
- B. Use of session cookies
- C. Cross-Site Scripting (XSS)
- D. Encryption of stored data

5. How can a web application defend against Cross-Site Request Forgery (CSRF) attacks?

- A. By using secure coding practices
- B. By encrypting stored data
- C. By implementing strong password policies
- D. By blocking access to certain IP addresses

6. How does user education and awareness contribute to web application security?

- A. By improving website aesthetics
- B. By helping users recognize and avoid security threats, such as phishing
- C. By optimizing server processing speed
- D. By designing efficient database structures

7. What is the role of a Web Application Firewall (WAF) in web application security?

- A. Designing website layouts

- B. Monitoring and filtering HTTP traffic between a web application and the Internet
- C. Enhancing server performance
- D. Managing user authentication

8. Why is it crucial to secure web applications?

- A. To increase website loading speed
- B. To prevent unauthorized access, attacks, and data breaches
- C. To enhance server storage capacity
- D. To optimize user interface design

9. Which of the following is defined as an attempt to harm, damage or cause threat to a system or network?

- a) Digital crime
- b) Threats
- c) System hijacking
- d) Cyber Attack

10. Where did the term “hacker” originate?

- a) MIT
- b) New York University
- c) Harvard University
- d) Bell’s Lab

FILL IN THE BLANKS

1. The full form of Malware is _____
2. _____ is a code injecting method used for attacking the database of a system / website.
3. _____ refers to protecting networks and computer systems from damage to or the theft of software, hardware, or data.
4. The Process of converting plain text to cipher text is called _____
5. URL stands for _____
6. A _____ is a small piece of textual information sent by the server to the client, stored on the client, and returned by the client for all requests to the server.
7. _____ creates a parallel public key infrastructure built upon the DNS system.
8. A _____ is issued by a Certificate Authority (CA) to authenticate the identity of a server.
9. In web security, _____ is a technique that ensures that only authorized users can access specific resources or perform certain actions.

10. _____ is a mechanism to ensure data integrity and protect against unauthorized alterations of messages or data during transmission.

UNIT-2

5. Which of the following actions compromise cyber security?
- a) Vulnerability
 - b) Attack
 - c) Threat
 - d) Exploit
6. Which of the following privacy protection mechanisms helps ensure that data sent over the internet is secure and encrypted?
- A) HTTPS (SSL/TLS)
 - B) Hashing
 - C) Pseudonymization
 - D) Data Minimization
7. Which of the following is a primary concern of physical security for servers?
- a) Preventing unauthorized access
 - b) Ensuring data encryption
 - c) Installing antivirus software
 - d) Updating the operating system
8. Which of the following is the most effective way to physically secure a server in a data center?
- a) Use of firewalls
 - b) Biometric authentication
 - c) Regular software updates
 - d) Password protection on the server OS

5. In a data center, what is the purpose of CCTV cameras?

- a) To detect server hardware failures
- b) To monitor and record physical access
- c) To analyze network traffic
- d) To ensure proper cooling

6. Which of the following measures helps ensure a server is protected from physical damage due to fire?

- a) Using firewalls
- b) Installing fire suppression systems
- c) Regularly patching the server OS
- d) Configuring backup power systems

7. Which of the following is a primary objective of data backups?

- a) To reduce data storage size
- b) To protect data from loss or corruption
- c) To increase network traffic
- d) To optimize system performance

8. Which of the following should be considered when choosing a backup medium for important data?

- a) The cost of storage
- b) The ease of retrieving data
- c) The security of data at rest
- d) All of the above

9. Which of the following methods can be used to track stolen devices?

- a) Use of full disk encryption
- b) Installation of a tracking software or hardware
- c) Regular data backups
- d) Use of biometric authentication

10. Which of the following best describes a “data breach” due to theft?

- a) Unauthorized access and/or theft of sensitive information
- b) Loss of data due to hardware failure
- c) Software vulnerability exploitation
- d) Corruption of data due to network failure

FILL IN THE BLANKS

11. A _____ is a technique that allows users to browse the web anonymously by routing internet traffic through a series of servers to mask their IP address and location

12. IDPS stands for _____

13. To reduce the potential impact of a security breach, it's important to regularly back up server data, which is known as _____.
14. A technique for preventing unauthorized access to a server by requiring two different types of verification is called _____.
15. Servers should be placed in _____ environments that control factors like temperature and humidity to prevent hardware damage.
16. To ensure that only authorized individuals can access the server, administrators should implement _____, which grants access based on user roles.
17. XSS stands for _____.
18. Use _____ systems to perform regular backups to ensure data is always up to date.
19. A complete copy of all files is called _____.
20. _____ is the practice of collecting only the minimum amount of personal data necessary to fulfill a specific purpose.

UNIT – 03

CHOOSE THE CORRECT ANSWERS

1. Which of the following is an essential component of database security?
 - a) Backup and recovery
 - b) Encryption
 - c) Access control
 - d) All of the above
2. Which type of attack involves gaining access to a database by exploiting weak or default credentials?
 - a) Phishing
 - b) Brute Force Attack
 - c) SQL Injection
 - d) Cross-Site Scripting (XSS)
3. Which of the following is true about XML-based Access Control Models?
 - a) XML Access Control Models are designed to manage access to XML documents based on user roles.
 - b) XML Access Control Models are used only for protecting web applications.
 - c) XML Access Control Models cannot be integrated with other security models.
 - d) None of the above.
4. What is the primary purpose of Role-Based Access Control (RBAC) in XML access control models?
 - a) To assign access based on the user's IP address.
 - b) To assign access based on the user's role or responsibility within an organization.
 - c) To encrypt XML documents.
 - d) To manage user sessions for XML files.
5. MySQL uses security based on ACL which stands for _____.
 - a) Access Control Language
 - b) Access Control Lists

- c) Automatic Control Lists
- d) Automatic Control Language

FILL IN THE BLANKS

- _____ refers to the protection of databases from unauthorized access, misuse, and threats that could compromise the confidentiality, integrity, and availability of stored data..
- _____ is widely used for storing and transmitting structured data in databases and web services.
- _____ is a key principle of the Attribute-Based Access Control (ABAC) model, which grants access based on attributes of users, objects, or the environment.
- An important challenge in XML access control is ensuring that policies are applied _____ across various documents and applications.
- A _____ is a mathematical scheme for verifying the authenticity and integrity of messages or documents.

XVII. TUTORIAL PROBLEMS WITH BLOOMS MAPPING

S.No	Questions	Bloom's Level
1	Define web security and explain its importance in modern web applications.	Remembering
2	Differentiate between HTTP and HTTPS protocols with suitable examples.	Analyzing
3	Explain the difference between authentication and authorization with real-world examples.	Analyzing
4	Identify vulnerabilities in the following SQL query and suggest mitigation strategies:	Analyzing
5	Design a secure login mechanism to prevent SQL injection attacks.	Creating
6	Describe the different types of XSS attacks and their impact on web applications.	Understanding
7	Analyze a given web application code and recommend techniques to prevent XSS attacks.	Analyzing
8	Explain how CSRF attacks work and suggest effective prevention techniques.	Understanding
9	Illustrate how TLS/SSL ensures secure communication between client and server.	Applying

10	Evaluate the impact of weak encryption algorithms in web security.	Evaluating
11	Define a Web Application Firewall (WAF) and list its functionalities.	Remembering
12	Design a secure session management protocol for an e-commerce application.	Creating
13	Discuss the importance of ethical hacking in web security.	Understanding
14	Explain session hijacking and how it can be mitigated.	Understanding

XVIII. ASSIGNMENT QUESTIONS WITH BLOOMS MAPPING

S.No.	Questions	Bloom's Level
1	What is Web Security? Explain in detail the Risk Analysis and Best Practices.	Understanding
2	Explain in detail about Web Server Security.	Understanding
3	How to provide security for web applications? Demonstrate with suitable example	Analyzing
4	Write the role of cryptography on web.	Remembering
5	Write the SSL protocol features.	Remembering
6	Write a detailed note on Cryptography and legal restrictions on cryptography.	Remembering
7	Explain in detail about Backups and Antitheft with examples	Understanding
8	Explain in detail about Backups and Antitheft with examples	Understanding
9	Explain about digital identification	Understanding

10	Explain privacy-protecting techniques.	Understanding
11	Explain access control models of XML.	Understanding
12	What are the database issues in trust management?	Understanding
13	Explain the security in OLAP systems.	Understanding
14	What is Database Security? Explain in detail about Security in Data Warehouses and OLAP Systems.	Understanding
15	Explain in detail about various techniques in Security Re-engineering for Databases.	Understanding
16	Write a detailed note on Privacy-enhanced Location-based Access Control	Remembering
17	Discuss about various antitheft techniques.	Understanding
18	Write a detailed note on Damage Quarantine and Recovery in Data Processing Systems.	Remembering
19	Explain about Bayesian perspective	Remembering
20	Write the goal of trustworthy record retention.	Understanding

XIX. List of students

Roll No.	Student Name
21C31A6601	ABUL FATAH MOHAMMED AFFANULLAH
21C31A6602	ADDAGUDURU KRISHNA Koushik
21C31A6603	ALUGOJU SARASWATHI
21C31A6604	AMANCHA VIVEK
21C31A6605	ANNARAPU VINAY
21C31A6606	ARENDRA DHARANI
21C31A6607	BAJJURI MAMATHA
21C31A6608	BHUKYA THRISHA
21C31A6609	BODDULA RAHUL
21C31A6610	BOLLA USHASREE
21C31A6611	BOLLOJU ANUSHA
21C31A6612	BUSIREDDY MADHURI
21C31A6613	CHALLURI DINESH KUMAR
21C31A6614	CHALLURI RAHUL
21C31A6615	CHELPURI RADHIKA
21C31A6616	CHITTHALURI ANUDEEP
21C31A6617	DEEKONDA CHANDU
21C31A6618	DENABOINA PRAVALIKA
21C31A6619	DUPATI SRICHARAN
21C31A6620	ENAGANTI MANOJ
21C31A6621	FAISAL SYED
21C31A6622	GANDI GOUTHAM
21C31A6623	GATTIKOPPULA AJAY
21C31A6624	GUDURU SAI RAJ
21C31A6625	GUMMADIRAJU REVATHI
21C31A6626	JADALA RAM SAGAR
21C31A6627	KALLEPELly ARCHANA
21C31A6628	KOMURAVELLI SHIVA KUMAR
21C31A6629	KORRA KAVYA
21C31A6630	KOYYADA CHANDAN RAJ
21C31A6631	KUCHANA RACHANA
21C31A6632	KUKKALA RAVI KIRAN
21C31A6633	KYATHAM ROHITH
21C31A6634	LADE KAVYASRI
21C31A6635	LAKAVATH VENKANNA
21C31A6636	MADIPELly MUKTHA NANDHINI
21C31A6637	MOHAMMED ABDUL RAHAMAN
21C31A6638	MOHAMMED RAJJU

21C31A6639	MOHAMMED SAMEER
21C31A6640	MOHAMMED YAKUB FARAZ KHAN
21C31A6641	MUNIGALA POORNACHANDER
21C31A6642	MUNIGANTI AKHIL
21C31A6643	NALLA ADITHYA
21C31A6644	NALLA LAXMI PRASANNA
21C31A6645	NARUGULA RAKESH
21C31A6646	NAVEEN ADEPU
21C31A6647	NUNAVATH BALARAJU
21C31A6648	PARUNANDHI PAVAN WESLY
21C31A6649	PILLALAMARRI SUDHEER
21C31A6650	PILLI HARSHASRI
21C31A6651	PITTA ARAVIND
21C31A6652	SABBANI RAKSHITHA
21C31A6653	SHAIK SALMAN
21C31A6654	SHANIGARAPU JHANSY
21C31A6655	SILUVERU PRINCE
21C31A6656	SINGARAPU SRAVANI
21C31A6657	SRIRAMULA SRILEKHA
21C31A6658	TAKKALLAPALLY KANISHKA
21C31A6659	THADAKA SRI POOJA
21C31A6660	THATIKONDA NARESH
21C31A6661	VALLAKATLA TEJA
21C31A6662	VELPURI NIHARIKA
21C31A6663	YARRAM SAI DATH
22C35A6601	AKULA ROHITH
22C35A6602	CHINDAM SHIVA KUMAR
22C35A6603	GADE SUSHMA SRI
22C35A6604	MOHAMMAD AVEZ
22C35A6605	MADHUKAR
22C35A6606	RAVIRAKULA SANDEEP

XX. SCHEME AND SOLUTION OF INTERNAL TESTS.

In CIE, for theory subjects, during a semester, there shall be two mid-term examinations. Each Mid-Term examination consists of two parts i) **Part – A** for 10 marks, ii) **Part – B** for 20 marks with a total duration of 2 hours as follows:

1. Mid Term Examination for 30 marks:

- Part - A : Objective/quiz paper for 10 marks.
- Part - B : Descriptive paper for 20 marks.

The objective/quiz paper is set with multiple choice, fill-in the blanks and match the following type of questions for a total of 10 marks. The descriptive paper shall contain 6 full questions out of which, the student has to answer 4 questions, each carrying 5 marks. The **average of the two Mid Term Examinations** shall be taken as the final marks for Mid Term Examination (for 30 marks).

The remaining 10 marks of Continuous Internal Evaluation are distributed as:

- 2. Assignment for 5 marks. (Average of 2 Assignments each for 5 marks)**
- 3. Subject Viva-Voce/PPT/Poster Presentation/ Case Study on a topic in the concerned subject for 5 marks.**

While the first mid-term examination shall be conducted on 50% of the syllabus, the second mid-term examination shall be conducted on the remaining 50% of the syllabus. Five (5) marks are allocated for assignments (as specified by the subject teacher concerned). The first assignment should be submitted before the conduct of the first mid-term examination, and the second assignment should be submitted before the conduct of the second mid-term examination. The average of the two assignments shall be taken as the final marks for assignment (for 5 marks). Subject Viva-Voce/PPT/Poster Presentation/ Case Study on a topic in the subject concerned for 5 marks before II Mid-Term Examination.


Marks Sheet

XXII. Marks Sheet

Sl. No	Roll Number	Name of the Candidate	Marks			Part - B	Part - A	A+B	Unit Test	Assessment	Grand
			Q1	Q2	Q3						
1	21C31A6601	Abul Fatah Mohammed Affanullah	ABSENT					0	5	4	9
2	21C31A6602	Addaguduru Krishna Koushik		4	4	8	10	18	5	5	28
3	21C31A660	Alugoju Saraswathi	5		5	10	10	20	5	5	30
4	21C31A660	Amancha Vivek		5	5	10	10	20	5	5	30
5	21C31A660	Annarapu Vinay	5	5		10	10	20	5	5	30
6	21C31A660	Arendra Dharani	5		4	9	10	19	5	5	29
7	21C31A660	Bajjuri Mamatha	5	4		9	9	18	5	5	28
8	21C31A660	Bhukya Thrisha	5	5		10	9	19	0	4	23
9	21C31A660	Boddula Rahul	4		5	9	10	19	0	5	24
10	21C31A661	Bolla Ushasree	4	4		8	10	18	5	4	27
11	21C31A6611	Bolloju Anusha	2	3		5	9	14	0	4	18
12	21C31A661	Busireddy Madhuri	4	5		9	10	19	0	5	24
13	21C31A661	Challuri Dinesh Kumar	5		3	8	7	15	3	4	22
14	21C31A661	Challuri Rahul	2		1	3	7	10	4	4	18
15	21C31A661	Chelpuri Radhika		5	2	7	6	13	5	5	23
16	21C31A661	Chitthaluri Anudeep	ABSENT					0	5	5	10
17	21C31A661	Deekonda Chandu	5		2	7	10	17	5	5	27
18	21C31A661	Denaboina Pravalika	5	5		10	9	19	0	4	23
19	21C31A661	Dupati Sricharan	4		3	7	9	16	4	4	24
20	21C31A662	Enaganti Manoj	3			3	9	12	4	4	20
21	21C31A662	Faisal Syed	2			2	8	10	0	3	13
22	21C31A662	Gandi Goutham	2			2	8	10	4	3	17
23	21C31A662	Gattikoppula Aiy	2			2	8	10	5	5	20

23	21C31A662	Ganikoppula Hjay	4			4	8	10	5	5	20
24	21C31A662	Guduru Sai Raj	5	5		10	8	18	5	4	27
25	21C31A662	Gummadiraju Revathi	5	5		10	9	19	0	5	24
26	21C31A662	Jadala Ram Sagar	3	1		4	9	13	4	4	21
27	21C31A662	Kallepelly Archana	5	5		10	9	19	5	5	29
28	21C31A662	Komuravelli Shiva Kumar	4			4	9	13	4	4	21
29	21C31A662	Korra Kavya	5	1		6	9	15	0	5	20
30	21C31A663	Koyyada Chandan Raj	4		3	7	9	16	5	5	26
31	21C31A663	Kuchana Rachana	5		5	10	9	19	5	5	29
32	21C31A663	Kukkala Ravi Kiran	3	3		6	9	15	5	5	25
33	21C31A663	Kyatham Rohith	4	4		8	9	17	4	5	26
34	21C31A663	Lade Kavyasri	4	4		8	9	17		5	22
35	21C31A663	Lakavath Venkanna		3	4	7	9	16	5	5	26
36	21C31A663	Madipelly Muktha Nandhini	5	5		10	9	19	5	5	29
37	21C31A663	Mohammed Abdul Rahaman	ABSENT					0	5	5	10
38	21C31A663	Mohammed Rajju	2			2	9	11	4	4	19
39	21C31A663	Mohammed Sameer		2	3	5	9	14		4	18
40	21C31A664	MD Yakub Faraz Khan	2		2	4	9	13	4	4	21
41	21C31A664	Munigala	1			1	9	10		4	14
42	21C31A664	Muniganti Akhil	4		4	8	9	17	4	5	26
43	21C31A664	Nalla Adithya	5	5		10	7	17	5	5	27
44	21C31A664	Nalla Lakmi Prasanna	5	5		10	8	18	5	5	28
45	21C31A664	Narugula Rakesh	5	3		8	9	17	5	5	27
46	21C31A664	Naveen Adepu	2			2	8	10	4	5	19
47	21C31A664	Nunavath Balaraju	2			2	8	10	0	4	14
48	21C31A664	Parunandhi Pavan	ABSENT					0	3	4	7
49	21C31A664	Pillalamarri Sudheer	5		5	10	10	20	5	5	30
50	21C31A665	Pilli Harshasri	5		3	8	9	17	5	5	27
51	21C31A665	Pitta Aravind	3		2	5	9	14	4	5	23
52	21C31A665	Sabbani Rakshitha	5	5		10	9	19	5	5	29
53	21C31A665	Shaik Salman		2	1	3	9	12	4	5	21
54	21C31A665	Shanigarapu Jhansy	4	3		7	9	16	5	5	26
55	21C31A665	Siluveru Prince	3	3		6	9	15	5	5	25
56	21C31A665	Singarapu Sravani	5			5	9	14	5	5	24
57	21C31A665	Sriramula Srilekha		2	3	5	9	14	5	5	24
58	21C31A665	Takkalapally Kanishka		5	5	10	9	19	5	5	29
59	21C31A665	Thadaka Sri Pooja		5	5	10	9	19	5	5	29
60	21C31A666	Thatikonda Nareesh	5	5		10	9	19	5	5	29
61	21C31A666	Vallakatla Teja	5	5		10	9	19	5	5	29
62	21C31A666	Velpuri Niharika	3	3		6	9	15	5	5	25
63	21C31A666	Yarram Sai Dath	5	3		8	9	17	5	4	26
64	22C35A66	Akula Rohith	5		4	9	9	18	5	5	28
65	02	Chindam Shiva Kumar		4	4	8	9	17	5	5	27
66	22C35A66	Gade Sushma Sri	ABSENT								
67	04	Mohammad Avez	3	3		6	10	16	0	5	26
68	05	Madhukar	3	3		6	9	15	0	5	20
69	06	Ravirakula Sandeep	2			2	9	11	0	4	15

XXIII. Result Analysis for internal exams(tests).

<div>  <div> Balaji Institute of Technology & Science Laknepally, Narsampet, Warangal - 506331 (AUTONOMOUS) Accredited by NBA (UG – CE, EEE, ME, ECE & CSE) & NAAC A+ Grade (Affiliated to JNTUH, Hyderabad and Approved by AICTE, New Delhi) www.bitswgl.ac.in, email: principal@bitswgl.ac.in, Ph: 98660 50044, Fax: 08718-230521 </div> </div>											
EVALUATION PROCESS: MID -I, MAR 2025 Course - B.Tech. Branch - CSE(AI&ML), Year & Sem: IV / II Subject: Web Security											
Name of the											
S.No.	Answer any two questions.					Mark	Level of		CO		
1	What is Web Security? Explain in detail the Risk Analysis and Best Practices.					5	Understand		CO1		
2	Explain in detail about Backups and Antitheft with examples.					5	Understand		CO2		
3	Explain the feature of Recent Advances in Ad					5	Remember		CO3		
Sl. No	Roll Number	Name of the Candidate	Marks			Part - B	Part - A	A+B	Unit Test	Assessment	Grand
			Q1	Q2	Q3						
1	21C31A6601	Abul Fatah Mohammed Affanullah	ABSENT					0	5	4	9
2	21C31A6602	Addaguduru Krishna Koushik		4	4	8	10	18	5	5	28
3	21C31A660	Alugoju Saraswathi	5		5	10	10	20	5	5	30
4	21C31A660	Amancha Vivek		5	5	10	10	20	5	5	30
5	21C31A660	Annarapu Vinay	5	5		10	10	20	5	5	30
6	21C31A660	Arendra Dharani	5		4	9	10	19	5	5	29
7	21C31A660	Bajjuri Mamatha	5	4		9	9	18	5	5	28
8	21C31A660	Bhukya Thrisha	5	5		10	9	19	0	4	23
9	21C31A660	Boddula Rahul	4		5	9	10	19	0	5	24
10	21C31A661	Bolla Ushasree	4	4		8	10	18	5	4	27
11	21C31A6611	Bolloju Anusha	2	3		5	9	14	0	4	18
12	21C31A661	Busireddy Madhuri	4	5		9	10	19	0	5	24
13	21C31A661	Challuri Dinesh Kumar	5		3	8	7	15	3	4	22
14	21C31A661	Challuri Rahul	2		1	3	7	10	4	4	18
15	21C31A661	Chelpuri Radhika		5	2	7	6	13	5	5	23
16	21C31A661	Chitthaluri Anudeep	ABSENT					0	5	5	10
17	21C31A661	Deekonda Chandu	5		2	7	10	17	5	5	27
18	21C31A661	Denaboina Pravalika	5	5		10	9	19	0	4	23
19	21C31A661	Dupati Sricharan	4		3	7	9	16	4	4	24
20	21C31A662	Enaganti Manoj	3			3	9	12	4	4	20
21	21C31A662	Faisal Syed	2			2	8	10	0	3	13
22	21C31A662	Gandi Goutham	2			2	8	10	4	3	17
23	21C31A662	Gattikoppula Ajay	2			2	8	10	5	5	20

23	21C31A662	Garikoppula Hjay	2			2	8	10	5	5	20
24	21C31A662	Guduru Sai Raj	5	5		10	8	18	5	4	27
25	21C31A662	Gummadiraju Revathi	5	5		10	9	19	0	5	24
26	21C31A662	Jadala Ram Sagar	3	1		4	9	13	4	4	21
27	21C31A662	Kallepelly Archana	5	5		10	9	19	5	5	29
28	21C31A662	Komuravelli Shiva Kumar	4			4	9	13	4	4	21
29	21C31A662	Korra Kavya	5	1		6	9	15	0	5	20
30	21C31A663	Koyyada Chandan Raj	4		3	7	9	16	5	5	26
31	21C31A663	Kuchana Rachana	5		5	10	9	19	5	5	29
32	21C31A663	Kukkala Ravi Kiran	3	3		6	9	15	5	5	25
33	21C31A663	Kyatham Rohith	4	4		8	9	17	4	5	26
34	21C31A663	Lade Kavyasri	4	4		8	9	17		5	22
35	21C31A663	Lakavath Venkanna		3	4	7	9	16	5	5	26
36	21C31A663	Madipelly Muktha Nandhini	5	5		10	9	19	5	5	29
37	21C31A663	Mohammed Abdul Rahaman	ABSENT					0	5	5	10
38	21C31A663	Mohammed Rajju	2			2	9	11	4	4	19
39	21C31A663	Mohammed Sameer		2	3	5	9	14		4	18
40	21C31A664	MD Yakub Faraz Khan	2		2	4	9	13	4	4	21
41	21C31A664	Munigala	1			1	9	10		4	14
42	21C31A664	Muniganti Akhil	4		4	8	9	17	4	5	26
43	21C31A664	Nalla Adithya	5	5		10	7	17	5	5	27
44	21C31A664	Nalla Lakmi Prasanna	5	5		10	8	18	5	5	28
45	21C31A664	Narugula Rakesh	5	3		8	9	17	5	5	27
46	21C31A664	Naveen Adepu	2			2	8	10	4	5	19
47	21C31A664	Nunavath Balaraju	2			2	8	10	0	4	14
48	21C31A664	Parunandhi Pavan	ABSENT					0	3	4	7
49	21C31A664	Pillalamarri Sudheer	5		5	10	10	20	5	5	30
50	21C31A665	Pilli Harshasri	5		3	8	9	17	5	5	27
51	21C31A665	Pitta Aravind	3		2	5	9	14	4	5	23
52	21C31A665	Sabbani Rakshitha	5	5		10	9	19	5	5	29
53	21C31A665	Shaik Salman		2	1	3	9	12	4	5	21
54	21C31A665	Shanigarapu Jhansy	4	3		7	9	16	5	5	26
55	21C31A665	Siluveru Prince	3	3		6	9	15	5	5	25
56	21C31A665	Singarapu Sravani	5			5	9	14	5	5	24
57	21C31A665	Sriramula Srilekha		2	3	5	9	14	5	5	24
58	21C31A665	Takkallapally Kanishka		5	5	10	9	19	5	5	29
59	21C31A665	Thadaka Sri Pooja		5	5	10	9	19	5	5	29
60	21C31A666	Thatikonda Nareesh	5	5		10	9	19	5	5	29
61	21C31A666	Vallakatta Teja	5	5		10	9	19	5	5	29
62	21C31A666	Velpuri Niharika	3	3		6	9	15	5	5	25
63	21C31A666	Yarram Sai Dath	5	3		8	9	17	5	4	26
64	22C35A66	Akula Rohith	5		4	9	9	18	5	5	28
65	02	Chindam Shiva Kumar		4	4	8	9	17	5	5	27
66	22C35A66	Gade Sushma Sri	ABSENT								
67	04	Mohammad Avez	3	3		6	10	16	0	5	26
68	05	Madhukar	3	3		6	9	15	0	5	20
69	06	Ravirakula Sandeep	2			2	9	11	0	4	15

XXVI. REFERENCES, JOURNALS, WEBSITES AND E-LINKS IF ANY

TEXT BOOKS:

1. Web Security, Privacy and Commerce Simson G Arfinkel, Gene Spafford, O'Reilly.
2. Handbook on Database security applications and trends Michael Gertz, Sushil Jajodia