NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	Integrated BTech (CSE)-MBA
Course Code:	3CS210ME24
Course Title:	Secured Application Development
Course Type:	Department Elective-V
Year of Introduction:	2024-25

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to –

1. illustrate building blocks for secured application development (BL2)
2. identify the need for secured application Development and its role (BL3)
3. build secured web applications considering various design principles for ensuring security standards (BL6)
4. develop secure code and test applications for vulnerabilities. (BL6)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Basics of Security:** Introduction to Laws, Standards & Guidelines on Cyber Security, Security v/s Safety, Threats and Risks, Security Attacks- Type of Attacks, Attack Agents, Security Vulnerabilities.	06
Unit-II	**Introduction to Secure Application Development Frameworks:** Microsoft Secure Development Lifecycle (SDL), Open Web Application Security Project (OWASP), Industrial Internet Consortium (IIC)	05
Unit-III	**Secure Application Development Methodologies:** Secure Software Development Lifecycle (SSDLC), Guidelines for Secure Software Development, Principles of Secured Software Development, Security Practices	06
Unit-IV	**Guidelines and standards for Secure Coding:** Secure coding guidelines and practices, Input validation and output encoding, Authentication and authorization, Error handling and logging	06
Unit-V	**Web Application Security:** Web application vulnerabilities (e.g., SQL injection, XSS, CSRF), Implementing secure session management, Web application firewalls (WAF), Security headers	07
Unit-VI	**Secure Architectural Design:** Threat Modelling, Asset, Threat, Attack, Introduction to Data Flow Diagram (DFD), Threat Tree (Attack Tree), STRIDE, DREAD. Security Architecture.	08
Unit-VII	**Security Testing Tools:** Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), Vulnerability Assessment & Penetration Testing (VAPT)	07

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw and Nancy Mead, Software Security Engineering: A Guide for Project Managers, Addison-Wesley Professional
2. Dafydd Stuttard and Marcus Pinto, The Web Application Hacker's Handbook, Wiley
3. Gary McGraw, Software Security: Building Security, Addison-Wesley.
4. Adam Shostack, Threat Modelling: Designing for Security, John Wiley and Sons Inc.
5. Mano Paul, 7 Qualities of Highly Secure Software, Taylor and Francis, CRC Press.
6. John Musa D, Software Reliability Engineering, Tata McGraw-Hill

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Explore Cyber Laws and prepare a consolidated report on Cyber Laws In context to Indian Scenario and compare it with Global Scenarios.	02
2	Comparative Study of various Secured Application Development Frameworks	02
3	Define functional & non-functional requirements for same. Prepare a SRS document for the project.	04
4	Identify the requirements of the application by incorporating concepts of Requirements Engineering for Secured Application.	04
5	Design & Define modules of the project.	02
6	Explore the secure coding guidelines and standard.	02
7	Development of modules by incorporating secure coding guidelines and principles.	08
8	Comparative study of Web Application Security concepts.	02
9	Comparative study and Hands-on for various Security Testing Tools	02
10	Prepare test strategy document. Design test cases for your project and perform security tests.	02