NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	3CSDE354
Course Title:	Secured Application Development
Course Type:	(□ Core/ □ Value Added Course / √ **Department Elective** / □ Institute Elective/ □ University Elective/ □ Open Elective / □ Any other)
Year of Introduction:	2022-23

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

Course Learning Outcomes (CLOs):

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

1. illustrate building blocks for secured application development (BL2)
2. identify the need of secured application development and its role (BL3)
3. examine the performance of various tools for application testing (BL4)
4. develop secured software applications (BL6)

Syllabus: **Total Teaching hours: 45**

Unit	**Syllabus**	**Teaching hours**
Unit-I	**Introduction:** Introduction to Laws, Standards & Guidelines on Cyber Security, Security v/s Safety, Threats and Risks, Security Attacks-Type of Attacks, Attack Agents, Security Vulnerabilities.	04
Unit-II	**Introduction to Secure Application Development Frameworks:** Microsoft Secure Development Lifecycle (SDL), Open Web Application Security Project (OWASP), Industrial Internet Consortium (IIC)	06
Unit-III	**Secure Application Development Methodologies:** Secure Software Development Lifecycle (SSDLC), Guidelines for Secure Software Development, Principles of Secured Software Development, Security Practices, Guidelines for Secure Coding, Secure coding standard.	08
Unit-IV	**Requirements Engineering for Secured Application**: Availability, Authenticity, Confidentiality, Efficiency, Integrity, Maintainability, Portability, Reliability, Trustworthiness, Threat Analysis and Risk Management.	06
Unit-V	**Secure Architectural Design:** Threat Modelling, Asset, Threat, Attack, Dataflow Diagram (DFD), Threat Tree (Attack Tree), STRIDE, DREAD (**an approach for analyzing the security of an application**). Security Architecture.	07
Unit-VI	**Security Testing Tools:** Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), Vulnerability Assessment & Penetration Testing (VAPT)	08

Unit-VII	**Secure Deployment**: Secure Default Configuration, Product Life Cycle, Automated Deployment Process, Secure Target Environment, Secure Delivery of Code, Trusted Origin, Code Signing, Least Privilege Permissions, ITIL Release and Deployment Management	06

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

Topic: Recent Trends in Secured Application Development

Suggested Readings/ References:

1. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw and Nancy Mead Software
2. Security Engineering: A Guide for Project Managers by. Addison-Wesley.
3. Gary McGraw Software Security: Building Security, Addison-Wesley.
4. Threat Modelling: Designing for Security by Adam Shostack, 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, 2nd Edition, Tata McGraw-Hill.
7. D. LeBlank, M. Howard, Writing Secure Code, Microsoft Press.

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

Students need to identify a project/system on which they would be working throughout the entire semester for developing an application and applying security aspects on it. **They are required to form a group of 3 students from within their batch itself.** Afterwards during each session, faculty member will introduce the objective and methodology of the practical to the students. Students are required to work on the said task for their own selected project/system. The designing or planning can be carried out using any CASE tool available, details of case tools will be discussed during the sessions.

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
	Risk Management Plan for the project.	
5	Design & Define modules of the project.	02

6	Development of modules by incorporating secure coding guidelines and principles.	08
7	Comparative study and Hands-on for various Security Testing Tools	02
8	Prepare test strategy document. Design test cases for your project and perform security tests.	02
9	Secure Deployment of the application	04