CO	PO						PSO		
	1	2	3	4	5	6	1	2	3
1.	√		√				√	√	
2.	√		√				√	√	
3.	√		√	√			√	√	√
4.	√		√				√	√	
5.	√		√	√			√	√	√

SE5075 **SOFTWARE SECURITY** **L T P C**
3 0 0 3

OBJECTIVES:

- Know the importance and need of software security.
- Know about various attacks.
- Learn about secure software design.
- Understand risk management in secure software development.
- Know the working of tools related to software security.

UNIT I LOW LEVEL ATTACKS 9

Need For Software Security – Memory Based Attacks – Low Level Attacks Against Heap and Stack - Stack Smashing – Format String Attacks – Stale Memory Access Attacks – ROP (Return Oriented Programming) – Malicious Computation Without Code Injection. Defense Against Memory Based Attacks – Stack Canaries – Non-Executable Data - Address Space Layout Randomization (ASLR), Memory-Safety Enforcement, Control-Flow Integrity (CFI) – Randomization

UNIT II SECURE DESIGN 9

Isolating The Effects of Untrusted Executable Content - Stack Inspection – Policy Specification Languages – Vulnerability Trends – Buffer Overflow – Code Injection - Generic Network Fault Injection– Local Fault Injection - SQL Injection - Session Hijacking. Secure Design - Threat Modeling and Security Design Principles - Good and Bad Software Design - Web Security- Browser Security: Cross-Site Scripting (XSS), Cross-Site Forgery (CSRF) – Database Security – File Security

UNIT III SECURITY RISK MANAGEMENT 9

Risk Management Life Cycle – Risk Profiling – Risk Exposure Factors – Risk Evaluation and Mitigation – Risk Assessment Techniques – Threat and Vulnerability Management.

UNIT IV SECURITY TESTING 9

Traditional Software Testing – Comparison - Secure Software Development Life Cycle - Risk Based Security Testing – Prioritizing Security Testing With Threat Modeling – Shades of Analysis: White, Grey and Black Box Testing.

UNIT V PENETRATION TESTING 9

Advanced Penetration Testing – Planning and Scoping – DNS Groper – DIG (Domain Information Graph) – Enumeration – Remote Exploitation – Web Application Exploitation - Exploits and Client Side Attacks – Post Exploitation – Bypassing Firewalls and Avoiding Detection - Tools for Penetration Testing

TOTAL : 45 PERIODS

OUTCOMES:

Upon completion of the course, the student will be able to

- Identify various vulnerabilities related to memory attack.
- Apply security principles in software development.
- Evaluate the extent of risks.
- Involve selection of testing techniques related to software security in testing phase of software development.
- Use tools for securing software.

REFERENCES:

1 Robert C. Seacord, “Secure Coding in C and C++ (SEI Series in Software Engineering)”, Addison-Wesley Professional, 2005.

2 Jon Erickson , “Hacking: The Art of Exploitation”, 2nd Edition, No Starch Press, 2008.

3 Mike Shema, “Hacking Web Apps: Detecting and Preventing Web Application Security Problems”, First edition, Syngress Publishing, 2012

4 Bryan Sullivan and Vincent Liu, “Web Application Security, A Beginner's Guide”, Kindle Edition, McGraw Hill, 2012

5 Evan Wheeler, “Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, First edition, Syngress Publishing, 2011

6 Chris Wysopal, Lucas Nelson, Dino Dai Zovi, and Elfriede Dustin, “The Art of Software Security Testing: Identifying Software Security Flaws (Symantec Press)”, Addison-Wesley Professional, 2006

7 Lee Allen, “Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide (Open Source: Community Experience Distilled)”, Kindle Edition, Packt Publishing,2012

CO	PO						PSO		
	1	2	3	4	5	6	1	2	3
1.	√		√	√		√	√	√	
2.	√		√	√		√	√	√	√
3.	√		√	√		√	√	√	√
4.	√		√	√	√	√	√	√	
5.	√		√	√		√	√	√	√