Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR1C2: Secure Computing Techniques	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

This course aims to provide an understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities. It gives an outline of the techniques for developing a secure application.

COURSE CONTENT

Unit-I: Introduction

Security: CIA (AIC) Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. *Malware Terminology*: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks, IP Spoofing, Tear drop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack. *Types of Security Vulnerabilities*: buffer overflows, invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

Unit-II: Secure Software Development Cycle & Threat Modelling

Need for Secure Systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC) , Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline.

Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege.

Unit – III: Secure Coding Techniques

Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, *Insecure Coding Practices in Java Technology*: ARP Spoofing and its countermeasures. Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors,FormatString Bugs. *Security Issues in C/C++ Language*: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks,Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM. Secure coding issues in Android Applications, Language Specific issues like C/C++, Perl, Python, Scripting Languages, Ada, Java, PHP etc.

Unit – IV: Database and Web-specific issues

SQL Injection Techniques and Remedies,Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters.

Unit – V: Testing Secure Applications

Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers.

Text and Reference books:

[1] Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press, 2nd Edition, 2004

[2] Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckar,Syngress,1st Edition, 2005

[3] Threat Modeling, Frank Swiderski and Window Snyder, Microsoft Professional, 1st Edition, 2004.

[4] Secure Programming HOWTO by David A. Wheeler

[5] Secure Coding: Principles & Practices by Mark G. Graff, Kenneth R. van Wyk