Devi Ahilya University, Indore, India Institute of Engineering & Technology				III Year B.E. (Computer Engg.) (Full Time)			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
CER5E2 Software Vulnerabilities and Security	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
	3	**1**	**2**	**3**	**1**	**1**	**5**
Duration of Theory Paper: 3 Hours							

Objective: To familiarize with aspects of software security and threats.

Prerequisite: Software Engineering, Cyber security fundamentals and machine learning algorithms are required to be understood before taking this course

COURSE CONTENTS

UNIT I

Software Security Essentials- Basic concepts of System Security, Security Policies, Security Expectations, Code Auditing, Software Vulnerabilities, Classifying Vulnerabilities, Design Vulnerabilities, Gray Areas, Trust Relationships, Environmental Attacks

UNIT II

Need of Security in Cyber Physical Space, Hacker Capability and System Complexity, Attacks, Classification of Attacks, Attack entry Points, Resource Access, Threats

UNIT III

Software Safety, Safety Life Cycle of Product, Evaluating Risks, Reducing the Risks, Managing Functional Safety, Cyber Security for Commercial Advantage, Security Critical Systems, Security Assurance

UNIT IV

Software Weapons, Types of Malware, Worms, Virus, Spam, Rootkit, Spyware, Attackers, Reciprocation, Defense, Code Hardening, Handling Attacks, LDAP Injection, FTP Injection, Script Injection, Memory injection, Threat Modeling,

UNIT V

Mitigation, Prevention Methods, Privacy Implementation, Authentication Policies, Access Control, Encryption, Cloud and Mobile Security

BOOKS RECOMMENDED:

[1] James Helfrich, Security for Software Engineers, Taylor and Francis Group, 2019
[2] Edward Griffor, handbook of System Safety and Security, NIST 2017
[3] Mark Dowd, John McDonald, Justin Schuh, The Art of Software Security Assessment – Identifying and Preventing Software Vulnerabilities, Addison Wesley, 2007
