GCS04SG082	**IT Application Security**	L	T	P	C
Version 1.0		2	0	0	2
Pre-requisites/Exposure	IT Data Security				
Co-requisites	--				

Course Objectives

1. Students should be able to identify application security threats.
2. Student should have understanding about secure software development methodology.
3. Students should be able identify the counter measure required for various application security threats.

Course Outcomes

On completion of this course, the students will be able to

1. Identify secure application development principles.
2. Describe input validation, authentication process, configuration management and parameter manipulation, exception management and session management.
3. Identify audit and logging needs in application development.
4. Apply countermeasures and code analysis to provide security against Web Application Vulnerabilities.

Catalog Description

Application Security is an integral part of Cyber Security. In this course, the focus will be on secure software development, input validation, authentication process, configuration management and parameter manipulation, exception management and session management. In addition, countermeasure like audit, logging and secure coding will be covered. Classroom activities will be designed to encourage students to play an active role in the construction of their own knowledge and in the design of their own learning strategies. We will combine traditional lectures with other active teaching methodologies, such as group discussions, cooperative group solving problems, analysis of video scenes and debates.

Course Content

Unit 1. Introduction to Software Development & Application Security
Introduction to software development & application security, Basics of programming languages Compiled versus interpreted, Program utilities, Programming concepts, Distributed programming, Threats and malware, Importance of software development life cycle, Software development methods, Adherence to secure software development principles, Web application security principles, Application design & development security, Environment and controls, Essence of secure software development, Auditing and assurance mechanisms.

Unit 2. Input Validation & Sensitive Data
Introduction to input validation & sensitive data, Implementation of input validation, Practical solutions, Input validation vulnerability, Buffer overflow, Cross-site scripting, SQL injection,

Canonicalization, Sensitive data, Sensitive data access, Sensitive data in storage, Information disclosure, Data tampering.

Unit 3. Authentication & Authorization

Introduction to authentication & authorization, Network eavesdropping, Brute force attack, Dictionary attack, Cookie replay attack, Credential theft, Elevation of privilege, Basics of authorisation, Data tampering, Luring attack, Phishing attack.

Unit 4. Configuration Management & Session Management

Introduction to configuration management & session management, Unauthorized access to administration interfaces, Unauthorized access to configuration stores, Retrieval of clear text configuration data, Lack of individual accountability, Over-privileged process and service accounts, Basics of Session Management, Hijacking attack, Session replay attack, Man in the middle attack.

Unit 5. Cryptography, Parameter Manipulation & Exception Management

Introduction, Poor key generation, or key management, Weak or custom encryption, Basics of parameter manipulation, Cookie manipulation, HTTP header manipulation, Basics of exception management, Denial of Service.

Unit 6. Web Application Security - I

Mitigating risk when connecting to the Internet, Mitigating website risks, threats and vulnerabilities, Prevention techniques for vulnerabilities, Securing web applications, Mitigating web application vulnerabilities, Maintaining PCI DSS compliance for E-commerce websites, Performing a website, vulnerability and security assessment.

Unit 7. Web Application Security - II

Web Application vs Cloud Application, how does Web Application security work? Web Application lifecycle management, Importance of Web Application security, Web Application security vs network security, what makes Web Application vulnerable? Web Application vulnerabilities, Broken access control, Broken authentication and session management, Buffer overflows, Cross site scripting flaws, Denial of Service, Improper error handling, Insecure configuration management, Insecure storage, SQL injection flaws, Unvalidated input, Defensive measures, Definition of Web Application security scanner, Tool types, Functional requirements, Issues with Web Application security scanner, Strengths and weaknesses, Definition of Web Application security testing, Importance of Web Application security testing, Is Web Application security testing a waste of time? Guide for Web Application security testing (Process and reporting), Tracking results, Test environment, Usability testing, Unit testing, Verifying the HTML, Load testing, User acceptance testing, testing security, Protecting against attack and misuse, Basic guidelines for providing security, Improving security, Web Application security plan introduction, Tips on securing Web Applications, Security flaws, Myth and reality, Best practices for creating secure Web Applications.

Unit 8. Secure Big Data Systems & Operate and Secure Virtual Environments

Application vulnerabilities and architecture or design environments, Operate and secure virtual environments.

Unit 9. Auditing & Logging, Countermeasures

Introduction to auditing & logging, countermeasures, Basic countermeasures, Installation, AppScan run procedure (Web services explorer).

Text Books

1. IBM Manual for Information Security Audit & Monitoring.

Reference Books

1. Bart De Win , Riccardo Scandariato, Koen Buyens, Johan Gre ´goire, WouterJoosen, On the secure software development process: CLASP, SDL and Touchpoints compared, ELSEVIER Publications

2. Bryan Sullivan, Vincent Liu (2011). Web Application Security, A Beginner's Guide. McGraw-Hill Education. ISBN: 0071776168

Modes of Evaluation: Quiz/Assignment/ presentation/ extempore/ Written Examination

Examination Scheme:

Components	**MSE**	**Presentation/Assignment/ etc**	**ESE**
Weightage (%)	**20%**	**30%**	**50%**

Relationship between the Course Outcomes (COs), Program Outcomes (POs) and Program Specific Objectives(PSOs)

Course Outcomes	PO 1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	1	1					1					1	2	1	3
CO2	1	1	2								1				1
CO3					1		1						1	2	
CO4	1		2		1										3
Average	1	1	2		1		1				1	1	1.5	1.5	2.33

1=weak 2= moderate 3=strong