COURSE TITLE	**WEB APPLICATION & SECURITY**
COURSE CODE	**01CC0502**
COURSE CREDITS	**4**

Objective:

1 The objective of this course is to provide an understanding of the architecture and components of modern web applications, along with secure design principles and common web vulnerabilities. It aims to develop the ability to apply secure coding practices throughout the software development lifecycle. Additionally, the course offers hands-on experience in identifying, analyzing, and mitigating web application security threats.

Course Outcomes: After completion of this course, student will be able to:

1 Explain the fundamental components and principles of web application architecture.

2 Apply information gathering techniques in the initial phase of web application penetration testing.

3 Apply design patterns such as MVC to develop secure and maintainable web applications.

4 Analyze web application architectures to identify and evaluate potential security weaknesses.

5 Explain the implementation of Secure Development Life Cycle (SDLC) and the use of security tools for assessment.

Pre-requisite of course: Basic understanding of computer networking concepts and protocols. Fundamental knowledge of HTML, CSS, and JavaScript for web development. Familiarity with server-side programming using languages like PHP, Python, or Node.js.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Web Application Fundamentals** Client-Server Model: Overview of the client-server architecture, roles of clients and servers, HTTP request/response cycle, Web Technologies: HTML, CSS, JavaScript, and their role in front-end development, Server-Side Technologies: Overview of popular server-side languages (PHP, Python, Java, etc.) and frameworks (Django, Flask, Spring, etc.)	8

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
2	**Web Application Architecture** Three-Tier Architecture: Presentation, business logic, and data access layers, MVC (Model-View-Controller) Pattern: Benefits and how it applies to web applications, RESTful APIs: Principles of REST, designing and securing REST APIs., Modern Web Architectures: Microservices, single-page applications (SPAs), and serverless architectures.	9
3	**Secure Coding Practices** Secure Coding Principles: Least privilege, defense in depth, secure defaults., Secure Development Lifecycle (SDL): Integrating security throughout the development process., Code Review and Testing: Manual and automated code review techniques, security testing methodologies	8
4	**Web Application Attacks** Injection Attacks: SQL Injection (SQLi) - In-band, Blind, Out-of-band, Cross-Site Scripting (XSS) - Reflected, Stored, DOM-based, Broken Authentication: Password cracking (Brute force, Dictionary attacks), Session management flaws, Sensitive Data Exposure: Insecure direct object references (IDOR), Information disclosure in error messages, Security Misconfiguration: Unpatched systems, default credentials, verbose errors, Cross-Site Request Forgery (CSRF).	11
Total Hours		**36**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Automated OS Installation: Performing an unattended installation of a Windows Server or Linux distribution	2
2	**Practical 2** Advanced Disk Management: Configuring LVM in Linux or creating dynamic disks and RAID volumes in Windows Server	2
3	**Practical 3** Scripting for User Management: Writing scripts to automate the creation, modification, or deletion of multiple user accounts.	2
4	**Practical 4** Configuring and Securing SSH and RDP: Setting up SSH key-based authentication on Linux and securing RDP access on Windows Server	2
5	**Practical 5** Advanced Web Server Configuration: Configuring virtual hosts, SSL certificates (self-signed), and basic access control for a web server.	2

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
6	**Practical 6** Implementing and Testing Server Backups and Restores: Configuring a backup job and performing a full or partial restoration of server data.	2
7	**Practical 7** Configuring Advanced Firewall Rules: Implementing more complex firewall rules based on ports, protocols, and source/destination IP addresses.	2
8	**Practical 8** Setting up Centralized Logging (Basic): Configuring multiple servers to send logs to a central log collection point and viewing them.	2
9	**Practical 9** Monitoring Server Performance and Setting Alerts: Using monitoring tools to track key performance indicators and configure alerts for thresholds.	2
10	**Practical 10** Deploying and Managing a Basic Server in the Cloud: Launching a virtual machine instance in a cloud environment (e.g., AWS EC2, Azure VM) and performing basic administration tasks.	2
Total Hours		**20**

Textbook :

1 Windows Server 2019 & PowerShell All-in-One For Dummies, Sara Perrott & Jeffrey R. Shapiro, John Wiley & Sons, Inc, 2019

References:

1 Linux Administration: A Beginner's Guide (Eighth Edition), Linux Administration: A Beginner's Guide (Eighth Edition), Wale Soyinka, McGraw-Hill Education, 2020

2 Mastering VMware vSphere 7, Mastering VMware vSphere 7, Nick Marshall, Sybex / John Wiley & Sons, 2018

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
10.00	25.00	30.00	15.00	10.00	10.00

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Instructional Method:

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1. “Microsoft Learn – Windows Server Documentation" https://learn.microsoft.com/en-us/windows-server/
2. “Red Hat or Ubuntu Server Guides (Linux Server Administration)” https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/
3. “Docker Documentation” https://docs.docker.com/
4. CIS Benchmarks (Server Security) - https://www.cisecurity.org
5. NIST Security Guidelines

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)