	FACULTY OF SCIENCE
	Effective from Academic Batch:2025-26
Programme:	**Master of Science(Cyber Security)**
Semester:	**II**
Course Code:	**101570201**
Course Title:	**Network Defense Essentials**
Course Group:	**CORE**

Course Objectives:

- To provide a strong foundation in the fundamentals of network defense, information security principles, and layered protection models.
- To develop practical skills in configuring and managing firewalls, VPNs, and other network security components for secure communication.
- To enable students to analyze and implement IDS/IPS tools, perform effective log management, and respond to security incidents.
- To expose students to advanced network defense strategies such as honeypots, deception technologies, and Zero Trust architecture for proactive threat mitigation.

Teaching & Examination Scheme:

Contact hours per week			Course Credits	Examination Marks (Maximum / Passing)				
				Theory		J/V/P*		Total
Lecture	Tutorial	Practical		Internal	External	Internal	External	
4	--	--	4	50/20	50/20	--	--	100/40

* **J**: Jury; **V**: Viva; **P**:Practical

Detailed Syllabus:

Sr.	Contents	Hours
1	**Introduction to Network Defence** • Fundamentals of network defense and information security • The CIA triad: Confidentiality, Integrity, and Availability • Understanding threat landscape and attack surfaces • Types of network attacks (DoS, MITM, spoofing, eavesdropping, phishing) • Security policies and frameworks (ISO 27001, NIST, CIS Controls) • Defense-in-depth strategy and layered protection • Network security models: Perimeter, Zonal, and Zero Trust • Risk management: threat modeling and vulnerability assessment • Security baselines and configuration management • Importance of network segmentation and access control lists (ACLs)	12

2	**Firewalls and VPNs** • Introduction to firewalls and their role in network defense • Types of firewalls: Packet-filtering, Stateful Inspection, Application Proxy, Next-Generation Firewalls • Firewall deployment architectures: Bastion host, DMZ, dual-homed gateway • Firewall configuration concepts – rules, policies, and filtering mechanisms • NAT, PAT, and port forwarding configuration • VPN fundamentals and benefits for secure communication • VPN tunneling protocols • Encryption and authentication in VPNs • VPN deployment using site-to-site and remote-access models • Real-world VPN configuration examples and troubleshooting scenarios	**15**
3	**IDS/IPS and Network Monitoring** • IDS vs IPS: working and differences • Types of IDS: Host-based, Network-based, Hybrid • Detection methods: Signature-based vs Anomaly-based • IDS/IPS tools: Snort, Suricata, Zeek • Network traffic capture and analysis (Wireshark basics) • Log management: Syslog, SIEM integration (Splunk/ELK) • Security baselining and anomaly detection • Incident detection and response workflow	**15**
4	**Advanced Network Defence Strategies** • Endpoint protection: Antivirus, EDR, XDR • Honeypots and honeynets: design and deployment • Deception technologies for attackers • Denial-of-Service and DDoS mitigation techniques • Intrusion prevention through content filtering and proxy servers • Zero Trust Network Architecture (ZTNA) principles and implementation • Threat intelligence and automated defense systems • Future trends: AI/ML in network defense, SOAR platforms	**18**

Reference Books:	
1	Network Security Essentials: Applications and Standards — William Stallings
2	The Practice of Network Security Monitoring: Understanding Incident Detection and Response — Richard Bejtlich.
3	Network Security: Private Communication in a Public World — Charlie Kaufman, Radia Perlman, Mike Speciner
Supplementary learning Material:	
1	• Cisco Networking Academy : https://www.cisco.com/site/us/en/learn/training-certifications/training/netacad/index.html?utm_source=chatgpt.com
2	• NPTEL : https://onlinecourses.nptel.ac.in/noc23_cs127/preview?utm_source=chatgpt.com
3	• Documentation & Tools for Snort and Wireshark: https://www.wireshark.org/docs/dfref/s/snort.html?utm_source=chatgpt.com

Pedagogy:
• Classroom sessions with case studies • Lab demonstrations of monitoring tools • Assignments and quizzes • Internal / External Examination as per the norms of CVM University

Suggested Specification table with Marks (Theory) (Revised Bloom's Taxonomy):

Distribution of Theory Marks in %						**R**: Remembering; **U**: Understanding; **A**: Applying; **N**: Analyzing; **E**: Evaluating; **C**: Creating
R	**U**	**A**	**N**	**E**	**C**	
20	40	15	15	5	5	

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcomes (CO):

Sr.	Course Outcome Statements	%weightage
CO-1	Explain the fundamental concepts of network defense, including layered security architecture, threat models, and common attack vectors, to understand how various defense mechanisms protect organizational networks.	**25**
CO-2	Configure, deploy, and manage security components such as firewalls and Virtual Private Networks (VPNs) to ensure secure communication, access control, and traffic filtering within enterprise networks.	**25**
CO-3	Analyze and implement Intrusion Detection and Prevention Systems (IDS/IPS), integrate them with log management and SIEM tools, and interpret system logs for detecting and mitigating potential threats.	**25**
CO-4	Evaluate and design advanced defense mechanisms by applying emerging strategies such as honeypots, deception-based security, and the Zero Trust architecture for proactive network protection and incident response.	**25**

Curriculum Revision:	
Version:	1.0
Drafted on (Month-Year):	Nov-2025
Last Reviewed on (Month-Year):	Dec- 2025
Next Review on (Month-Year):	Feb-2027

	FACULTY OF SCIENCE
	Effective from Academic Batch:2025-26
Programme:	**Master of Science(Cyber Security)**
Semester:	**II**
Course Code:	**101570202**
Course Title:	**Digital Forensics Essentials**
Course Group:	**CORE**

Course Objectives:

- To understand digital forensics principles and investigation processes.
- To perform forensic analysis on systems, memory, and networks.
- To use forensic tools for data acquisition and examination.
- To ensure legal admissibility and ethical investigation practices.

Teaching & Examination Scheme:

Contact hours per week			Course Credits	Examination Marks (Maximum / Passing)				
				Theory		J/V/P*		Total
Lecture	Tutorial	Practical		Internal	External	Internal	External	
4	--	--	4	50/20	50/20	--	--	100/40

* **J**: Jury; **V**: Viva; **P**:Practical

Detailed Syllabus:

Sr.	Contents	Hours
1	**Fundamentals of Digital Forensics** • Introduction and need for digital forensics • Phases of forensic investigation • Role of digital evidence in cybercrime • Evidence handling and chain of custody • Forensic lab setup and hardware/software requirements • Imaging techniques and verification (hashing, MD5/SHA) • File systems: FAT, NTFS, EXT basics • Data recovery and carving concepts • Documentation of evidence • Common forensic tools overview	15
2	**Operating System & File System Forensics** • Windows artifacts: registry, event logs, prefetch, recent files • Linux artifacts: bash history, syslogs, journal • File metadata and timestamps • Hidden and deleted file recovery • Analyzing user activity and session details • Browser and email forensic analysis	15

	• Live vs Dead system investigation • Disk imaging using FTK Imager/dd • Case study: tracking insider activity • Report creation with screenshots and logs	
3	**Memory and Network Forensics** • Volatile data acquisition procedures • Memory dump analysis with Volatility framework • Process, DLL, and network connection extraction • Malware memory footprint analysis • Network forensic tools (Wireshark, tcpdump) • Log correlation in network activity • Email header and message analysis • DNS and proxy log inspection • Identifying lateral movement in attacks • Hands-on case analysis	**15**
4	**Legal, Ethical & Emerging Trends** • Cyber laws and digital evidence admissibility • Indian IT Act and global legal frameworks • Privacy and data protection standards • Ethical responsibilities of forensic investigators • Report presentation and courtroom testimony basics • Mobile and IoT forensic overview • Cloud forensics: acquisition and challenges • Blockchain and cryptocurrency forensics • AI and automation in forensic analysis • Real-world forensic investigation case studies	**18**

Reference Books:	
1	Nelson, Phillips & Steuart – *Guide to Computer Forensics and Investigations*, Cengage Learning.
2	Eoghan Casey – *Digital Evidence and Computer Crime*, Academic Press
Supplementary learning Material:	
1	• Autopsy Forensic Tool Documentation (Sleuth Kit)..
2	• **NPTEL Online Networking Courses** – https://nptel.ac.in/
3	• **Coursera - Networking Courses** – https://www.coursera.org/

Pedagogy:

- Assignments / Quiz / Presentation / Participation for continuous evaluation and assessment
- Internal / External Examination as per the norms of CVM University

Suggested Specification table with Marks (Theory) (Revised Bloom's Taxonomy):

Distribution of Theory Marks in %						**R**: Remembering; **U**: Understanding; **A**: Applying; **N**: Analyzing; **E**: Evaluating; **C**: Creating
R	**U**	**A**	**N**	**E**	**C**	
20	40	15	15	5	5	

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcomes (CO):

Sr.	Course Outcome Statements	%weightage
CO-1	Conduct forensically sound digital investigations by following proper evidence-handling, chain-of-custody, and legal procedures.	**25**
CO-2	Analyze artifacts from Windows, Linux, and various file systems to identify, recover, and interpret digital evidence.	**25**
CO-3	Utilize memory and network forensic tools effectively to extract volatile data, trace malicious activities, and reconstruct incidents.	**25**
CO-4	Document, interpret, and present forensic findings through professional reports in compliance with legal and organizational standards.	**25**

Curriculum Revision:	
Version:	1.0
Drafted on (Month-Year):	Nov-2025
Last Reviewed on (Month-Year):	Dec- 2025
Next Review on (Month-Year):	Feb-2027

	FACULTY OF SCIENCE
	Effective from Academic Batch:2025-26
Programme:	**Master of Science(Cyber Security)**
Semester:	**II**
Course Code:	**101570204**
Course Title:	**Advanced Ethical Hacking**
Course Group:	**CORE**

Course Objectives:

- To master advanced techniques of ethical hacking and penetration testing.
- To explore exploit development, privilege escalation, and red teaming.
- To perform attacks on wireless, IoT, and cloud infrastructures.
- To learn professional penetration testing standards and documentation.

Teaching & Examination Scheme:

Contact hours per week			Course Credits	Examination Marks (Maximum / Passing)				
				Theory		J/V/P*		Total
Lecture	Tutorial	Practical		Internal	External	Internal	External	
4	--	--	4	50/20	50/20	--	--	100/40

*J: Jury; V: Viva; P:Practical

Detailed Syllabus:

Sr.	Contents	Hours
1	**Footprinting and Reconnaissance** • Footprinting Concepts • Footprinting through Search Engines • Website Footprinting • Email Footprinting • Whois Footprinting • DNS Footprinting • Network Footprinting • Footprinting through Social Engineering • Various Footprinting Tools • Footprinting Countermeasures	15

2	**Sniffing** • Sniffing Concepts • Sniffing Technique: MAC Attacks • Sniffing Technique: DHCP Attacks • Sniffing Technique: ARP Poisoning • Sniffing Technique: Spoofing Attacks • Sniffing Technique: DNS Poisoning • Sniffing Tools • Sniffing Countermeasures	**15**
3	**Session Hijacking** • Session Hijacking Concepts • Application-Level Session Hijacking • Network-Level Session Hijacking • Session Hijacking Tools • Session Hijacking Countermeasures	**15**
4	**Evading IDS, Firewalls, and Honeypots** • IDS, IPS, Firewalls, and Honeypot Concepts • IDS, IPS, Firewalls, and Honeypot Solutions • Evading IDS • Evading Firewalls • IDS/Firewall Tools • IDS/Firewall Evasion Countermeasures	**15**

Reference Books:	
1	Patrick Engebretson – *The Basics of Hacking and Penetration Testing*, Syngress.
2	Kevin Mitnick – *The Art of Invisibility / The Art of Intrusion*.
Supplementary learning Material:	
1	• TryHackMe & Hack The Box Labs..
2	• **NPTEL Online Networking Courses** – https://nptel.ac.in/
3	• **Coursera - Networking Courses** – https://www.coursera.org/
Pedagogy:	
• Justify all the topics unit-wise • Assignments / Quiz / Presentation / Participation for continuous evaluation and assessment • Internal / External Examination as per the norms of CVM University	

Suggested Specification table with Marks (Theory) (Revised Bloom's Taxonomy):

Distribution of Theory Marks in %						**R**: Remembering; **U**: Understanding; **A**: Applying; **N**: Analyzing; **E**: Evaluating; **C**: Creating
R	**U**	**A**	**N**	**E**	**C**	
20	40	15	15	5	5	

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table

Course Outcomes (CO):

Sr.	Course Outcome Statements	%weightage
CO-1	Conduct advanced reconnaissance and exploitation tasks.	**25**
CO-2	Perform privilege escalation and persistence techniques.	**25**
CO-3	Assess vulnerabilities in wireless, IoT, and cloud systems.	**25**
CO-4	Execute red team operations and generate professional reports.	**25**

Curriculum Revision:	
Version:	1.0
Drafted on (Month-Year):	April-2025
Last Reviewed on (Month-Year):	May- 2025
Next Review on (Month-Year):	Feb-2027

	FACULTY OF SCIENCE
	Effective from Academic Batch:2025-26
Programme:	**Master of Science(Cyber Security)**
Semester:	**II**
Course Code:	**101570203**
Course Title:	**Web Server Management**
Course Group:	**CORE**

Course Objectives:

- To study architecture and management of modern web servers.
- To configure secure, optimized, and monitored web environments.
- To perform backup, load balancing, and failure recovery.
- To develop security awareness for server deployment.

Teaching & Examination Scheme:

Contact hours per week			Course Credits	Examination Marks (Maximum / Passing)				
				Theory		J/V/P*		Total
Lecture	Tutorial	Practical		Internal	External	Internal	External	
4	--	--	4	50/20	50/20	--	--	100/40

* **J**: Jury; **V**: Viva; **P**:Practical

Detailed Syllabus:

Sr.	Contents	Hours
1	**Introduction to Web Servers** • Web server architecture and functioning • Apache, Nginx, and IIS overview • HTTP/HTTPS protocol concepts • Installation and configuration on Windows/Linux • Directory structures and permissions • Virtual hosting (name-based and IP-based) • URL rewriting and redirection rules • Logging and access control basics • MIME types and compression configuration	15
2	**Secure Web Server Deployment** • SSL/TLS fundamentals and certificate management • Creating and installing digital certificates • HTTPS configuration and redirection • Authentication and authorization methods • Hardening Apache/Nginx/IIS servers • Security headers and best practices • Restricting access with .htaccess and firewalls	15

	• Application whitelisting and patch management • Reverse proxy setup • Web security audit checklist	
3	**Monitoring and Optimization** • Server performance metrics (CPU, RAM, I/O) • Log analysis and visualization • Tools: Nagios, Zabbix, SolarWinds • Resource utilization and tuning • Caching mechanisms (Varnish, Redis, Memcached) • Load testing tools (JMeter, ApacheBench) • Troubleshooting slow server responses • Automation with shell scripts • Error handling and recovery planning • Case study: Server performance tuning	**15**
4	**Backup, Recovery & Advanced Administration** • Backup strategies and frequency planning • Incremental and differential backups • Restoring from backups using command line tools • Database backup (MySQL/MongoDB) • Load balancing and clustering methods • Failover and redundancy design • Cloud hosting administration (AWS, Azure, GCP) • Server migration process and downtime minimization • Disaster recovery documentation • Real-world web server security incidents	**18**

Reference Books:	
1	Brian P. Hogan – *Web Server Management and Security*, Pragmatic Bookshelf.
2	Ben Laurie & Peter Laurie – *Apache: The Definitive Guide*, O'Reilly Media.
Supplementary learning Material:	
1	• Apache HTTP Server Official Documentation..
2	• Nginx and IIS Configuration Guides (Microsoft Docs).
3	• Tutorials on SSL/TLS and Certificate Management (Let's Encrypt).

Pedagogy:

- Justify all the topics unit-wise
- Assignments / Quiz / Presentation / Participation for continuous evaluation and assessment
- Internal / External Examination as per the norms of CVM University

Suggested Specification table with Marks (Theory) (Revised Bloom's Taxonomy):

Distribution of Theory Marks in %						**R**: Remembering; **U**: Understanding; **A**: Applying; **N**: Analyzing; **E**: Evaluating; **C**: Creating
R	**U**	**A**	**N**	**E**	**C**	
20	40	15	15	5	5	

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcomes (CO):

Sr.	Course Outcome Statements	%weightage
CO-1	Install, configure, and manage web servers on multiple platforms to support secure and efficient web hosting environments.	**25**
CO-2	Implement secure, optimized, and scalable server configurations by applying best practices in performance tuning and security hardening.	**25**
CO-3	Monitor, analyze, and troubleshoot web server performance issues using appropriate tools and techniques to ensure reliability and uptime.	**25**
CO-4	Plan, document, and execute backup, recovery, and failover strategies to maintain data integrity and business continuity during server failures.	**25**

Curriculum Revision:	
Version:	1.0
Drafted on (Month-Year):	Nov-2025
Last Reviewed on (Month-Year):	Dec- 2025
Next Review on (Month-Year):	Feb-2027

	FACULTY OF SCIENCE
	Effective from Academic Batch:2025-26
Programme:	**Master of Science(Cyber Security)**
Semester:	**II**
Course Code:	**101570205**
Course Title:	**Hacking Web Server & Web Application**
Course Group:	**Elective - I**

Course Objectives:

- To provide an in-depth understanding of common web application and web server vulnerabilities and their exploitation.
- To develop practical skills in using tools and techniques for ethical hacking and penetration testing of web environments.
- To understand defensive coding practices and security mechanisms to mitigate web-based attacks.

Teaching & Examination Scheme:

Contact hours per week			Course Credits	Examination Marks (Maximum / Passing)				
				Theory		J/V/P*		Total
Lecture	Tutorial	Practical		Internal	External	Internal	External	
2	--	4	4	25/10	25/10	25/10	25/10	100/40

* **J**: Jury; **V**: Viva; **P**:Practical

Detailed Syllabus:

Sr.	Contents	Hours
1	**Introduction to Web Application Security & Reconnaissance** • Fundamentals of Ethical Hacking and Penetration Testing Methodology • Overview of OWASP Top 10 Vulnerabilities • Reconnaissance & Footprinting • Passive Information Gathering • Active Information Gathering • Using Proxy Tools (Burp Suite) for Interception and Mapping	15

2	**Injection & Client-Side Attacks** • Injection Flaws • SQL Injection (Error-Based, Blind, Advanced Concepts) • Client-Side Exploitation • Cross-Site Scripting (XSS): Stored, Reflected, DOM-Based • Broken Authentication & Session Management • Session Hijacking • Cookie Manipulation • Basics of JWT (JSON Web Tokens)	**15**
3	**Access Control, CSRF & Server-Side Exploitation** • Insecure Direct Object Reference (IDOR) • Access Control Vulnerabilities & Authorization Bypass • Cross-Site Request Forgery (CSRF) • Token-Based Defenses • Server-Side Request Forgery (SSRF): Exploitation & Mitigation • File Inclusion Attacks • Local File Inclusion (LFI) • Remote File Inclusion (RFI) • Command Injection & Executing System Commands	
4	**Web Server Security, Misconfigurations & Defensive Mechanisms** • Web Server Fingerprinting & Vulnerability Mapping • Exploiting Web Server Misconfigurations • Directory Traversal & Common Security Gaps • Web Application Firewalls (WAFs) • Functionality • Limitations • Bypass Techniques (Basic) • Defensive Coding & Secure Practices • Input Sanitization • Output Encoding • Secure Server Hardening	

Sr. No.	**Title / Description of Practical**
1	**Practical based on setting up a controlled lab environment and using a proxy tool (Burp Suite) for application analysis.**
2	**Practical based on Information Gathering using reconnaissance tools and techniques.**
3	**Practical based on identifying and exploiting Reflected and Stored Cross-Site Scripting (XSS).**
4	**Practical based on performing various types of SQL Injection attacks, including Blind SQLi**

Sr. No.	Title / Description of Practical
5	**Practical based on exploiting Broken Authentication flaws and Session Hijacking.**
6	**Practical based on exploiting Insecure Direct Object Reference (IDOR) vulnerabilities.**
7	**Practical based on exploiting Cross-Site Request Forgery (CSRF).**
8	**Practical based on exploiting Local File Inclusion (LFI) to read sensitive server files.**
9	**Practical based on exploiting Command Injection to execute arbitrary OS commands.**
10	**Practical based on Web Server Fingerprinting and identifying outdated server versions/misconfigurations.**
11	**Practical based on creating a defensive code solution (input validation) for a known vulnerability (XSS or SQLi).**
12	**Practical based on applying security hardening steps to a basic web server configuration.**

Reference Books:	
1	Dafydd Stuttard & Marcus Pinto — **The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws**, Wiley.
2	Peter Yaworski — **Web Hacking 101**, Self-published.
Supplementary learning Material:	
1	• **OWASP Top 10** — https://owasp.org/www-project-top-ten/
2	• **OWASP Web Security Testing Guide** (WSTG) — https://owasp.org/www-project-web-security-testing-guide/
3	• PortSwigger Web Security Academy — https://portswigger.net/web-security
Pedagogy:	
• Justify all the topics unit-wise • Assignments / Quiz / Presentation / Participation for continuous evaluation and assessment • Internal / External Examination as per the norms of CVM University	

Suggested Specification table with Marks (Theory) (Revised Bloom's Taxonomy):

Distribution of Theory Marks in %						**R**: Remembering; **U**: Understanding; **A**: Applying; **N**: Analyzing; **E**: Evaluating; **C**: Creating
R	**U**	**A**	**N**	**E**	**C**	

20	40	15	15	5	5	

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcomes (CO):

Sr.	Course Outcome Statements	%weightage
1.	Learners will be able to understand the fundamentals of ethical hacking, penetration testing methodology, and OWASP Top 10 vulnerabilities, and perform reconnaissance and footprinting using passive, active, and proxy-based techniques (e.g., Burp Suite).	**50%**
2.	Learners will be able to analyze and exploit key web vulnerabilities such as **SQL Injection**, **Cross-Site Scripting (XSS)**, **Broken Authentication**, **Session Hijacking**, and **Insecure Direct Object Reference (IDOR)**, and understand their impact on application security.	**50%**
3	Learners will be able to exploit server-side vulnerabilities including **SSRF**, **LFI/RFI**, **Command Injection**, and **Web Server Misconfigurations**, and perform web server fingerprinting and vulnerability mapping to evaluate system weaknesses.	
4	Learners will be able to implement preventive security measures such as **input sanitization**, **output encoding**, **CSRF token protection**, **WAF-based defenses**, and apply secure coding and server hardening practices to mitigate common web application attacks.	

Curriculum Revision:	
Version:	1.0
Drafted on (Month-Year):	April-2025
Last Reviewed on (Month-Year):	May- 2025
Next Review on (Month-Year):	Feb-2027

	FACULTY OF SCIENCE
	Effective from Academic Batch:2025-26
Programme:	**Master of Science(Cyber Security)**
Semester:	**II**
Course Code:	**101570206**
Course Title:	**Web Technology – II**
Course Group:	**CORE**

Course Objectives:

- To provide advanced knowledge of modern web technologies and frameworks.
- To develop client-side scripting and interactive web applications using JavaScript and frameworks.
- To understand backend integration and full-stack concepts.
- To ensure secure web application development practices

Teaching & Examination Scheme:

Contact hours per week			Course Credits	Examination Marks (Maximum / Passing)				
				Theory		J/V/P*		Total
Lecture	Tutorial	Practical		Internal	External	Internal	External	
4	--	--	4	25/10	25/10	25/10	25/10	100/40

* **J**: Jury; **V**: Viva; **P**:Practical

Detailed Syllabus:

Sr.	Contents	Hours
1	**Frontend Fundamentals (HTML, CSS, JS)** • HTML5 structure and semantic elements • Responsive web design principles • CSS3 styling: transitions, animations, flexbox, grid layout • JavaScript basics: variables, functions, arrays, objects • DOM manipulation and event handling • Form validation and dynamic content creation • Asynchronous JavaScript: Fetch API and JSON data handling	8
2	**PHP Fundamentals** • Introduction to PHP and server-side scripting • PHP syntax, variables, data types, and operators • Conditional statements, loops, and control structures • Working with forms and handling user input (GET & POST) • PHP functions and arrays (structured coding) • Modular programming using include and require • PHP error handling and debugging	6

3.	**PHP with MySQL Integration** • Introduction to relational databases and MySQL • Connecting PHP with MySQL using mysqli and PDO • CRUD Operations — Create, Read, Update, Delete • User Authentication: login, logout, and session tracking • Cookies and session management • File upload and download functionality	**8**
4	**Web Security and Advanced Concepts** • Input sanitization and preventing SQL injection • PHP JSON — REST API creation and consumption • Error handling, logging, and exception management • Secure coding: preventing XSS, CSRF, directory traversal • MVC architecture basics in PHP	**8**

List of Practical's

Sr. No.	Title / Description of Practical
1	Practical based on creating a **responsive webpage** using HTML5 semantic elements and CSS3 layout models (Flexbox/Grid).
2	Practical based on **designing a web form** using HTML5 validation attributes and JavaScript-based input validation.
3	Practical based on **implementing dynamic webpage behavior** using JavaScript (DOM manipulation and event handling).
4	Practical based on **displaying external JSON data** on a webpage using the Fetch API.
5	Practical based on **PHP syntax, variables, data types, and control structures** to produce formatted output.
6	Practical based on **handling HTML form data** using PHP (GET and POST methods).
7	Practical based on **creating and using PHP functions, arrays, and loops** for structured coding.
8	Practical based on **modular PHP programming** using Include and Require statements.
9	Practical based on **establishing connection between PHP and MySQL** using `mysqli` or PDO.
10	Practical based on **performing CRUD (Create, Read, Update, Delete)** operations in PHP with MySQL database.
11	Practical based on **developing a user authentication system** using sessions and cookies.
12	Practical based on **validating user inputs and handling errors** in PHP web forms.
13	Practical based on **file upload and download functionality** in PHP with security validation.
14	Practical based on **creating and consuming RESTful APIs** using PHP and JSON.
15	Practical based on **implementing secure coding practices** in PHP (preventing XSS, CSRF, and SQL Injection).

Reference Books:	
1	Luke Welling & Laura Thomson — *PHP and MySQL Web Development*, Pearson.
2	Robin Nixon — *Learning PHP, MySQL & JavaScript: With jQuery, CSS & HTML5*, O'Reilly.
Supplementary learning Material:	
1	• PHP Official Documentation — https://www.php.net/docs.php
2	• W3Schools PHP Tutorials — https://www.w3schools.com/php/
3	• MySQL Reference Manual — https://dev.mysql.com/doc/
Pedagogy:	
• Assignments / Quiz / Presentation / Participation for continuous evaluation and assessment • Internal / External Examination as per the norms of CVM University	

Suggested Specification table with Marks (Theory) (Revised Bloom's Taxonomy):

Distribution of Theory Marks in %						**R**: Remembering; **U**: Understanding; **A**: Applying; **N**: Analyzing; **E**: Evaluating; **C**: Creating
R	**U**	**A**	**N**	**E**	**C**	
20	40	15	15	5	5	

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Course Outcomes (CO):

Sr.	Course Outcome Statements	%weightage
CO-1	Learners will be able to design and develop responsive, accessible, and visually structured web interfaces using **HTML5 semantic elements**, **CSS3 (flexbox, grid, transitions, animations)**, and **JavaScript** for DOM manipulation, event handling, form validation, and asynchronous data processing using the Fetch API and JSON.	**25**
CO-2	Learners will demonstrate the ability to implement server-side logic using **PHP syntax, variables, operators, control structures, functions, arrays**, and modular programming through **include/require**, along with effective handling of user input using **GET and POST** methods.	**25**
CO-3	Learners will be able to integrate **PHP with MySQL** using mysqli/PDO, perform **CRUD operations**, and develop functional features such as **user authentication, session and cookie management, and file upload/download**, enabling the development of robust, data-centric applications.	**25**
CO-4	Learners will apply secure coding techniques by implementing **input sanitization**, preventing **SQL injection, XSS, CSRF, and directory traversal**, managing errors and exceptions effectively, and understanding the fundamentals of **REST APIs** and **MVC-based architecture** in PHP.	**25**

Curriculum Revision:	
Version:	1.0
Drafted on (Month-Year):	Nov-2025
Last Reviewed on (Month-Year):	Dec- 2025
Next Review on (Month-Year):	Feb-2027