B.Sc. Information Technology with Cyber Security

Semester	Course Code	Course Category	Hours/ Week	Credits	Marks for Evaluation		
					CIA	ESE	Total
III	24UICVAC1	VALUE ADDED COURSE	6	-	-	100	100
Course Title	Bug Bounty Hunting						

SYLLABUS		
Unit	**Contents**	**Hours**
I	Introduction to Bug Bounty Programs: Objectives, benefits, and platforms. Overview of Web Application Security: Common vulnerabilities and attack vectors. Legal and Ethical Considerations: Responsible disclosure, scope limitations, and non-disclosure agreements. Setting up Tools and Environments: Introduction to Burp Suite, OWASP ZAP, and Virtual Machines. Hands-on Exercises: Basic reconnaissance techniques, understanding common web vulnerabilities.	6
II	Understanding the Importance of Reconnaissance: Gathering information about the target. Passive Reconnaissance Techniques: OSINT (Open-Source Intelligence) gathering, footprinting. Active Reconnaissance Techniques: Port scanning, service identification, and fingerprinting. Content Discovery: Identifying hidden directories, files, and endpoints using tools like DirBuster, DirSearch, and Gobuster. Hands-on Labs: Performing reconnaissance and content discovery on target web applications.	6
III	Injection Attacks: SQL Injection (SQLi), Cross-Site Scripting (XSS), and Command Injection. Authentication and Session Management: Brute force attacks, session fixation, and cookie manipulation. Authorization Flaws: Insecure Direct Object References (IDOR), broken access controls. Information Leakage: Error handling, verbose responses, and sensitive data exposure. Hands-on Exercises: Exploiting vulnerabilities in vulnerable web applications, bypassing authentication mechanisms.	6
IV	Server-Side Request Forgery (SSRF) and XML External Entity (XXE) attacks. Remote Code Execution (RCE) and File Upload Vulnerabilities. Business Logic Flaws: Account takeover, transaction tampering, and privilege escalation. Web Application Firewall (WAF) Bypass Techniques. Hands-on Labs: Exploiting advanced vulnerabilities in real-world scenarios, bypassing security controls.	6
V	Bug Reporting Best Practices: Writing clear, detailed, and actionable vulnerability reports. Providing Proof of Concept (PoC) Code and Evidence. Collaborating with Organizations: Communicating findings, verifying fixes, and retesting. Responsible Disclosure Policies: Understanding organization-specific disclosure guidelines. Hands-on Exercises: Drafting and submitting vulnerability reports, engaging with organizations on bug fixes.	6

Text Book(s):

1. Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilitiesby Vickie Li
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by DafyddStuttard and Marcus Pinto

Web Resource(s):
1. https://archive.org/details/opensource?and%5B%5D=subject%3A%22penetration+testing%22&sort=reviewdate&page 2. https://owasp.org/www-chapter-czech-republic/slides/Getting_Started_with_Bug_Bounty.pdf 3. https://www.nitttrchd.ac.in/imee/Labmanuals/Lab%20manual%20on%20Bug%20_%20Bounty.pdf 4. https://www.youtube.com/watch?v=QqrK294l_oI

Course Outcomes		
Upon successful completion of this course, the students will be able to:		
CO No.	**CO Statement**	**Cognitive Level (K-Level)**
CO1	Find the basic of Web Application Security and Common vulnerabilities	K1
CO2	Understand reconnaissance and content discovery	K2
CO3	Identify Common vulnerabilities in web applications	K3
CO4	Analyse advanced vulnerabilities in real-world scenarios	K4
CO5	Estimate a vulnerability report and engaging with organizations on to Implement bug fixes.	K5

Course Coordinator: Mr. P. Mohamed Thahir