CTMSCS SI P3: Web Application Security

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE						
Th	Tu	Pr	C	TCH	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	Marks	Hrs.	
03	00	00	03	03	25	00:45	50	01:30	100	03:00	-	-	200

Objectives

1. To learn the concept of web application technology
2. Learn various aspects of web application security
3. Learn to vulnerability assessment of web application security
4. Exploitation of potential found vulnerability
5. Learn industry standard techniques to exploit advanced vulnerability

UNIT – I
Introduction to web technology and information Gathering

TCP, HTTP/S Protocol Basics, Encoding, Origin, Cookies, Sessions, Fingerprinting the web server, Subdomain's enumeration, finding virtual hosts, fingerprinting custom applications, Enumerating resources, Relevant information through misconfigurations, Google hacking.

UNIT – II

Web Application Security Vulnerability Terminology

Introduction to Vulnerability Assessment, Life cycle of Vulnerability Assessment, Vulnerability Scanners, Unknown Vulnerability, False Positive, CVE, CWE, Common Vulnerability Scoring System (CVSS), STRIDE, DREAD, Secure Source Code Review.

UNIT – III
Proxy and Interception

Burp Suite / OWASP Zed Attack Proxy (ZAP): Logging and monitoring, learning tools to spider a website, analyzing website content, Brute forcing unlinked files and directories via ZAP and ffuf, Web authentication mechanisms, Fuzzing with Burp Intruder, Username harvesting and password guessing, Burp sequencer, Session management and attacks, Authentication and authorization bypass.

UNIT – IV
Attack Landscape - Web Application Security

OWASP 10 Ten – Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Control, Security Misconfiguration, Cross Site Scripting, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring, Cross Site Request Forgery, File Inclusion, Click Jacking, File Inclusion, File Upload, Insecure Captcha, SSRF/XSPA.

UNIT – V
Advanced Web Security Pen-Testing

Web Service concepts, REST concepts, SQL Injection - Vulnerable code, Sensitive data in GET, Weak Auth tokens & IDOR, Leaky APIs, Automated Scanning with FuzzAPI / Astra / other industry standard tools, Introduction to CMS and Docker containers security.

Reference Books

1. Web Application Security, A Beginner's Guide by Bryan Sullivan, Vincent Liu, McGraw-Hill Education Publication (2011).
2. Hands-On Bug Hunting for Penetration Testers A Practical Guide to Help Ethical Hackers Discover Web Application Security Flaws by Joseph Marshall, Packt Publication (2018).
3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard, Marcus Pinto, 2nd Edition, Wiley Publication (2007).
4. The Penetration Tester's Guide to Web Applications by Serge Borso, Artech House Publication (2019).
5. Web Application Security Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman, O'Reilly Media Publication (2020)

0734