GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering
Level: UG
Subject Code : 3174806
Subject Name : Web Application Security

w. e. f. Academic Year:	A.Y. 2025-26
Semester:	VII
Category of the Course:	PEC

Prerequisite:	Web Technologies, Cybersecurity, Databases and SQL
Rationale:	With the increasing reliance on web-based systems and online services, web applications have become a primary target for cyberattacks. This course focuses on providing students with a strong foundation in web application security by covering key principles, vulnerabilities, and secure development practices. Understanding threats such as XSS, SQL Injection, and CSRF, as well as authentication and authorization mechanisms, is crucial for building resilient applications. The course introduces frameworks and models like OWASP and SDL to instill a security-first approach in the software development lifecycle. Prior knowledge of programming, web technologies, and basic cybersecurity is essential to effectively grasp the practical and theoretical aspects of the subject.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
1	Understand the fundamentals of web application security	U
2	Apply security principles in developing a secure web application	Ap
3	Identify common web vulnerabilities that are exploited by hackers	An
4	Identify the secure model for web application development and deployment	An
5	Apply best practices for mitigations of vulnerabilities	Ap

**Revised Bloom's Taxonomy (RBT)*

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering
Level: UG
Subject Code : 3174806
Subject Name : Web Application Security

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
3	0	2	4	70	30	20	30	150

Course Content:

Unit No.	Content	No. of Hours
1.	**INTRODUCTION** :History of Software Security – OWASP Top Ten List 2021 – Input Validation – Attack Surface Reduction – Classifying and Prioritizing Threats	06
2.	**WEB APPLICATION SECURITY PRINCIPLES** Authentication - Access Control Overview - Two Factor and Three Factor Authentication - Web Application Authentication – Authorization - Session Management Fundamentals - Securing Web Application Session Management.	08
3	**COMMON WEB APPLICATION VULNERABILITIES** Cross Site Scripting- Reflected XSS- Stored XSS- DOM based XSS- Mutation based XSS – Cross Site Request Forgery - SQL Injection – Code Injection – Insecure Direct Object References (IDOR)	08
4	**SECURE DEVELOPMENT AND DEPLOYMENT** Application Security- Training- Threat Modelling- Secure Coding Libraries- Code Review- Security TestingSecurity Incident Response Planning – Microsoft Security Development Lifecycle (SDL) – OWASP Comprehensive Lightweight Application Security Process (CLASP) – Software Assurance Maturity Model (SAMM)	10
5.	**MITIGATIONS AND COUNTERMEASURES** Anti XSS Coding Best Practices- Sanitizing User Input – Anti CSRF Coding Best Practices – Mitigating Against SQL Injection – Generic Injection Defenses – Defending Against IDOR – Architecture Level Mitigations	08

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)				
U Level	**A Level**	**N Level**	**E Level**	**C Level**
15	**30**	**25**	**15**	**15**

Where U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. Andrew Hoffman, "Web Application Security: Exploitations and Countermeasures for Modern Web Applications", 2nd Edition, O'Reilly, 2024
2. Brian Sullivan and Vincent Liu, "Web Application Security: A Beginners Guide", 1st Edition, McGrawHill, 2012
3. Ron Lepofsky, "The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web", Apress, 2015
4. Joseph Marshall, "Hands-On Bug Hunting for Penetration Testers: A practical guide to help ethical hackers discover web application security flaws", Packt, 2018

Sample List of Experiments:

1. Identify security issues in web application – Walking An Application in TryHackMe Platform
2. Burp Suite Basics in TryHackMe Platform
3. OWASP ZAP to scan authenticated web application in TryHackMe Platform
4. SQL Injection Lab in TryHackMe Platform
5. Explore OWASP Top Ten -2021 Vulnerabilities in TryHackMe Platform
6. SQLmap to exploit web application in TryHackMe Platform
7. Exploit File Inclusion and Path Traversal Vulnerabilities in TryHackMe Platform
8. Server Side Template Injection in TryHackMe Platform
9. DejaVu Code Injection Vulnerability in TryHackMe Platform
10. NoSQL Injection on MongoDB in TryHackMe Platform

****