Uka Tarsadia University

B. Tech.

Semester VI

WEB AND MOBILE SECURITY

CY5010

Effective from June-2023

Syllabus version: 1.00

Subject Code	Subject Title	Teaching Scheme			
		Hours		Credits	
		Theory	Practical	Theory	Practical
CY5010	Web and Mobile Security	3	2	3	1

Subject Code	Subject Title	Theory Examination Marks		Practical Examination Marks	Total Marks
		Internal	External	CIE	
CY5010	Web and Mobile Security	40	60	50	150

Objectives of the course:

- To understand the basic concepts of web and mobile security fundamentals.
- To understand authentication, authorization methods used in web and mobile security.
- To implement browser, database security, analyse fingerprint and application threats.

Course outcomes:

Upon completion of the course, the student shall be able to,

CO1: Understand the basic concepts of web and mobile security.

CO2: Understand different authentication methods used in web and mobile security.

CO3: Describe different authorization methods used in web and mobile security.

CO4: Understand and implement browser and database security principles.

CO5: Understand mobile wireless attacks and remediation in the context of web and mobile security.

CO6: Analyse fingerprinting malware and application-based threats in web and mobile security.

Sr. No.	Topics	Hours
	Unit – I	
1	**Introduction:** Introduction to Web security, The OWASP top ten list, Input validation, Attack surface reduction, Classifying and prioritizing threats, Mobile phone threats and vulnerabilities exploits, Tools and techniques, Mobile device security models.	6
	Unit – II	

2	**Authentication:** Access control overview, Authentication fundamentals, Two-factor and three-factor authentication, Web application authentication, Securing password-based authentication, Secure authentication best practices.	9
Unit – III		
3	**Authorization:** Authorization overview, Session management, Authorization fundamentals, Authorization goals, Detailed authorization check process, Types of permissions, Authorization layers, Custom authorization mechanisms, Session management fundamentals, Securing web application session management.	8
Unit – IV		
4	**Browser and Database Security Principles:** Defining the same-origin policy, Exceptions to the same-origin policy, Cross-site scripting, Cross-site request forgery, Structured Query Language (SQL) injection, Setting database permissions, Stored procedure security.	8
Unit – V		
5	**Mobile Wireless Attacks and Remediation:** Security awareness, The kali Linux security platform, Client and infrastructure exploits, Other USB exploits, Network security protocol exploits, Mobile software exploits and remediation.	8
Unit – VI		
6	**Fingerprinting Malware and Application-Based Threats:** Fingerprinting, cookies, Cross-site profiling, Fingerprinting methods, unique device identification, New methods of mobile fingerprinting, Spyware for mobile devices, Malware on android devices, Madware, mobile malware and social engineering.	6

Sr. No.	**Web and Mobile Security (Practical)**	**Hours**
1.	Introduction installation and configuration of OWASP ZAP.	4
2.	Demontration of how to Proxy Web Traffic through OWASP ZAP.	4
3.	Demonstration to Intercept HTTP Requests with OWASP ZAP.	2
4.	Demonstration of Spidering a Website with OWASP ZAP.	4

5.	Implementation and testing for Weak SSL/TLS HTTPS ciphers.	2
6.	Implementation of how Secure Cookies Works.	2
7.	Demonstration of XSS Protection Header.	2
8.	Demonstration to check HTTPS certificates for common issues.	2
9.	Demonstration to check HTTP Headers from Browser.	2
10.	Introduction installation and configuration of Burp Suite.	2
11.	Demonstration to Intercept HTTP Requests with Burp Suite.	2
12.	Demonstration to HTTP headers with Burp Suite.	2

Text book:

1. Liu, Vincent Sullivan, and Bryan, “Web application security a beginner's guide”, McGraw-Hill.
2. Jim Doherty, “Wireless and Mobile Device Security”, Jones & Bartlett Learning.

Reference Books:

1. Dafydd Stuttard, “The Web Application Hacker’s Handbook”, Wiley India Pvt. Ltd.

Course objectives and Course outcomes mapping:

- To understand the basic concepts of web and mobile security fundamentals: CO1 and CO2
- To understand authentication, authorization methods used in web and mobile security: CO3 and CO4
- To implement browser, database security, analyse fingerprint and application threats: CO5 and CO6

Course units and Course outcomes mapping:

Unit No.	Unit Name	Course Outcomes					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction	✓					
2	Authentication		✓				
3	Authorization			✓			
4	Browser and Database Security				✓		

	Principles						
5	Mobile Wireless Attacks and Remediation					✓	
6	Fingerprinting Malware and Application-Based Threats						✓

Programme outcomes:

PO 1: Engineering knowledge: An ability to apply knowledge of mathematics, science, and engineering.

PO 2: Problem analysis: An ability to identify, formulates, and solves engineering problems.

PO 3: Design/development of solutions: An ability to design a system, component, or process to meet desired needs within realistic constraints.

PO 4: Conduct investigations of complex problems: An ability to use the techniques, skills, and modern engineering tools necessary for solving engineering problems.

PO 5: Modern tool usage: The broad education and understanding of new engineering techniques necessary to solve engineering problems.

PO 6: The engineer and society: Achieve professional success with an understanding and appreciation of ethical behavior, social responsibility, and diversity, both as individuals and in team environments.

PO 7: Environment and sustainability: Articulate a comprehensive world view that integrates diverse approaches to sustainability.

PO 8: Ethics: Identify and demonstrate knowledge of ethical values in non-classroom activities, such as service learning, internships, and field work.

PO 9: Individual and team work: An ability to function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO 10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give/receive clear instructions.

PO 11: Project management and finance: An ability to demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO 12: Life-long learning: recognition of the need for, and an ability to engage in life-long learning.

Programme outcomes and Course outcomes mapping:

Programme Outcomes	Course Outcomes					
	CO1	CO2	CO3	CO4	CO5	CO6
PO1						
PO2						
PO3			✓	✓		
PO4				✓		✓
PO5						
PO6		✓				
PO7						
PO8					✓	
PO9						
PO10						
PO11						
PO12	✓			✓		