INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

INTRODUCTION TO WEB SECURITY								
VI Semester: CSE (CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
ACCD17	**Elective**	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: Computer Networking, Operating System								

I. COURSE OVERVIEW:

This course provides foundational knowledge on securing web applications and services against cyber threats. It explores common vulnerabilities, secure coding practices, and protective measures to ensure the integrity, confidentiality, and availability of web systems. Students will gain practical exposure to tools and techniques for analyzing and mitigating web security risks.

II. COURSE OBJECTIVES:

The students will try to learn:

I	The understanding of fundamental principles of web security and the threat landscape.
II	The study of common web vulnerabilities and their exploitation techniques.
III	The adoption of best practices for secure web application development.
IV	The utilization of tools and frameworks for securing and auditing web applications

III. COURSE OUTCOMES:

At the end of the course, students should be able to:

CO1	Understand the basic concepts of web security and threat models.
CO2	Identify and analyze common web application vulnerabilities.
CO3	Develop secure web applications by implementing security best practices.
CO4	Use tools to test and secure web applications against attacks.
CO5	Formulate strategies for monitoring, detecting, and responding to web-based threats.
CO6	Understand legal and ethical considerations in web security practices

IV. COURSE CONTENT:

MODULE – I: INTRODUCTION TO WEB SECURITY (09)
Basics of Web Security, OWASP Top 10 Vulnerabilities, Threats to Web Applications, Security Goals (Confidentiality, Integrity, Availability), Understanding the HTTP Protocol and HTTPS

MODULE – II: COMMON WEB VULNERABILITIES (10)
Injection Attacks (SQL, Command, Code), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Insecure Deserialization, Security Misconfigurations

MODULE – III: SECURE WEB APPLICATION DEVELOPMENT (09)
Input Validation and Sanitization, Authentication and Authorization Mechanisms, Session Management, Secure Storage of Credentials, Secure APIs.

Authentication and Authorization Mechanisms, Input Validation and Output Encoding, SQL Injection and Database Security.

MODULE - IV: WEB SECURITY TESTING TOOLS AND TECHNIQUES (10)
Penetration Testing Basics, Tools like Burp Suite, OWASP ZAP, Fuzzing Techniques, Vulnerability Scanning, Web Application Firewalls (WAFs).

MODULE – V: EMERGING TRENDS AND LEGAL ASPECTS (10)
Trends in Web Security: AI for Threat Detection, Serverless and Cloud Security Challenges, Legal and Ethical Issues, International Standards and Compliance (e.g., GDPR, PCI DSS).

V. TEXTBOOKS:

1. Bryan Sullivan and Vincent Liu “Web Application Security: A Beginner's Guide”, McGraw-Hill Education, 1st Edition, 2011.
2. Dafydd Stuttard and Marcus Pinto, “The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws”, Wiley, 2nd Edition, 2011.

VI. REFERENCE BOOKS:

1.Mark Curphey and Tanya Janca, “Alice and Bob Learn Application Security”, Wiley, 1st Edition, 2020.
2.Michal Zalewski, “The Tangled Web: A Guide to Securing Modern Web Applications”, No Starch Press, 1st Edition, 2011.

VII. ELECTRONIC RESOURCES:

1. https://owasp.org/
2. https://developer.mozilla.org/en-US/docs/Web/Security
3. https://portswigger.net/web-security

VIII. MATERIALS ONLINE

1. Course template
2. Tutorial question bank
3. Tech talk topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes

10. PowerPoint presentation
11. E-Learning Readiness Videos (ELRV)