PRESIDENCY UNIVERSITY

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi

Itgalpur, Rajankunte, Yelahanka, Bengaluru – 560064

Course Code: CSE3097	**Course Title:** Web Security **Type of Course:** Integrated course		**L- T-P- C**	2	0	2	3
Version No.		1.0				
Course Pre-requisites		**Advanced Computer Networks (CSE3070)**				
Anti-requisites		**NIL**				
Course Description		The purpose of this course is to introduce you to the field of web security by understanding web functionality and various security validations. The web is our gateway to many critical services and is quickly evolving as a platform to connect all our devices. Web vulnerabilities are growing on a year-to-year basis and designing secure web applications is challenging. The course covers fundamental concepts of web security principles, web vulnerability and exploitation, various attacks on web applications, and a few basic topics on web encryption.				
Course Objective		The objective of the course is to familiarize the learners with the concepts of Web Security and attain Skill Development through Experiential Learning techniques.				
Course Outcomes		**On successful completion of this course the students shall be able to:** 1. **Define** the fundamentals of Web applications and validation. (Remember) 2. **Recognize** the significance of password and authentication in web applications. (Understand) 3. **Explain** the importance of session management in web. (Understand) 4. **Apply** web attack techniques to find vulnerabilities in web applications. (Apply)				
Course Content:						
Module 1	**Introduction to Web Security**	Quiz	Knowledge		**14 Sessions - L[08]+P[06]**	
	Topics: Web Functionality, Encoding Schemes, Mapping the Application - Enumerating the Content and Functionality, Analyzing the Application Bypassing, Client-Side Controls: Transmitting Data Via the Client, Capturing User Data, Handling Client-Side Data Securely - Input Validation, Blacklist Validation, Whitelist Validation. The Defense in-Depth Approach - Attack Surface Reduction, Rules of Thumb, Classifying and Prioritizing Threats.					

Module 2	**Web Application Authentication**	Assignments	Comprehension		**16 Sessions L[08] +P[08]**
	Topics: Authentication Fundamentals- Two Factor and Three Factor Authentication - Password Based, Built-in,HTTP, Single Sign-on Custom Authentication- Secured Password Based Authentication: Attacks againstPassword, Importance of Password Complexity, Design Flaws in Authentication Mechanisms - Implementation, Flaws in Authentication Mechanisms - Securing Authentication.				
Module 3	**Session Management &Web Security Principles**	Quiz	Comprehension		**16 Sessions L[08] +P[08]**
	Topics: Need for Session Management, Weaknesses in Session Token Generation, Weaknesses in Session Token Handling, Securing Session Management; Access Control: Access Control Overview, Common Vulnerabilities, Attacking Access Controls, Securing Access Control. Origin Policy, Exceptions, Browser security Principles- Cross Site Scripting and Cross Site Request Forgery, File Security Principles: Source Code Security, Forceful Browsing, Directory Traversals.				
Module 4	**Web Application Vulnerability**	Assignment	Application		**14 Sessions L[06] +P[08]**
	Topics: Attacking data-stores and backend components- Injecting into Interpreted Contexts, injecting into SQL, NoSQL, XPath, LDAP, Injecting OS Commands, Manipulating File Paths, Injecting into XML Interpreters, Injecting into Back-end HTTP Requests, Injecting into Mail Services, Attacking application logic-real world logic flaws, Attacking users-Cross site scripting-varieties of XSS,XSS attacks in action, finding and exploiting XSS vulnerabilities, preventing XSS attacks, Other techniques-cookie based Attacks, HTTP Header Injection				

List of Laboratory Tasks:

1. Practical knowledge of known vulnerabilities in CGI, LAMP stacks, REST APIs cross-site scripting

Practical knowledge of known vulnerabilities in CGI, LAMP stacks, REST APIs cross-site scripting: Use the **Nessus tool** to scan the network for vulnerabilities.

i. Basic Network scanning
ii. Advanced scanning in general search
iii. Ntstat port scanning:
iv. Vulnerability Mapping
v. Policies:
vi. Plugins:
vii. General Scanning
viii. Port Scanning

Level 1: Identification of vulnerabilities
Level 2: Apply the concept

2. HTTP and setting up stacks, the various types of databases Access Controls, Vulnerabilities

HTTP and setting up stacks

i. Create a simple web application that can store information sent to it. For example, you could create a web application that will store to a text file anything provided in a URL parameter
ii. Write or modify an existing application that legitimately needs access to a sensitive resource ,but uses it at a time when it does not actually need it

Various types of databases Access Controls

i. Role-Based Access Control (RBAC)
iii. Mandatory Access Control (MAC)

Vulnerability: Study and work with KF Sensor

STEP1: Download **KF** Sensor tool Evaluation Setup File from KF Sensor Website.
STEP-2: Install with License Agreement and appropriate directory path.
STEP-3: Reboot the Computer now. The KF Sensor automatically starts during Windows boot.
STEP-4: Click Next to setup wizard.
STEP-5: Select all port classes to include and Click Next.
STEP-6: "Send the email and Send from email", enter the ID and Click Next.
STEP-7: Select the options such as Denial of Service[DOS], Port Activity, Proxy Emulsion, Network Port Analyzer, Click Next.
STEP-8: Select Install as System service and Click Next.

Level 1: Identification of vulnerabilities
Level 2: Apply the concept

3. Study of web authoring tools (any 2-3 tools)

i. Study and work with Net Stumbler tool
ii. Study and work with Snort
iii. Study and work with Nmap

Level 1: Install the tools required
Level 2: Apply the concept

4. Testing web applications

Study and work with Word press tool

i. Create an Online Community website and test the website
ii. Showcase Your Work Online and test its worth
iii. Create a Local Business Website and test the website.

Level 1: Define the test cases
Level 2: Apply the concept to test the web application

5. SQL injection and prevention

From the given data set ,

i. Put limits on all result sets
ii. Cleanse and Validate Freeform User Input
iii. Remove Freeform User Input When Possible
iv. Validate Data Prior to Processing
v. Ensure Errors are Not User-Facing
vi. Use Stored Procedures to Abstract Business Logic and Control parameters
vii. Use LIKE Operators Carefully

viii. Limit Use of xp_cmdshell and Other Extended Stored Procedures
ix. Perform Penetration Tests
x. Code Review
xi. Minimizing the Impact of SQL Injection
xii. Principle of Least Privilege & Login Security
xiii. Secure Linked Servers and Data Sources

Level 1: Recognize and acquire the data
Level 2: Apply the concept

6. Cross site request forgery attack lab

With the usage of Virtual Machines

i. Configure the Virtual Machines:
ii. Observing HTTP Request in Victim VM
iii. CSRF Attack using GET Request
iv. CSRF Attack using POST Request
v. Implementing a countermeasure

Level 1: Identify and acquire the data
Level 2: Apply the concept

7. Web tracking

Tracking the Web based scenario by

- Environment Configuration
- clear history and cookies
- open a new private window in Firefox

Task 1: Understand the basic working of the web tracking
Task 2: Importance of cookie in Web tracking
Task 3: Tracked user interests and data
Task 4: How ads are displayed in a website
Task 5: Tracking in a Private browser window
Task 6: Real world tracking
Task 7: Countermeasures

Level 1: Identify and acquire the data logs
Level 2: Apply the concept

Targeted Application & Tools that can be used:

(1) Word press tool can be used for building websites with possible vulnerabilities.
(2) Tools such as Nmap and Nessus can be used for web attack demonstration.
(3) KF Sensor advanced 'honeypot' intrusion and insider threat detection system for Windows networks
(4) Snort can be used for network intrusion detection system and intrusion prevention system
(5) Net Stumbler tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards.

Textbook(s):

T1. Dafydd Stuttard, Marcus Pinto, “The Web Application Hacker’s Handbook”, Willey Publishing Inc. ,2008

References:

R1. B. Sullivan, V. Liu, and M. Howard, *"Web Application Security"*, A B Guide. New York: McGraw-Hill Education, 2011.

R2. *Web Application Security:* Exploitation and Countermeasure for Modern Web Applications, byAndrew Hoffman.

E-book Links

T1: https://www.oreilly.com/library/view/web-application-security/9780071776165/
T2: https://www.oreilly.com/library/view/web-application-security/9781492053101/

Web links-

1.	**NPTEL course**	:	Introduction to Information Security I, IIT Madras https://nptel.ac.in/courses/106106129
2.	**Coursera Link**	:	https://www.coursera.org/learn/security-and-authentication

Topics related to development of "Skills":
Web technology fundamentals, web security measures and webvulnerability/attacks.

Topics related to development of "Experimental Learning":
Writing different web exploits to demonstratevulnerabilities in web applications.

Catalogue prepared by	Ms. Sreelatha PK
Recommended by the Board of Studies on	
Date of Approval by the AcademicCouncil	