SILVER OAK UNIVERSITY

School of Technology, Design and Computer Application
Silver Oak College of Computer Application
Department of Computer Application
Master of Science Cyber Security & Digital Forensics
Course Name: Web Application Security
Course Code: 1040147102
Semester: 1st

Prerequisite: Understanding of Http and Https protocols basics. Basics of SQL**.**

Course Objective: To identify and exploit potential vulnerabilities in web applications, assessing their impact on both the front end and source code, with the aim of understanding and mitigating security risks.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
3	1	0	4	4

Content:

Unit No.	Topics	Teaching Hours	% Weightage
1	**Web App Information Gathering:** HTTP Request, Response, Header Fields, and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering (whois, nsLookup, Netcraft for web server fingerprinting, subdomain enumeration), Fingerprinting frameworks, Hidden resource enumeration, Security misconfigurations, Google Hacking Database, ShodanHQ.	10	26
2	**Web Application Attacks 1:** SQL Statements, Finding SQL Injections, Exploiting SQL Injections, Bypass Authentication, XPath Injection, Error-Based Injection, Double Query Injection, Time-Based Injections, Union-Based Injections, SQL Map, Mitigation Plans, SQLi to Server Rooting, Advanced MySQL and MS-SQL Exploitation, Cross-Site Scripting (Anatomy of an XSS Exploitation, Reflected XSS, Persistent XSS, DOM-Based XSS), Browsers and XSS, Cookie Stealing, Defacements, Advanced Phishing Attacks, BeEF Framework, Mitigation	12	30

3	**Web Application Attacks 2:** Single-factor and two-factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious requests, user enumeration, random password guessing, remember-me functionality, no-limit attempts, password reset feature, logout flaws, CAPTCHA, insecure direct object reference, security missing function level access control, unvalidated redirects and forwards, Session ID.	8	17
4	**Advanced Topics in Industrial Web Application Security :** Exploring advanced attack scenarios such as Cross-Site Scripting (XSS),Handling session attacks and Cross-Site Request Forgery (CSRF) in industrial contexts,Addressing business logic flaws and denial-of-service threats specific to industrial web applications	8	17
5	**The Secure Development Lifecycle (SDL):** Threat modeling to identify and prioritize vulnerabilities, implementation of secure design principles-least privilege and defense in depth, enforcement of secure coding practices, utilization of code reviews and static analysis for early vulnerability detection, integration of security testing techniques- dynamic testing and penetration testing, deployment of secure configuration management and update mechanisms.	4	10

Course Outcomes:

Sr. No.	CO-Statement	Unit No
CO-1	Perform information gathering using whois, nsLookup, and Netcraft.	1
CO-2	Identify SQL statements and potential SQL injection vulnerabilities.	2
CO-3	Perform security testing for random password guessing and ensure secure implementations.	3
CO-4	Identify and mitigate web threats, tackle business logic flaws, and counter DoS attacks effectively	4
CO-5	Analyse secure development lifecycle to ensure security of industrial web applications.	5

Teaching & Learning Methodology: -

1. The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
2. Projector and Computer

List of Tutorials: **Total Hours: 14**

Sr. No.	Tutorials Name
1.	Prepare Case Study On Below Topics: 1. Netcraft 2. SQL Map 3. Sql Injection vulnerability 4. Google dorks+ ShodanHQ 5. Cross site scripting attack 6. CSRF (Cross Site Request Forgery) 7. Clickjacking 8. To simulate the deployment of an industrial web application while emphasizing secure configuration management and update mechanisms.

Major Equipment:

1. Computer System
2. LAN cable

Books Recommended:

1. Shema, M. & Adam "Seven deadliest web application attacks" Amsterdam: Syngress Media.
2. John & Sons - Stuttard, D. & Pinto, M. "The web application hacker's handbook: Discovering and exploiting security flaws", Wiley,Indianapolis,IN.
3. Sullivan, Bryan "Web Application Security, A Beginner's Guide." McGraw- Hill Education

CO-PO-PSO MATRIX:

Co.No.	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO-1	1	2	1	2				3	2
CO-2	1	2	3	1		2		3	3
CO-3	2	1	2		1			3	2
CO-4	1	2		3				2	1
CO-5	1	2	2	3	1			2	1