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: Practical-1(Web Application Security)
Course Code: 1040147105
Semester: 1st

Prerequisite: Http and Https basics. Basics of SQL. Basics of JavaScript

Course Objective: The objective of Web Vulnerability Assessment and Penetration Testing (VAPT) is to find all potential loopholes within web application's front end and source code and explore the severe impact of those loopholes by exploiting them.

Teaching Scheme:

Teaching Scheme				
L	T	P	Contact Hours	Credit
0	0	8	8	4

List of Experiments: **Total Hours: 112**

Sr. No.	Practicals Name
1.	Exploring Web Footprinting and Information Gathering: Utilize a variety of tools and techniques to gather comprehensive information and insights about web entities and their digital footprints.
2.	Information gathering using Google Dorking Database, Use of Google Dork to Find Vulnerable parameters, Shodan.io (Shodan Dorks) , Webcam Access.
3.	Command Injection(Php Command Shell Injection)
4.	Sql Authentication Bypass, Broken Access control, Privilege Escalation, 2FA bypass, HTML Injection.
5.	XML External Entities, XXE (Tryhackme)
6.	Exploit Insecure Direct Object Reference (IDOR) vulnerability within the website. Execute Unvalidated Redirects by manipulating URL redirections on the web application. Discover and demonstrate the presence of Cross-Site Request Forgery (CSRF) vulnerability within the website.
7.	Remote File Inclusion, Local File Inclusion(Path Traversal), Cross Origin Resource Sharing.
8.	Implementing and Evaluating Mitigation Strategies for Cross-Site Scripting (XSS) Attacks in Corporate Web Applications.
9.	Detecting and Handling Session Attacks and Defending Against Cross-Site Request Forgery (CSRF) in E-Commerce Platforms.

10.	Identifying and Addressing Business Logic Flaws in Industrial Control Systems.
11	Analyzing and Preventing Denial-of-Service (DoS) Threats in Critical Industrial Networks.

Course Outcomes:

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

Major Equipment:

1. Computer System
2. LAN cable

Teaching & Learning Methodology: -

1. Projector and Computer
2. Experiments shall be performed in the laboratory related to course contents

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. Heiderich, M., Nava E.A.V.Heyes, G., & Lindsay, D.” Web application obfuscation” Amsterdam Syngress Media,U.S
4. 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	2	1	2	3				3	3
CO-2	3	1	1	1		2		2	3

CO-3	2	3	2	2	1			2	2
CO-4	3	2	1					3	2
CO-5	2	1	2	2				2	2