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(Mobile Application Security)
Course Code: 1040147111
Semester: 2nd

Prerequisite: Fundamentals of Android and iOS architecture. Mobile rooting and Jailbreaking.

Course Objective: The objective of Mobile Vulnerability Assessment and Penetration Testing (VAPT) is to find all potential loopholes in the mobile applications, operating system and hardware 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.	Setting up Mobile App Pentesting Environment, interact with the Devices, Starting withDrozer
2.	Configuring, Burp and Traffic Interception of Mobile Applications between client and server
3.	Configuring Live Device for Penetration Testing, Mitigation Approach for all Vulnerabilities.
4.	Performing static Analysis of Mobile Application using MOBSF
5.	Perform the jailbreak/Root the Android phone and get admin level Privilege by using tools such as Superoneclick, superboot.
6.	Performing Cross-application scripting error in Android Browser which leads to hacking the devices.
7.	Detects application communication vulnerabilities and performs exploitation using Com Droid.
8.	Performing reverse engineering & network communication attacks on android applications
9.	Perform static and dynamic analysis on a mobile application using MobSF.
10	Conduct a comprehensive security assessment of a web application using OWASP ZAP.
11	Implement penetration test on a web application using OWASP ZAP and Burp Suite.

12	Perform a penetration test on a mobile application using Burp Suite.

Course Outcomes:

Sr. No.	CO-Statement
CO-1	Recall the historical evolution of Android, tracing its development from inception to its current state.
CO-2	Compare and contrast the security models of Android and iOS platforms, highlighting their similarities and differences.
CO-3	Evaluate the implications of rooting (Android) and jailbreaking (iOS) devices on security and explore potential mitigation strategies.
CO-4	Utilize security testing tools to simulate attacks and identify vulnerabilities.

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 content

Books Recommended:

1. FL: Auerbach Publications - Fried, S “Mobile device security: A comprehensive guide to securing your information in a moving world. Boca Raton”
2. IN: Wiley, John & Sons - Stuttard, D. & Pinto, M “The web application hacker’s handbook: Discovering and exploiting security flaws.” Indianapolis
3. Dwivedi, H., Clark, C., & Thiel, D “Mobile application security. New York: McGraw-Hill Companies.

CO-PO-PSO MATRIX:

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