Semester - 1
Paper 103: Fundamentals of Web Designing and Web Application Security

Marks: 100 **Lectures 60**

Objective: Moving from networks the most important component any technology stack is the software which is positioned at the top of infrastructure. We will start with the necessities of how software applications are built, where students will understand and build their applications to have the real world feel on how the internet stack is working, along with showing them real loopholes while coding himself so that they understand the real world attacks which are possible on applications, and simulate them so that they can themselves come to conclusions and understand the best practices involved in application security.

Unit I: Web Designing and Penetration Testing Process

Scope Understanding, Liabilities and Responsibilities, Allowed Techniques, Deliverables, OWASP Top 10 Attack Testing Guidelines, Reporting- Executive Summary, Risk Exposure over time, Successfully Attacks by whom, Vulnerability causes, Vulnerability report, Remediation report, Report Design Guidelines, Malware Analysis.

PHP Basics: Variables, data types, strings, constants, operators, if else, else if statements, switch, while loops, for loops, functions, arrays, php forms, form handling, validation, form input page with database attachment, XAMPP Server Setup.

Unit II: Web Application and Information Gathering

HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration, fingerprinting frameworks, hidden resource enumeration, security misconfigurations, google hacking database, Shodan HQ.

Unit III: Web Application Attacks Part I: SQL Injections & Cross Site Scripting

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, Advance MY-SQL 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.

Unit IV: Web Application Attacks Part II

Single factor and two factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious request, user enumeration, random password guessing, remember me functionality, no limit attempts, password reset feature, logout flaws, CAPTCHA, insecure direct object reference and security, missing function level access control, unvalidated redirects and forwards, Session ID, LFI and RFI ,Session Attacks via packet sniffing or accessing via web server and Fixation, CSRF (Cross Site Request Forgery), Pentesting Flash -based applications, HTML 5, Cross Origin Resource Sharing Policy, Cross Windows Messaging, Web Storage, Web Sockets, Sandbox, Path Traversal, Arbitrary file uploading, Clickjacking, HTTP Response Splitting, Business Logic Flaws, denial of services attacks.

Practical: This paper will have 30 lectures for the practical work.

Suggested Readings:

1. Shema, M. & Adam. (2010). *Seven deadliest web application attacks*. Amsterdam: Syngress Media.

2. Stuttard, D. & Pinto, M. (2011). *The web application hacker's handbook: Discovering and exploiting security flaws* (2nd ed). Indianapolis, IN: Wiley, John & Sons.

3. Heiderich, M., Nava E.A.V., Heyes, G., & Lindsay, D. (2011). *Web application obfuscation*. Amsterdam: Syngress Media,U.S.

4. Sullivan, Bryan (2012). *Web Application Security, A Beginner's Guide*. McGraw- Hill Education.

Latest research papers from refereed journals discussed by the faculty may also be referred.