

(2). “Computer Forensics and Cyber Crime An Introduction”- Marjie T. Britz, Pearson, Third Edition, 2013

(3). “ Learning Python for Forensics - Leverage the power of Python in forensic investigations”, Preston Miller, Chapin Bryce, Packt Publishing, Second Edition, 2019

(4). “ A Practical Guide to Computer Forensics Investigations”, Dr. Darren R. Hayes, Pearson Education, 2015

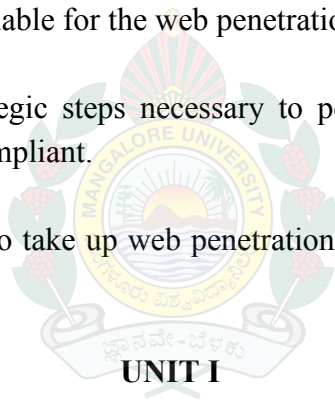
### **CSCH 502 : Web Penetration Testing**

**CO1 :** To assess the vulnerabilities available in a website, with a written consent from the owner of the website.

**CO2:** To master various tools available for the web penetration testing.

**CO3:** To understand all the strategic steps necessary to perform the web penetration testing professionally and to be legally compliant.

**CO4:** To encourage the students to take up web penetration testing as a profession and make a living out of it.



### **UNIT I**

**Introduction to Penetration Testing and Web Applications :** Proactive security testing, Considerations when performing penetration testing, Kali Linux, A web application overview for penetration testers, **Setting Up Your Lab with Kali Linux :** Kali Linux, Important tools in Kali Linux, Vulnerable applications and servers to practice on, **Reconnaissance and Profiling the Web Server :** Reconnaissance, Information gathering, Scanning – probing the target, **Authentication and Session Management Flaws :** Authentication schemes in web applications, Session management mechanisms, Common authentication flaws in web applications, Detecting and exploiting improper session management, Preventing authentication and session attacks

**(16 hours)**

### **UNIT II**

**Detecting and Exploiting Injection-Based Flaws :** Command injection, SQL injection, XML injection, NoSQL injection, Mitigation and prevention of injection vulnerabilities, **Finding and Exploiting Cross-Site Scripting (XSS) Vulnerabilities :** An overview of Cross-Site Scripting,

Exploiting Cross-Site Scripting, Scanning for XSS flaws, Preventing and mitigating Cross-Site Scripting, **Cross-Site Request Forgery, Identification, and Exploitation** : Testing for CSRF flaws, Exploiting a CSRF flaw, Preventing CSRF, **Attacking Flaws in Cryptographic Implementations** : A cryptography primer, Secure communication over SSL/TLS, Identifying weak implementations of SSL/TLS, Custom encryption protocols, Common flaws in sensitive data storage and transmission, Preventing flaws in cryptographic implementations

(16 hours)

### UNIT III

**AJAX, HTML5, and Client-Side Attacks** : Crawling AJAX applications, Analyzing the client-side code and storage, HTML5 for penetration testers, Bypassing client-side controls, Mitigating AJAX, HTML5, and client-side vulnerabilities, **Other Common Security Flaws in Web Applications** : Insecure direct object references, File inclusion vulnerabilities, HTTP parameter pollution, Information disclosure, Mitigation, **Using Automated Scanners on Web Applications** : Considerations before using an automated scanner, Web application vulnerability scanners in Kali Linux, Content Management Systems scanners, Fuzzing web applications, Post-scanning actions

(16 hours)

#### Text Books :

- (1). “Web Penetration Testing with Kali Linux”, Gilberto Najera-Gutierrez, Juned Ahmed Ansari, Packt Publishing, Third Edition, 2018
- (2). “Kali Linux Revealed”, Mastering the Penetration Testing Distribution, Raphaël Hertzog, Offsec Press, 2017
- (3). “ Learn Kali Linux 2019”, Glen D. Singh, Packt Publishing, 2019
- (4). “ Quick Start Guide to Penetration Testing”, Sagar Rahalkar, Apress, 2019

### CSCH 503: Cybersecurity with Blockchain

**CO1** : To understand the new form of disruptive technology which is coming up in the world wide economy, as a way to assure data security.

**CO2:** To offer an alternative form of DNS servers, based on blockchain with better security aspects.