Web Application Penetration Testing

SevenMentor PVT.LTD

www.sevenmentor.com

1. Introduction

- Pre-engagement
- Methodologies
- Reporting

2. Introduction to Web Applications

- HTTP/S Protocol Basics
- Encoding
- Same Origin
- Cookies
- Sessions
- Web Application Proxies by using BURP SUIT AND OWASP ZAP

3.Information Gathering

- Gathering information on your target
- Infrastructure
- Fingerprinting frameworks and applications
- Fingerprinting custom applications
- Enumerating resources
- Relevant information through
- misconfigurations

- Google hacking
- Shodan HQ

4. Cross-Site Scripting

- Cross-Site Scripting
- Anatomy of an XSS Exploitation
- The three types of XSS
- Finding XSS
- XSS Exploitation
- Mitigation

5. SQL Injection

- Introduction to SQL Injections SQLi
- Finding SQL Injections
- Exploiting Error-based SQL Injections
- Exploiting blind SQLi
- Finding SQL through Tools
- Mitigation Strategies

6. Authentication and Authorization

- Introduction
- Common Vulnerabilities
- Bypassing Authorization

7. Session Security & CSRF

- Weaknesses of the session identifier
- Session hijacking
- Session Fixation
- Cross-Site Request Forgeries

8. Remote code execution

- Introduction
- Remote code Attack
- Mitigation Strategies

9. HTML5

- Cross-Windows Messaging
- Web Storage
- WebSocket
- Sandboxed frames

10. File and Resource Attacks

- File Inclusion Vulnerabilities
- Unrestricted File Upload

11. Other Attacks

- Command Injection
- Price Manipulation
- OTP BYPASSING
- Denial of Services

12. Web Services

- Introduction
- Web Services
- The WSDL Language
- Attacks

13. XPath Injection

- Xpath & XPath expression and syntax
- Detecting XPath
- Best Defensive Techniques

14.Penetration Testing Content Management Systems

- Introduction
- WordPress

- Joomla
- Brute Force Attack Through WP

15. Penetration Testing NoSQL Databases

- Introduction
- NoSQL Fundamentals & Security
- NoSQL Exploitation