Web Penetration

Lecture and Demonstration: 10 Days
Daily Classes **:** 02 Hours

1. Introduction of Web Basics

- Introduction of Web Applications
- Client & Server Relation
- Server & Database Working
- How to configure a Server
- Setup a Lab for testing

2. Introduction to Backend

- What is Backend
- How it Works
- How to take Input from users
- How to send values to Server
- How to work with Database
- How to make a Web Application

3. Injections

- Simple SQL Injection
- Blind SQL Injection
- Advanced SQL Injection
- Shell Injection

4. Broken Authentication

- Brute Forcing
- Dictionary Based Attacks
- Session Hijacking
- Cookie Stealing

5. Sensitive Data Exposure

- ARP Poisoning
- LFI (Local File Inclusion)
- RFI (Remote File Inclusion)

6. XML External Entities

- Introduction to XML
- Testing Vulnerability
- Exploiting XML External Entities
- Counter Measures

7. Broken Access Control

- Checking for Privilege Escalation
- Parameter Tampering
- Exploitation
- Privilege Expansion
- Counter Measures

8. Cross Site Scripting

- Reflected XSS
- Stored XSS
- DOM XSS
- Exploitation
- Preventions

9. Burp Suite

- Burp Suite Configuration
- Manual Mapping
- Spidering a Website
- Active & Passive Scan
- Intruder
- Repeater

10. Penetration Testing

- Black Box Testing
- White Box Testing
- Automated Penetration Testing