Burpsuite for Web Application

Duration: 40 hrs

Module Overview

Module	Name
Module 1	**Introduction & Initial Setup**
Module 2	**Scoping & Mapping in Burpsuite**
Module 3	**Interception and Request Manipulation**
Module 4	**Manual Attacks**
Module 5	**Manual Request Crafting**
Module 6	**Collaborator – External Service Interaction**
Module 7	**Token Analysis**
Module 8	**Decoder – Encode/Decode/Hash Playground**
Module 09	**Enhanced Visibility**
Module 10	**Extensions – Supercharging Burp**

Detailed Syllabus – Module Wise

- **Module 1: Introduction & Initial Setup**
  - What is Burp Suite?
  - Burp Suite Community vs Pro
  - Installing Burp CE and setting up test labs
  - Installing CA certificate in browsers
  - Setting up PortSwigger Labs, DVWA, bWAPP
  - Overview of dashboard layout
  - Managing background tasks
  - Configuring project options
  - Limitations in CE: No active/passive scanner
  - Real-world workflow: Monitor activities, manage recon progress

- **Module 2: Scoping & Mapping in Burpsuite**
  - Site Map breakdown: URLs, methods, params, status codes
  - Setting scope (Include / Exclude)
  - Using tree view vs table view
  - Passive recon and endpoint discovery
  - Right-click tricks: Send to Repeater/Intruder, Copy as curl
  - Real-world use: Building your attack surface map

- **Module 3: Interception and Request Manipulation**
  - Setting up browser with Burp Proxy
  - Intercepting requests and modifying in real time
  - HTTP History tab (filtering, searching, analyzing)
  - WebSockets messages (basic monitoring)
  - Proxy Options: Match and Replace, Invisible proxying
  - Analyzing login flows, token capture, custom header testing

- **Module 4: Manual Attacks**
  - **Positions tab: § markers and placement**
  - **Attack types: Sniper, Battering Ram**
  - **Payloads tab: Lists, payload processing**
  - **Payload markers for brute-force logins**
  - **Using Turbo Intruder (extn)**
  - **Username enumeration, password brute-forcing, fuzzing headers**

- **Module 5: Manual Request Crafting**
  - **Sending intercepted requests to Repeater**
  - **Understanding request/response panel**
  - **Header modification, cookie tampering**
  - **Manual XSS, SQLi, SSRF testing**
  - **Adding new tabs for organizing attacks**
  - **Custom payload injection and testing bypasses**

- **Module 6: Collaborator – External Service Interaction**
  - **What is OAST (Out-of-Band App Security Testing)**
  - **dnslog.cn, interact.sh with Collaborater**
  - **Testing SSRF, blind XSS, XXE, log4j-style attacks**

- **Module 7: Token Analysis**
  - **Capturing tokens**
  - **Entropy analysis basics**
  - **Manual interpretation of results**
  - **Checking session predictability and token strength**

- **Module 8: Decoder – Encode/Decode/Hash Playground**
  - **URL, Base64, HTML, Hex encodings**
  - **MD5, SHA1 hashing**

- **Decoding JWT manually (vs using jwt.io)**
- **Contextual payload creation for XSS, SQLi**
- **Real-world use: Decode input/output and generate precise payloads**
- **Word-level and byte-level diff**
- **Comparing login success vs fail responses**
- **Analyzing application behaviour changes**

◆ **Module 09: Enhanced Visibility**

- **Installing Logger++ (from BApp Store)**
- **Viewing real-time traffic logs**
- **Searching, filtering, tagging, exporting**
- **Track every request without relying on HTTP history only**
- **What is Organizer in burp**
- **Manual workarounds in CE:**
    - **Naming Repeater tabs**
    - **Keeping notes externally or via extensions**
- **Manage big web apps, categorize findings**

◆ **Module 10: Extensions – Supercharging Burp**

Must-have Free Extensions for CE:

- **Logger++ – Enhanced logging**
- **Turbo Intruder – Fast bruteforcing**
- **Hackvertor – Encode, obfuscate payloads**
- **JSBeautifier – Readable JS**
- **Param Miner – Discover hidden parameters**
- **Autorize – IDOR and privilege testing**

PS: Burp suite Community Edition will be used in this course.