# Module 14: Hacking Web Applications - Practical Guide

This guide focuses on the technical tools and step-by-step procedures used to identify and exploit logic-based vulnerabilities in web applications, primarily focusing on the OWASP Top 10.

## 1. Comprehensive Web App Toolset

### Intercepting Proxies (The Essential Tools)

* **Burp Suite:** The industry standard. It acts as a Man-in-the-Middle between your browser and the server.
  + *Proxy Tab:* Intercepts and modifies requests.
  + *Repeater:* Resends individual requests to test server responses.
  + *Intruder:* Automates attacks like brute-forcing or fuzzing.
* **OWASP ZAP (Zed Attack Proxy):** A powerful, free, and open-source alternative to Burp Suite. It includes an automated scanner and a "HUD" mode for real-time browser interaction.

### Enumeration & Discovery

* **Gobuster:** A fast tool used to brute-force URIs (directories and files) and DNS subdomains.
* **Dirsearch:** A Python-based command-line tool designed to brute-force directories and files in webservers.
* **Wappalyzer:** A browser extension that identifies technologies used on websites (CMS, Frameworks, JavaScript libraries).

### Vulnerability & Exploitation Frameworks

* **SQLmap:** The go-to tool for automating the detection and exploitation of SQL injection flaws.
* **BeEF (Browser Exploitation Framework):** Focuses on the "Hooked" browser. It allows an attacker to control a victim's browser once they visit a malicious link.
* **Metasploit:** Contains numerous modules for exploiting web application vulnerabilities and managing web shells.

## 2. Hands-On Lab Sessions

### Lab 1: Intercepting and Manipulating Traffic (Burp Suite)

**Goal:** Manipulate a hidden form parameter (Parameter Tampering) to change a product price.

1. **Launch Burp:** Open Burp Suite and ensure the **Intercept** is ON in the Proxy tab.
2. **Configure Browser:** Set your browser's proxy settings to 127.0.0.1:8080.
3. **Perform Action:** On a lab site (like DVWA), add an item to a cart.
4. **Modify Request:** In Burp, locate the price=100 parameter. Change the value to price=0.01.
5. **Forward:** Click **Forward**.
6. **Verify:** Check the web application to see if the item was added with the modified price.

### Lab 2: Exploiting Reflected XSS

**Goal:** Execute a JavaScript payload that steals a user's session cookie.

1. **Identify Entry Point:** Find a search box or URL parameter that reflects user input back onto the page.
2. Craft Payload: ```html  
   <script>alert(document.cookie);