**Web Application Vulnerability Detection with OWASP ZAP**

**Introduction**

In this project, students will learn the basics of web application vulnerability detection using OWASP ZAP (Zed Attack Proxy), a popular open-source tool for finding security vulnerabilities in web applications. By the end of this project, students will be able to set up OWASP ZAP, perform basic vulnerability scans, and analyse scan results.

**Pre-requisites**

* Basic understanding of web applications and HTTP protocols
* Familiarity with Linux or Windows command line
* A computer with a Linux or Windows operating system

**Lab Set-up and Tools**

* OWASP ZAP installed (instructions provided in the first task)
* A target web application for scanning (can be a locally hosted application or a deliberately vulnerable web application like DVWA)

**Exercises**

**Exercise 1: Installing OWASP ZAP**

**Steps:**

1. Download OWASP ZAP from the official site.
2. Install OWASP ZAP:
   * On Windows: Run the downloaded installer and follow the installation instructions.

**Expected Output:**

* OWASP ZAP is installed and running. You should see the ZAP GUI interface.

**Exercise 2: Configuring OWASP ZAP**

**Steps:**

1. Launch OWASP ZAP.
2. Configure ZAP to use the browser's proxy settings:
   * Open the browser and navigate to the proxy settings.
   * Set the proxy server to localhost and the port to 8080.
3. In ZAP, confirm that the proxy is active by checking the "Local Proxy" settings under the "Tools" menu.

**Expected Output:**

* OWASP ZAP is configured as a proxy for the browser, allowing it to intercept and analyse web traffic.

**Exercise 3: Performing a Passive Scan**

**Steps:**

1. In OWASP ZAP, navigate to the "Sites" tab.
2. Open a browser and navigate to the target web application with ZAP running as the proxy.
3. Browse through the web application to capture the traffic.
4. In ZAP, observe the requests and responses captured under the "Sites" tab.

**Expected Output:**

* OWASP ZAP captures and displays the HTTP requests and responses, identifying potential vulnerabilities passively.

**Exercise 4: Performing an Active Scan**

**Steps:**

1. In the OWASP ZAP interface, right-click on the target site under the "Sites" tab.
2. Select "Attack" and then "Active Scan".
3. Configure the scan settings and start the scan.
4. Monitor the progress of the active scan in the "Active Scan" tab.

**Expected Output:**

* OWASP ZAP performs an active scan on the target web application, identifying potential vulnerabilities through active testing.

**Exercise 5: Reviewing and Analysing Scan Results**

**Steps:**

1. Once the active scan is complete, navigate to the "Alerts" tab in OWASP ZAP.
2. Review the list of identified vulnerabilities, categorized by severity.
3. Click on each vulnerability to view detailed information, including the description, risk level, and suggested remediation steps.
4. Generate a scan report by navigating to "Report" > "Generate Report" and selecting the desired format (e.g., HTML, XML).

**Expected Output:**

* A detailed report of the scan results, highlighting vulnerabilities, their severity, and recommended remediation actions.