OWASP ZAP - Lab

Lab - Use the OWASP Web Security Testing Guide

- The ***Open Worldwide Application Security Project*** (***OWASP***) nonprofit foundation developed the ***Web Security Testing Guide*** (***WSTG***) to test the most common web application security issues
    - The guide is useful for various stakeholders such as developers, software testers, security specialists, and project managers
    - The OWASP Web Security Testing Guide is a free tool that is available to organizations and individuals
    - The testing guide is also a useful tool for ethical hacking. Ethical hackers can use the guide to test their clients' running web applications for common security vulnerabilities
    - In this lab, you will review the WSTG and then scan a web application for vulnerabilities using the ***OWASP Zed Attack Proxy*** (***ZAP***)
        - You will investigate some of the vulnerabilities that were discovered and reference one back to the WSTG
- Part 1: Investigate the WSTG
    - Step 1: Explore the OWASP WSTG Project Site
        - Navigate to the OWSAP Web Security Testing Guide site at https://owasp.org/www-project-web-security-testing-guide/
        - Review the information on the main page
        - Click the Release Versions tab
        - Click the most recent released version and review the Table of Contents
    - Step 2: Review the content
        - Click and review the Foreword by Eoin Keary in the Table of Contents
        - Return to the Table of Contents and select Introduction

        - Return to the Table of Contents and select OWASP Testing Framework
        - Return to the Table of Contents and select Web Application Security Testing
        - Return to the Table of Contents and select Reporting
    -
- Part 2: Scan a Website and Investigate Vulnerability References
    - Step 1: Open ZAP and start a scanning
        - Start the Kali VM as needed. Navigate to the Kali menu. Search for zap and start the OWASP Zap scanner
        - Click the topmost radio button to persist the session. This means that you can return to the session at a later time
        - Close the Manage Add-ons dialog window
        - In the ZAP main window, click the Automated Scan to initiate a scan
        - In the URL to Attack field, enter **172.17.0.2/dvwa**
        - Click the Attack button to begin the scan
            - The scan will should take less than 10 minutes to complete
        - First, ZAP uses a web spider to crawl the URL to identify the resources that are available there. It then will apply vulnerability scans to each resource
    - Step 2: Investigate the results
        - Select the **Alerts** tab if it is not already selected
            - When the scan finishes, you will be automatically switched to there
        - Locate and click the **Remote Code Execution** – **CVE-2012-1823** alert
            - Scroll through the details of the alert
        - Scroll down to the **Alert Tags** section of the vulnerability
            - Note the WSTG key and value
            - Click the **value** and use the **Ctrl-C** keys to copy the URL to the clipboard

- Open a browser and paste the URL
    - Navigate to the WSTG site and read about the vulnerability and methods of testing for it
    - Review this information about the vulnerability to understand what WSTG offers to the penetration tester