OWASP

Web Security Testing Guide

Deborah Binyanya | binyanyadebby@gmail.com

Lab - Use the OWASP Web Security Testing Guide

Objectives

In this lab, you will complete the following objectives:

- Part 1: Investigate the WSTG
- Part 2: Scan a Website and Investigate Vulnerability References

Background / Scenario

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.

Required Resources

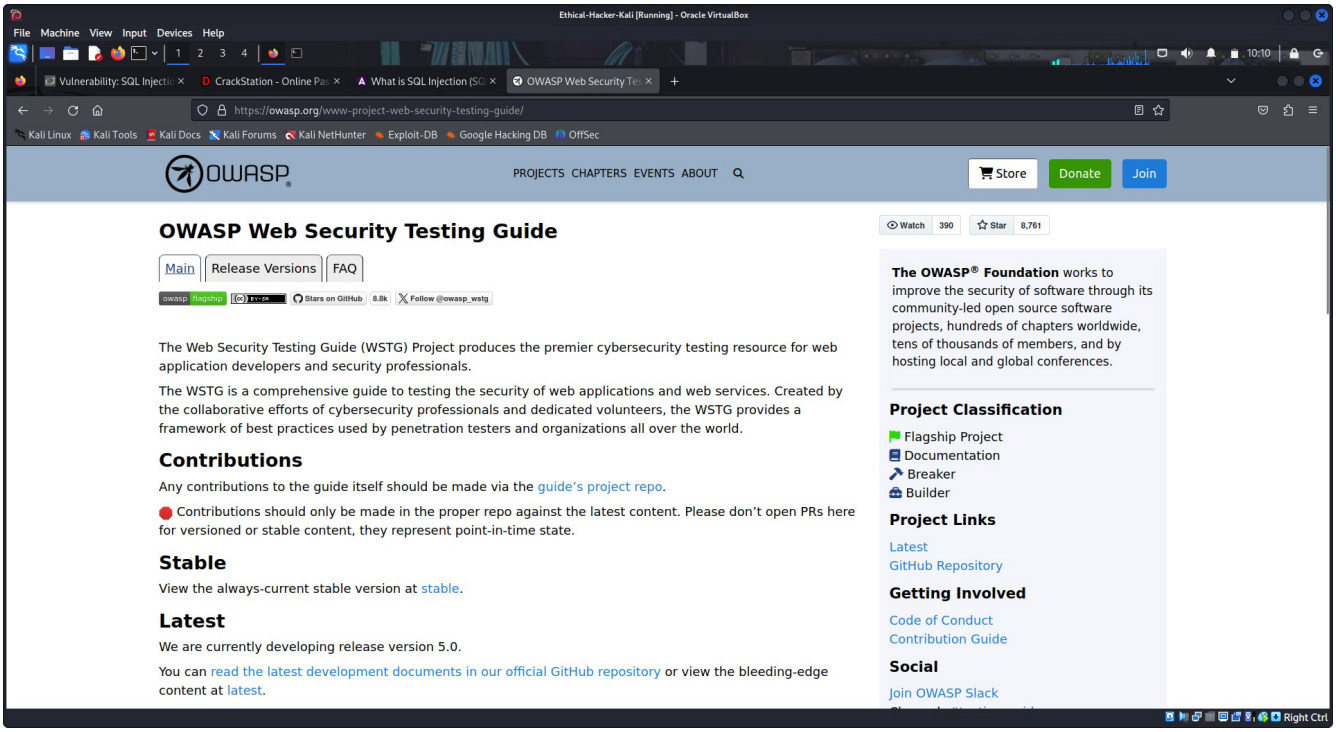
- Kali VM customized for the Ethical Hacker course
- Internet access

Instructions

Part 1: Investigate the WSTG

Step 1: Explore the OWASP WSTG Project Site.

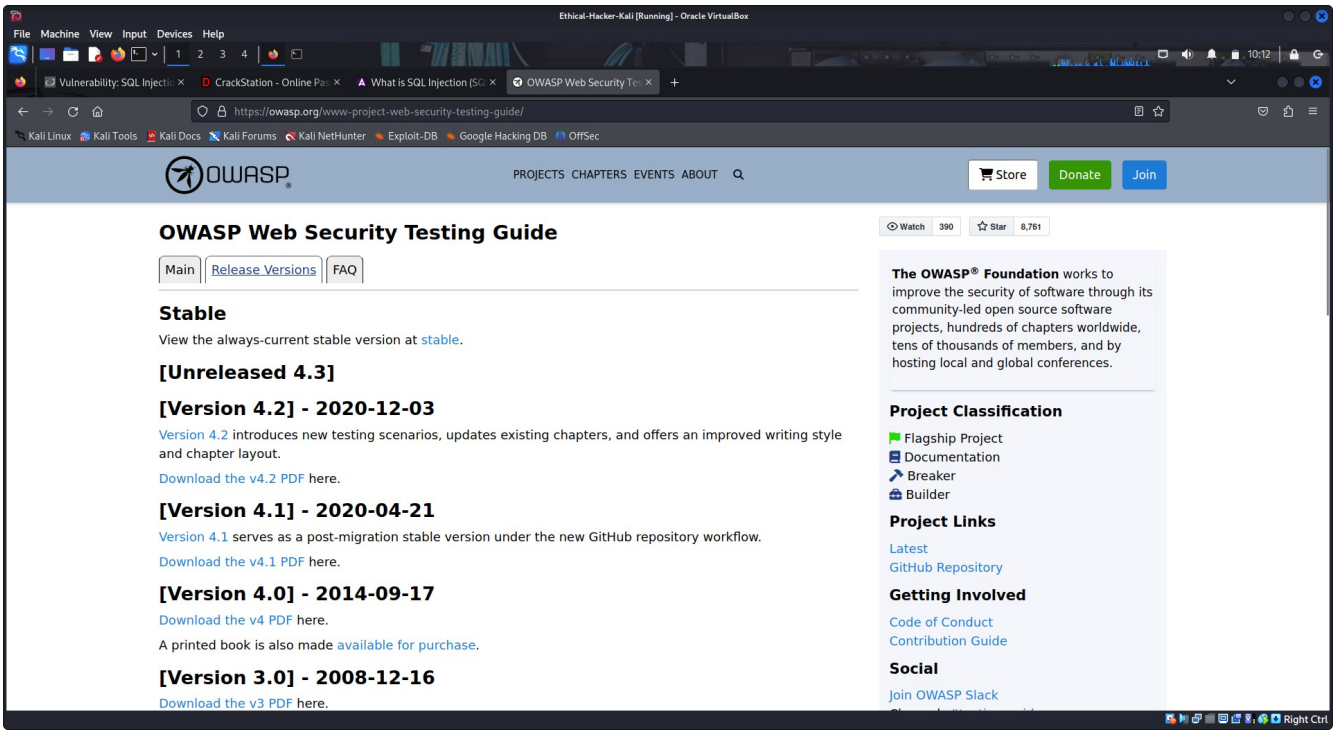
a. Navigate to the OWSAP Web Security Testing Guide site at https://owasp.org/www-project-web-security-testing-guide/.
b. Review the information on the main page.



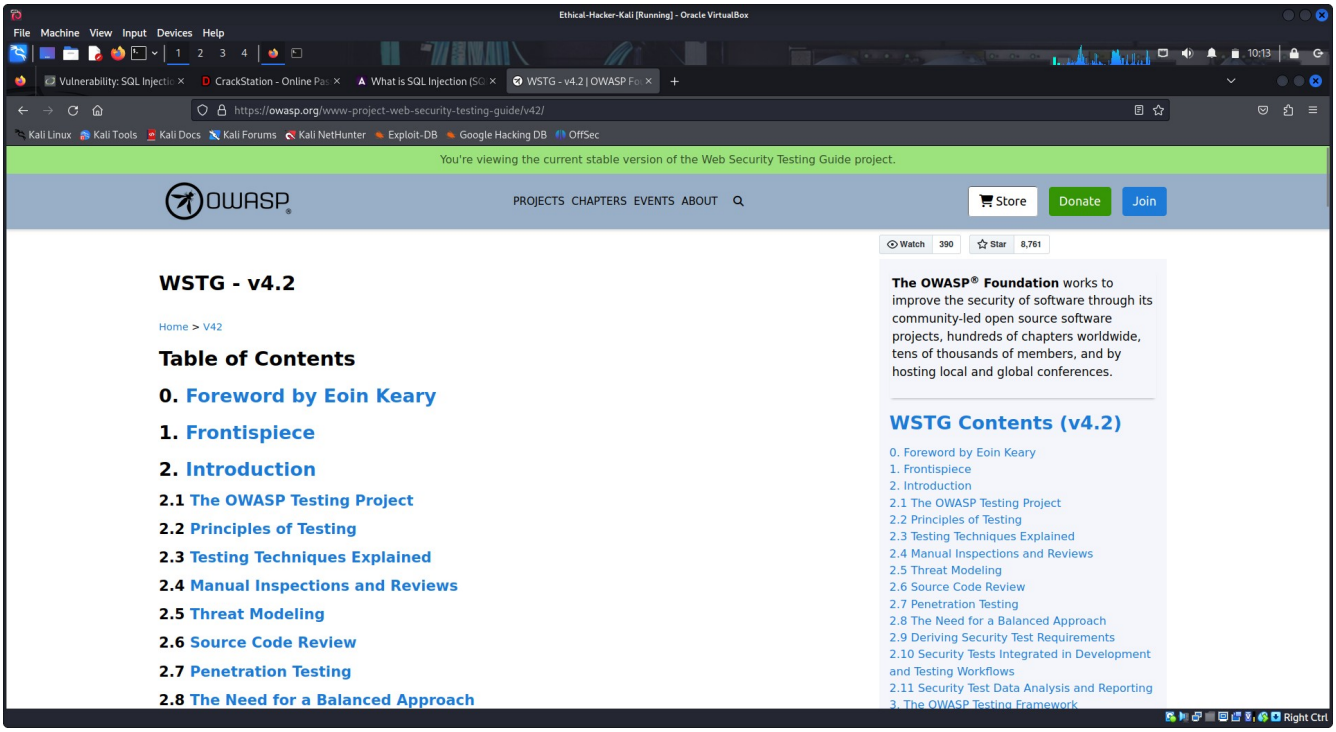
What is the purpose of the OSWASP Web Security Testing Guide?

It is designed to guide the testing of security of web applications. It describes techniques, methods, tools, and resources for testing for the most common web application security issues. It provides a framework of best practices.

Click the **Release Versions** tab. What is the current release version of the guide? **Version 4.2**

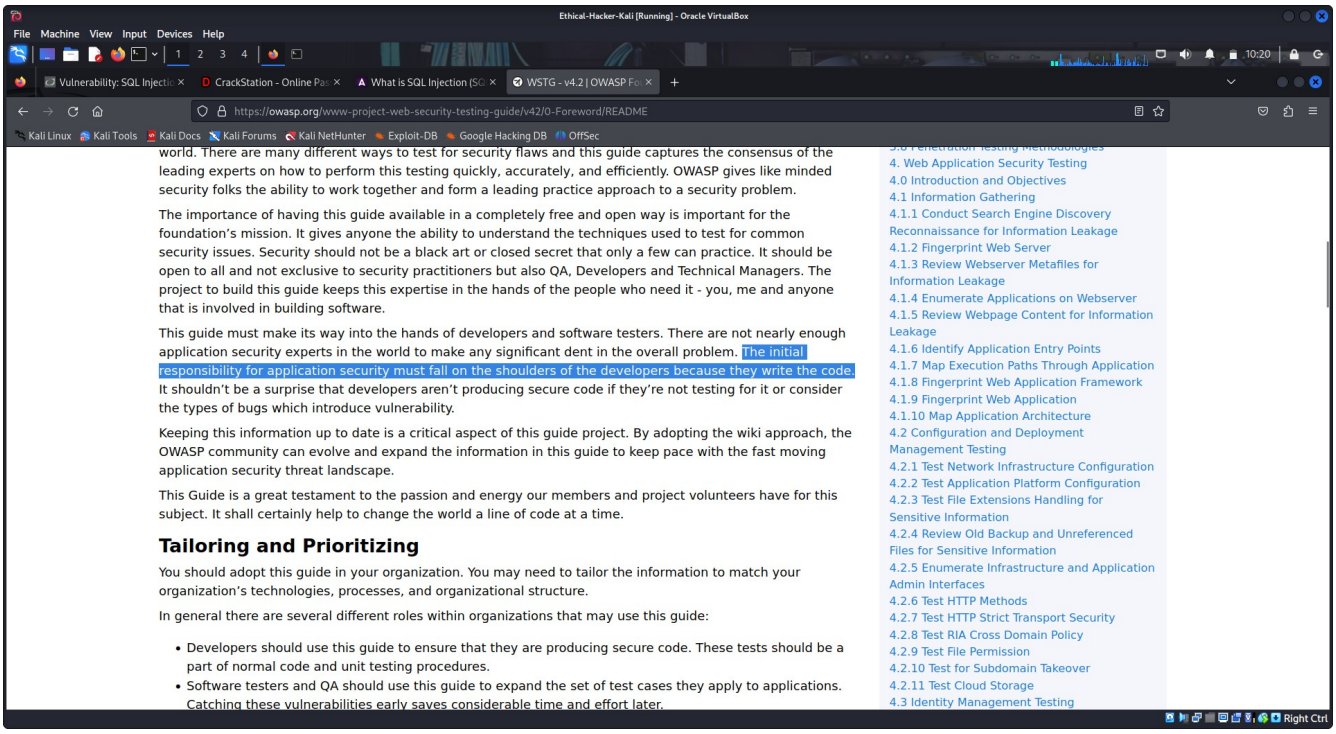


Click the most recent released version and review the Table of Contents.



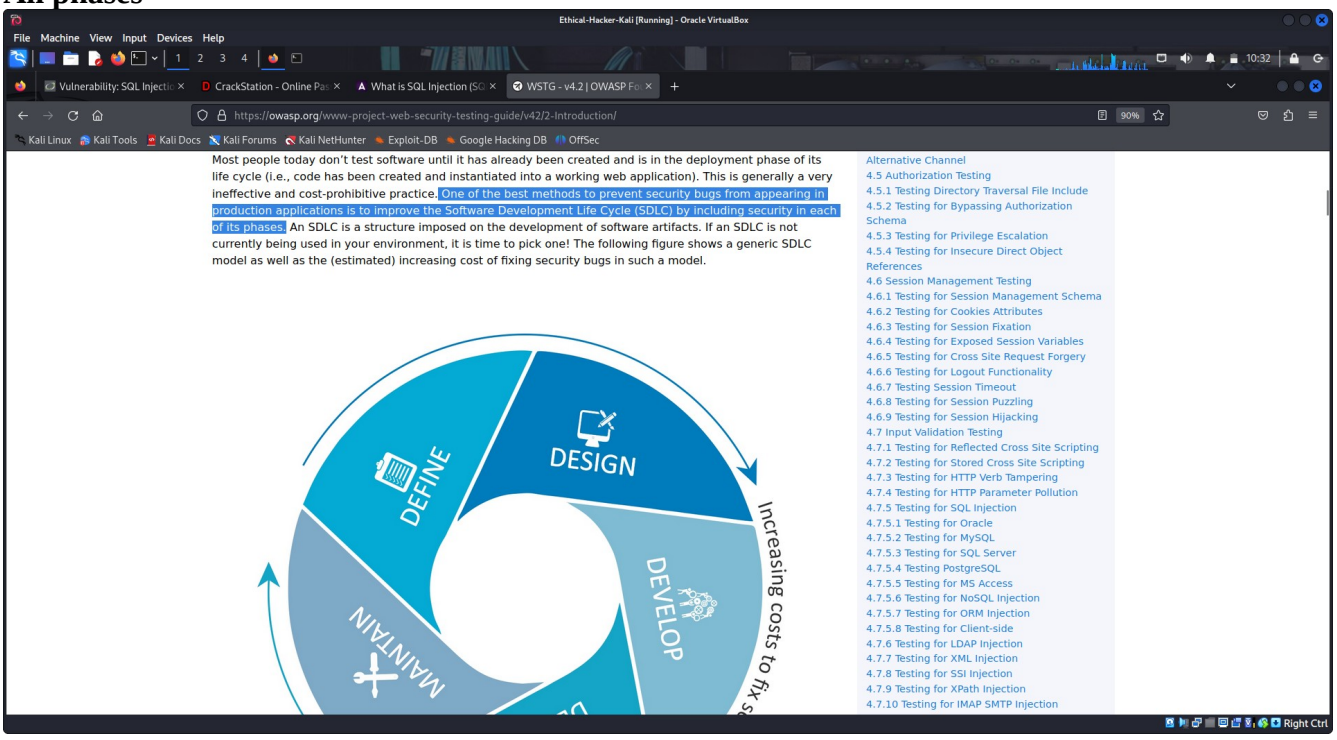
Step 2: Review the content.

Click and review the **Foreword** by Eoin Keary in the Table of Contents. According to Mr. Keary, who is initially responsibility for application security? **developers**

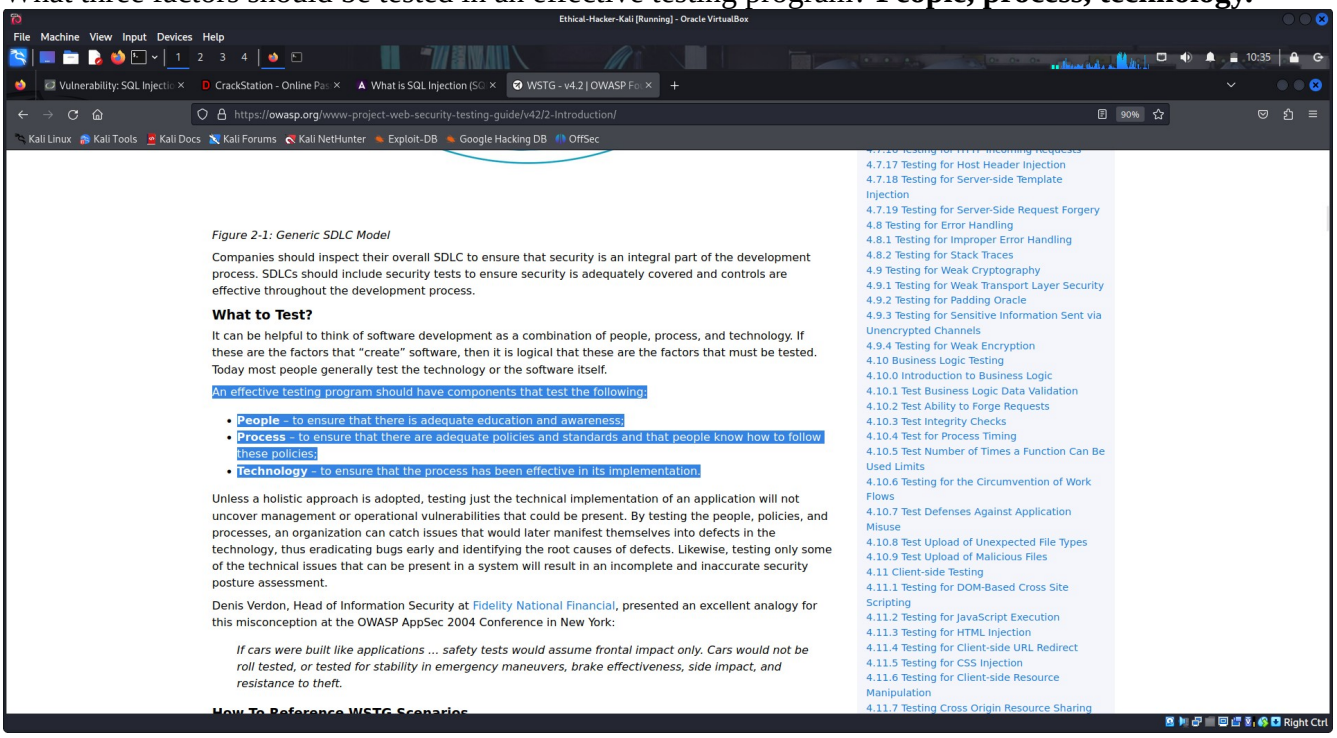


Return to the **Table of Contents** and select **Introduction**.

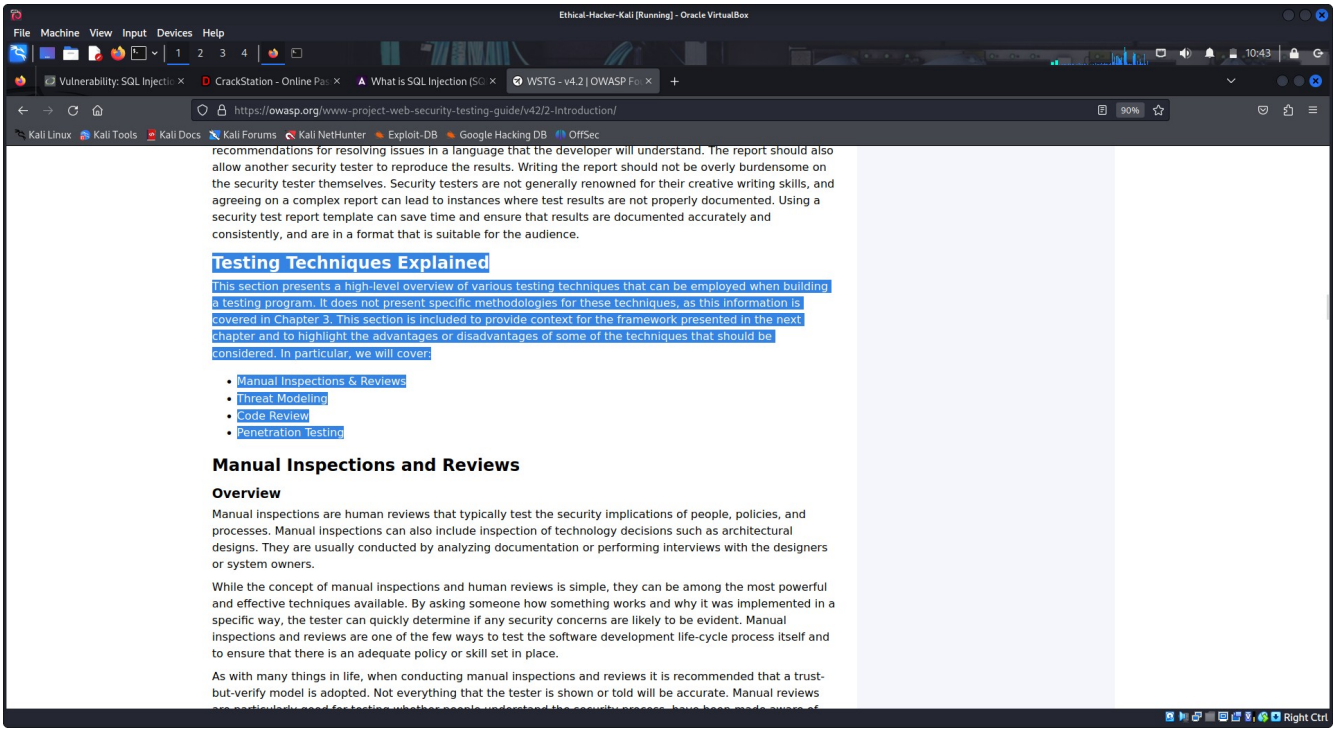
Security testing should be included in which phase(s) of the Software Development Lifecycle (SDLC)?
All phases



What three factors should be tested in an effective testing program? **People, process, technology.**

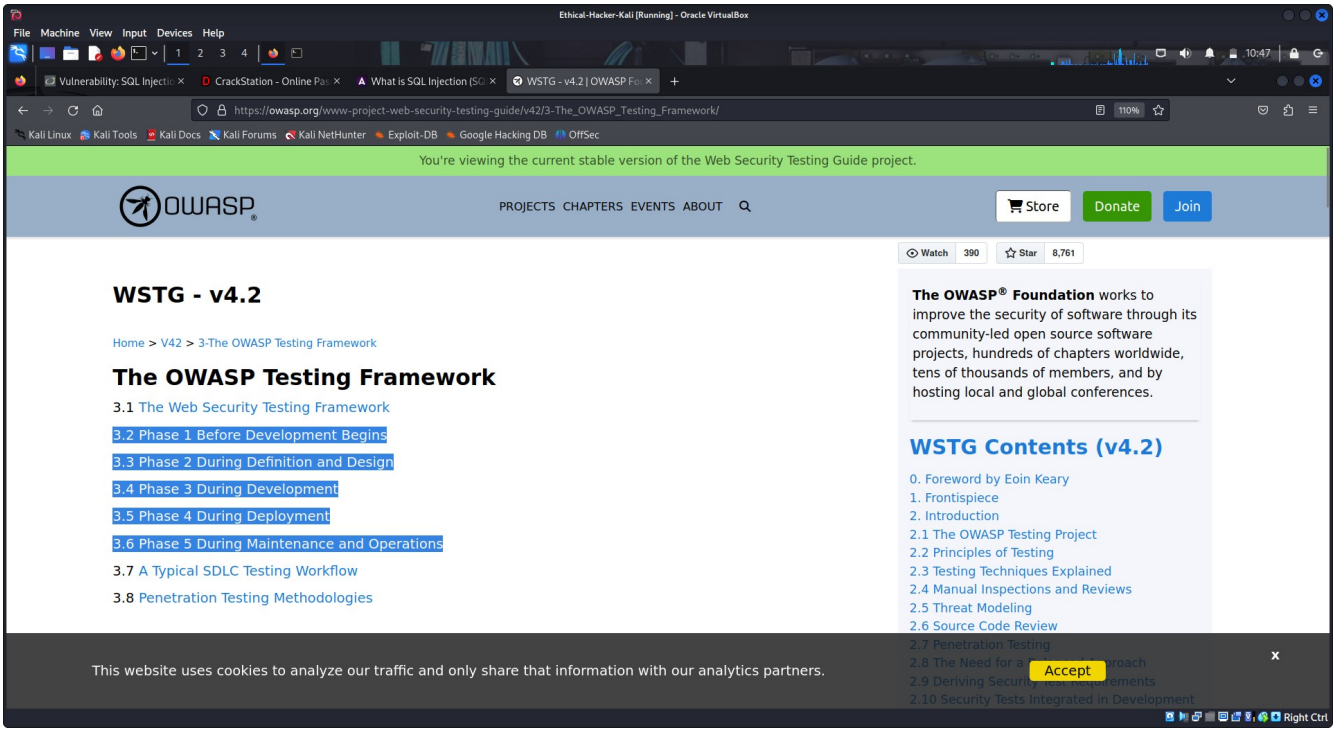


What four testing techniques are presented in the introduction of the OWASP Web Testing Guide? Complete the table with the techniques and their definitions. Define the techniques in your own words.

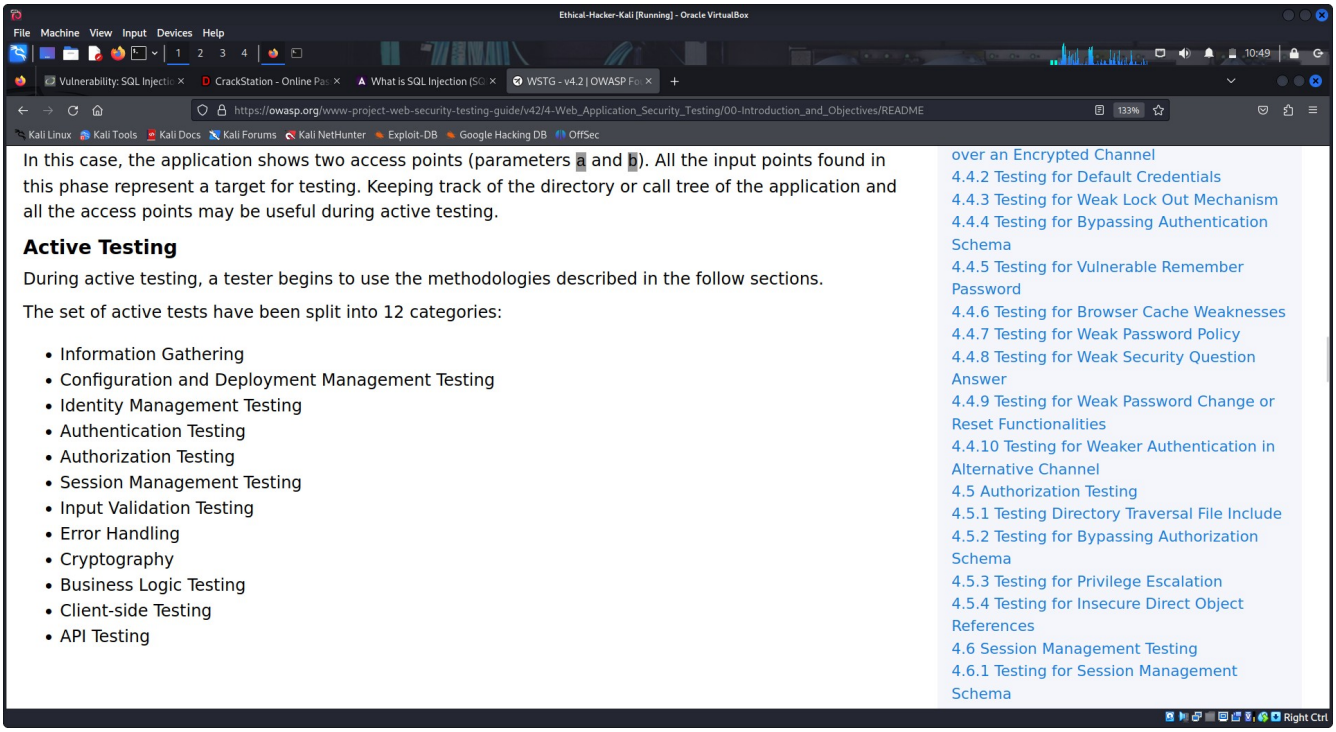


Techniques	**Definition**
Manual Inspections & Reviews	This involves people manually checking systems, designs, configurations, or processes to identify security weaknesses, mistakes, or policy violations without using automated tools.
Threat Modeling	Threat modeling is the process of identifying possible security threats, understanding how an attacker might exploit a system, and determining how to prevent or reduce those risks.
Code Review	Code review is the practice of examining source code to find security flaws, bugs, or poor coding practices that could be exploited by attackers.
Penetration Testing	Penetration testing is a controlled attempt to exploit vulnerabilities in a system to evaluate how secure it is and to understand the potential impact of real-world attacks.

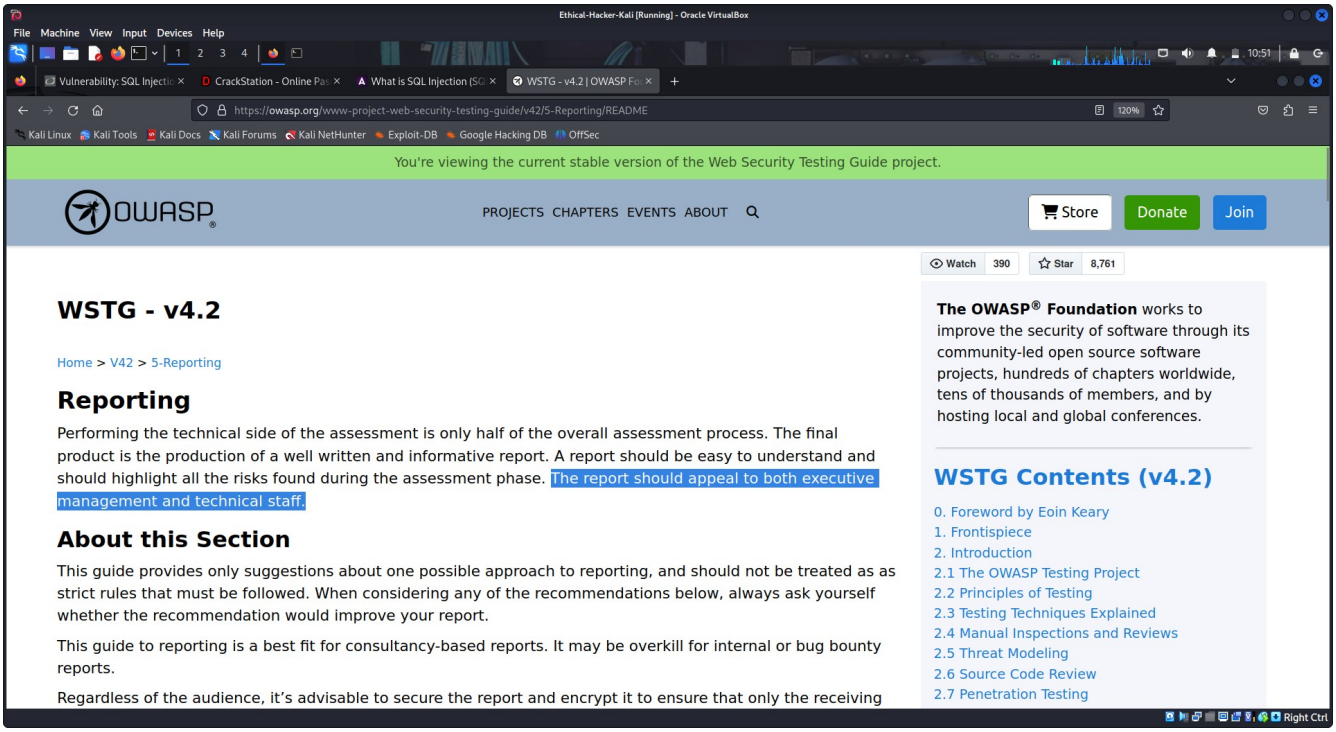
Return to the **Table of Contents** and select **OWASP Testing Framework**. According to the framework, what are the phases in which testing activities should take place?



Return to the **Table of Contents** and select **Web Application Security Testing**. What are the 11 categories of active testing described in the guide?



Return to the **Table of Contents** and select **Reporting**. The final report should be targeted to what two groups of stakeholders?

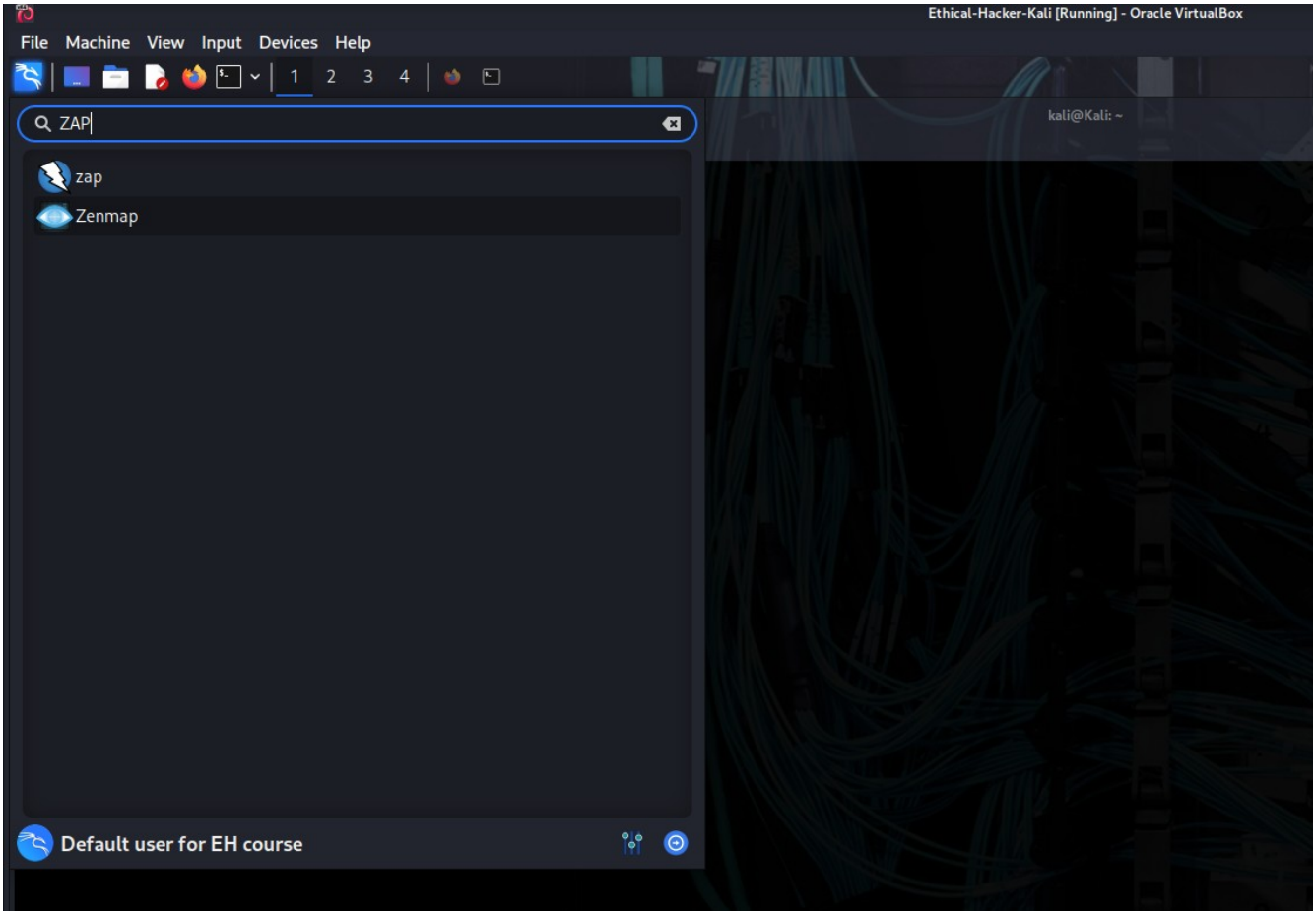


Part 2: Scan a Website and Investigate Vulnerability References

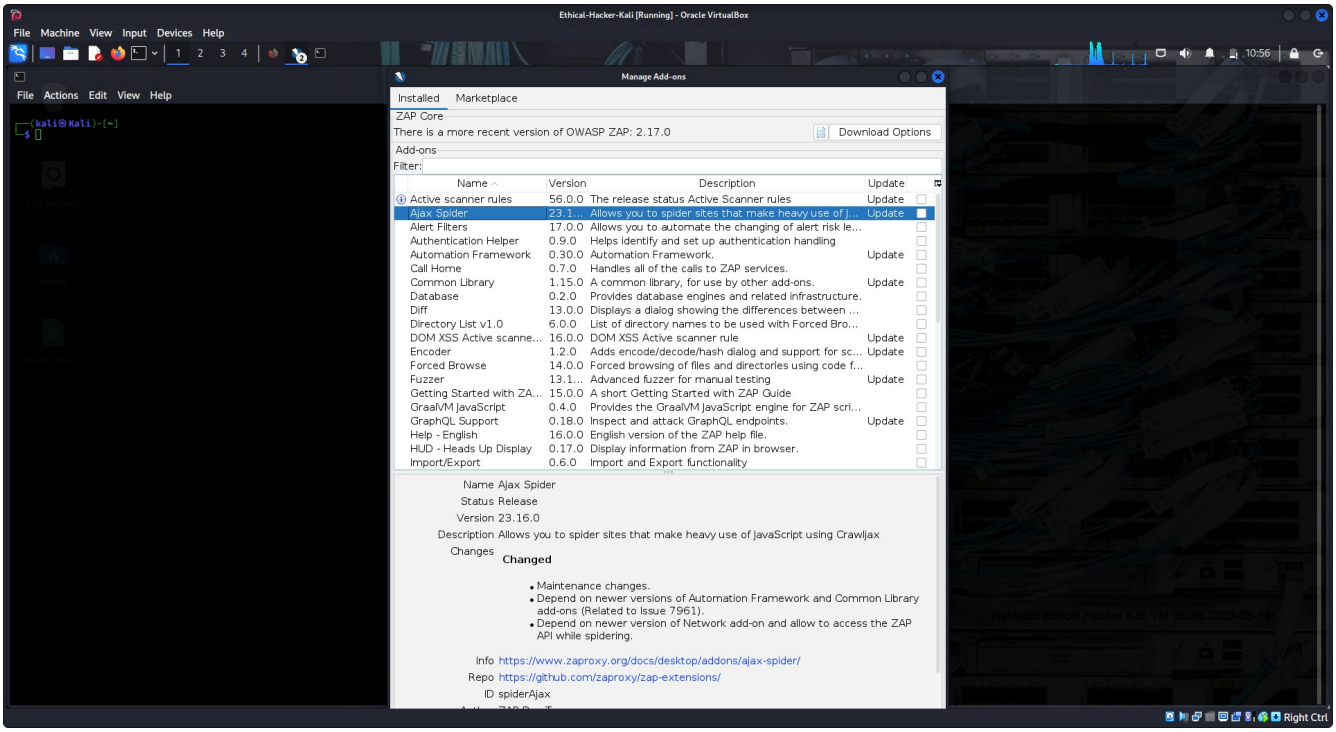
In this part of the lab, you will conduct a vulnerability scan using the Zed Attack Proxy (ZAP). Your target is an intentionally vulnerable website that is available on your VM. You will then use WSTG to learn more about a vulnerability that you discovered.

Step 1: Open ZAP and start a scanning.

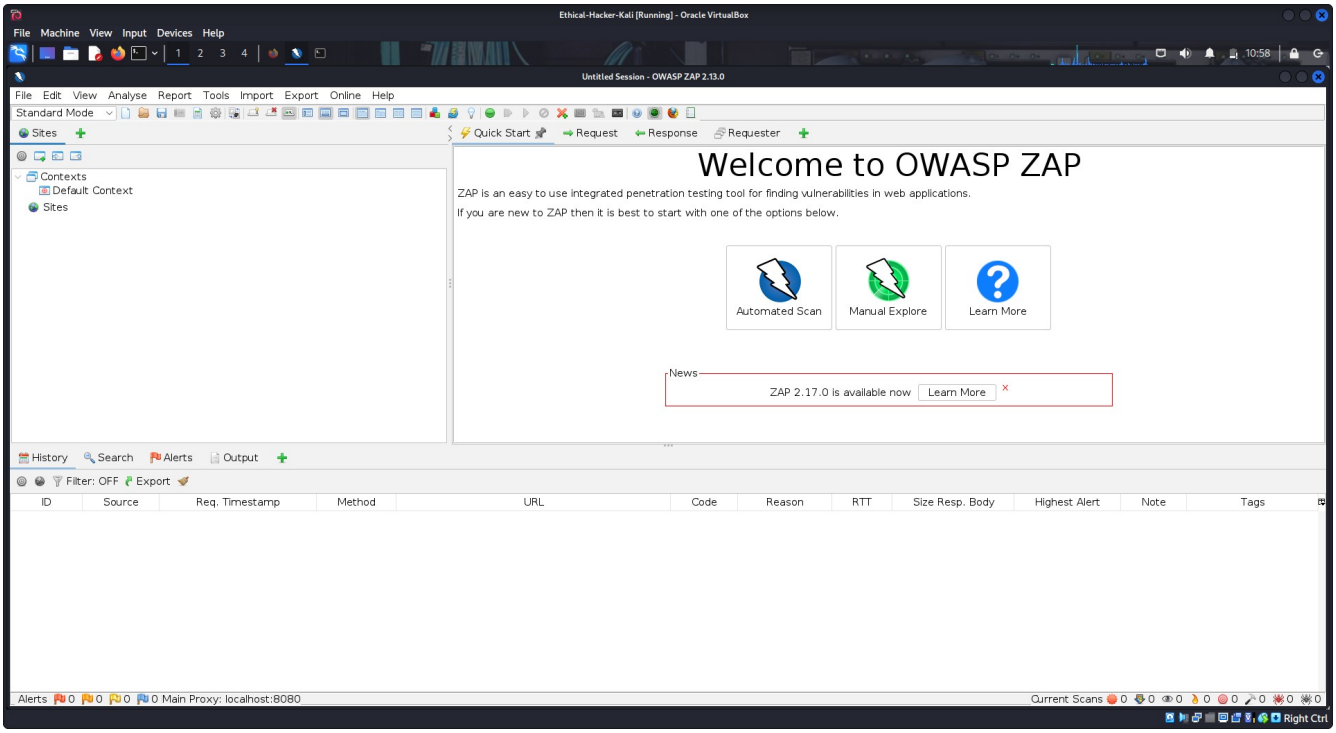
a. Start the Kali VM as needed. Navigate to the Kali menu. Search for **zap** and start the OWASP Zap scanner.



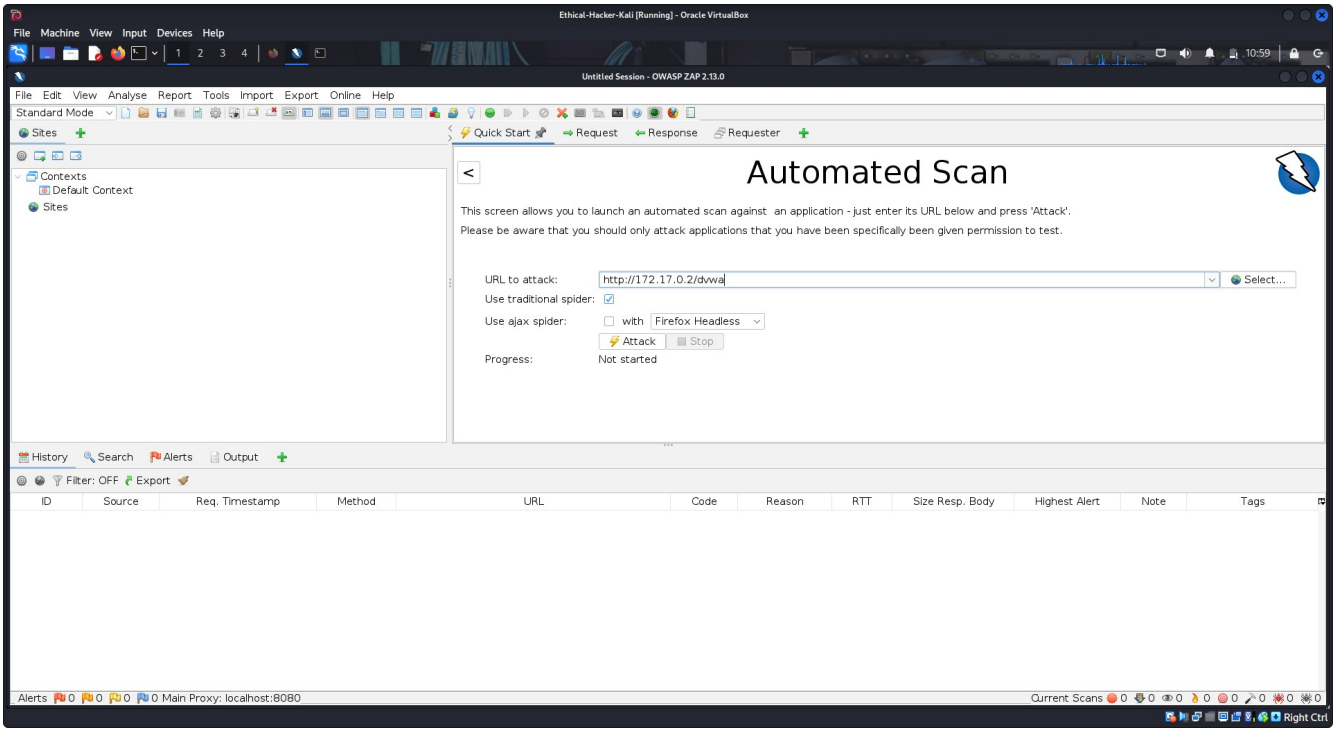
b. Click the topmost radio button to persist the session. This means that you can return to the session at a later time.
c. Close the Manage Add-ons dialog window.



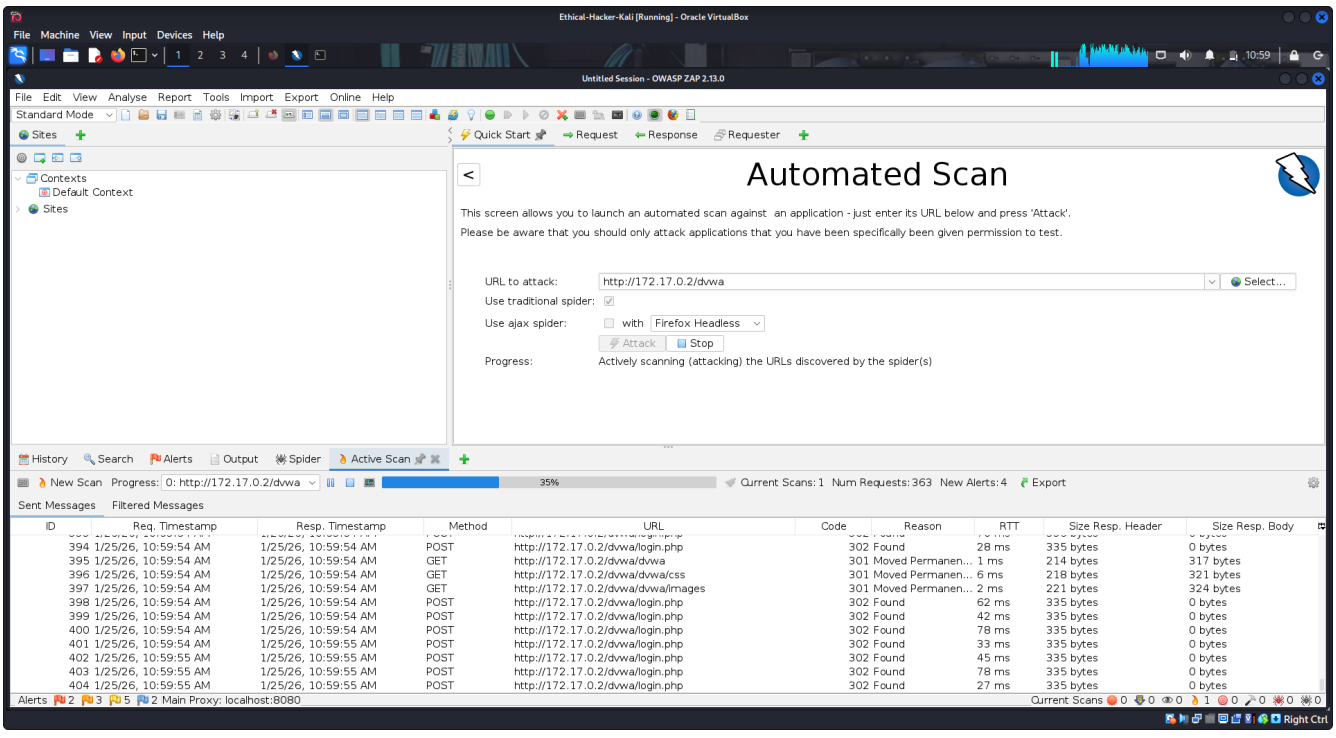
d. In the ZAP main window, click the **Automated Scan** to initiate a scan.



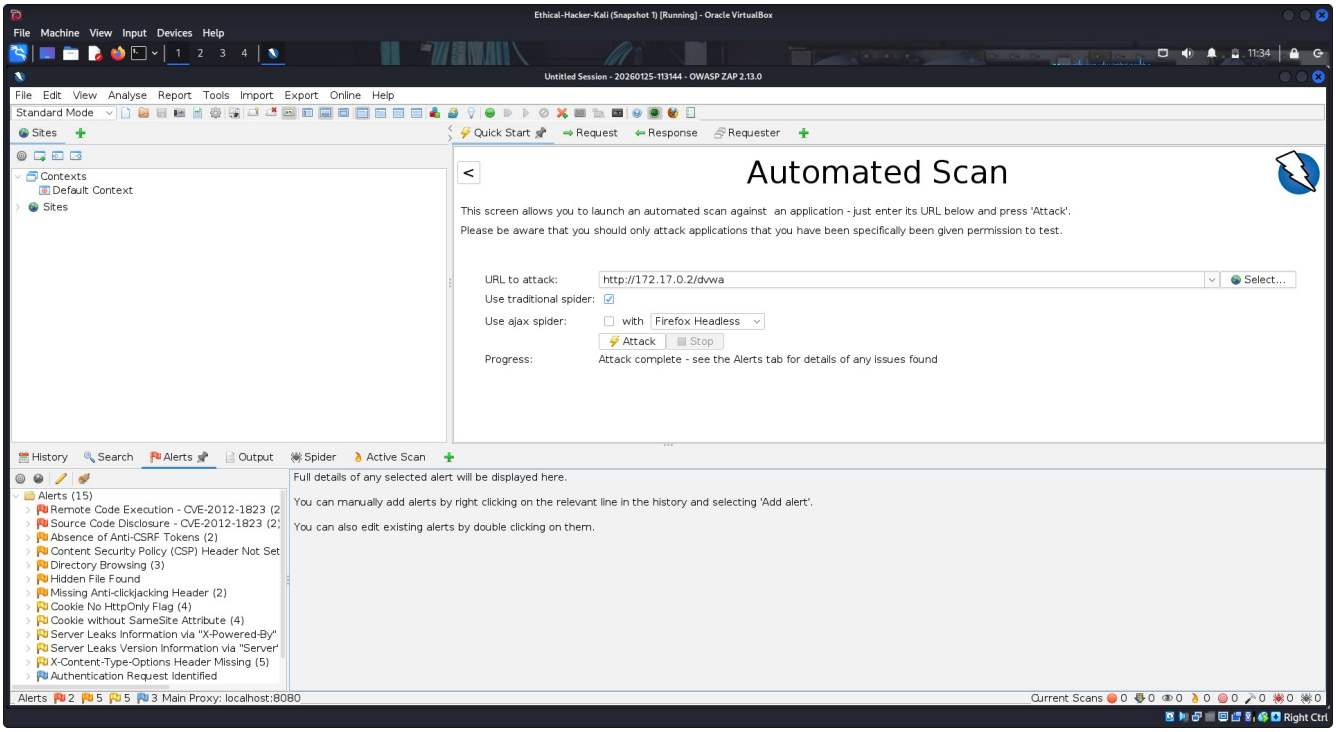
e. In the **URL to Attack** field, enter **172.17.0.2/dvwa**.
f. Click the **Attack** button to begin the scan. The scan should take less than 10 minutes to complete.



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.



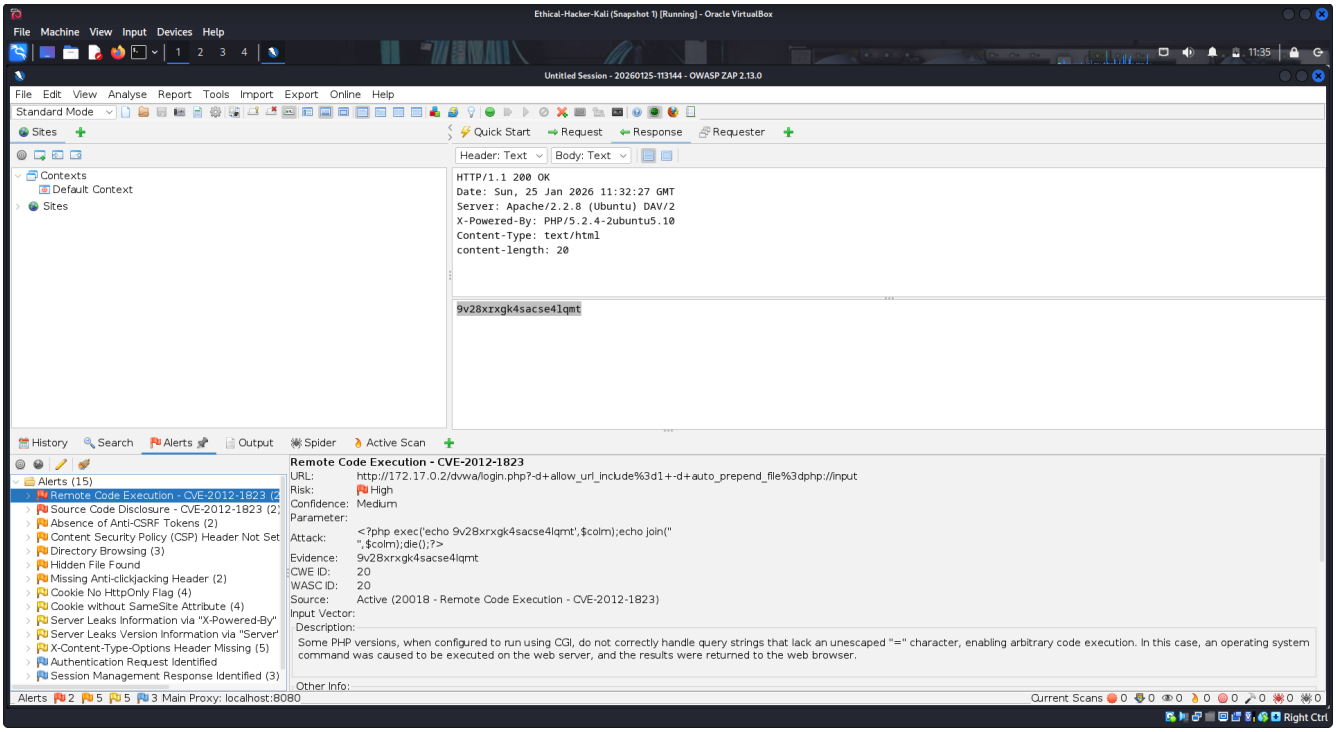
Complete scan:



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. How many alerts were returned? **15**

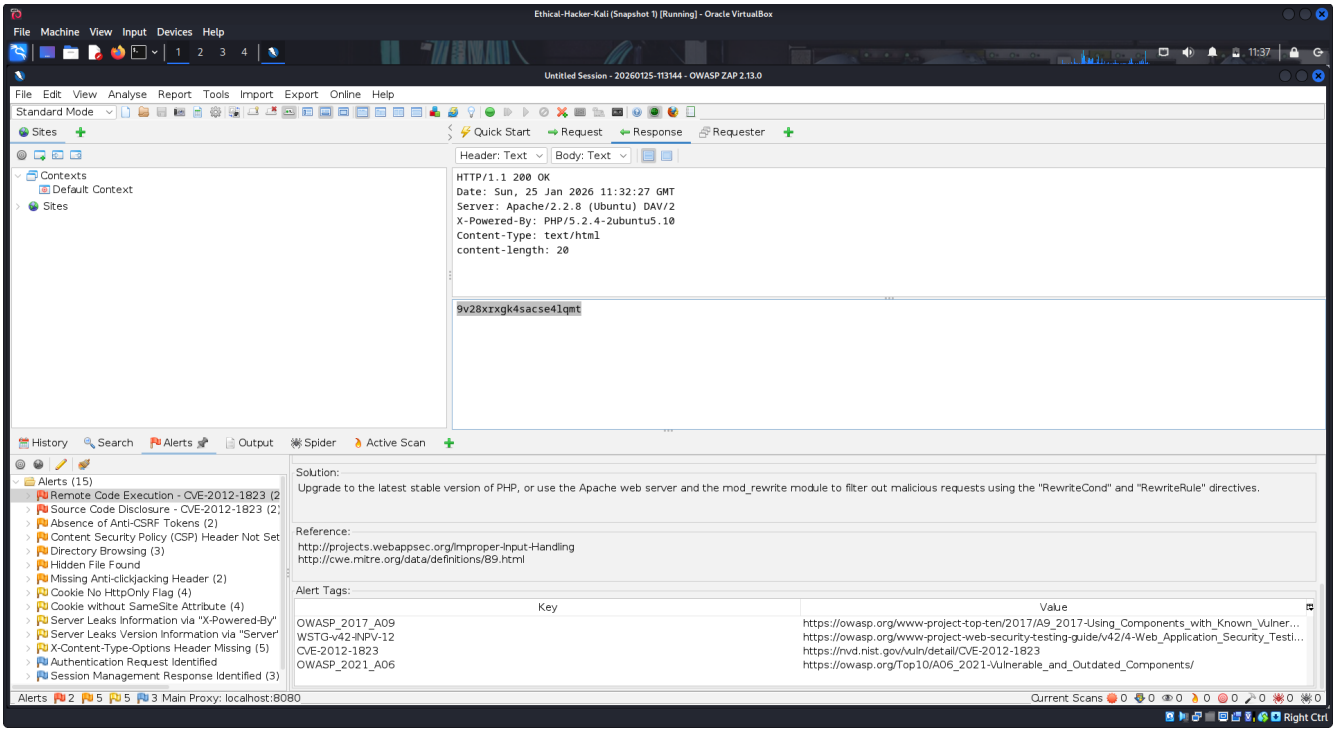
Locate and click the **Remote Code Execution – CVE-2012-1823** alert. Scroll through the details of the alert.



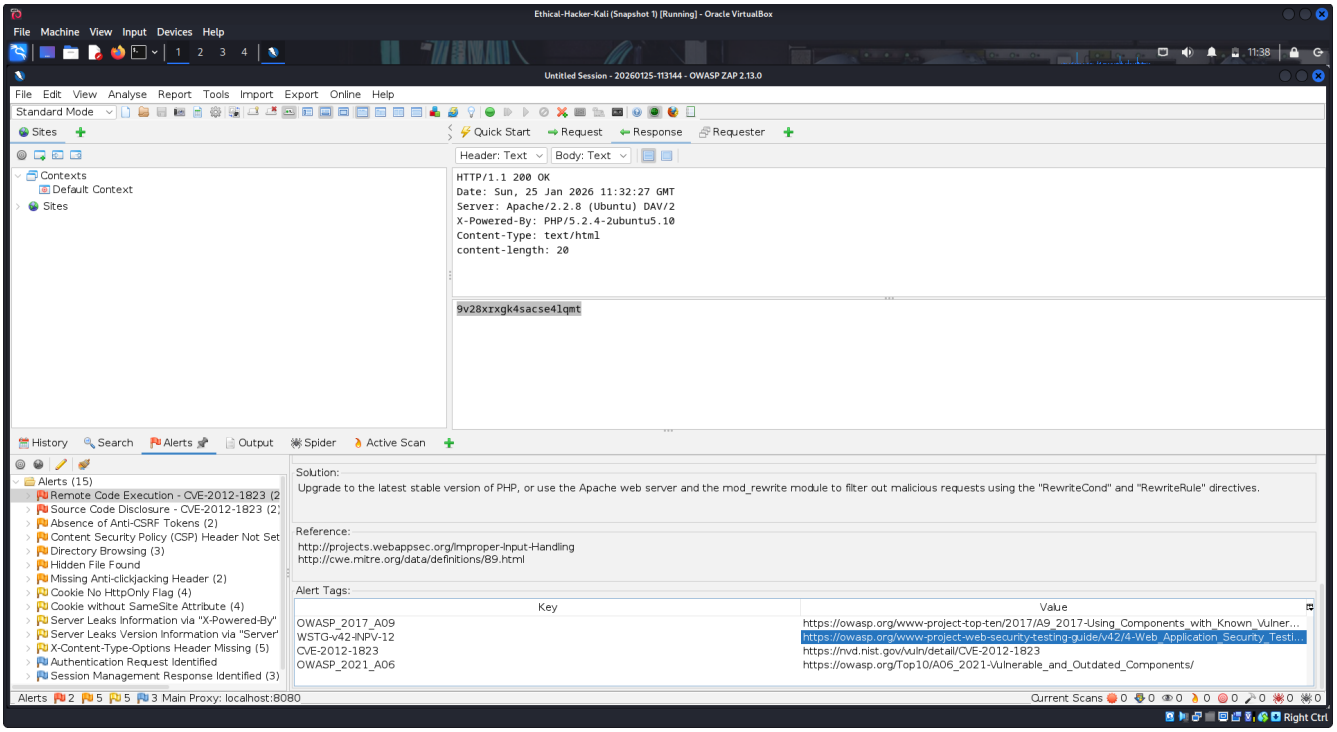
What is the source of this vulnerability? **Active (20018 - Remote Code Execution - CVE-2012-1823)**

How can this vulnerability be exploited? **Some PHP versions, when configured to run using CGI, do not correctly handle query strings that lack an unescaped "=" character, enabling arbitrary code execution. In this case, an operating system command was caused to be executed on the web server, and the results were returned to the web browser.**

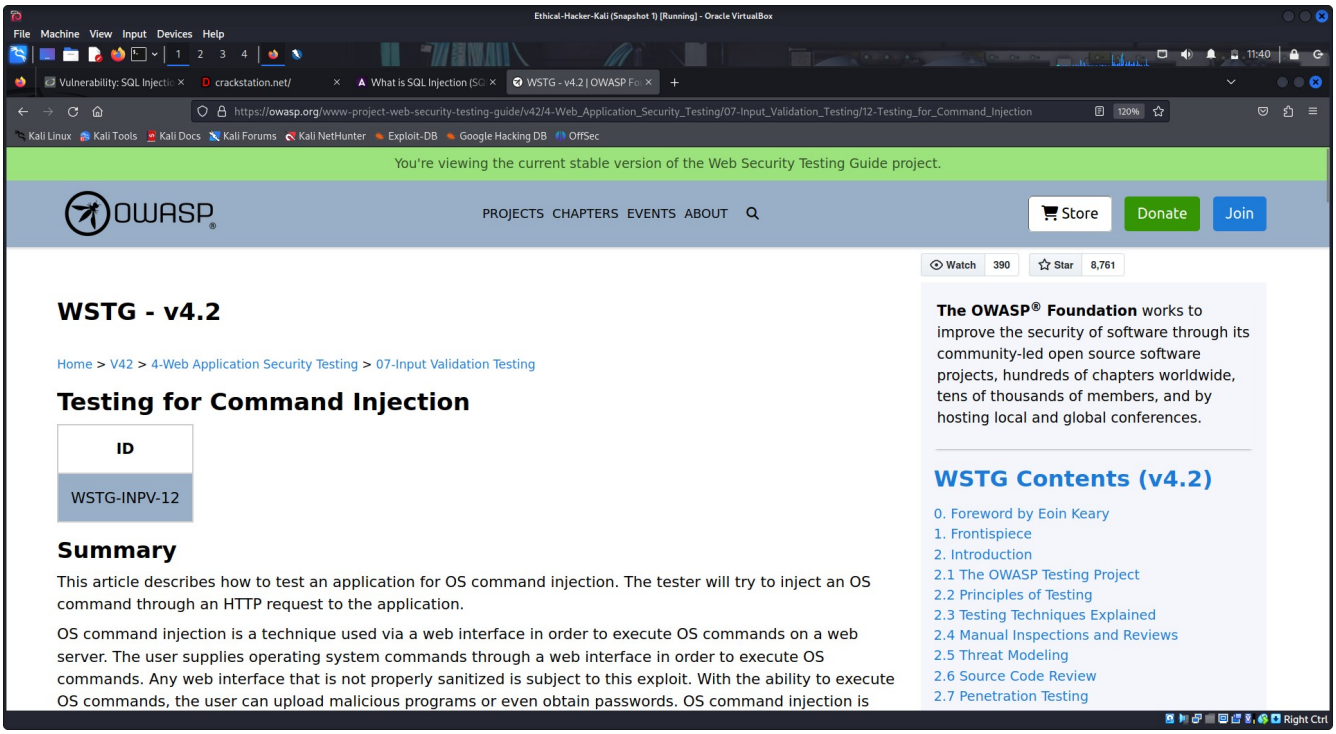
Scroll down to the **Alert Tags** section of the vulnerability. Note the WSTG key and value.



Click the value and use the Ctrl-C keys to copy the URL to the clipboard.



- Open a browser and paste the URL in 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.



In what ways can the OWASP Web Security Testing Guide assist organizations to secure their applications?

Provides a Standardized Security Testing Framework

Enables Early Identification of Vulnerabilities

Supports Risk-Based Security Assessments

Improves Developer and Tester Security Skills

Facilitates Compliance and Audit Readiness

Enhances Communication Between Technical Teams

Supports Both Manual and Automated Testing

Encourages Continuous Security Improvement

When conducting a penetration test of a client's web applications, how could you use the WSTG as a guide? **When conducting a penetration test, the OWASP Web Security Testing Guide (WSTG) can be used as a checklist and roadmap to ensure all key areas of a web application are tested. It helps the tester plan the scope, follow a structured testing approach, perform relevant test cases and report findings using standardized terminology. This ensures the penetration test is thorough, consistent, and aligned with industry best practices.**