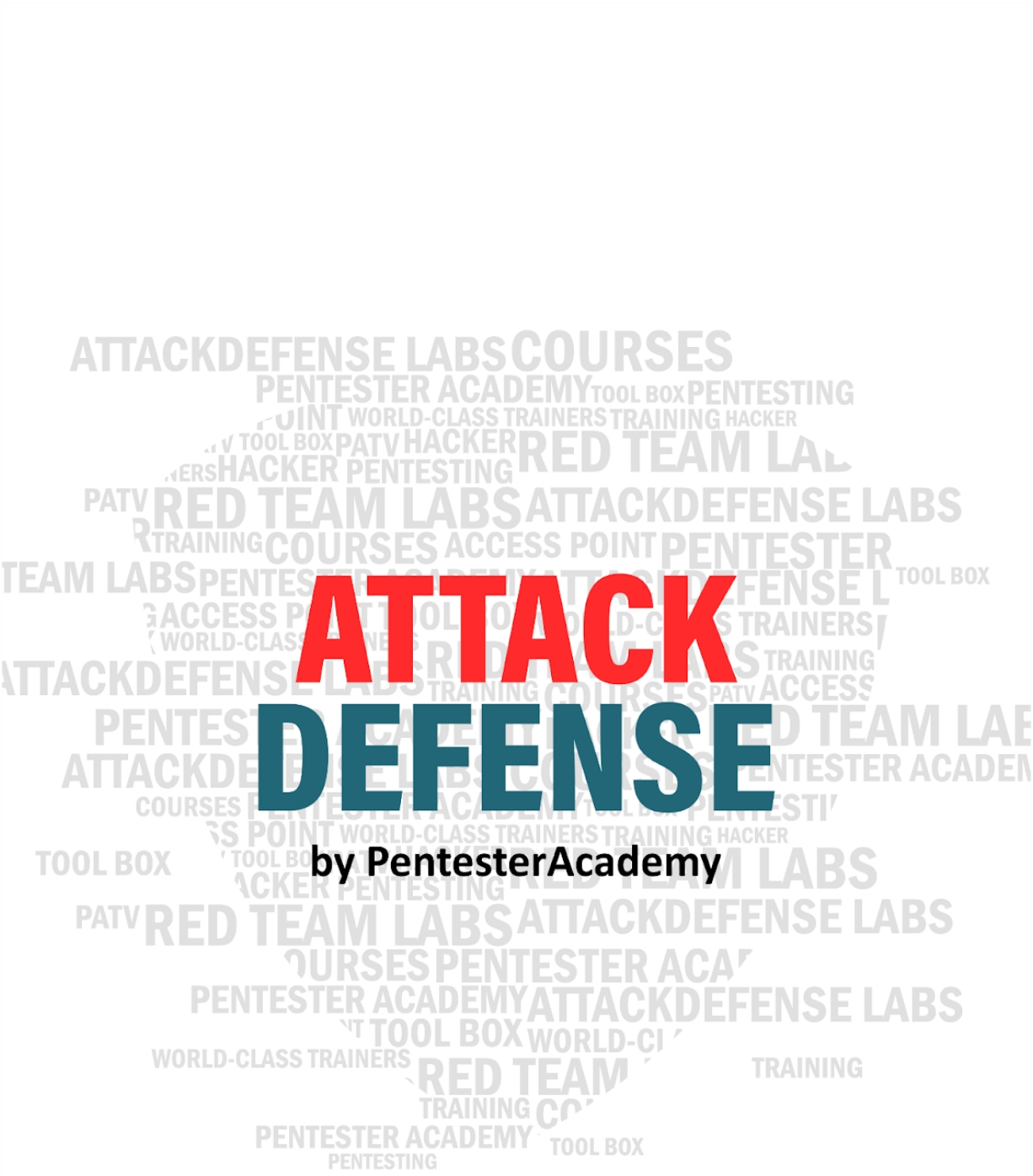

ATTACK
DEFENSE
by PentesterAcademy

Name	OWASP ZAP: Detecting Vulnerabilities in WebApps
URL	https://www.attackdefense.com/challengedetails?cid=2055
Type	DevSecOps Basics: Dynamic Code Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Challenge Description

OWASP ZAP is an open-source framework for performing dynamic analysis on web applications.

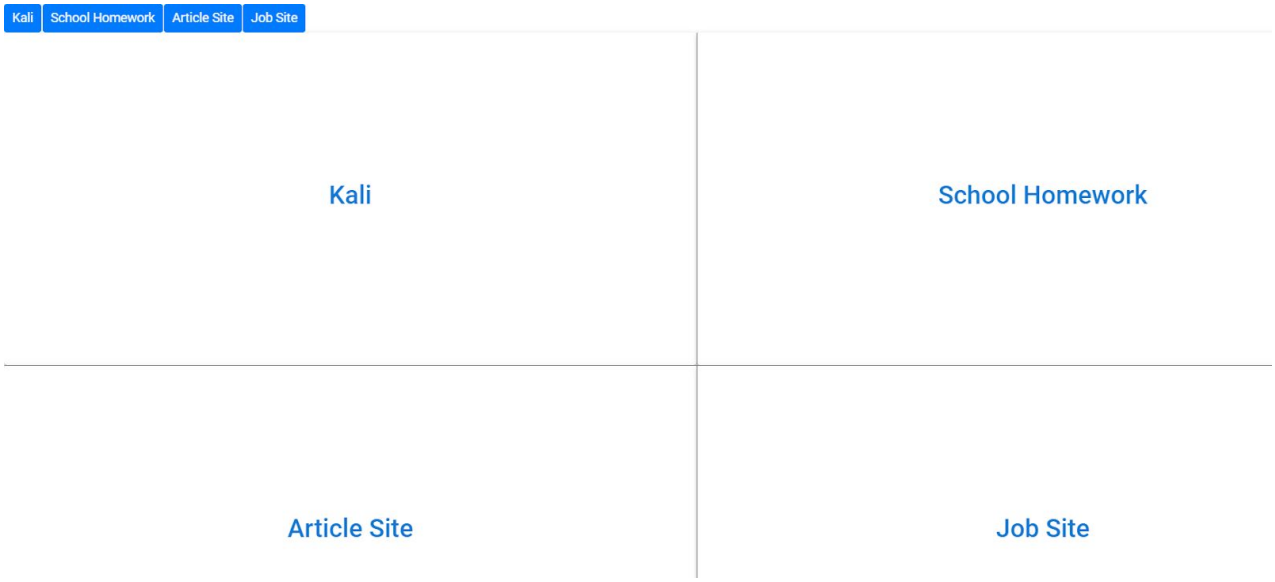
A Kali GUI machine (kali-gui) is provided to the user with OWASP ZAP available on it. Three example of vulnerable web portals are also provided. The details of these portals:

Web Portal	Web Portal URL
School Homework Web Portal	school-homework
Article Web Portal	article-site
Job Advertisement Web Portal	job-site

Objective: Analyze the web applications with OWASP ZAP and identify the vulnerabilities!

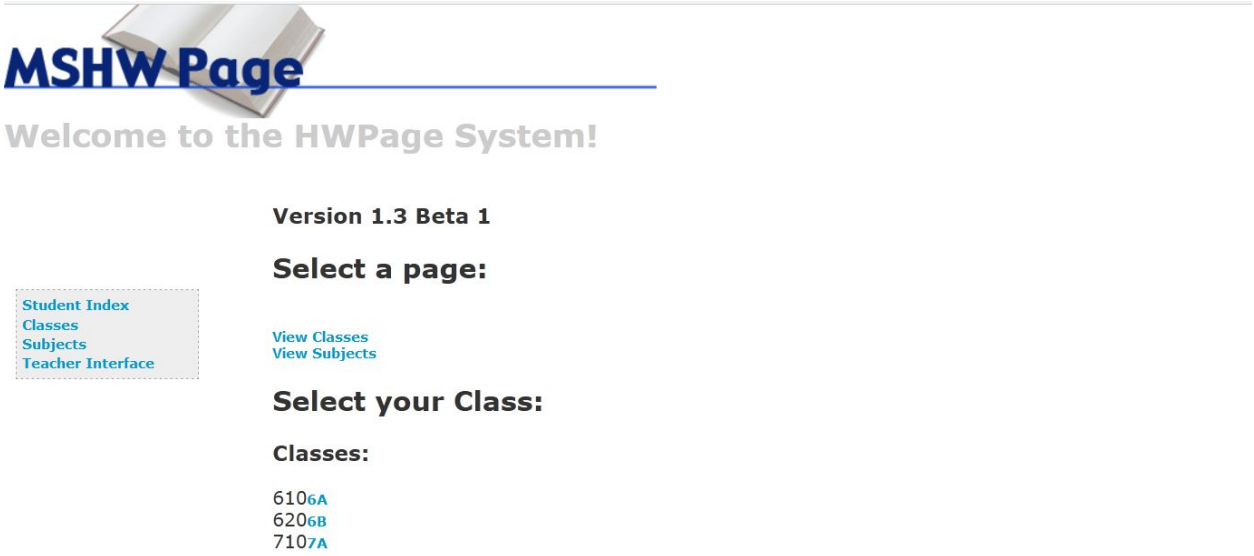
Lab Setup

On starting the lab, the following interface will be accessible to the user.

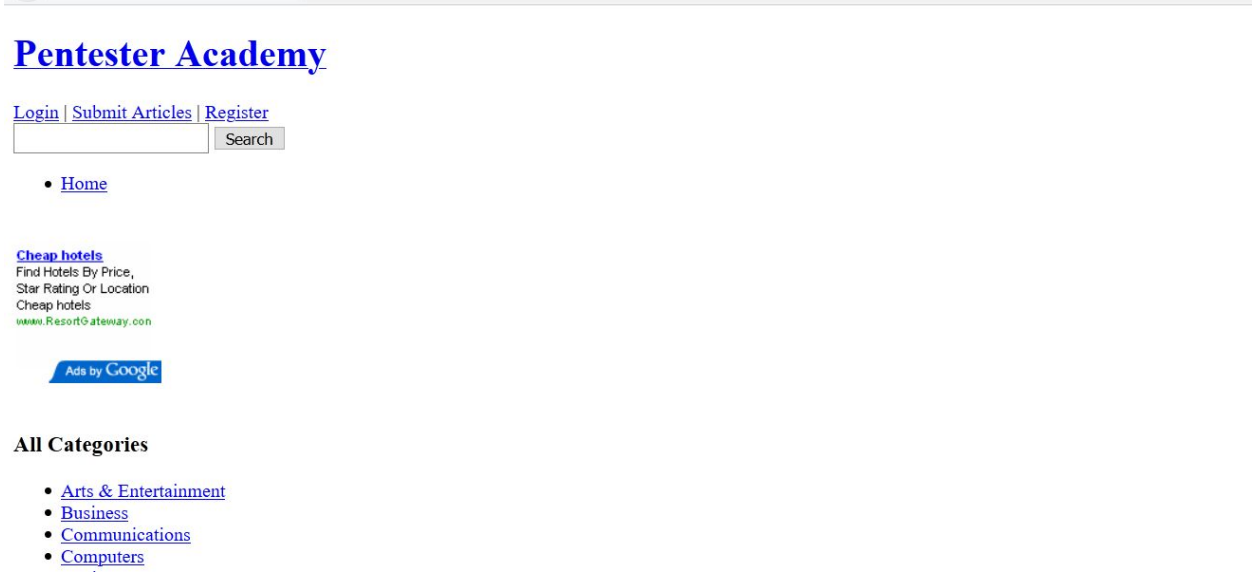


On choosing (clicking the text in the center) top left panel, **KALI GUI** will open in a new tab

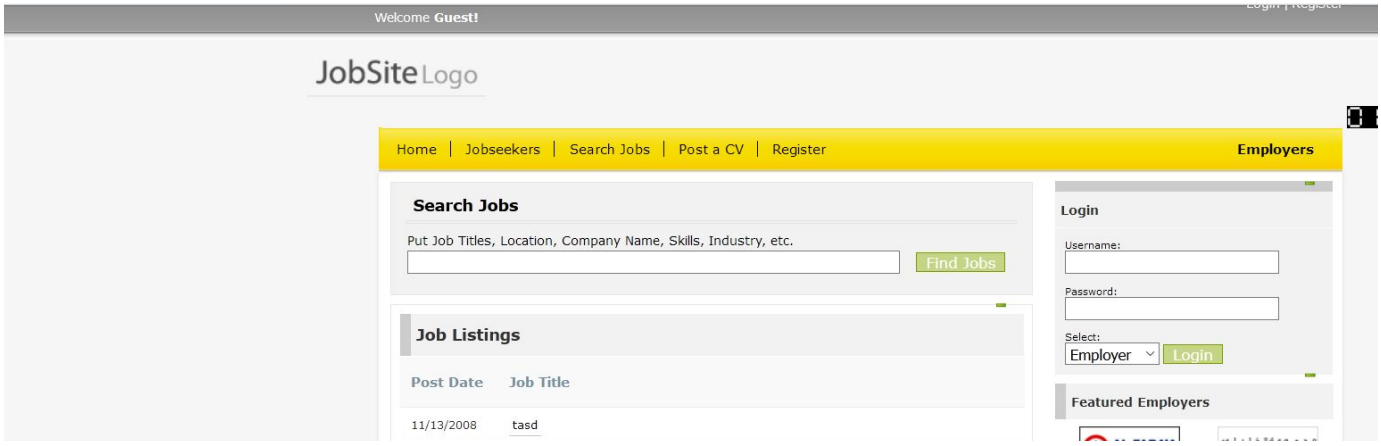
Similarly on selecting the top right panel, a web UI of **School Homework UI** will open in a new tab.



On selecting the bottom left panel, a web UI of **Article Site UI** will open in a new tab.

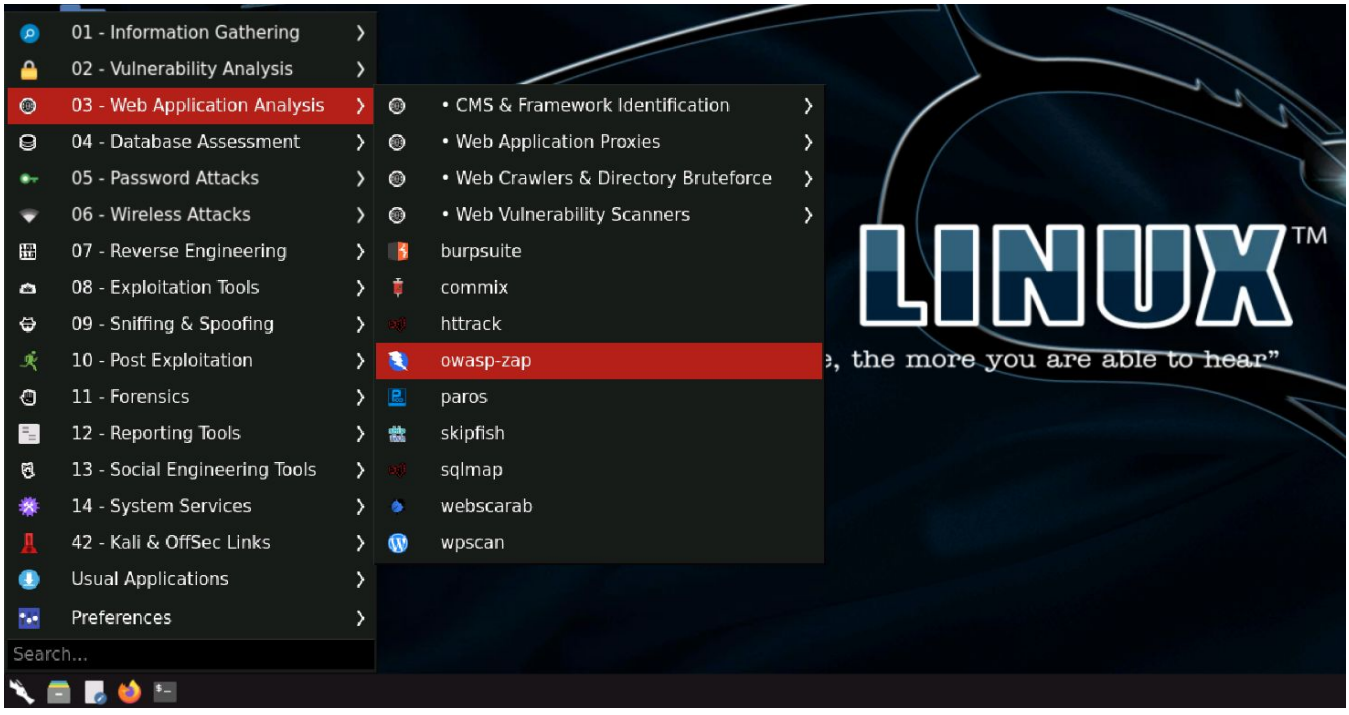


And on selecting the bottom right panel, a web UI of **Job Site UI** will open in a new tab.

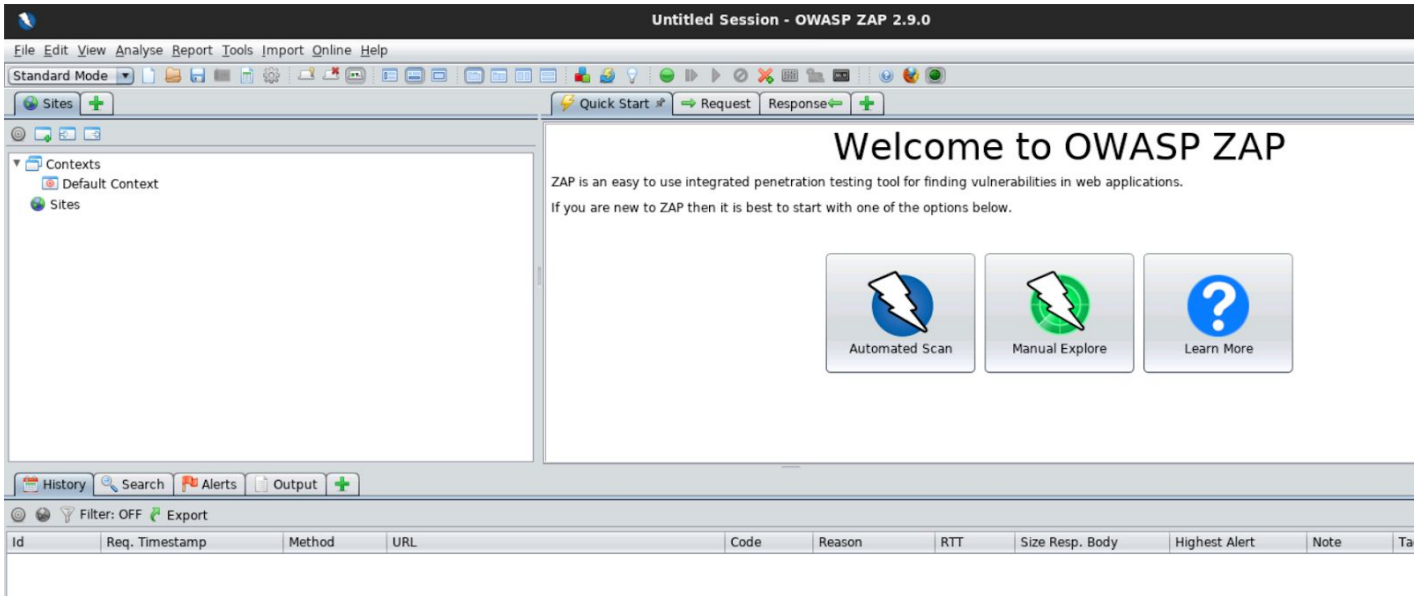


Solution

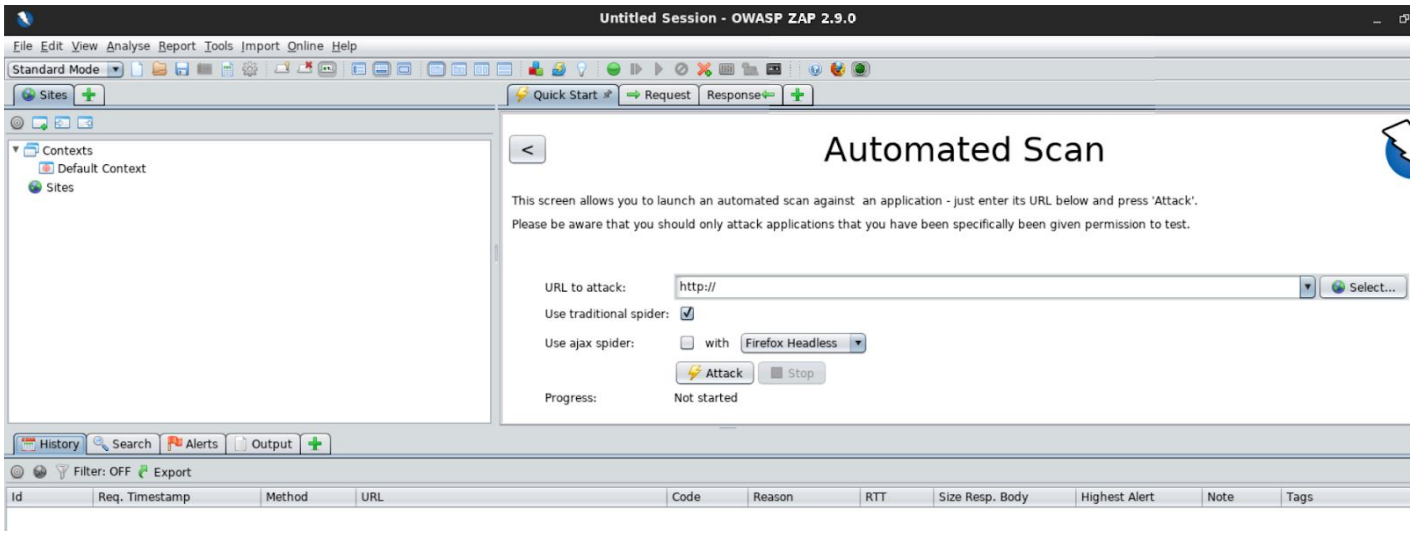
Step 1: Start the OWASP ZAP located under Web Application Analysis



Click on the owasp-zap.



Step 2: Click on the Automated Scan button

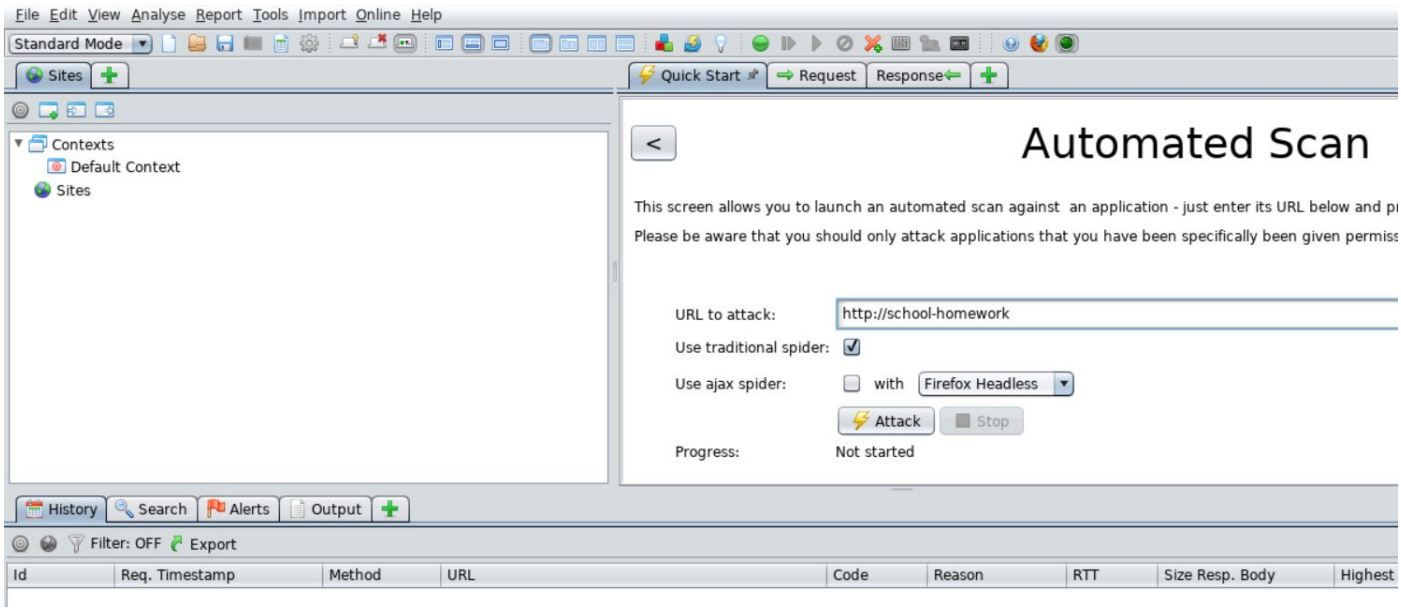


We will take one example at a time and run the tool on that.

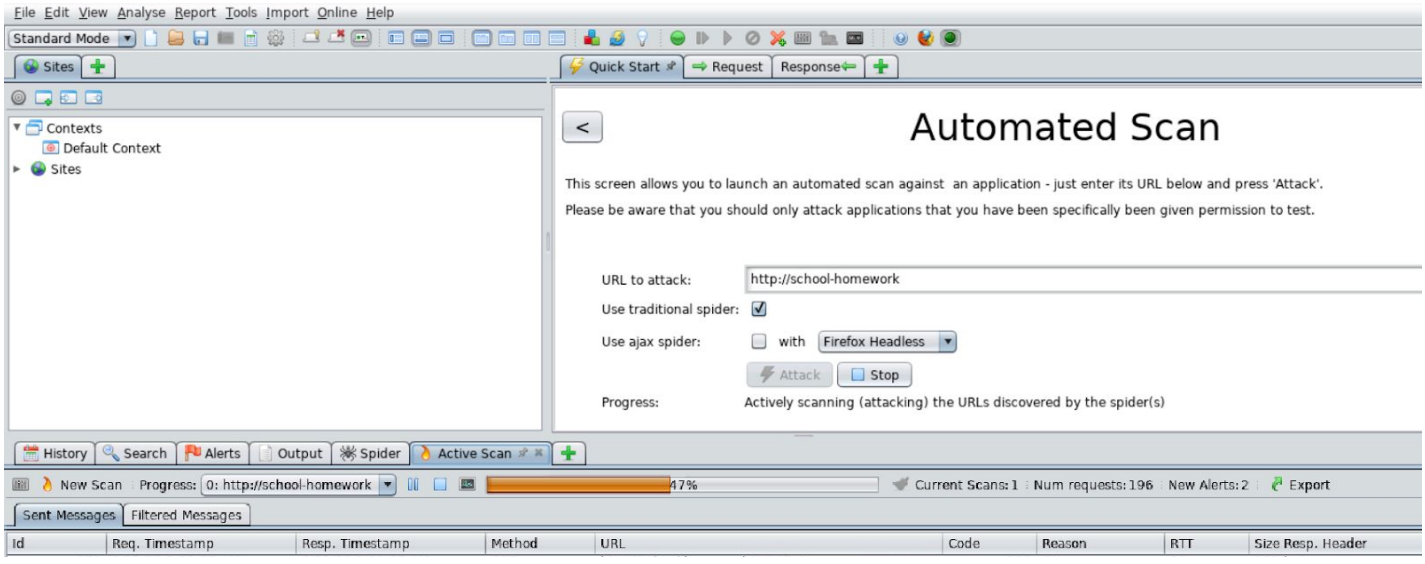
Example 1: School Homework

Step 1: Enter the target URL in the “URL to attack” field.

URL: http://school-homework

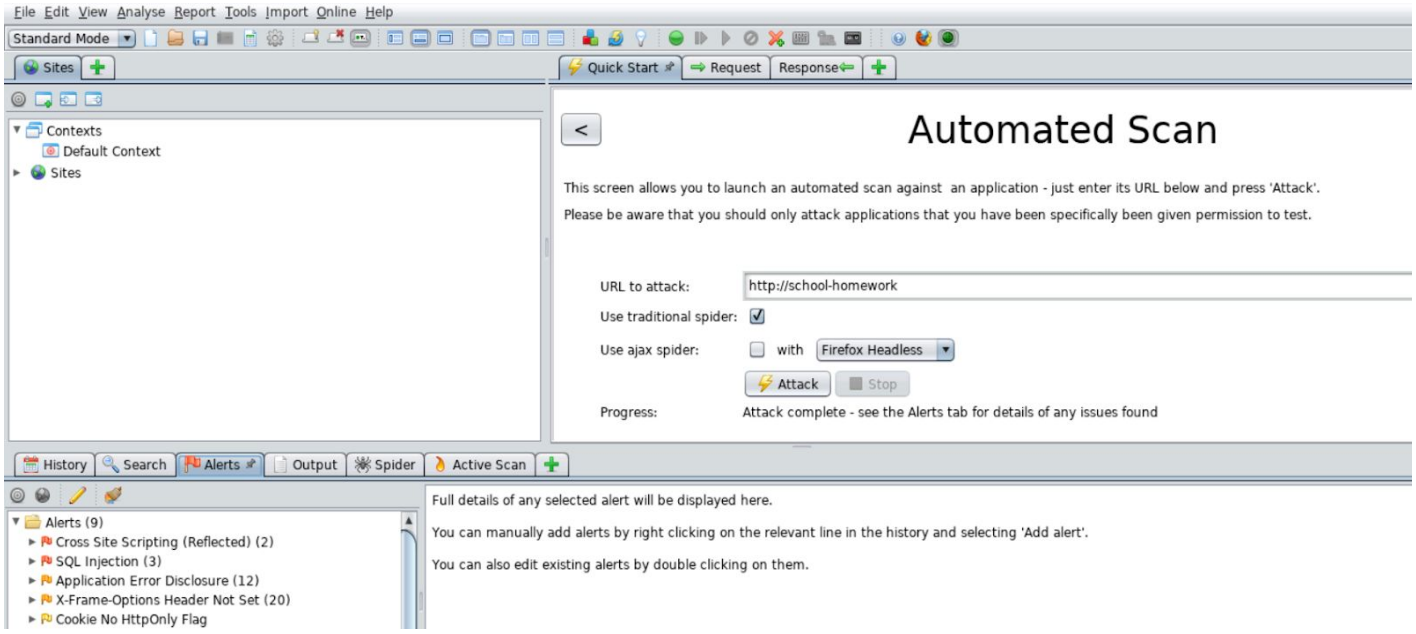


Click on the Attack button.



The tool will start the automated attack on the target website.

Step 2: Click on the Alerts button to get the list of potential vulnerabilities found by ZAP

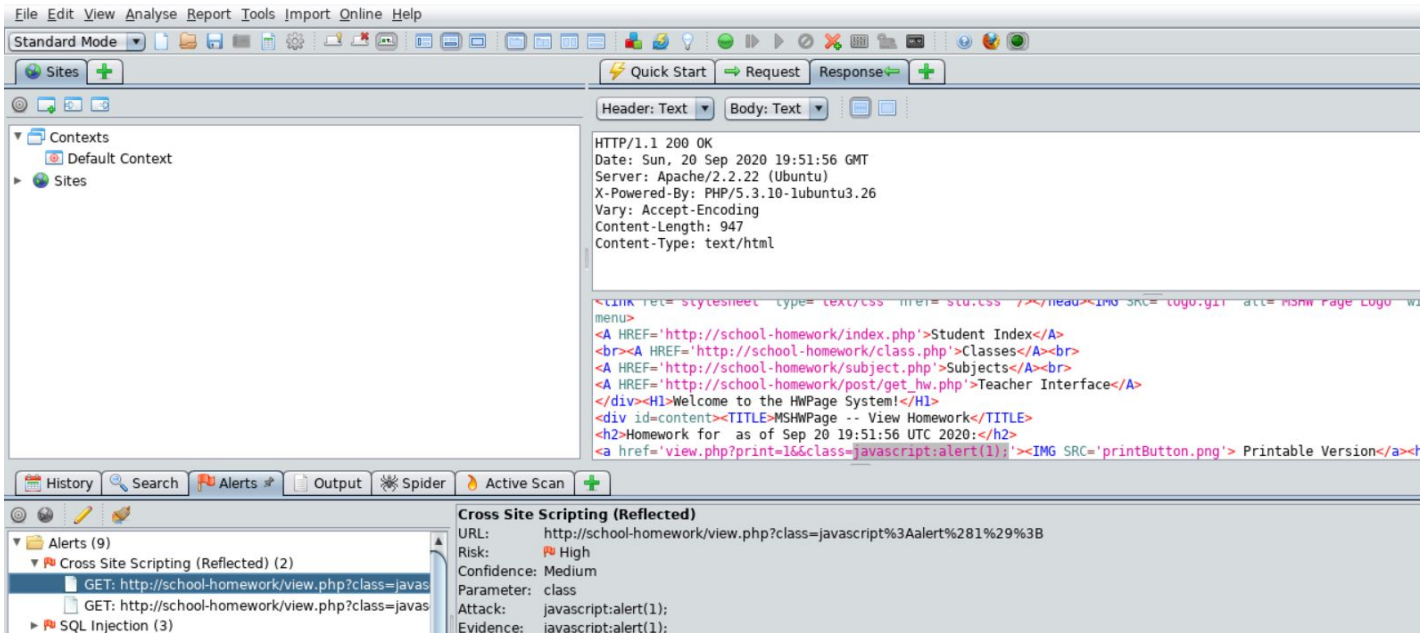


Issues Detected

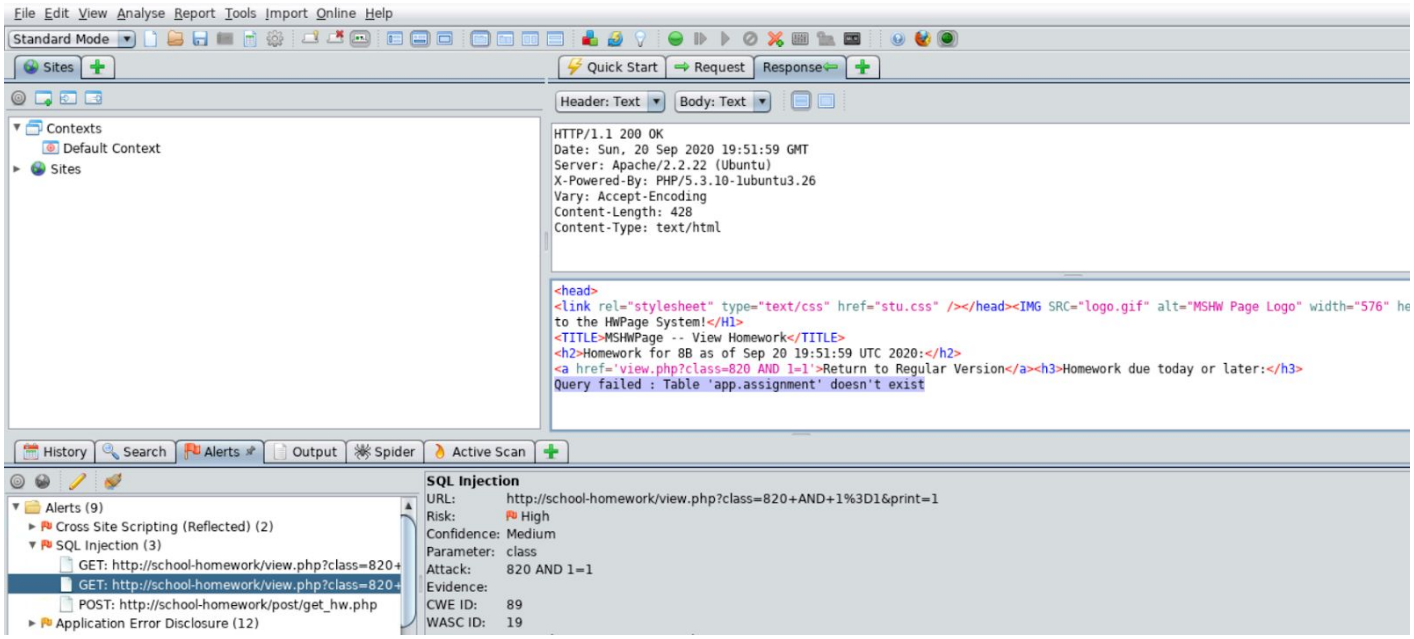
- Cross-Site Scripting
- SQL Injection
- Application Error Disclosure

Step 3: The details on these issues can be checked by selecting the issue/alert from the left-down side window.

Check the endpoints affected with XSS vulnerability.



Similarly, one can also check the endpoints affected with SQL Injection vulnerability.

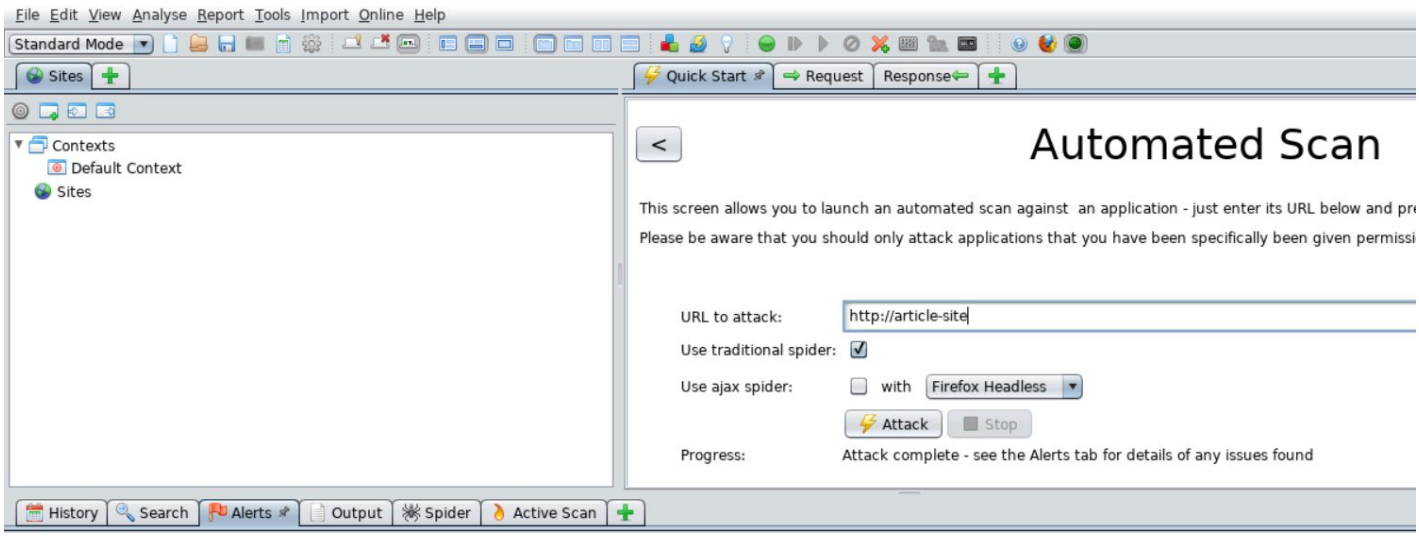


Note: Start a new session by clicking on the File and select “New Session”

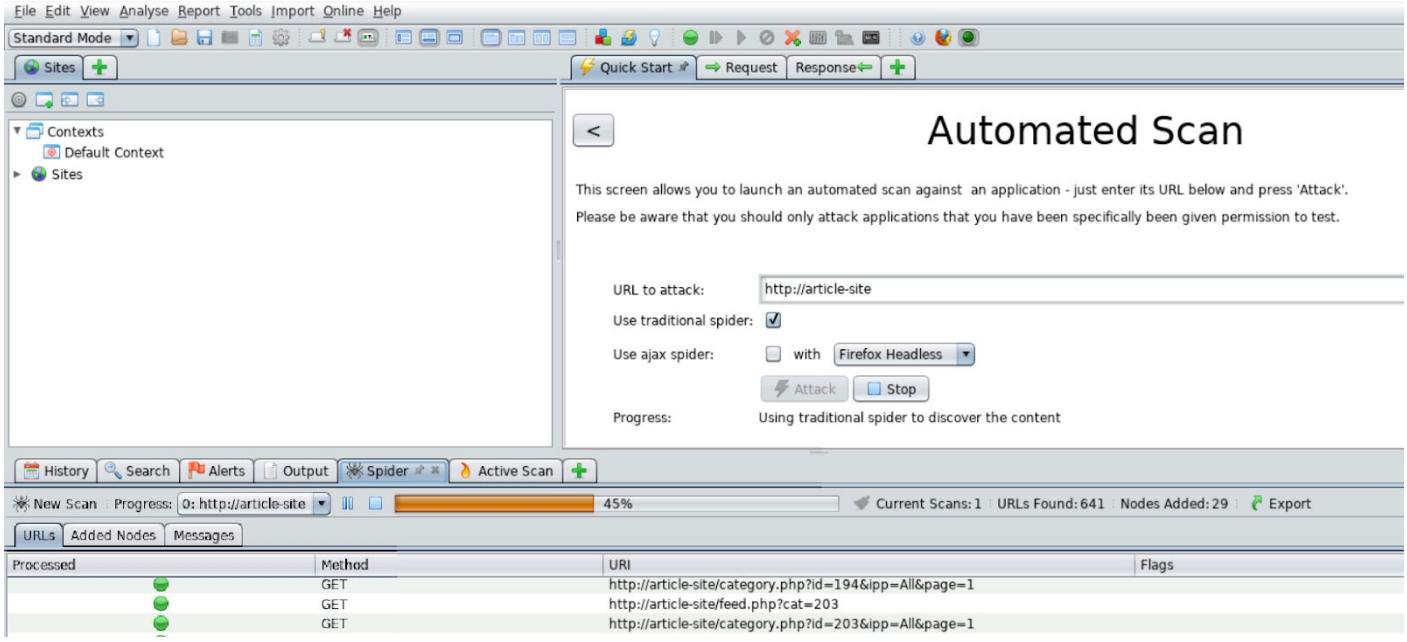
Example 2: Article Site

Step 1: Enter the target URL in the “URL to attack” field.

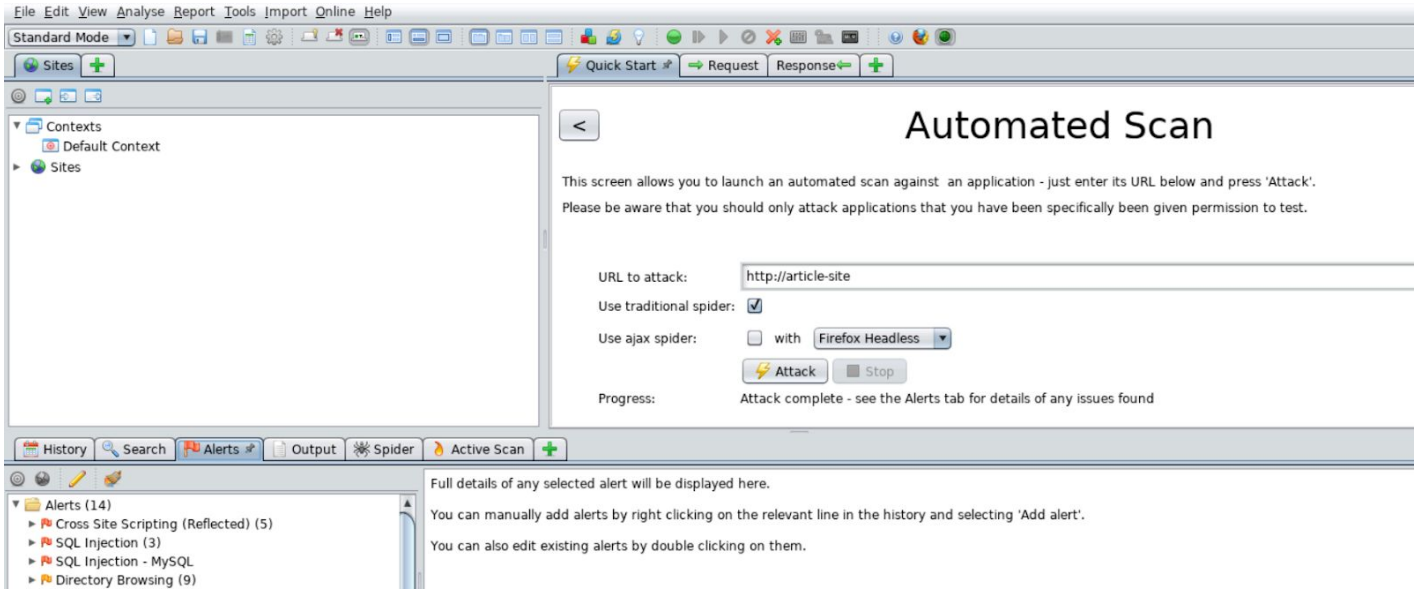
URL: http://article-site



Click on the Attack button to start the attack on the website.



Step 2: Navigate to the Alerts tab to get information about the weaknesses found on the website.

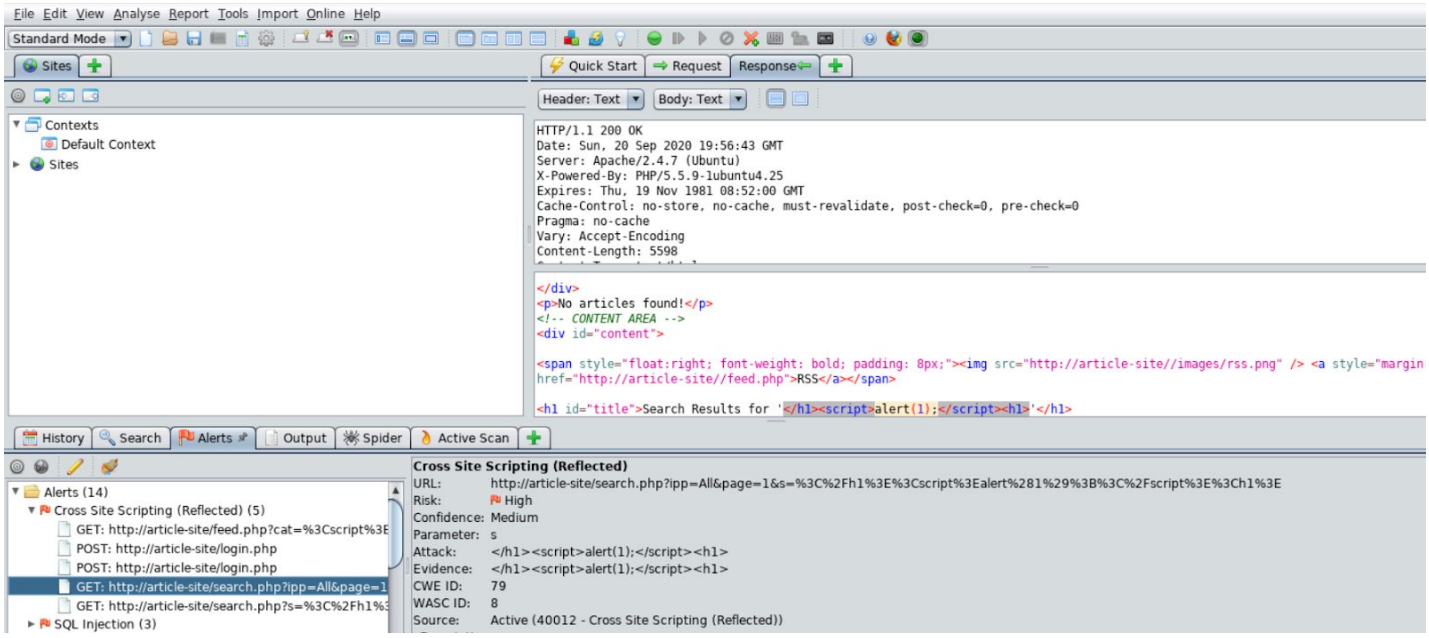


Issues Detected

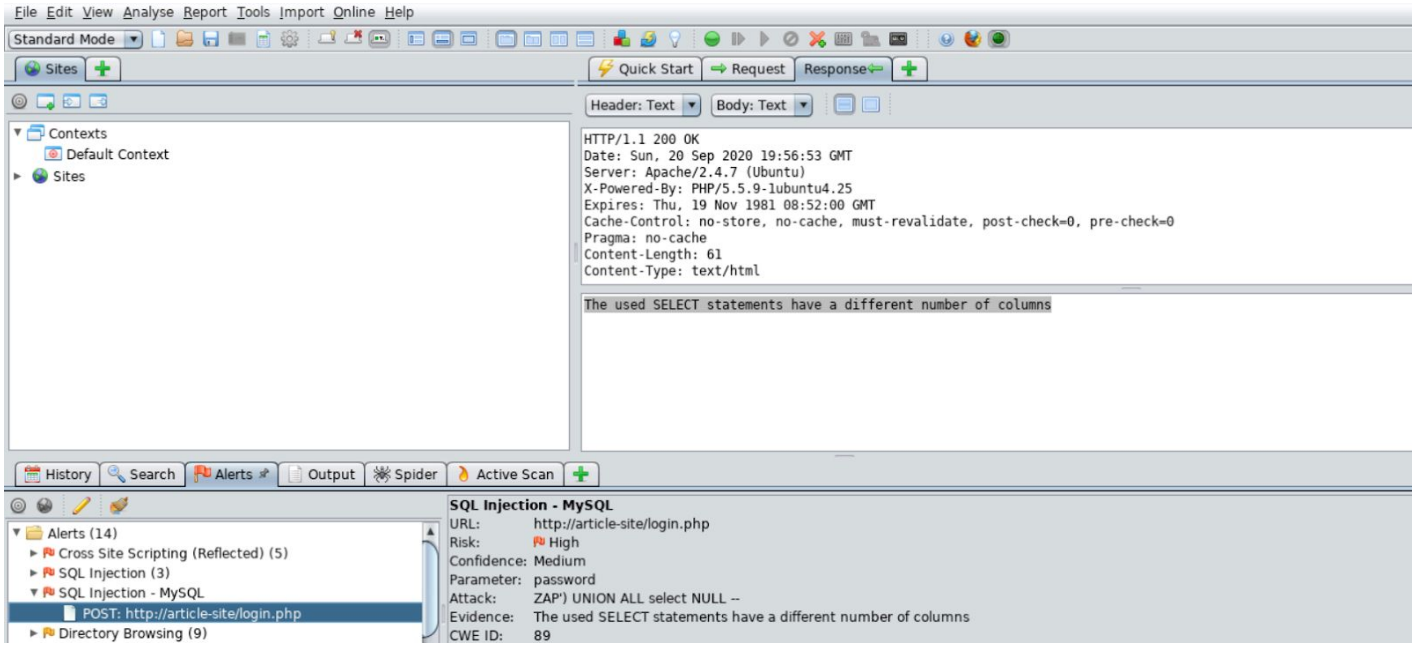
- Cross-Site Scripting
- SQL Injection
- Directory Listing

Step 3: The details on these issues can be checked by selecting the issue/alert from the left-down side window.

Check the endpoints affected with XSS vulnerability.



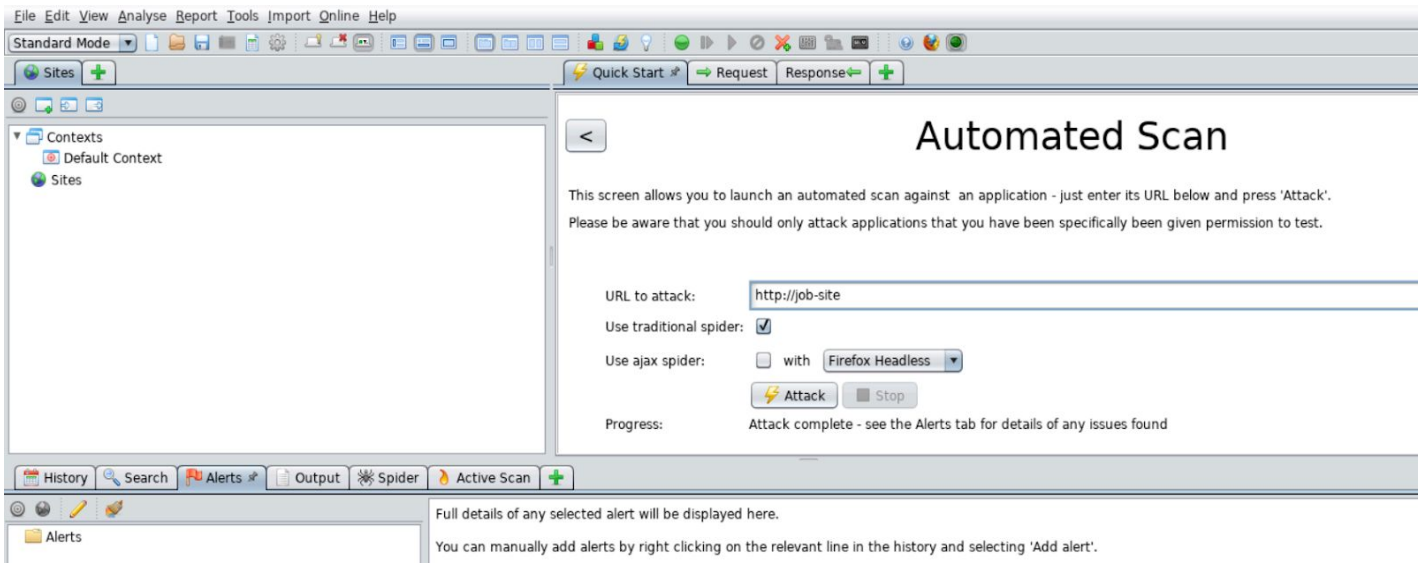
Similarly, one can also check the endpoints affected with SQL Injection vulnerability.



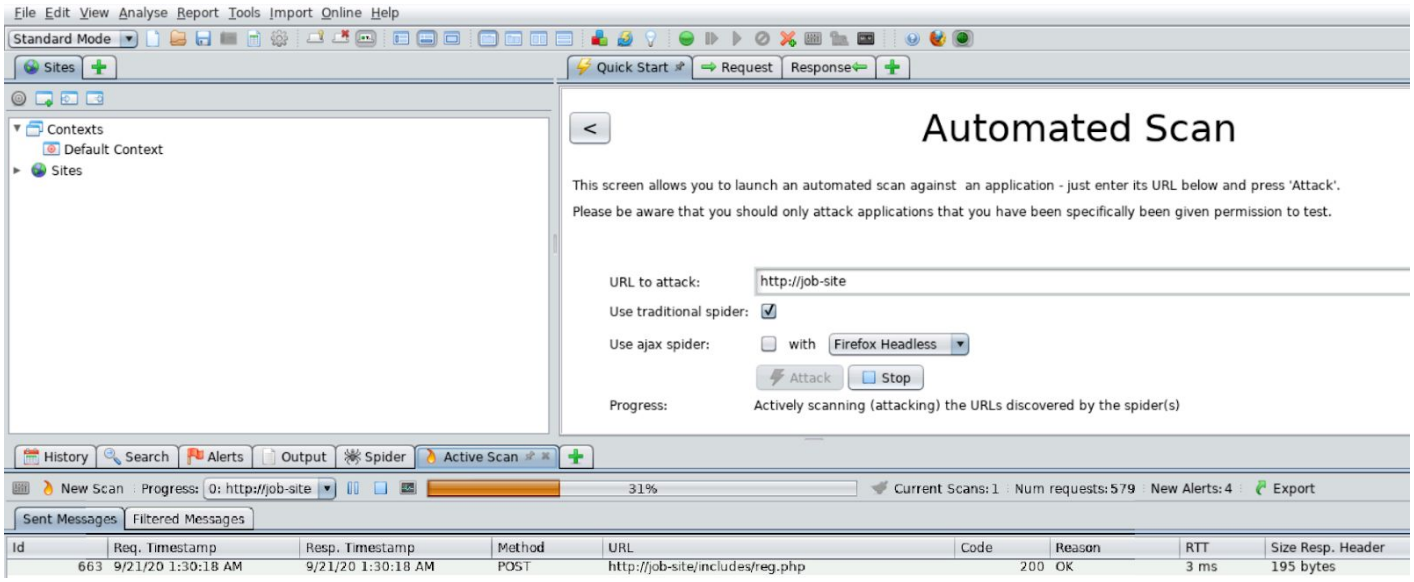
Example 3: Job Site

Step 1: Create a new session and enter the target URL in the “URL to attack” field.

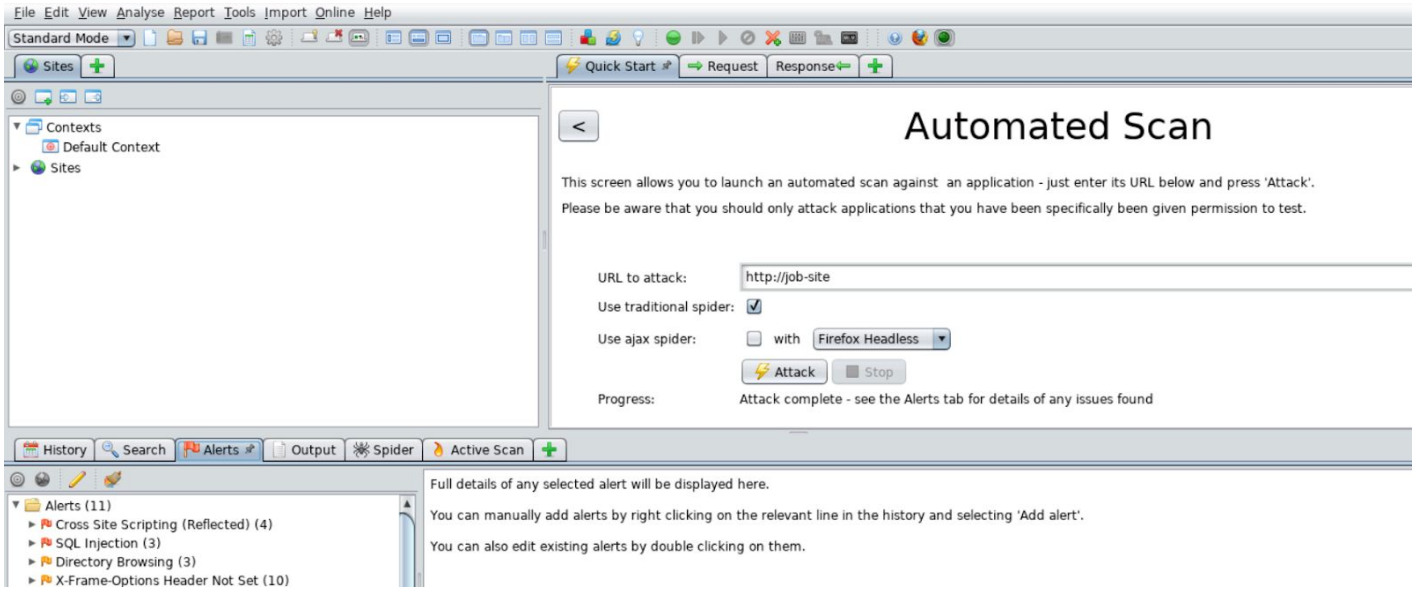
URL: http://job-site



Click on the Attack button.



Step 2: Navigate to the Alerts tab.

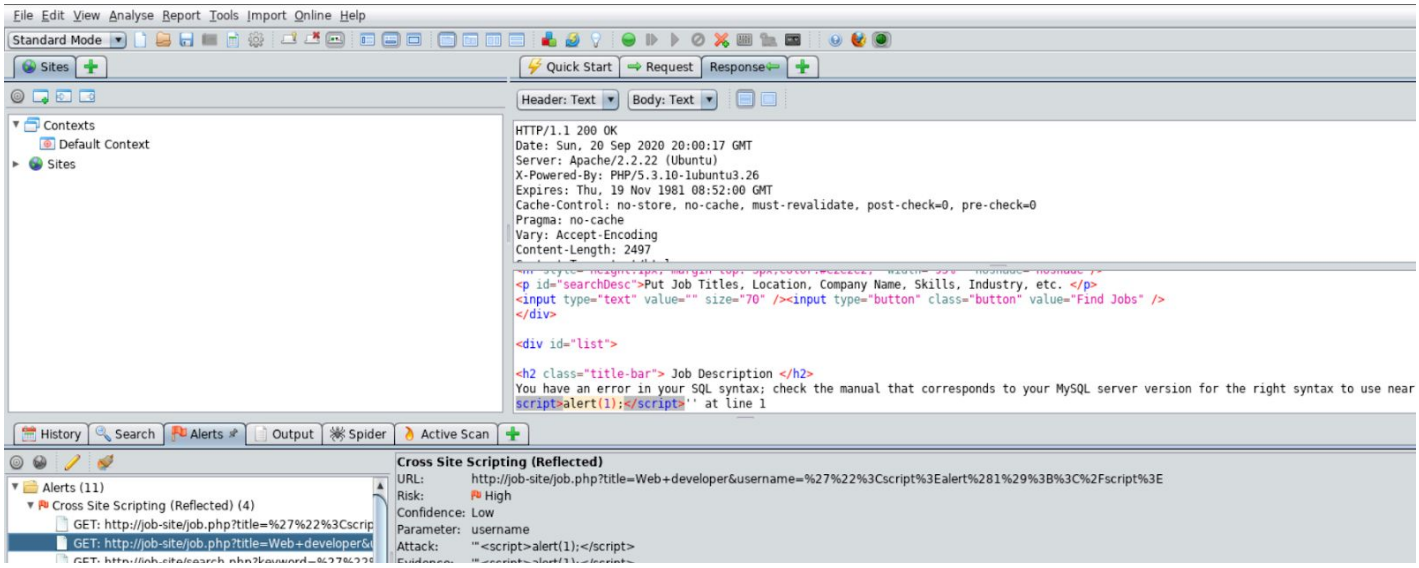


Issues Detected

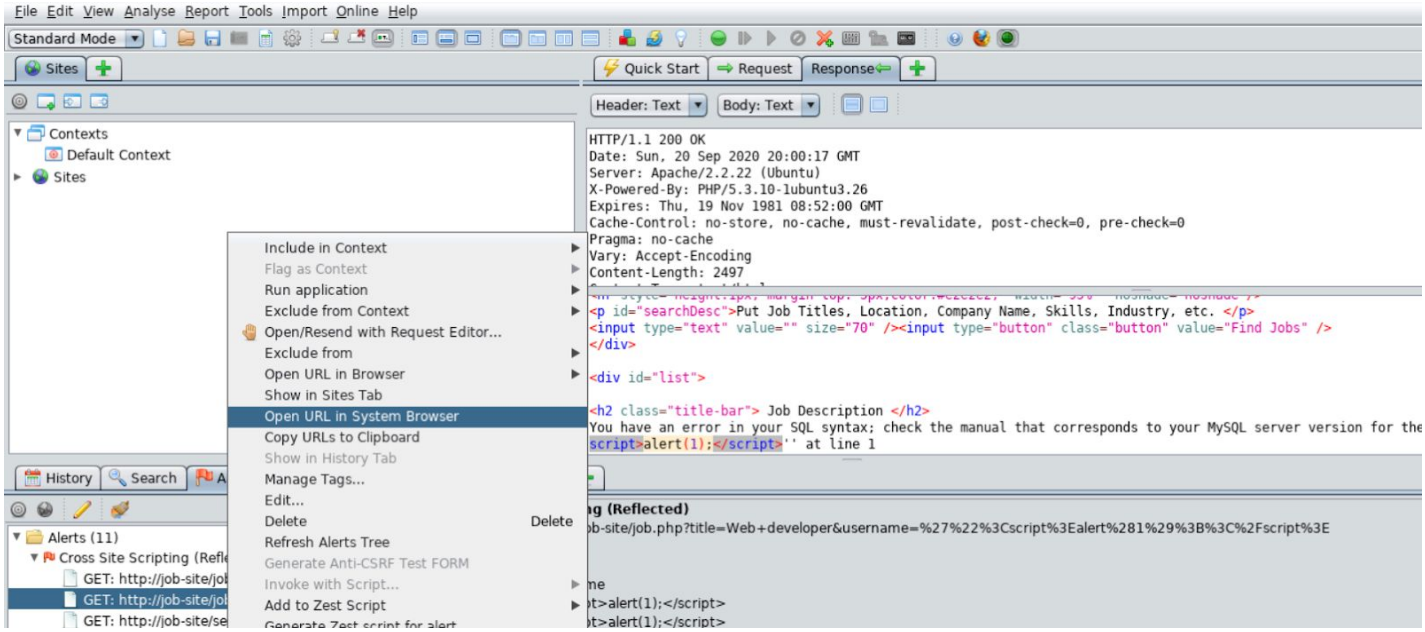
- Cross-Site Scripting
- SQL Injection
- Directory Listing

Step 3: The details on these issues can be checked by selecting the issue/alert from the left-down side window.

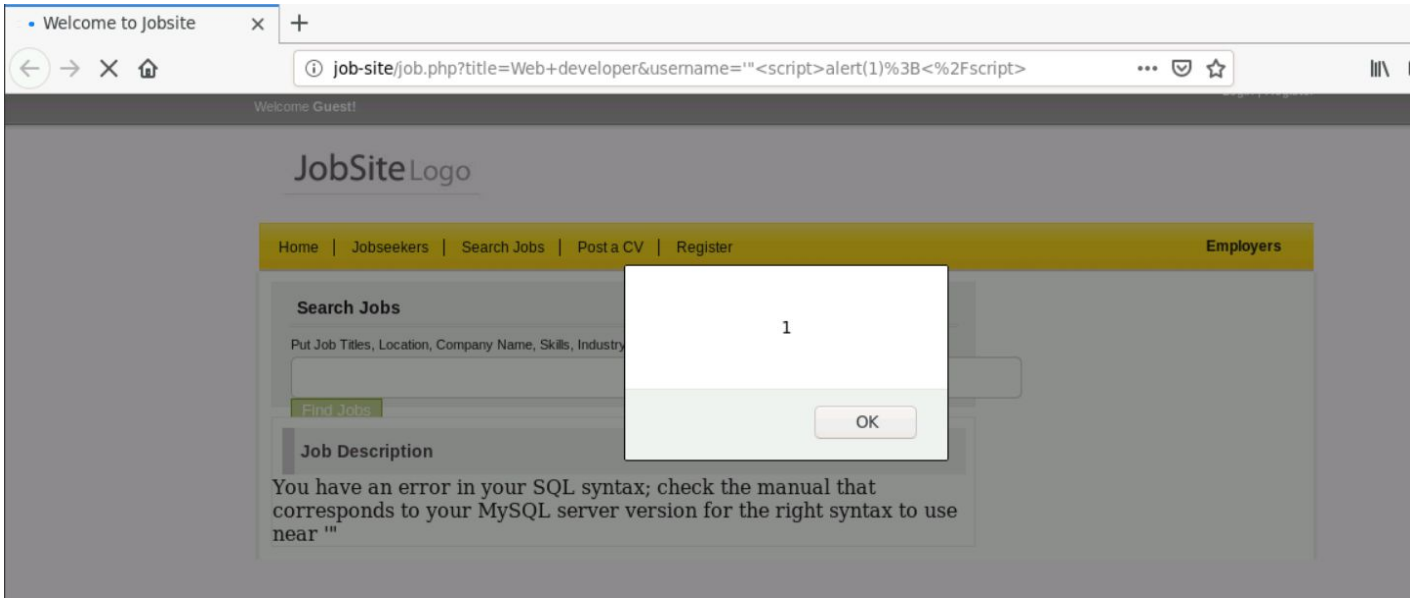
Check the endpoints affected with XSS vulnerability.



Also, to see the vulnerability in action, Right-click on the endpoint and select “Open URL in System Browser”.



The request will open in the system browser with the payload and the exploitation can be observed.



XSS vulnerability in action.

Learnings

Perform dynamic code analysis on web applications using OWASP ZAP.