ATTACK DEFENSE

by PentesterAcademy

Name	ArcherySec: Vulnerability Management Framework
URL	https://attackdefense.com/challengedetails?cid=2256
Type	DevSecOps Basics: Vulnerability Management

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

Archerysec is an open-source assessment and management framework for performing dynamic analysis on web applications.

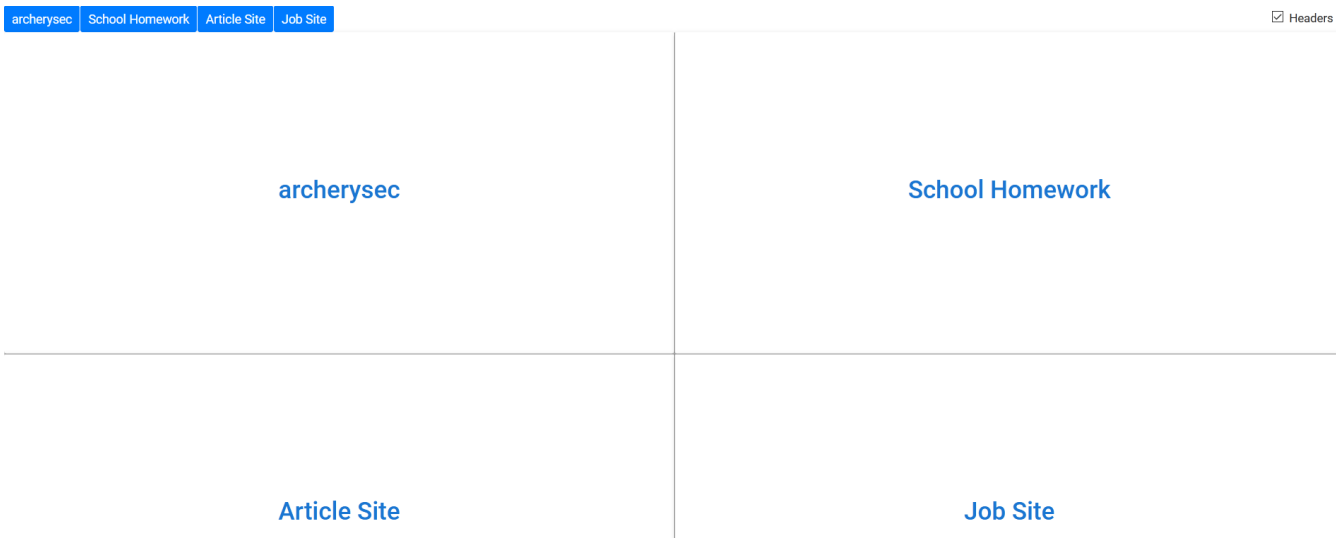
An Archerysec instance is provided to the user to perform tests on the websites. Three examples of vulnerable web portals are also provided. The details of these portals:

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

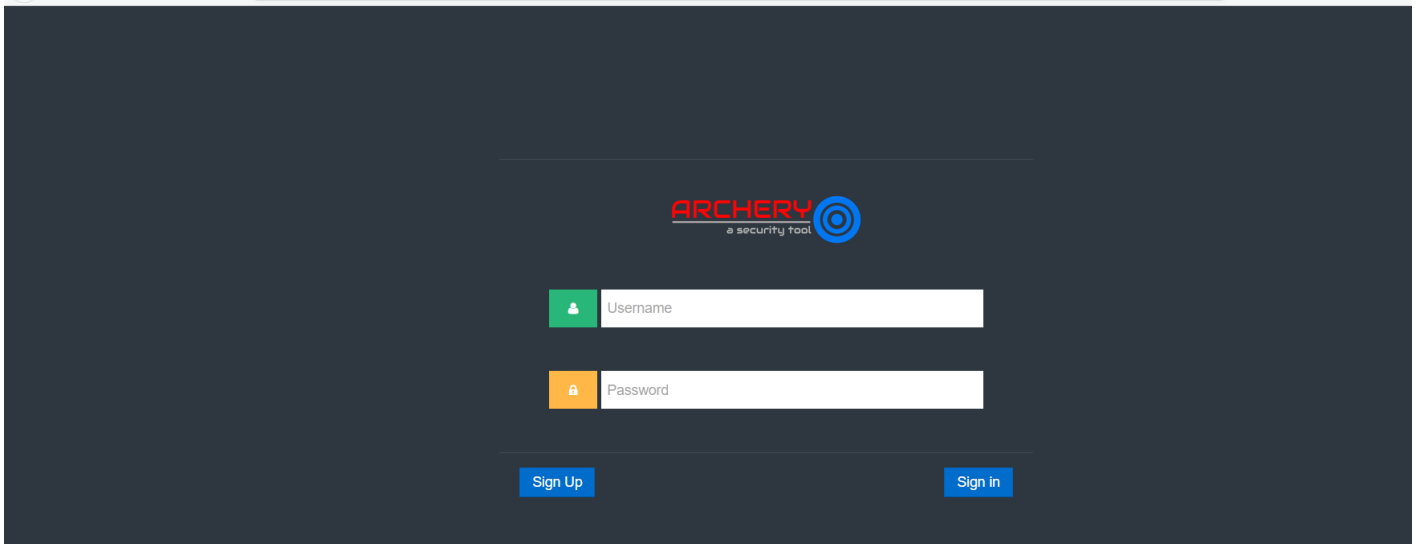
Objective: Analyze the web applications with Archerysec and identify the vulnerabilities!

Lab Setup

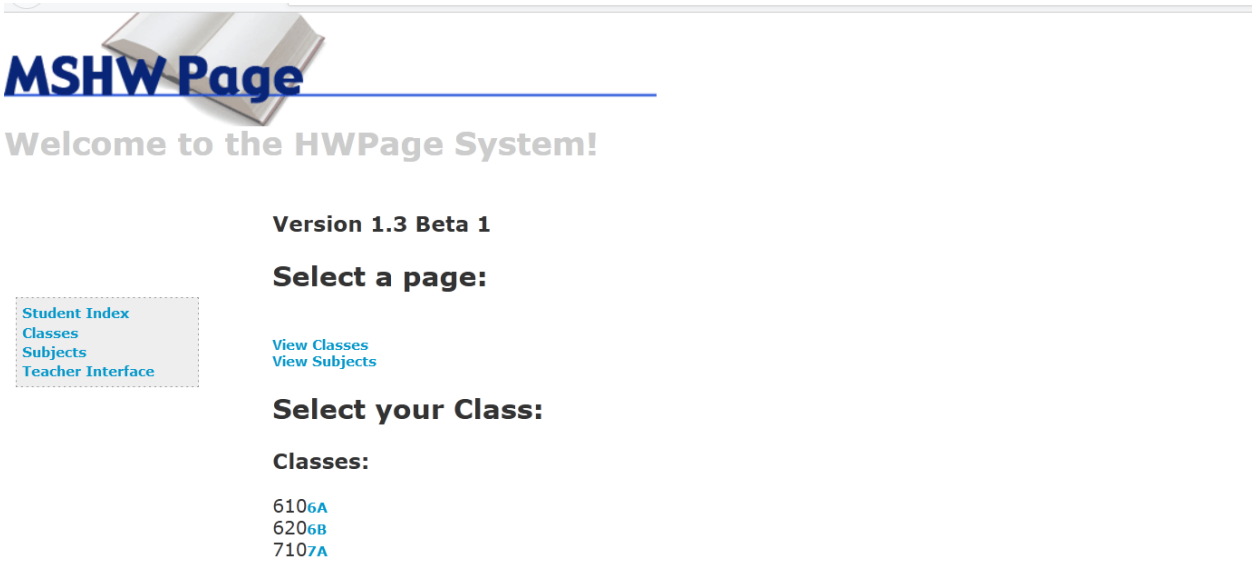
On starting the lab, the following interface will be accessible to the user.



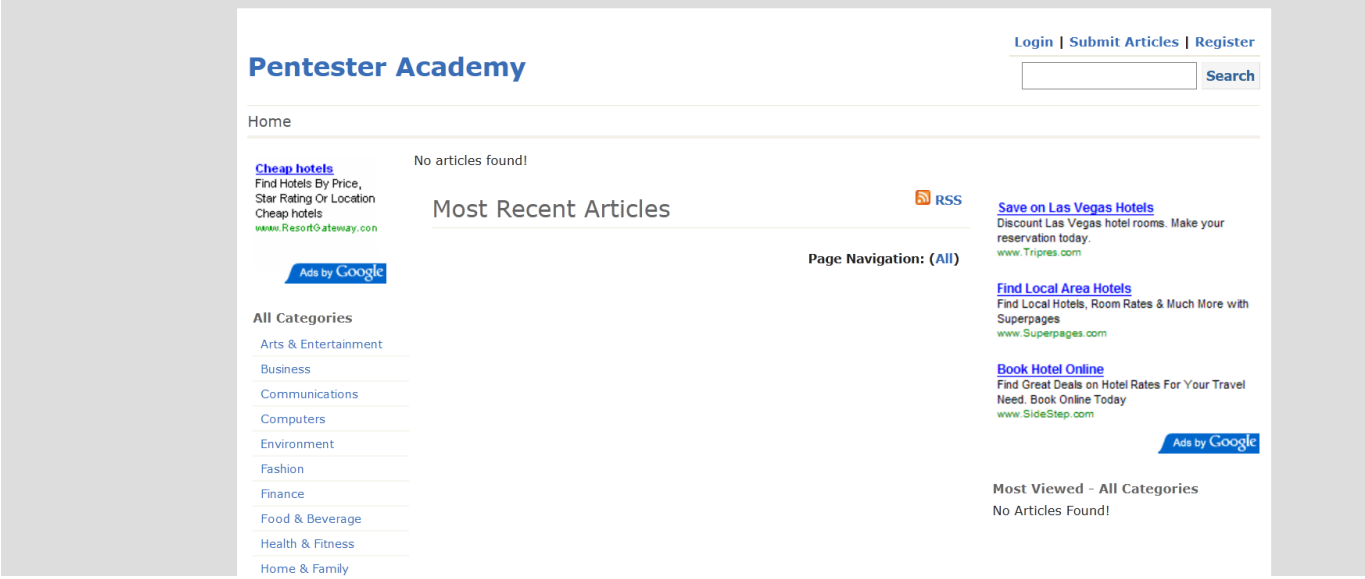
On choosing (clicking the text in the center) top left panel, **Archerysec** will open in a new tab



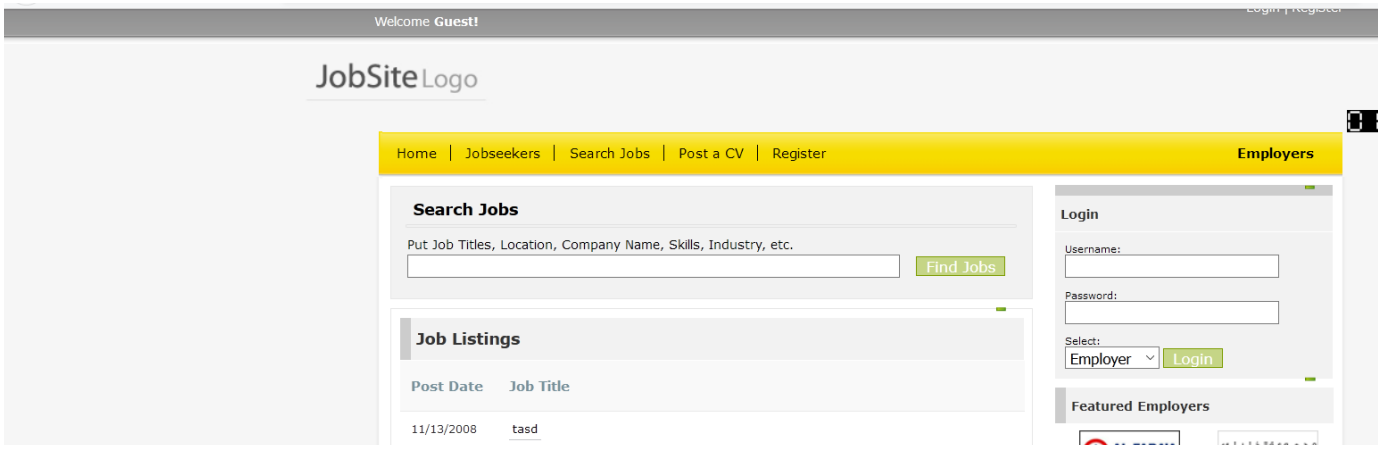
Similarly on selecting the top right panel, a web UI of **School Homework UI** will open in a new tab.



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.

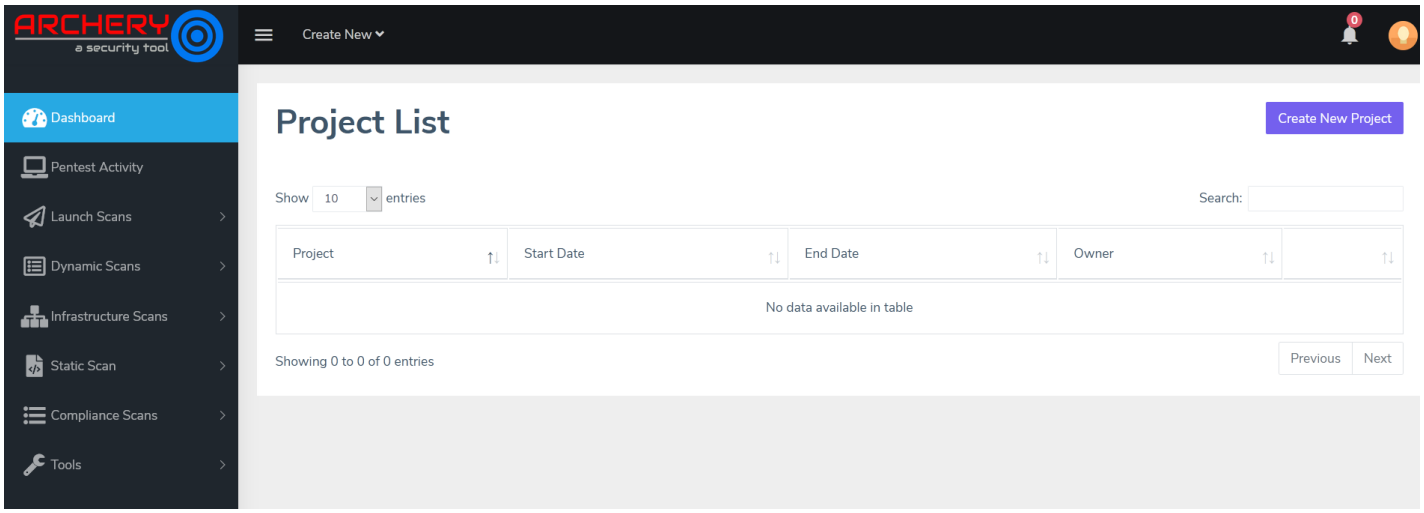


Solution

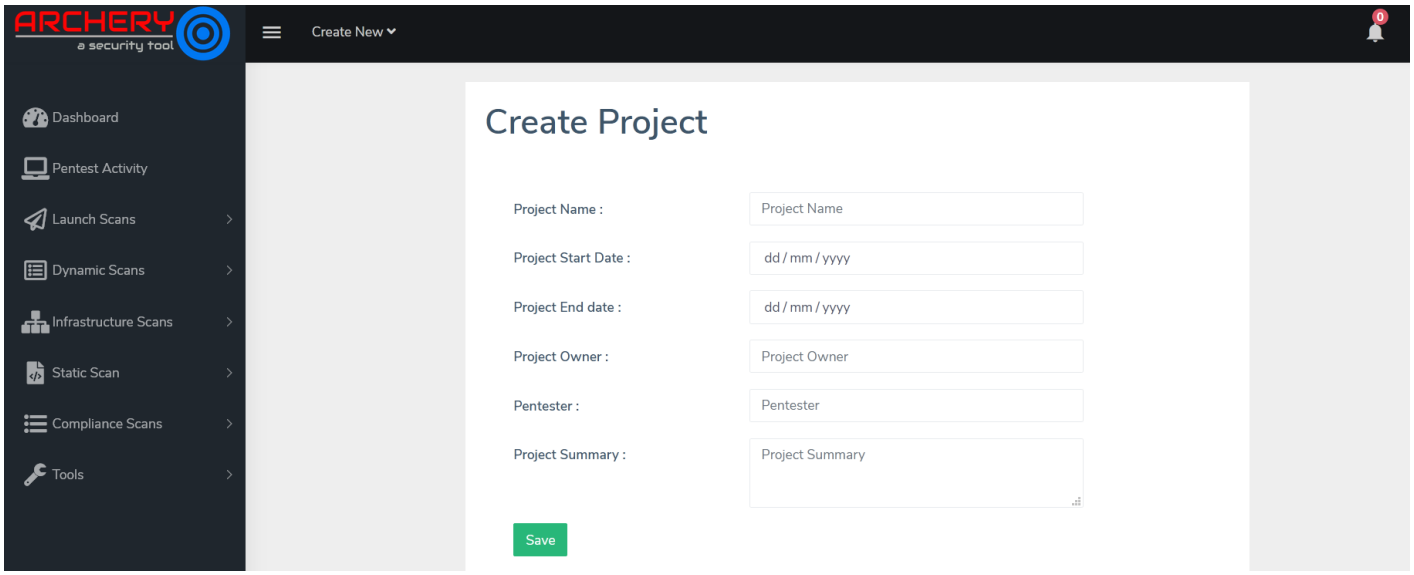
Step 1: Open the Archerysec page and log in using the credentials provided in the challenge description.

Credentials:

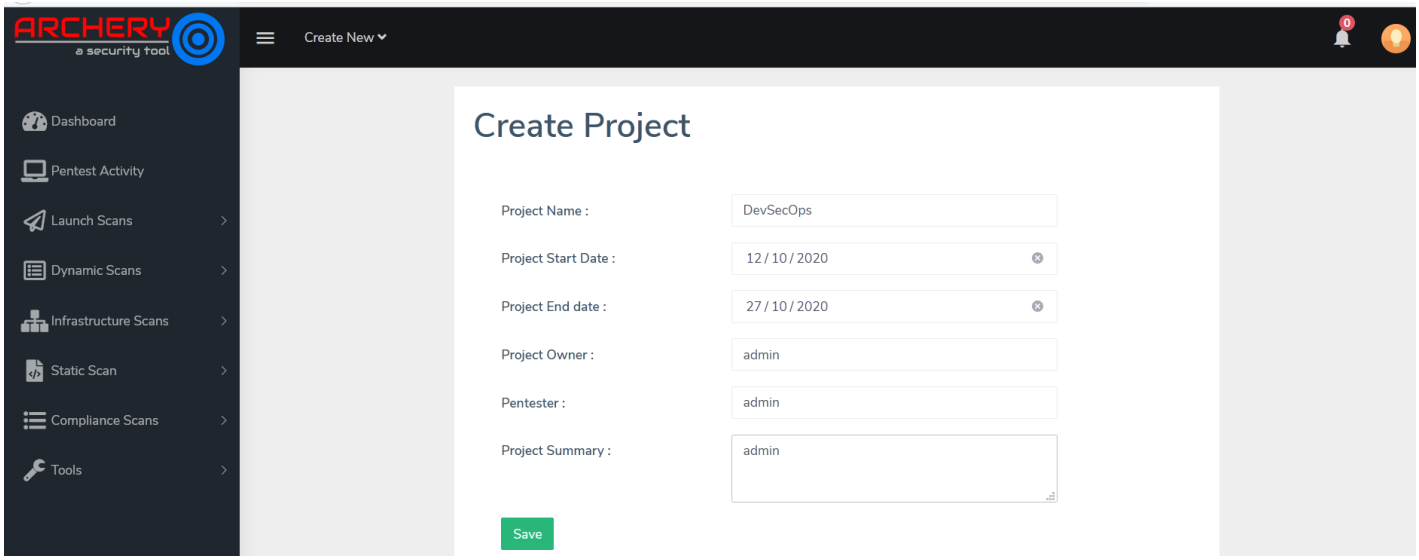
- **Username:** admin
- **Password:** admin



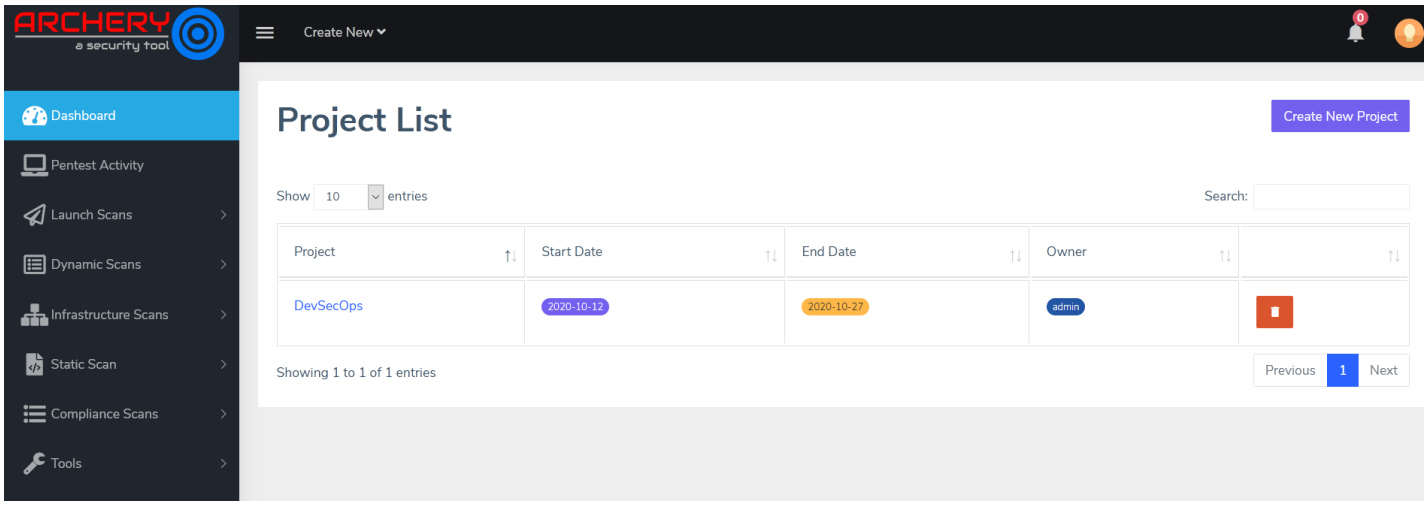
Click on the Create New Project.



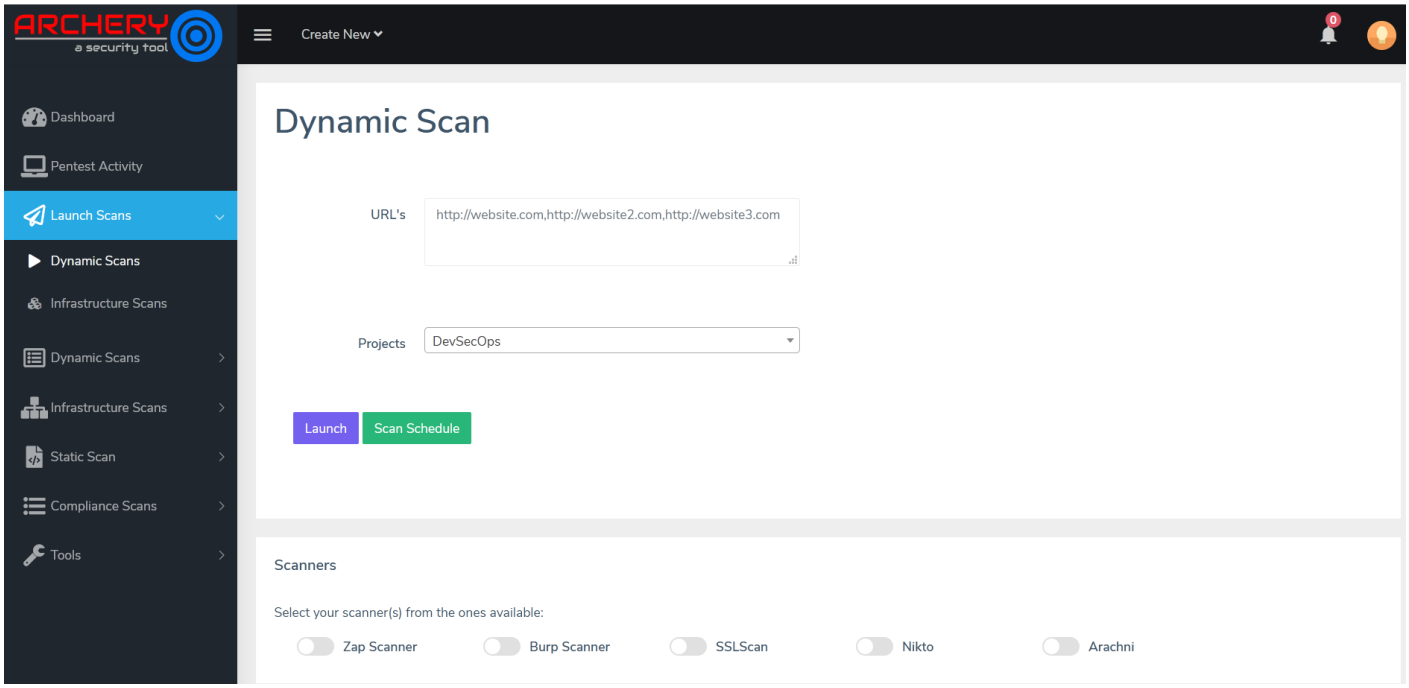
Step 2: Enter any data in the required fields.



Click on the Save button.



Step 3: Navigate to the “Dynamic Scans” sub-section located under “Launch Scans” section.

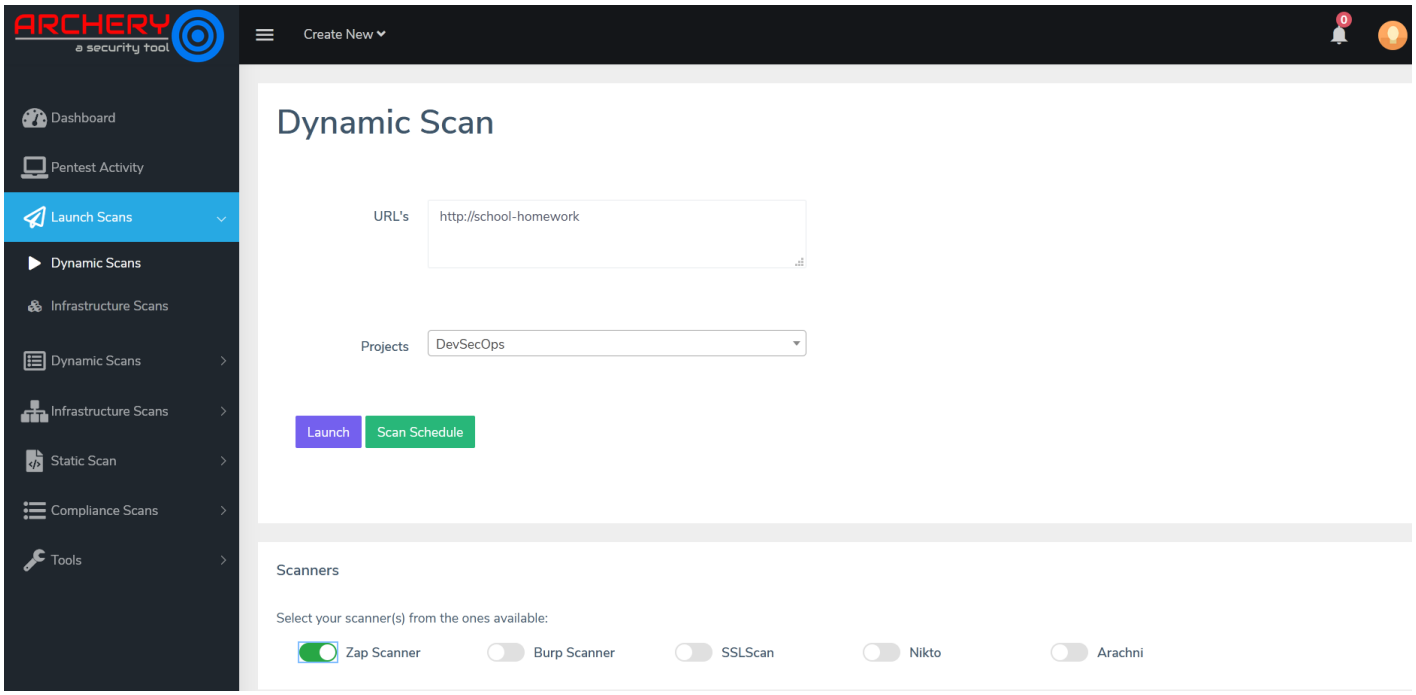


We will take one example at a time and run the tool on that.

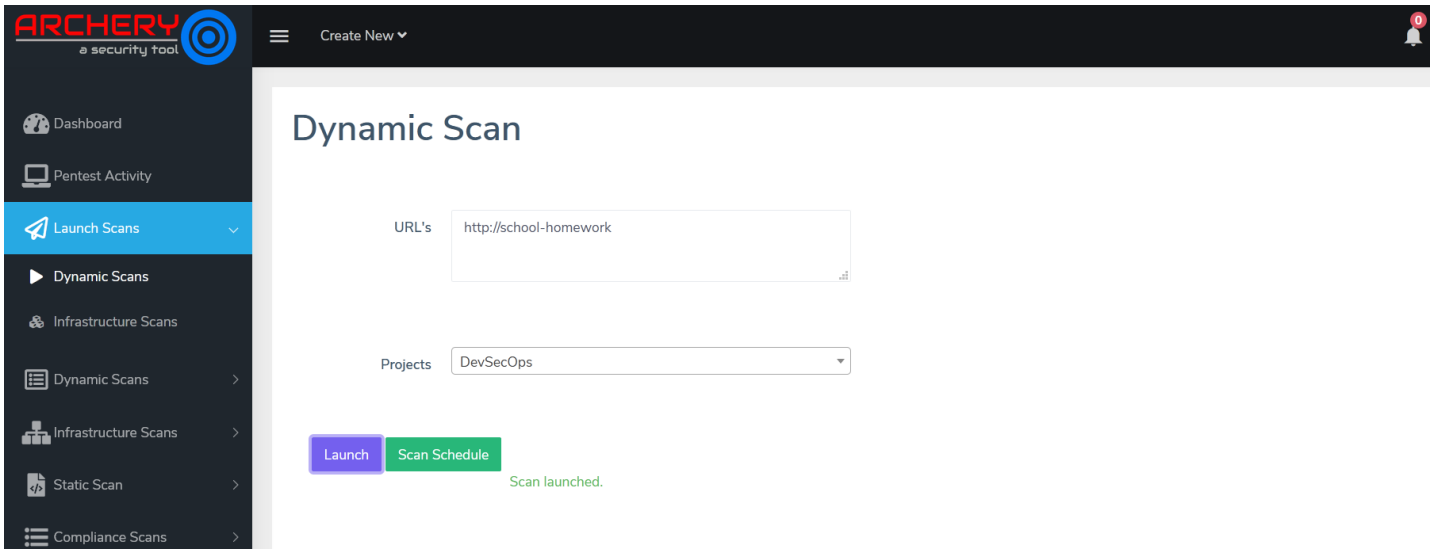
Example 1: School Homework

Step 1: Enter the target URL in the “URL’s” field and select “Zap Scanner”

URL: http://school-homework

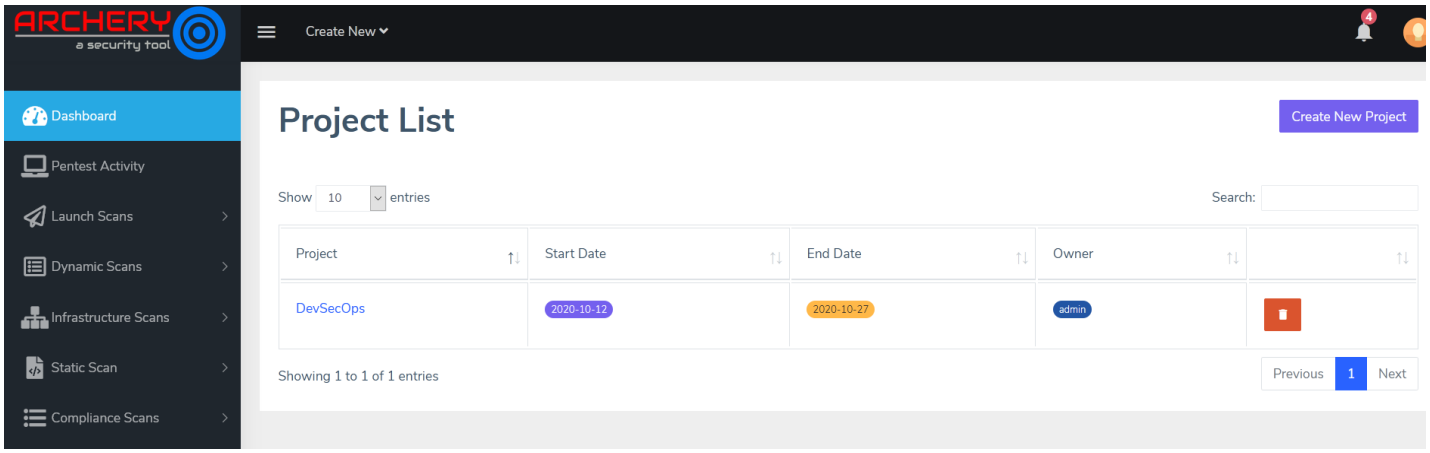


Click on the Launch button.

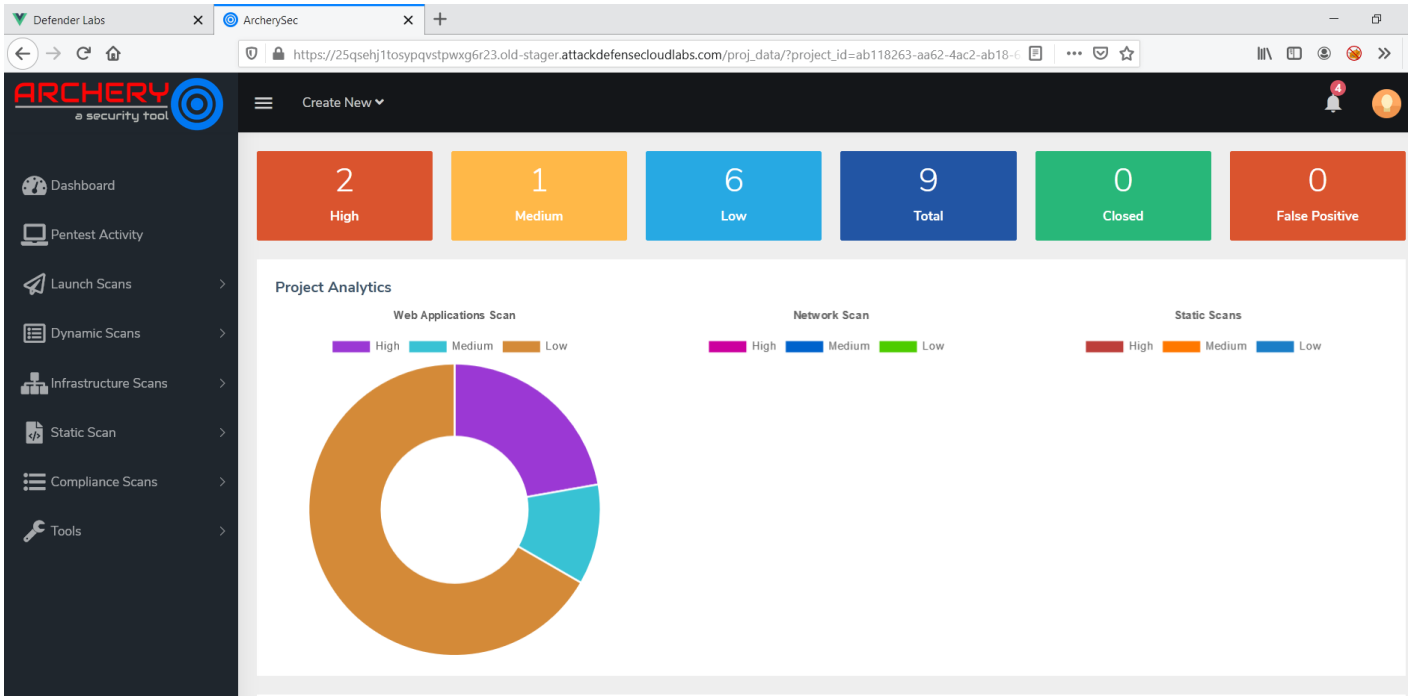


The tool will start the automated attack on the target website.

Step 2: Navigate to the Dashboard of the Archerysec.



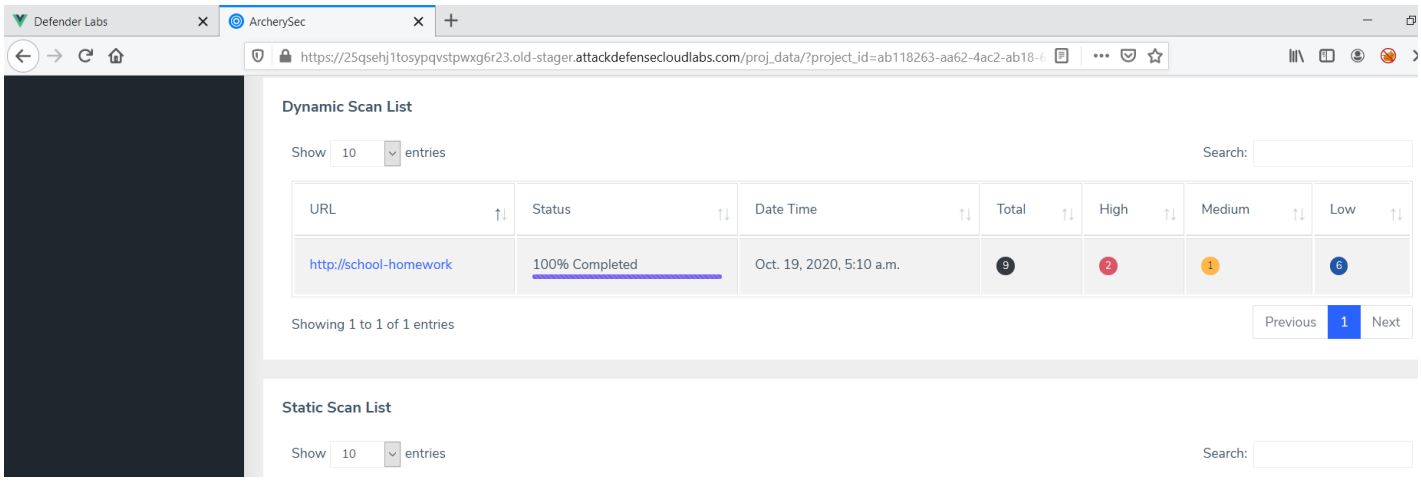
Click on the Project name “DevSecOps”.



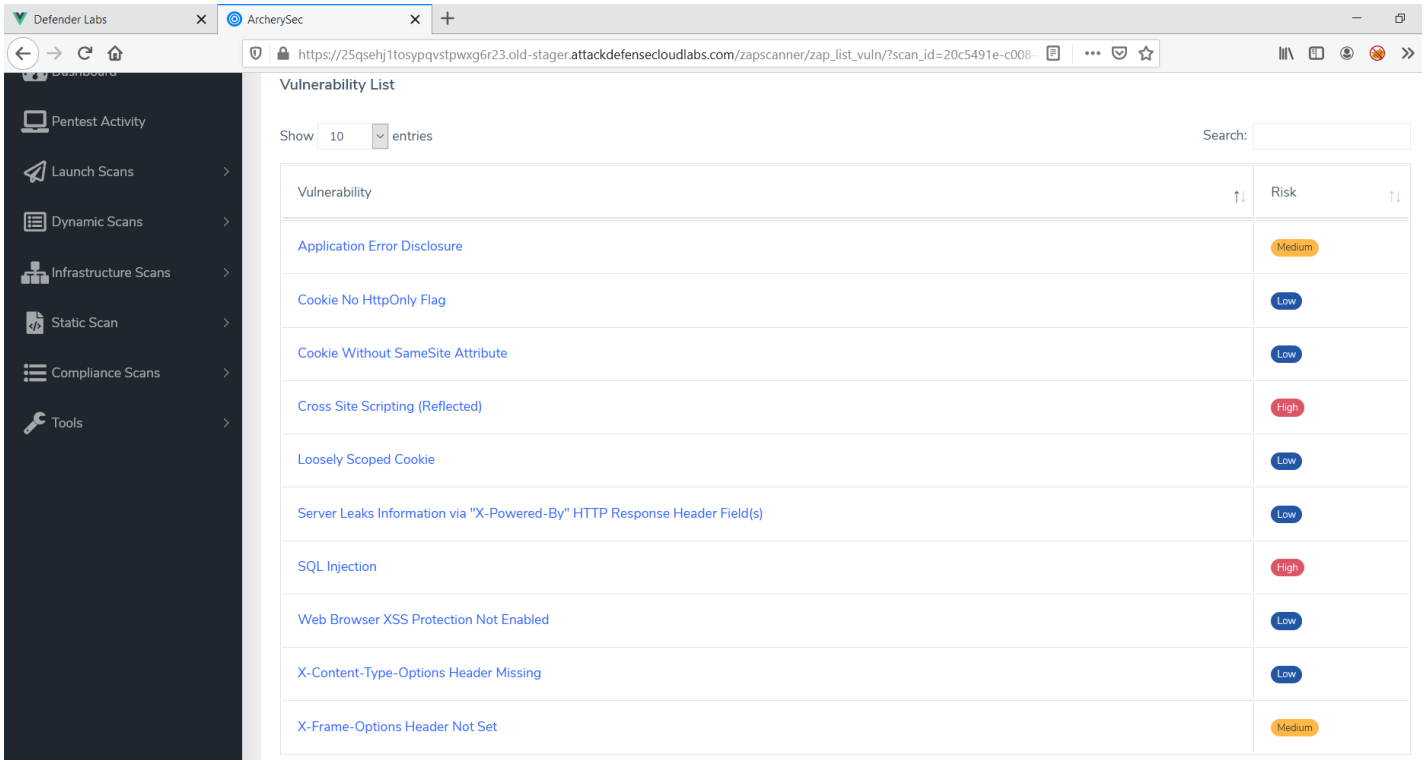
The summary is available for the scan performed on school-homework website.

Note: It could take some time to scan and generate the report. Refresh the page in between time intervals to check.

Step 3: Scroll down to the “Dynamic Scan List”



Click on the scanned website name “http://school-homework”



Note: The results from the scan can vary. Sometimes some more results are shown but sometimes not, as OWASP ZAP is performing Quick scan in the background.

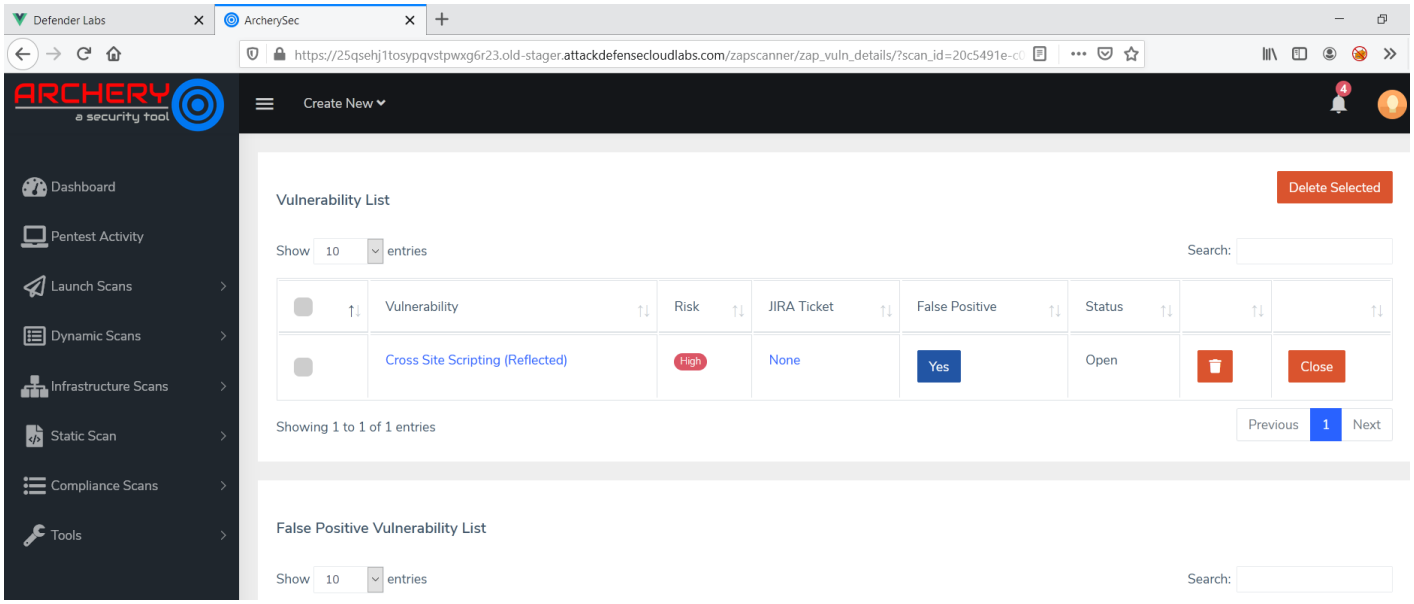
Issues Detected

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

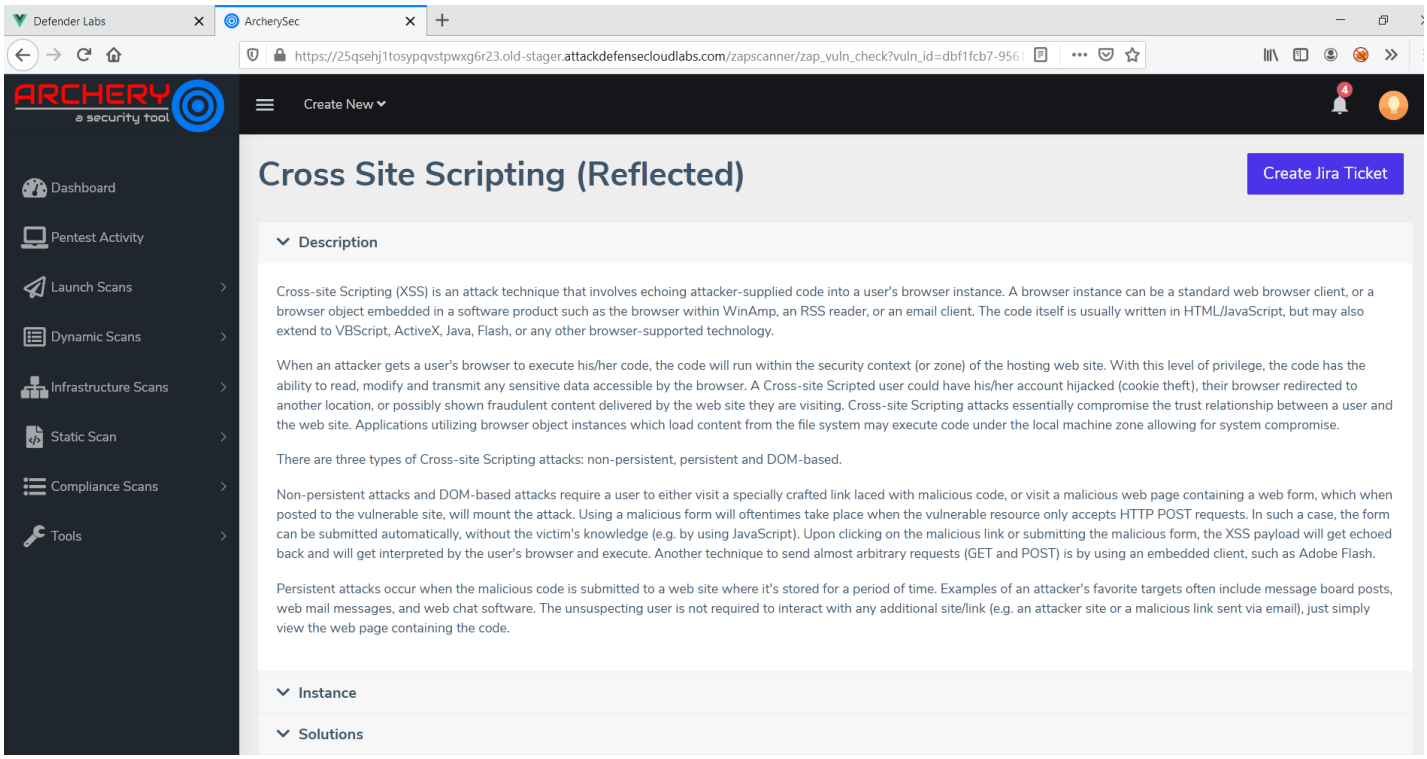
Note: Only the ‘Medium’ and ‘High’ risk issues are written above.

Step 4: The details on these issues can be checked by clicking on the issue name.

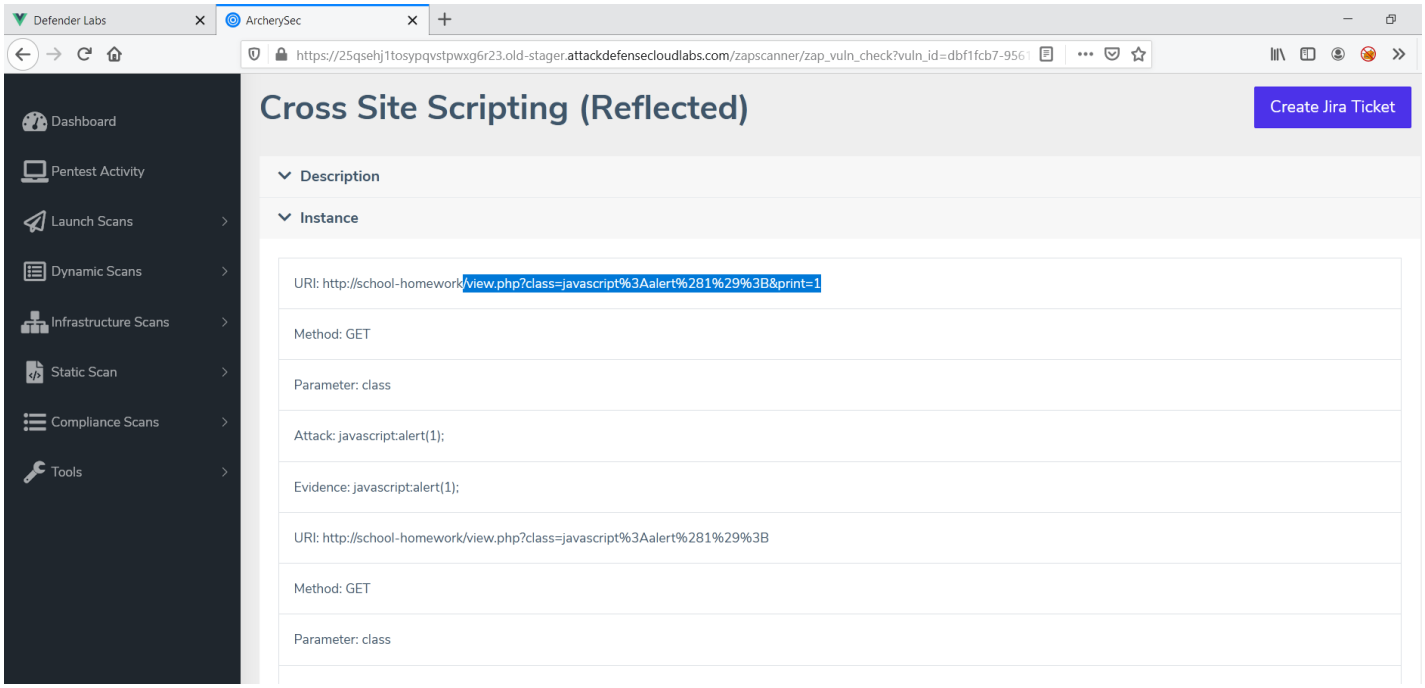
Check the endpoints affected with XSS vulnerability.



Click on the vulnerability name “Cross Site Scripting (Reflected)”.



Click on the “Instance” drop-down to check the vulnerable endpoint.

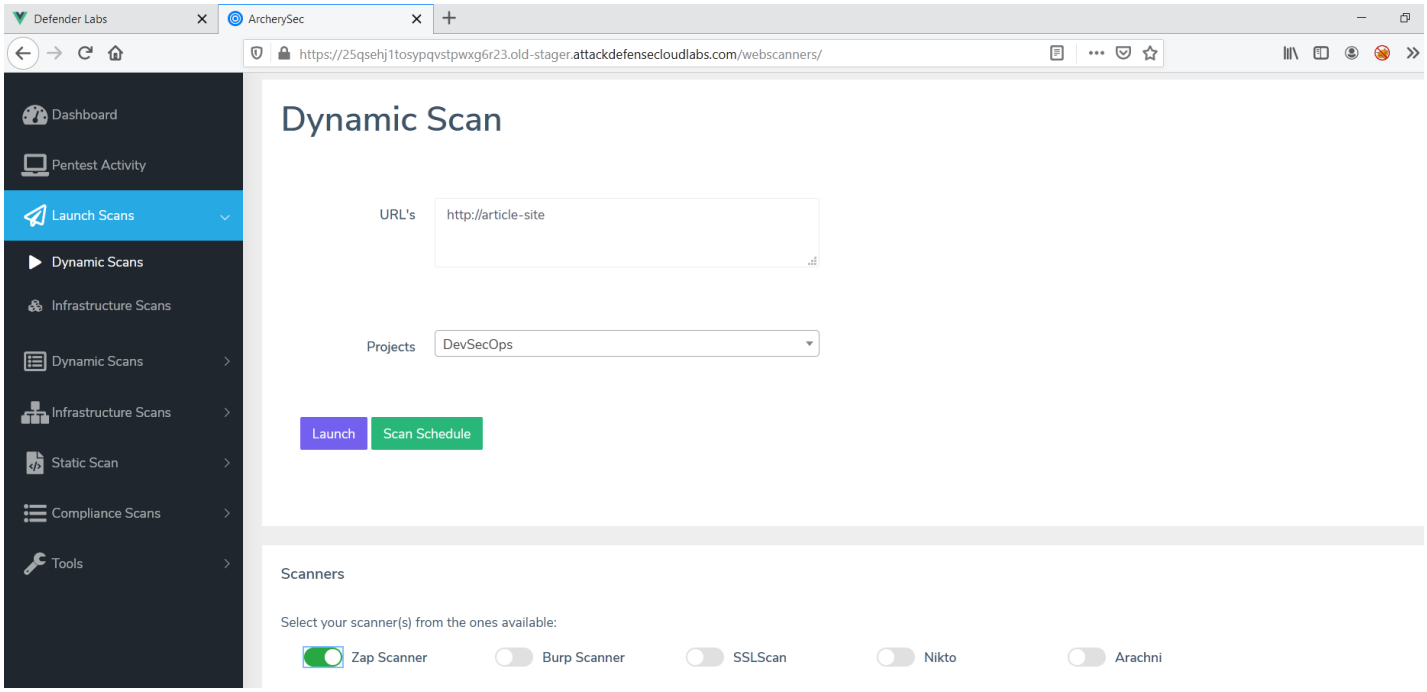


The XSS payload and the vulnerable endpoint is shown in the report.

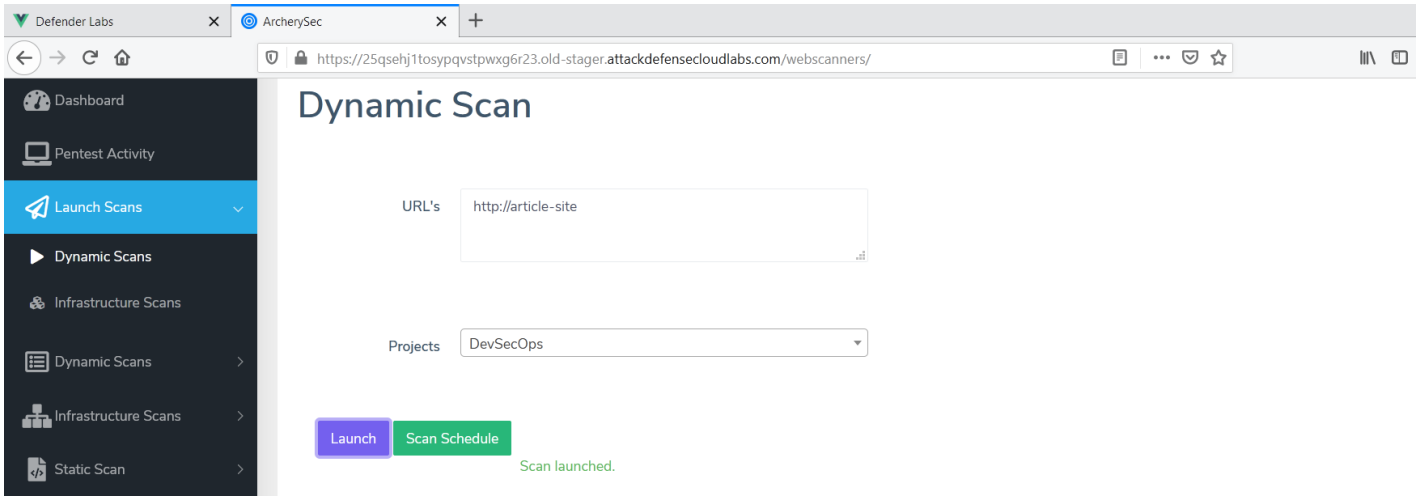
Example 2: Article Site

Step 1: Navigate to the “Dynamic Scans” sub-section under “Launch Scans” section and enter the URL in the URL’s field and select “Zap scanner”.

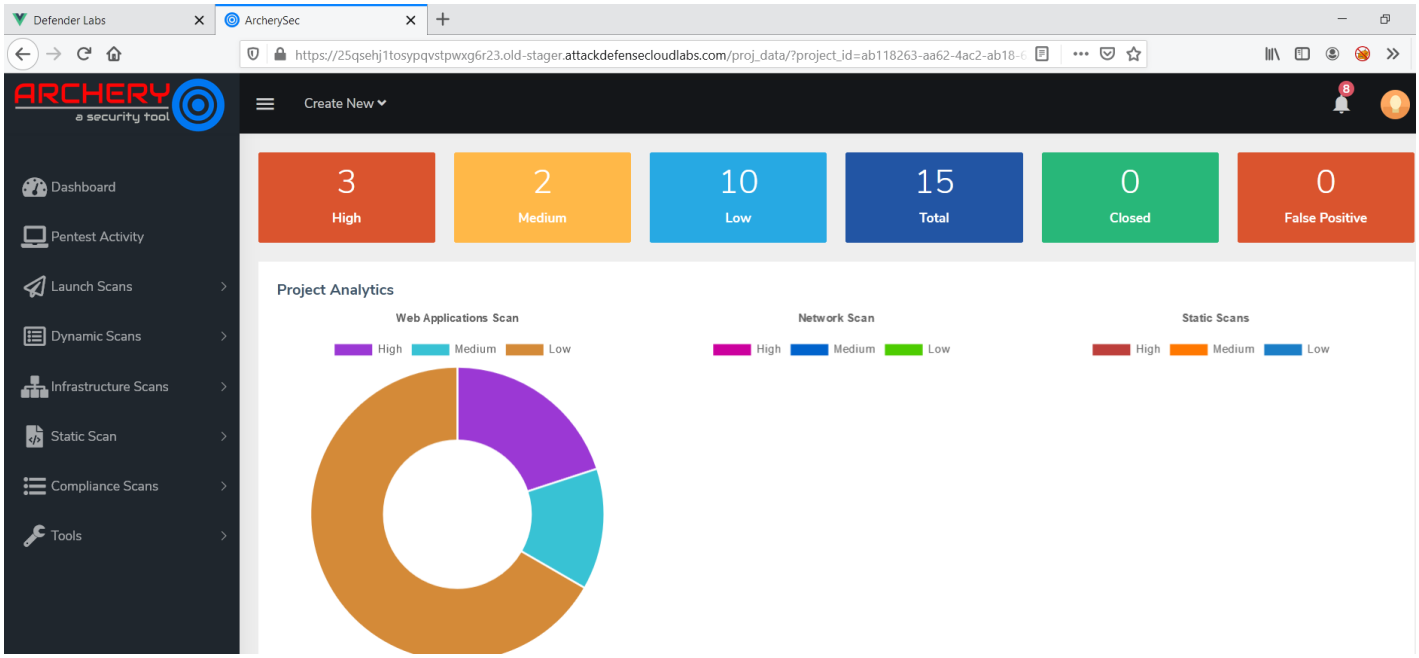
URL: http://article-site



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

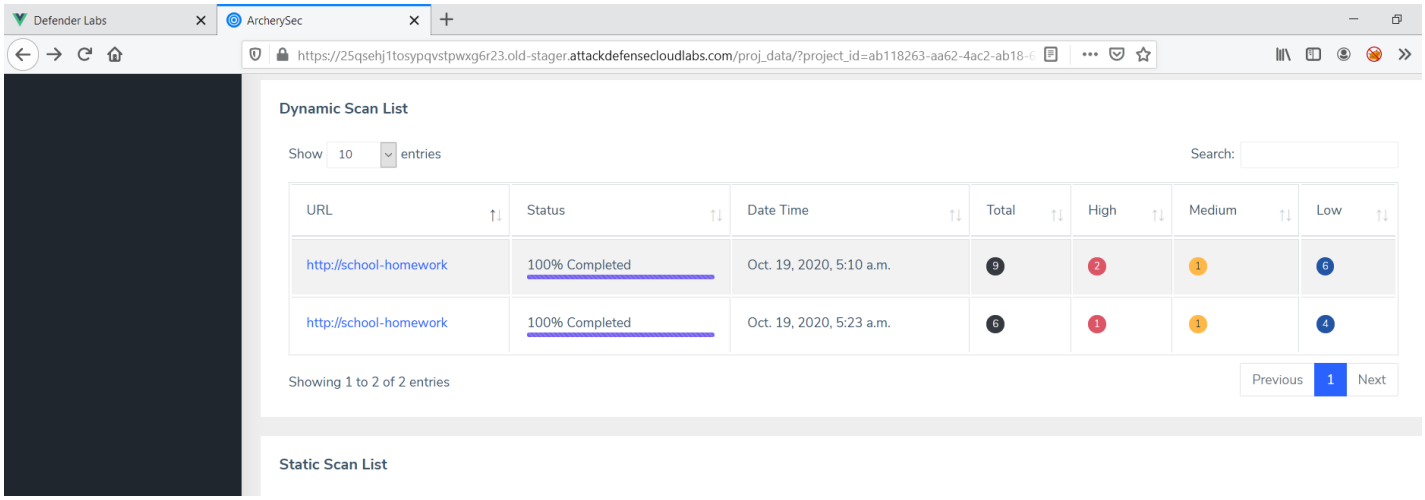


Step 2: Navigate to the “DevSecOps” project tab located on the Dashboard.

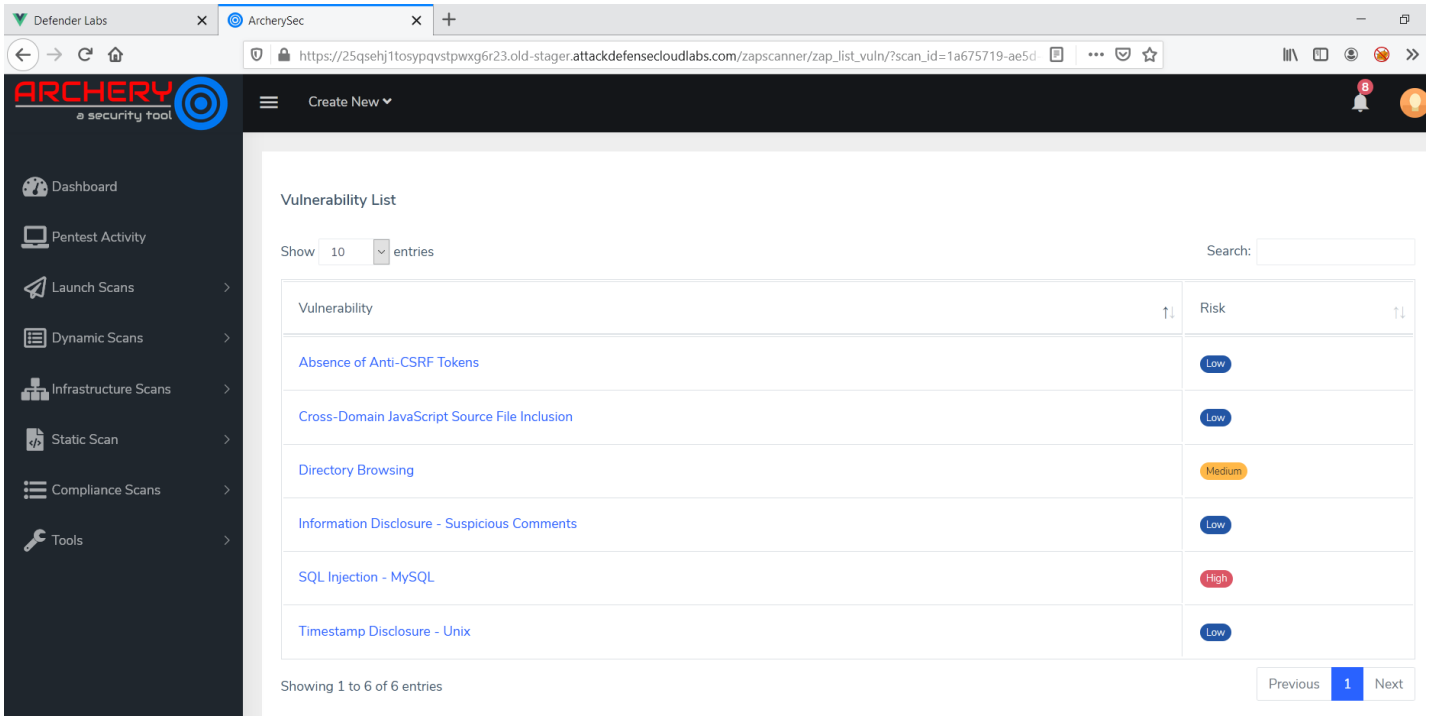


The sheet has been updated with the new scan report. It might take some time to reflect results on the page

Step 3: Scroll down to the "Dynamic Scan List"



Note: The list shows the same URL name. This is a glitch and to check the results of the article-site, click on the URL name with the latest timestamp.

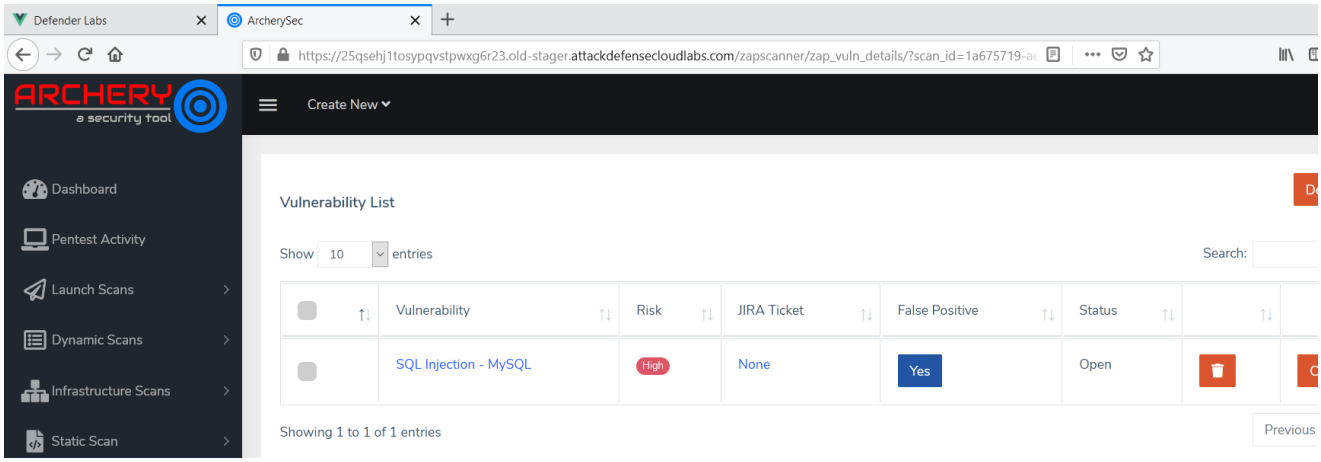


Issues Detected

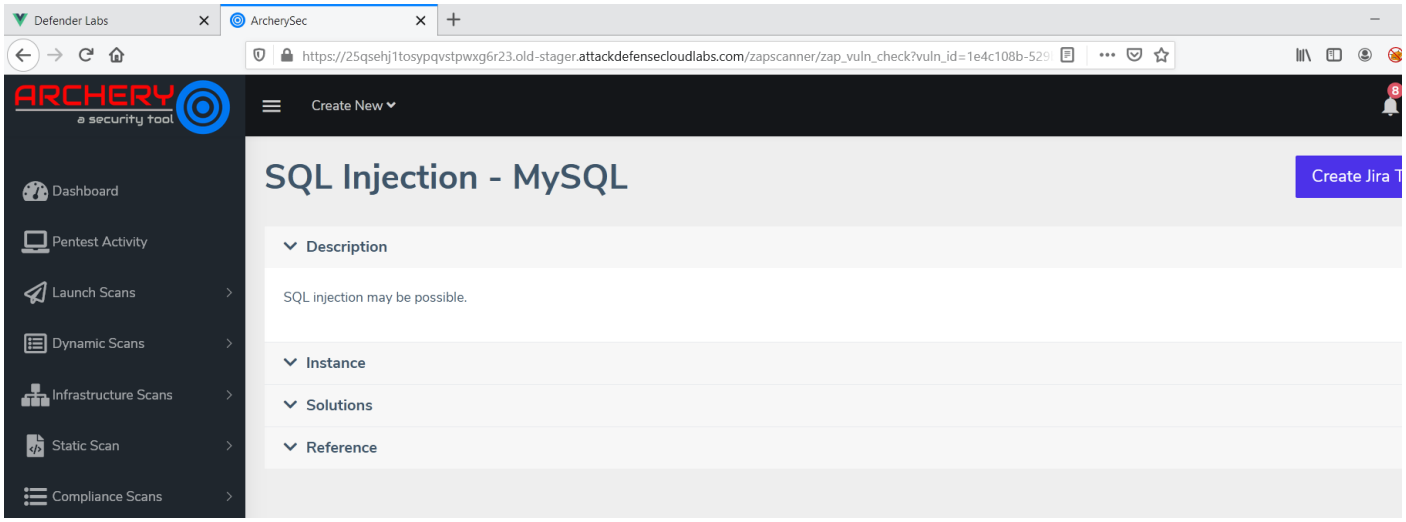
- Directory Browsing
- SQL Injection

Step 4: The details on these issues can be checked by clicking on the issue name.

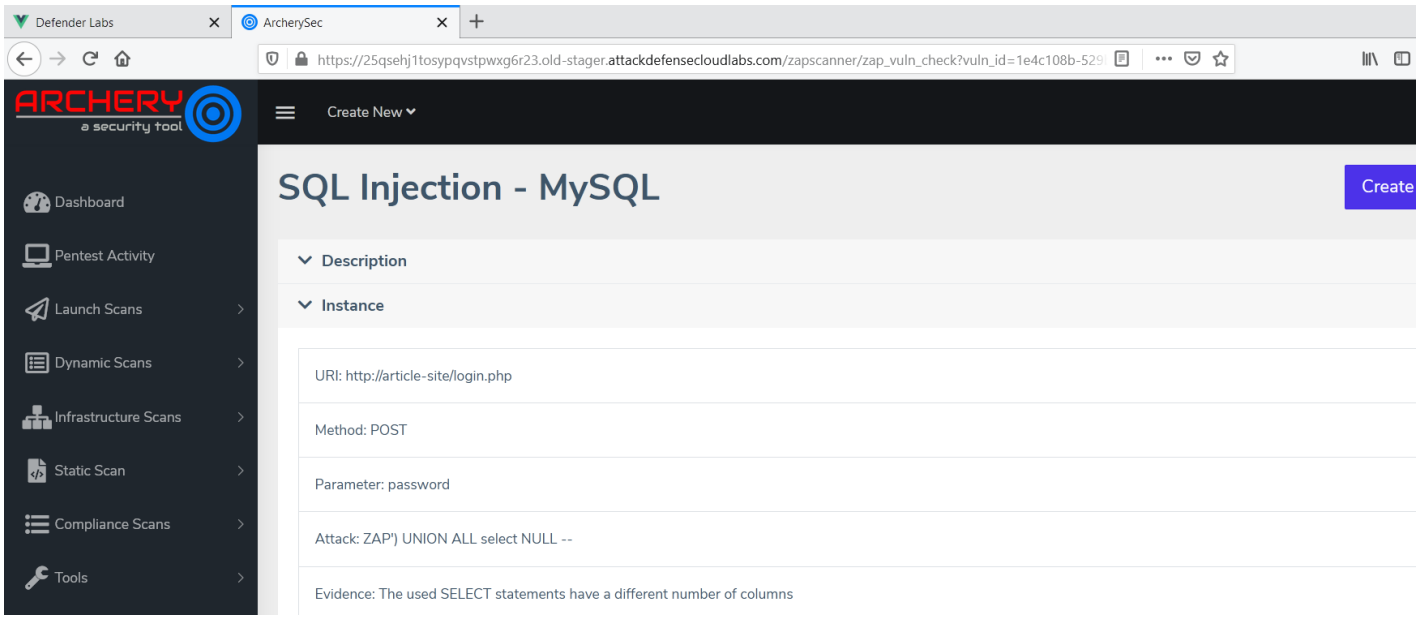
Check the endpoints affected with SQL Injection vulnerability.



Click on the vulnerability name “SQL Injection - MySQL”



Click on the “Instance” drop-down to check the vulnerable endpoint.

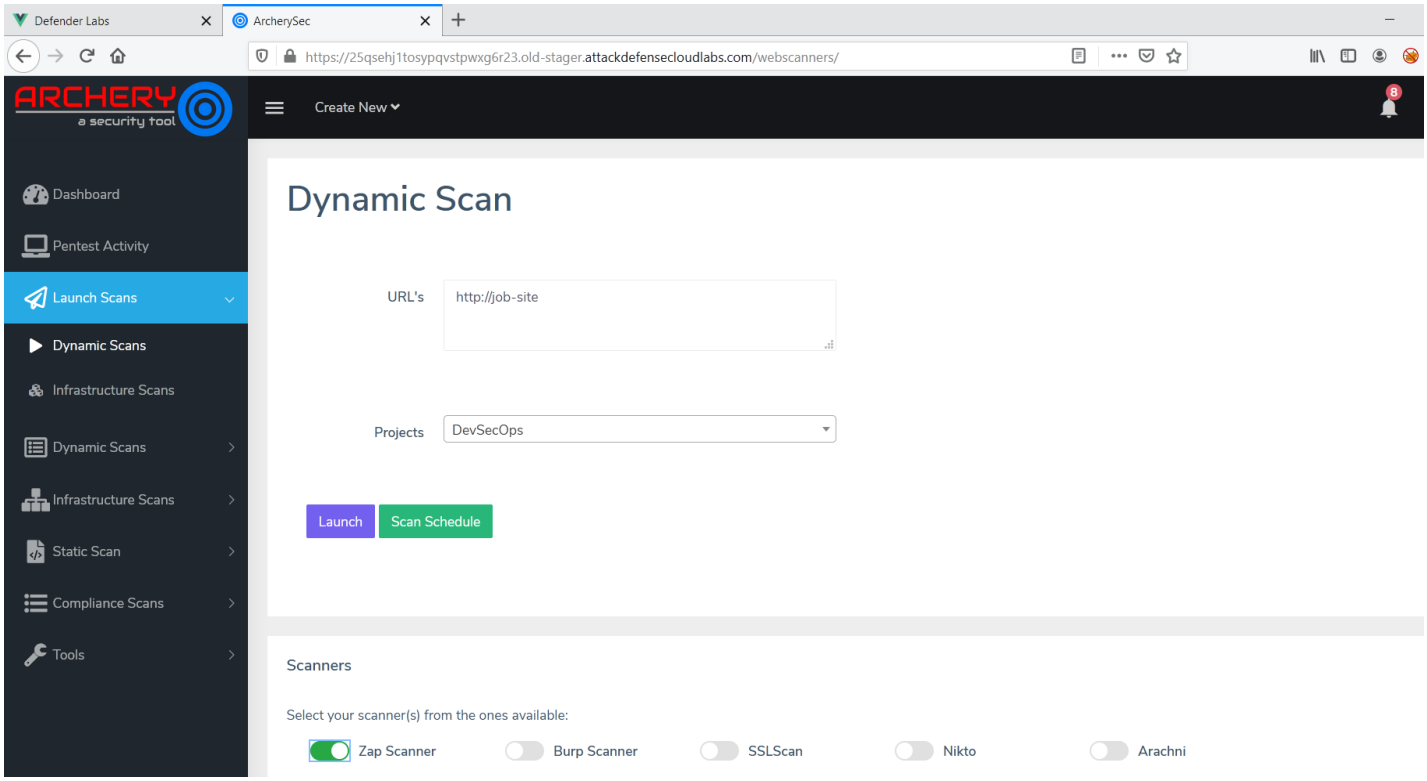


The POST request contains the payload in the password field which is vulnerable to SQL injection attack.

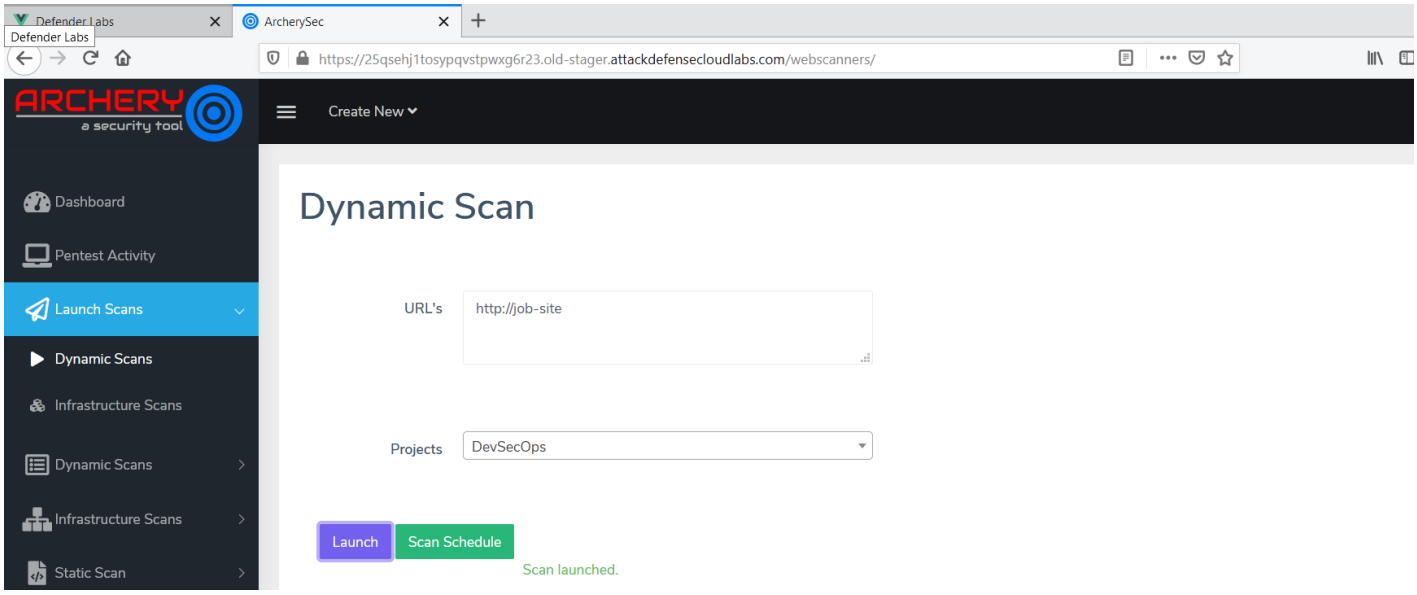
Example 3: Job Site

Step 1: Navigate to the “Dynamic Scans” under “Launch Scans” section and enter the URL in the URL’s field and select “Zap scanner”.

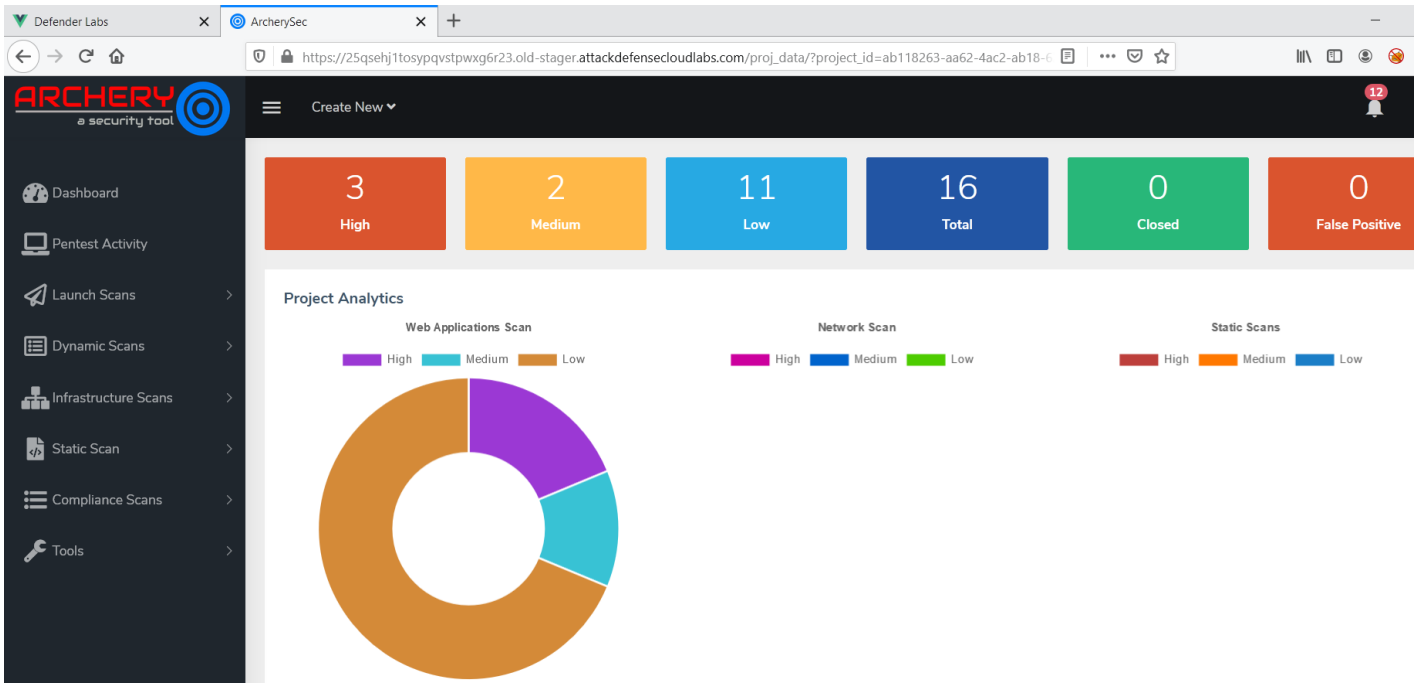
URL: http://job-site



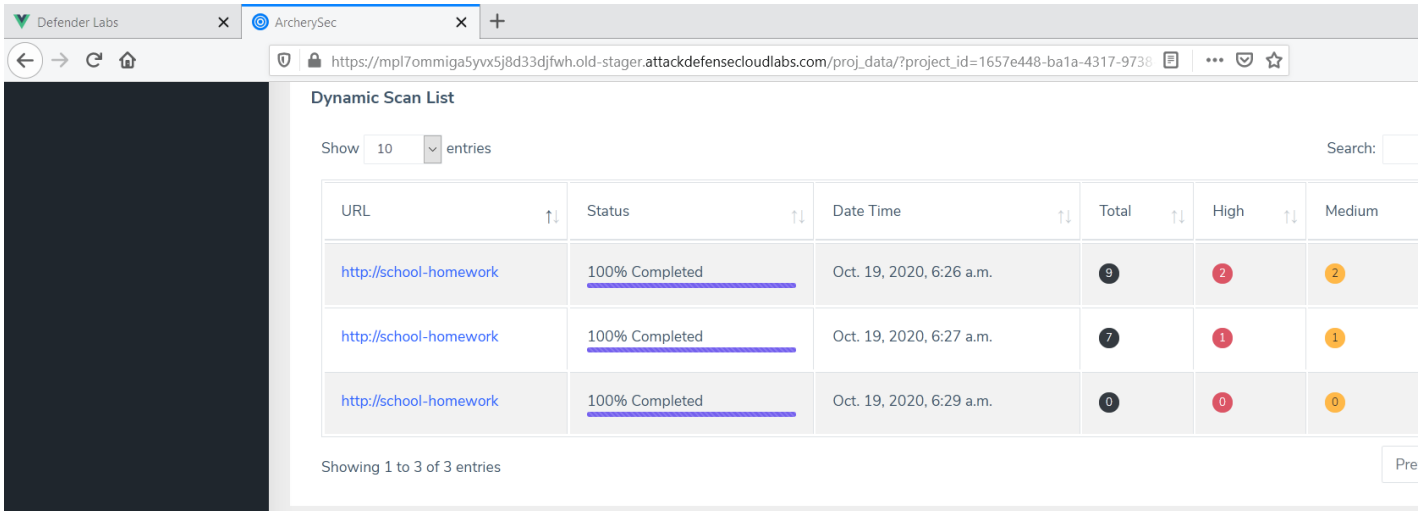
Click on the Launch button.



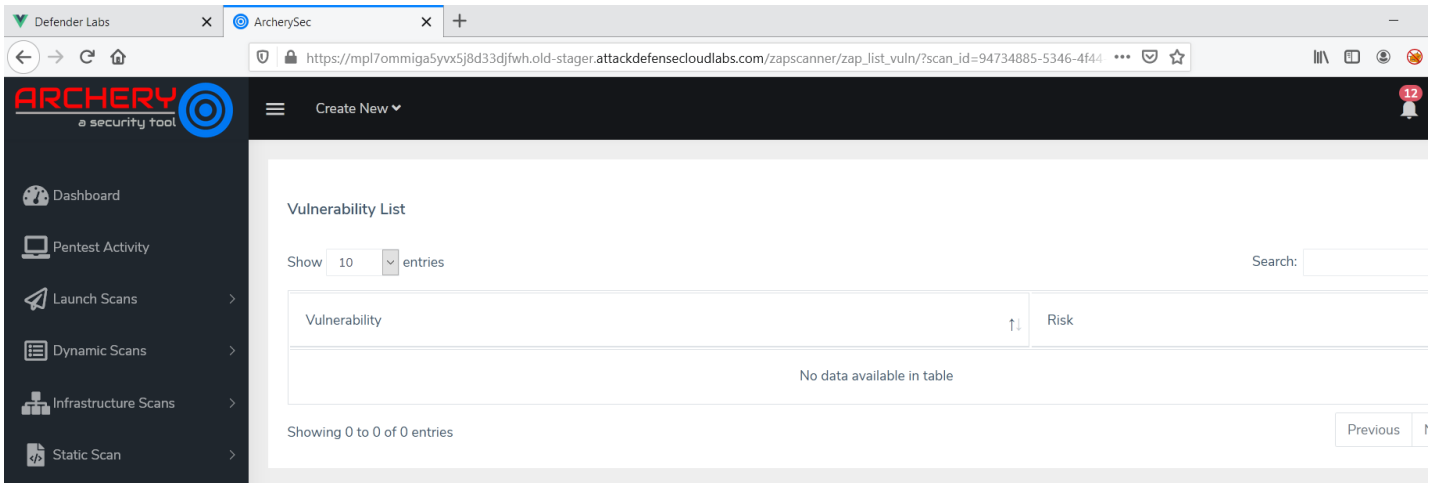
Step 2: Navigate to the "DevSecOps" project tab located on the Dashboard.



Step 3: Scroll down to the “Dynamic Scan List”



Click on the URL name with the latest timestamp



There were no issues found. The results might vary from instance to instance.

Learnings

Perform dynamic code analysis on web applications using ArcherySec.