VULNERABILITY SCANNING USING BURPSUITE TO FIND VULNERABILITIES IN CHAMELEON WEBSITE.

AASHRITH GK- 220573707

CONTENTS

BURPSUITE VULNERABILITY SCANNER:

A dynamic application security testing (DAST) online vulnerability scanner that is automated is known as Burp Scanner. Replicating the activities and procedures of a trained manual tester is the purpose of this design. The Burp Scanner is capable of handling practically any target. It is able to handle the obstacles that scanning current online applications might provide because of its complex features, which include state management and automatic logins. Scans typically consist of two primary stages, despite the fact that the operations that are carried out during a scan might vary based on the specific setup and target.

Crawling: is the process by which the scanner provides a catalog of the application's content as well as the navigational pathways that are included inside it. The application is navigated by Burp Scanner in a manner that is roughly equivalent to how a person would do it. In order to generate a map of the application's content, it does actions such as following links, submitting forms, and logging in at appropriate points.

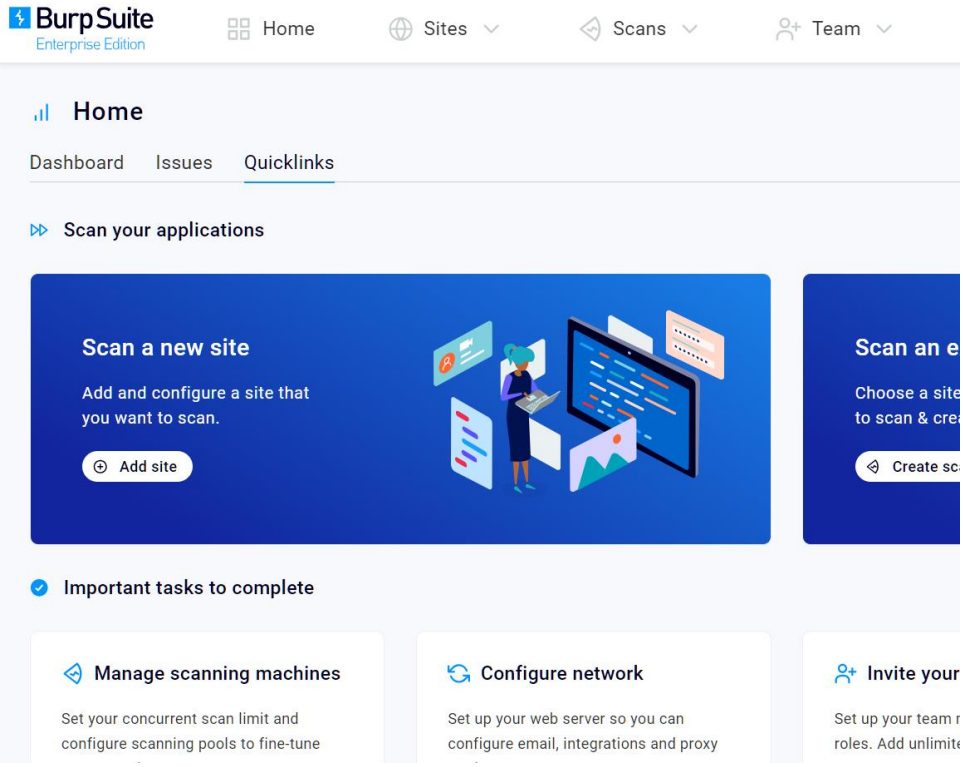
Auditing: The scanner examines the traffic and behavior of the program to uncover several types of problems, including security vulnerabilities. Burp Scanner interacts with the program by sending it a series of queries and then analyzing the responses it receives. The information that was gathered during the crawl phase is used with the purpose of determining the most effective method of operation.

Personalization: Users have the flexibility to customize the scanning rules and regulations in order to personalize the scanning process to meet their own individual needs.

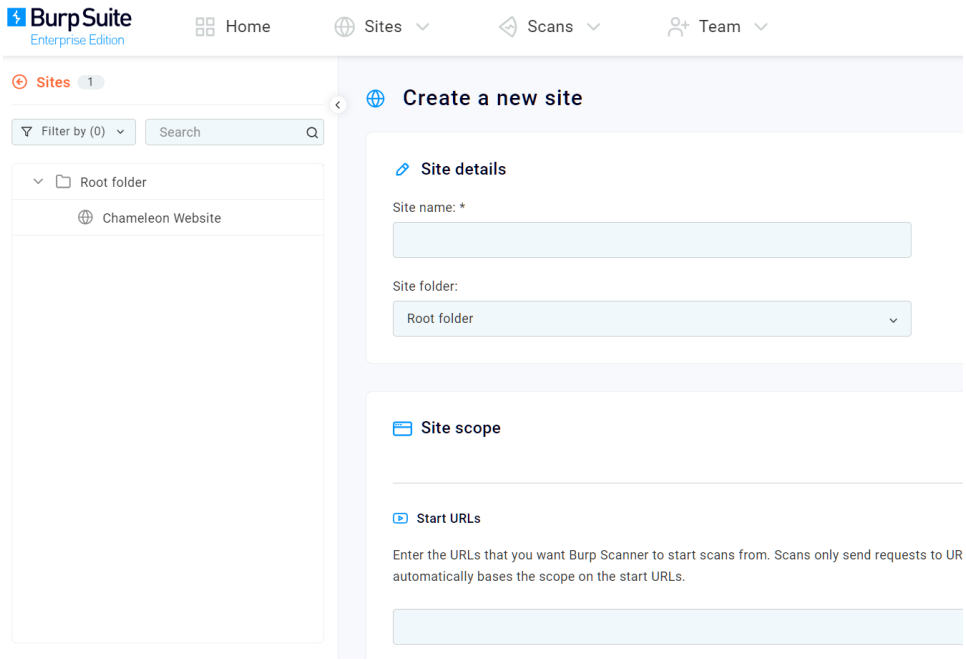
Burp is capable of functioning as a proxy, which enables users to intercept and modify HTTP requests and answers in order to analyze the behavior of applications. This is accomplished via the usage of Vega's monitoring capabilities.

SETTING UP BURP FOR SCAN:

Open Burpsuite.



Schedule a New scan.



The following are some of the prerequisites that may be used to setup Burpsuite before we begin the scan:

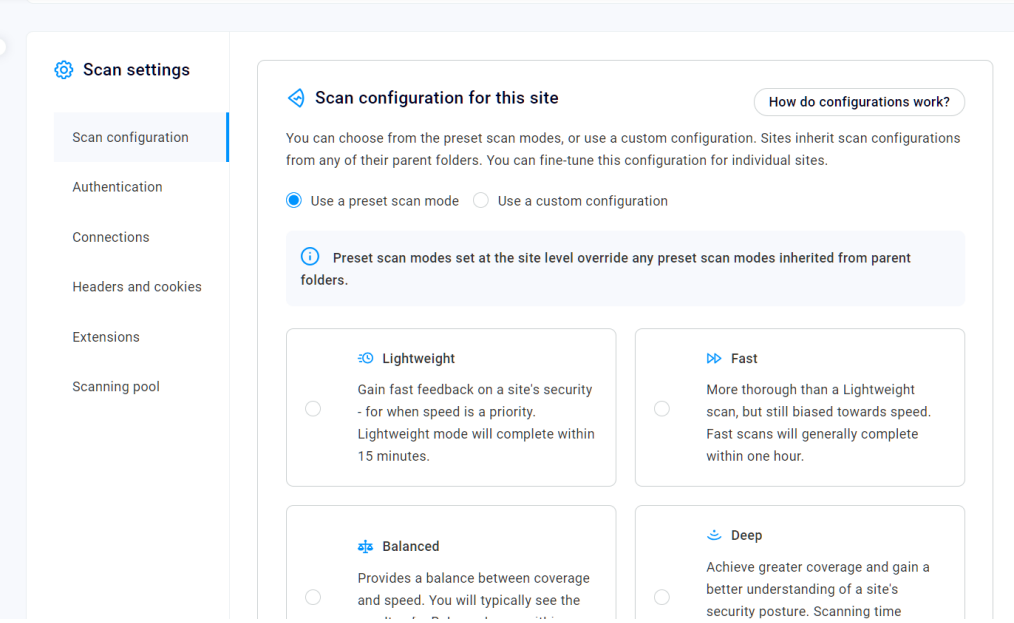
• Proxy Settings: If necessary, configure proxy settings inside Burpsuite to redirect traffic via the program. To define the scope of your scan, you must first indicate the website or web application that you want to examine.

The URL. You also have the option of specifying whether or not to include certain URLs or subdomains.

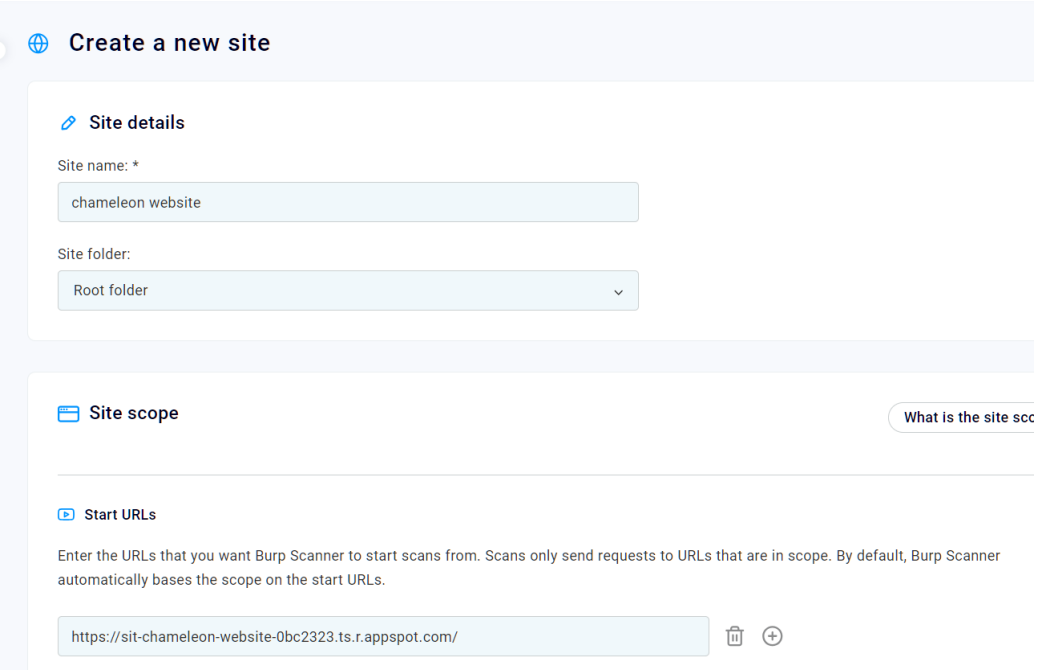
• Authentication: It is recommended that Burpsuite be configured to log in using the required credentials if the website needs authentication.

Configure scan policies and rules to indicate the vulnerabilities you wish to test for. This is referred to as the "scan policies" feature.

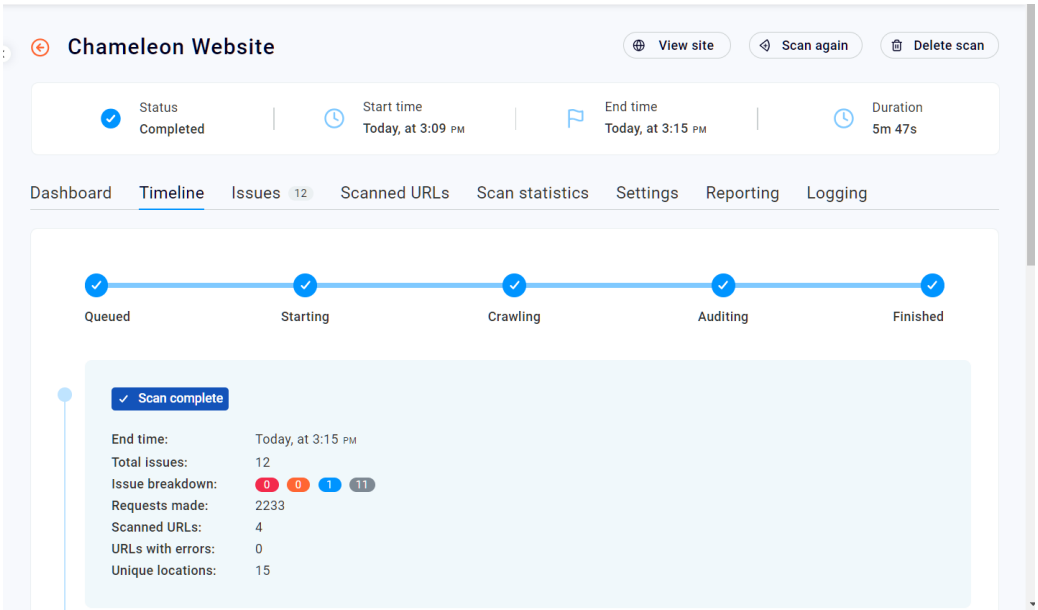
Adjust the parameters that are associated with the process of crawling the website, such as the maximum depth and the time between queries. This is referred to as the Crawling Options.



Enter the Chameleon website URL to save and start the scan

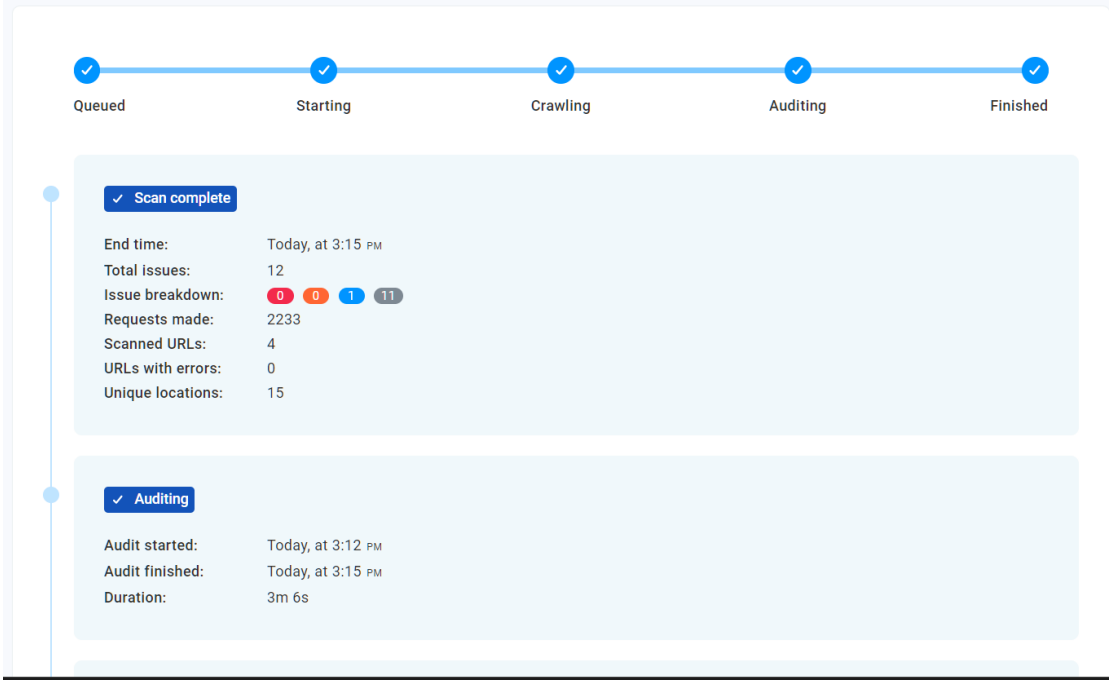


Start the scan



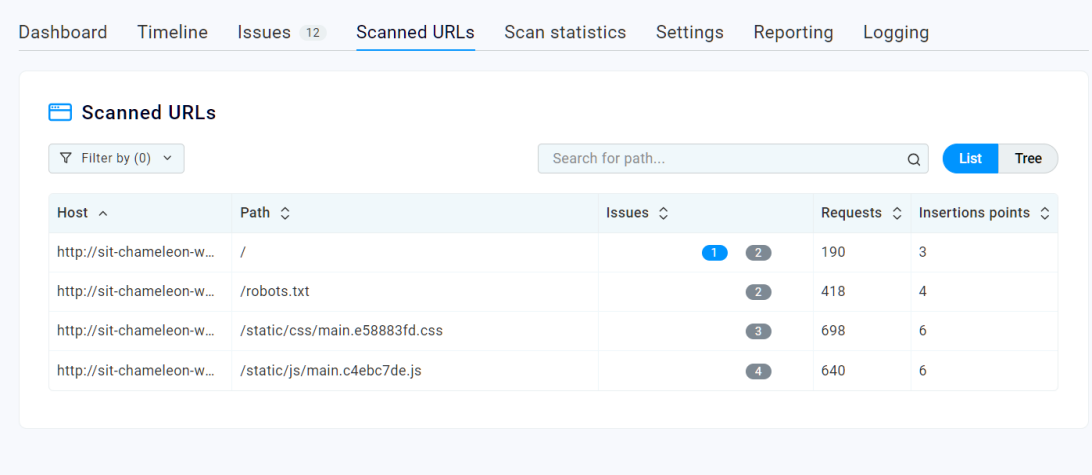
Track the Scan

As soon as you hit the finish button, Burpsuite will begin scanning the specified website and running security checks according to your settings. You can keep track of the scan's progress and see the vulnerabilities found as they happen.

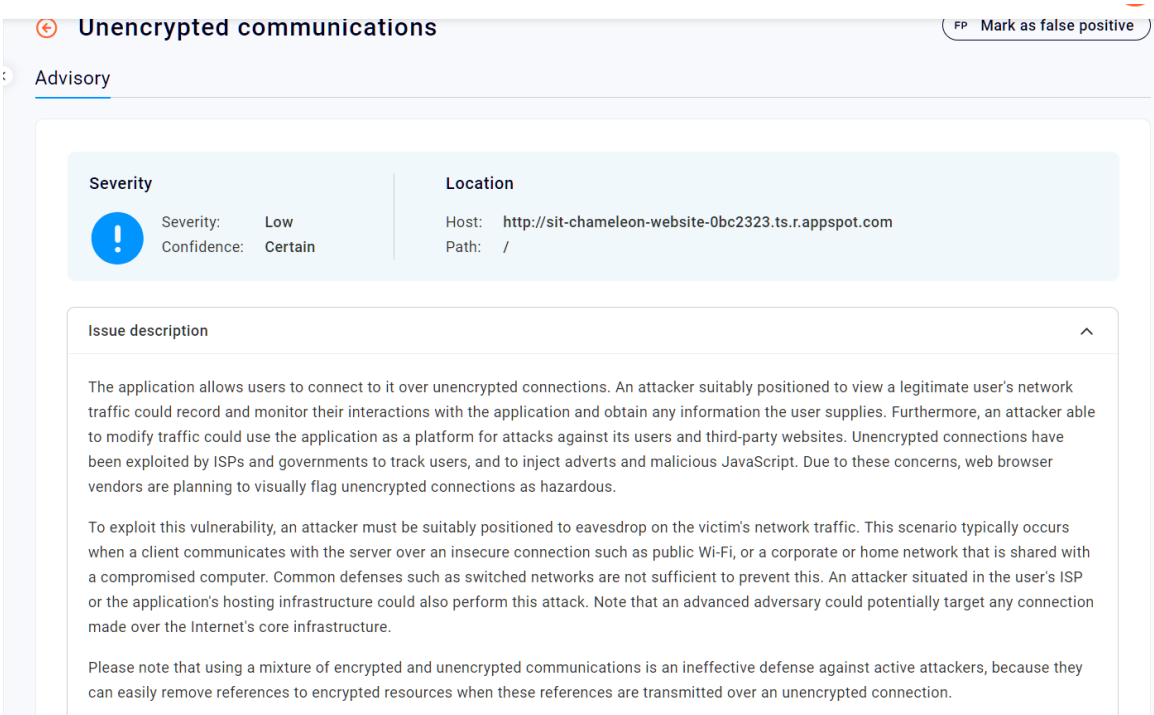


Review the results:

Once the scan is finished, Vega will provide a report that highlights any vulnerabilities that were detected. It will describe the vulnerabilities in detail, including how serious they are and how to fix them.



About the vulnerabilities:



To prevent attacks like the one described above, applications should encrypt data in transit between the client and server using SSL or TLS. If you want customers to avoid connecting to your server using unsecured connections, you should use the Strict-Transport-Security HTTP header.

This Risk is vulnerable to:

1. CWE-326: Inadequate Encryption Strength

2. CAPEC-94: Man in the Middle Attack

3. CAPEC-157: Sniffing Attacks

Here are some of the other vulnerabilities found in the chameleon: