Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 12/09/2023

Assignment Details

Assigned Date: 11/09/2023

Due Date: 12/09/2023

Topic: Spidering (Directory BruteForce)

Introduction

Spidering is the process of systematically navigating a website's structure by following links from one page to another. It is commonly used to create a map of a website, identifying its various pages and resources. This process is crucial for understanding a web application's architecture and how different components interact.

Crawling, on the other hand, is the automated traversal of web pages by a web crawler or bot. Search engines often use crawlers to index web content for search results. In the context of web security, crawling involves programmatically navigating a website to discover its pages and endpoints. This can be used to identify potential vulnerabilities or misconfigurations in the application.

Crawl and audit is a security testing process that combines crawling and auditing. It entails systematically scanning a web application's pages, forms, and functionalities to uncover security vulnerabilities, such as SQL injection, cross-site scripting (XSS), or insecure authentication mechanisms. This process helps security professionals assess and improve the security posture of a web application.

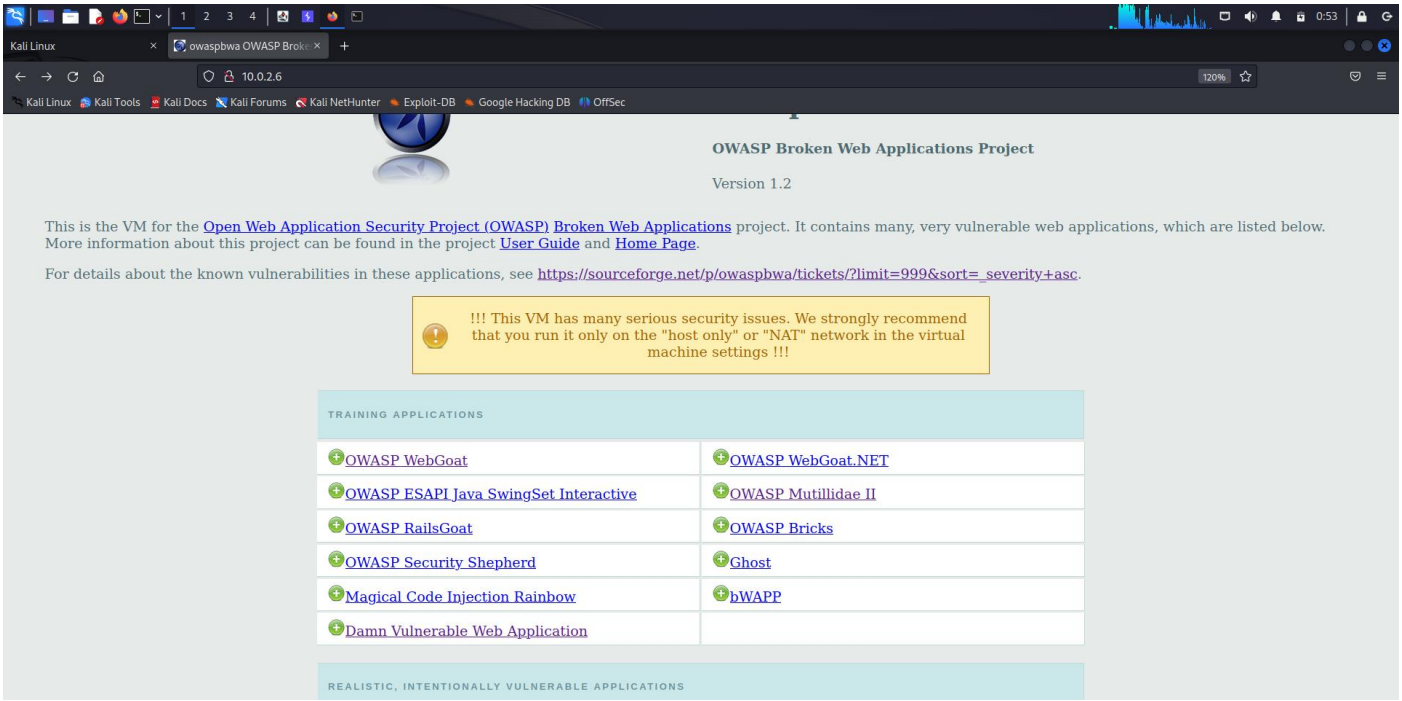
Spidering with Burp Suite is a specialized technique within the field of web application security testing. Burp Suite is a popular cybersecurity tool that includes a web spidering feature. Security professionals use it to automatically crawl a web application, map its structure, and identify potential security issues. Burp Suite's spidering capabilities are particularly useful for finding hidden or less obvious vulnerabilities, making it a valuable tool in the arsenal of ethical hackers and security analysts.

Scanning for vulnerabilities is the core of Burp Suite's automated testing capability. Burp Scanner can crawl a target to discover content and functionality, and then audit what it finds for vulnerabilities. Alternatively, you can use it to audit items that you have found manually.

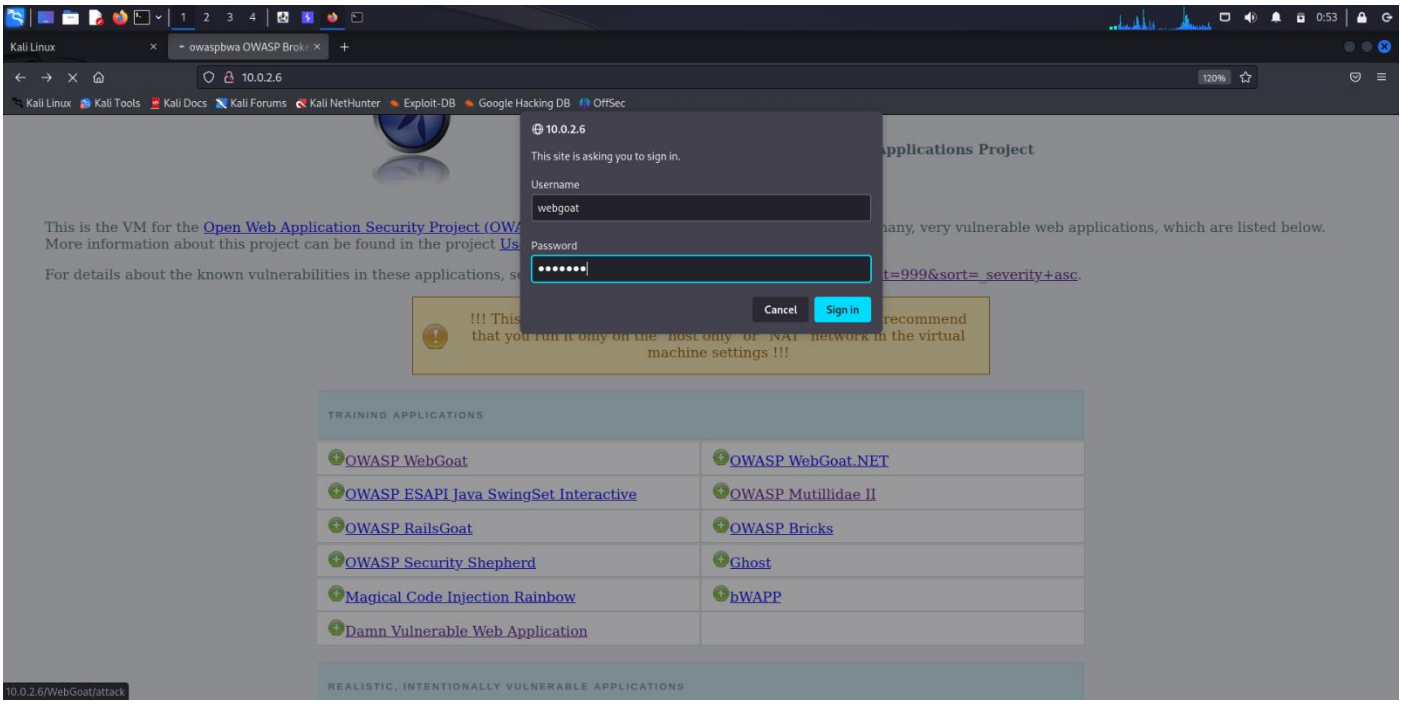
Content

OWASP (Open Web Application Security Project) Broken Web Application project

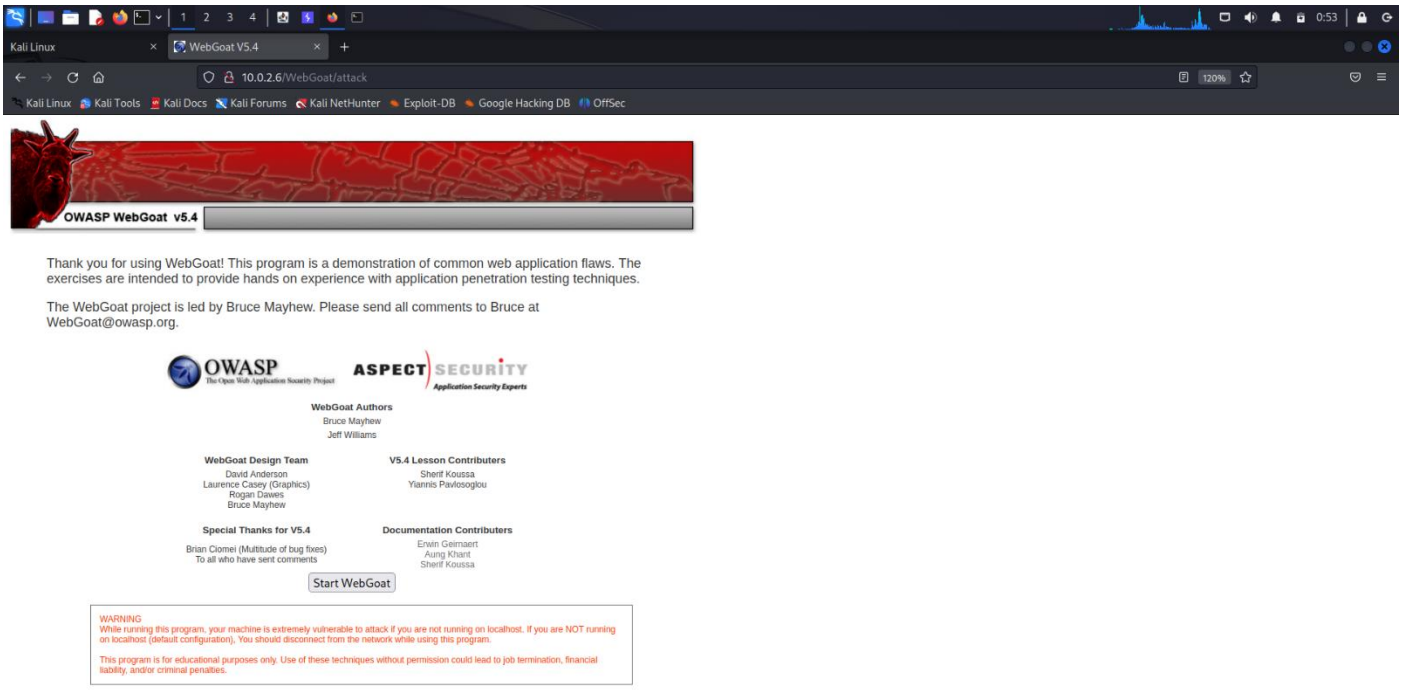
Home page of OWASP



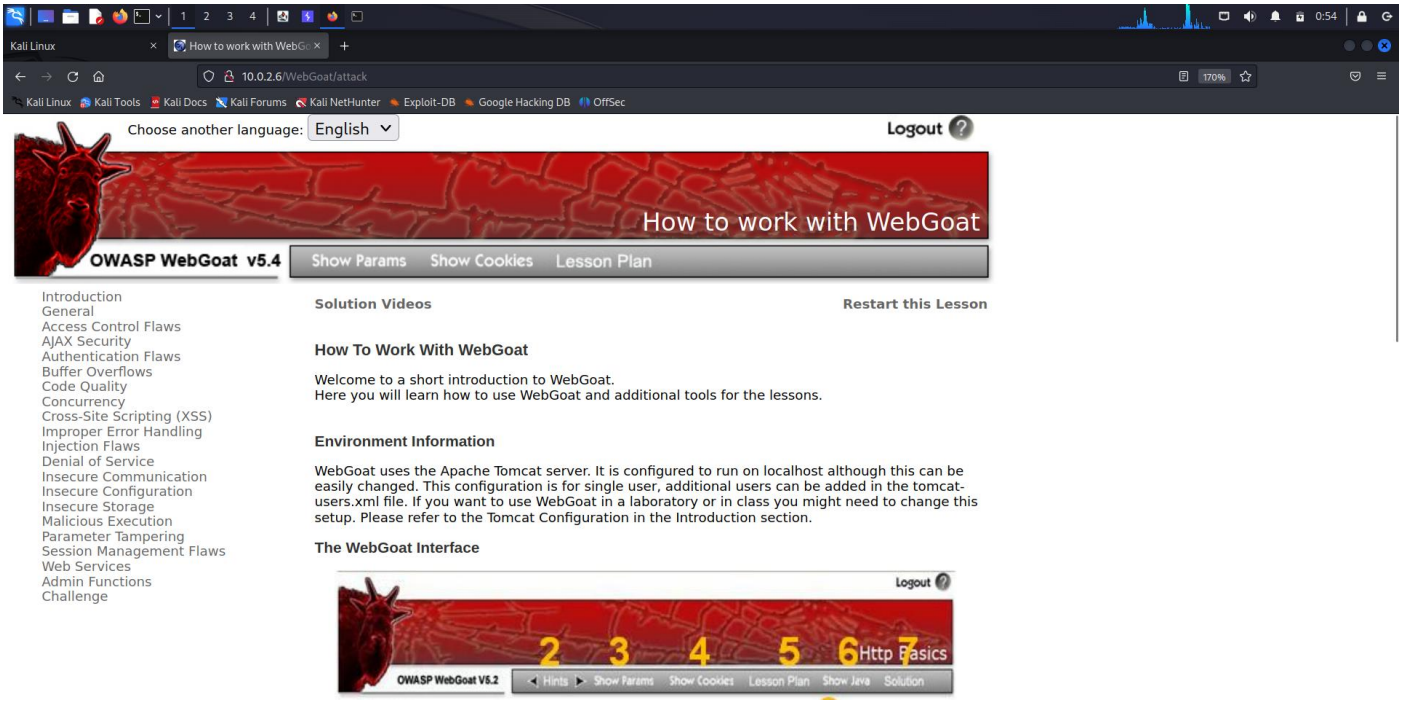
Logging into OWASP WebGoat application



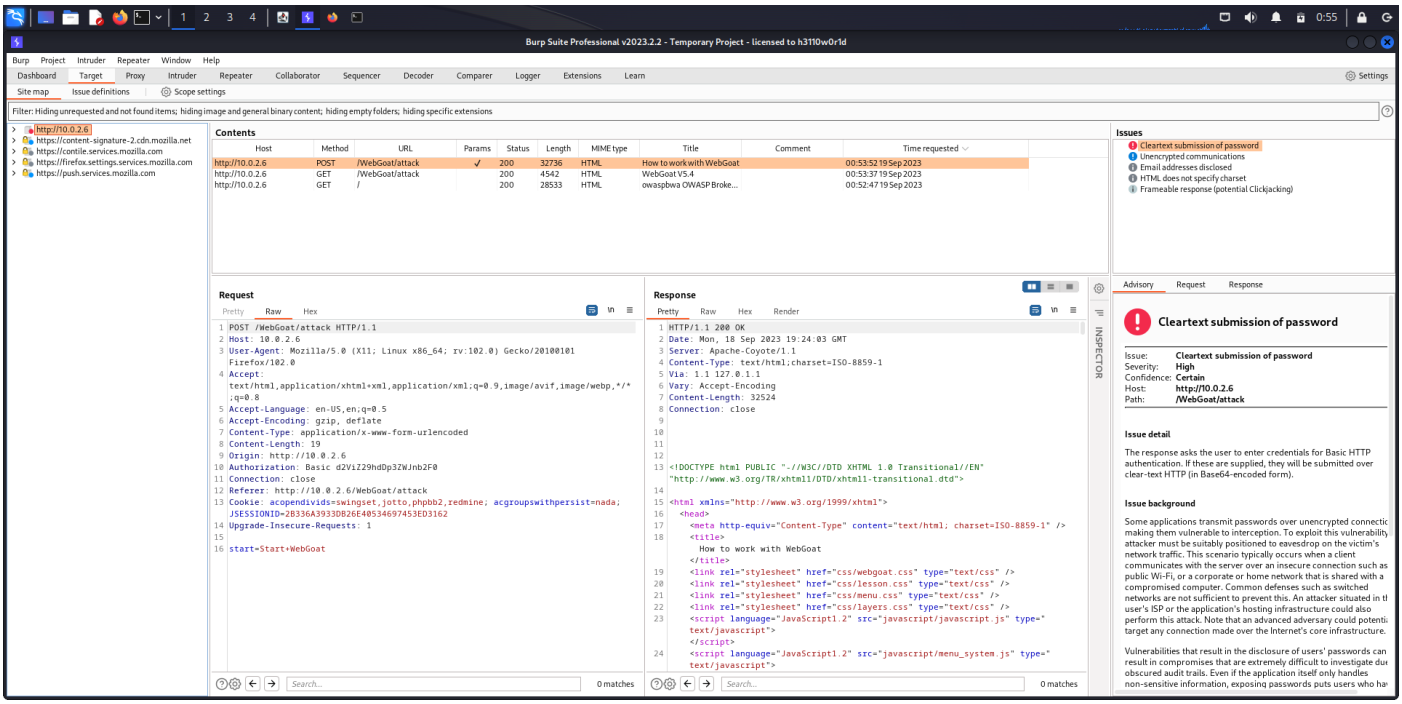
Starting WebGoat



Home page of WebGoat web application



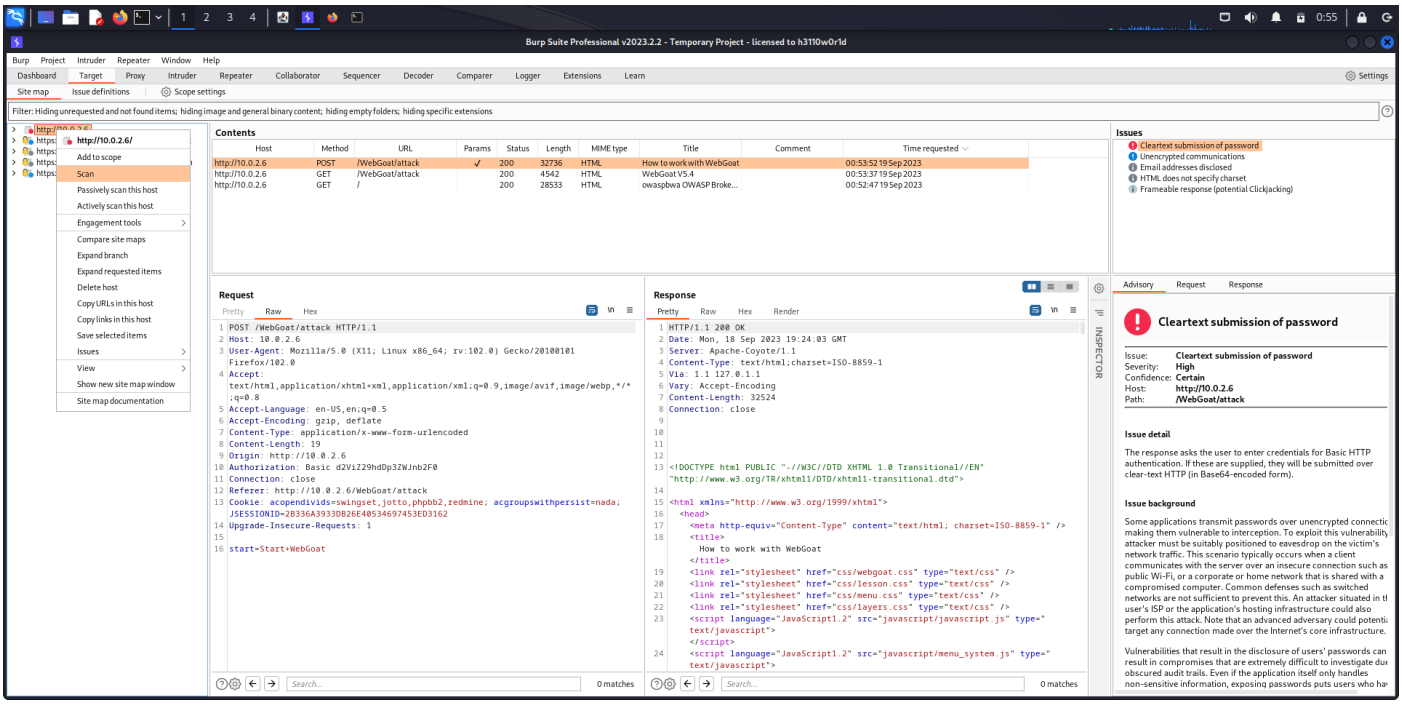
Capture the actions performed in the browser in Burpsuite.



Right click on the website address on which the scan is to be performed.

In this case, right click on http://10.0.2.6/

The option Scan is displayed in the list.

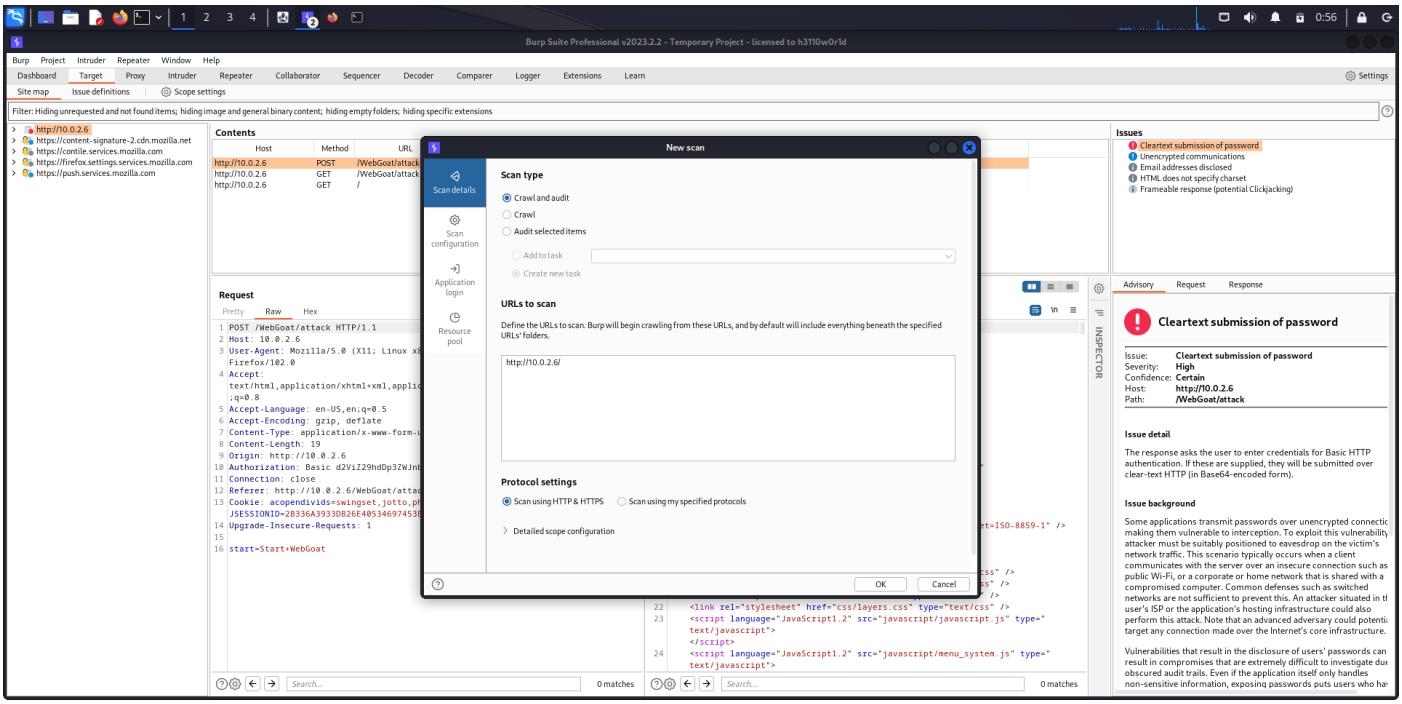


After clicking on the Scan option, a new window is opened.

The window provides all the configuration to be done to perform scanning.

First tab displays the Scan Details. Select the first button, Crawl and Audit.

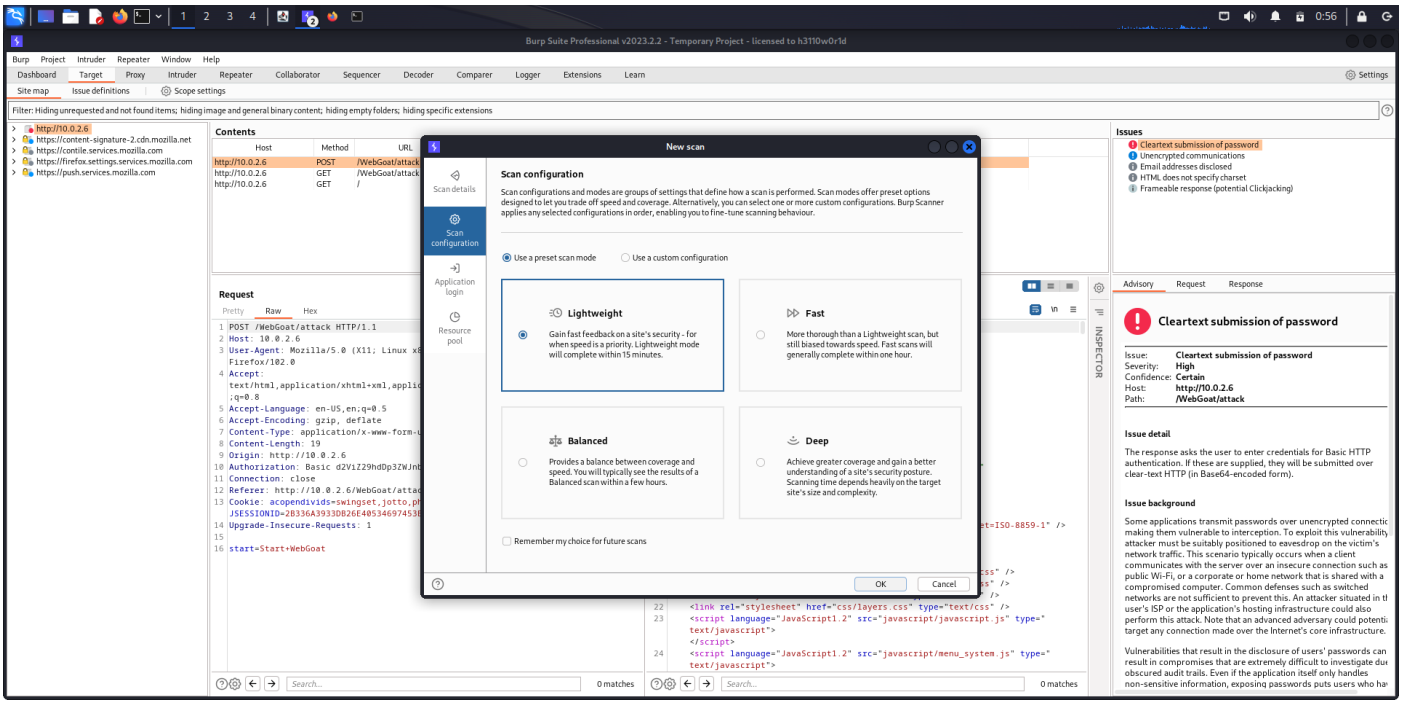
The URL to be scanned has already been selected.



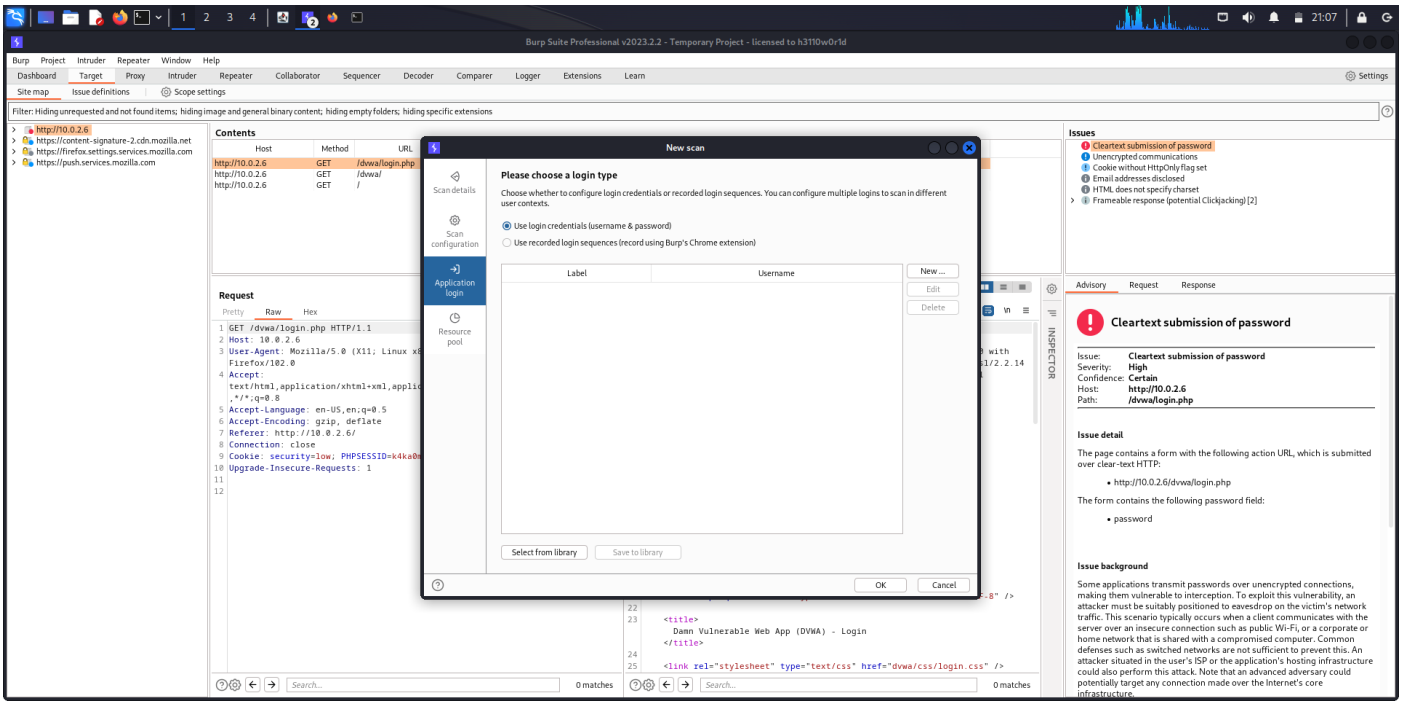
The second tab displays the Scan Configuration.

You can customize the configuration. To perform a basic crawl and audit Use a present scan mode.

Set the scan type as Lightweight.



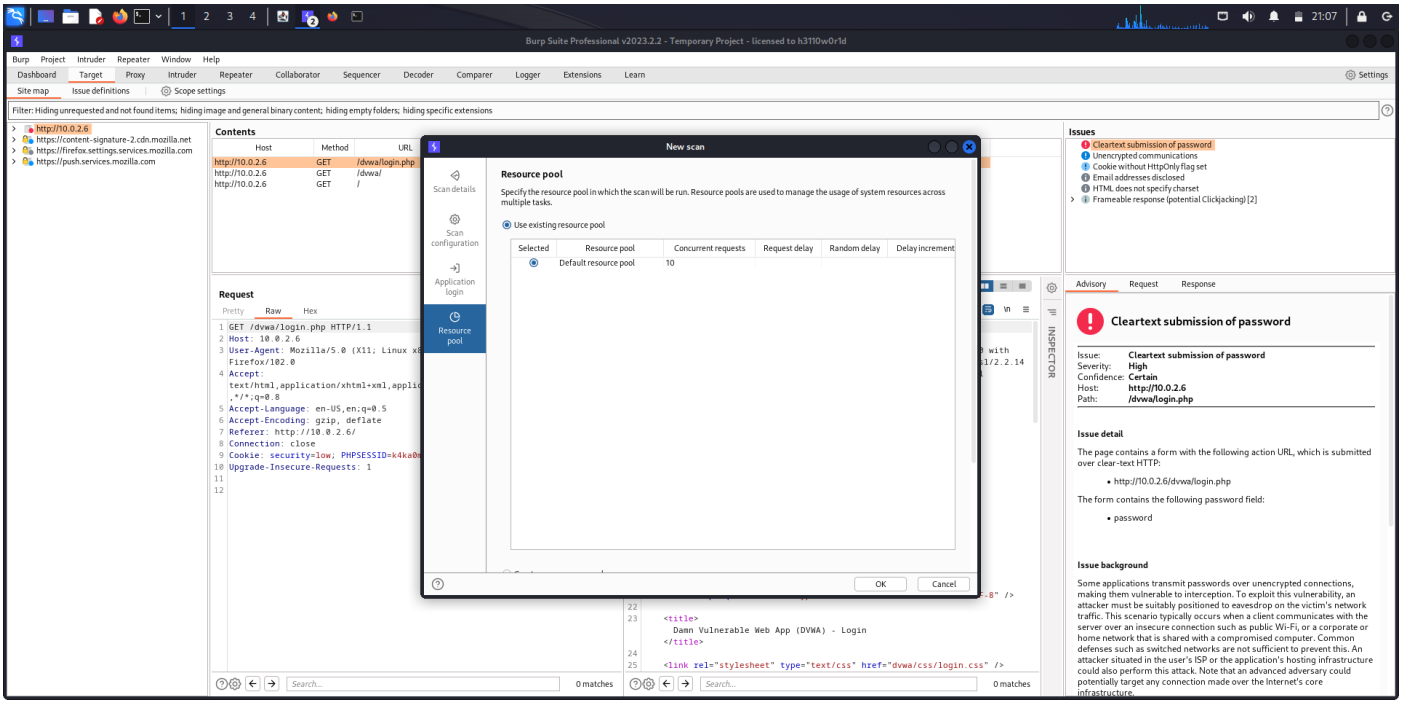
In Application Login, you can provide burp with credentials for known accounts that exists which will be used during the crawl and audit. You can add multiple login credentials, for example one for ordinary users, one for manager role within an application or an admin.



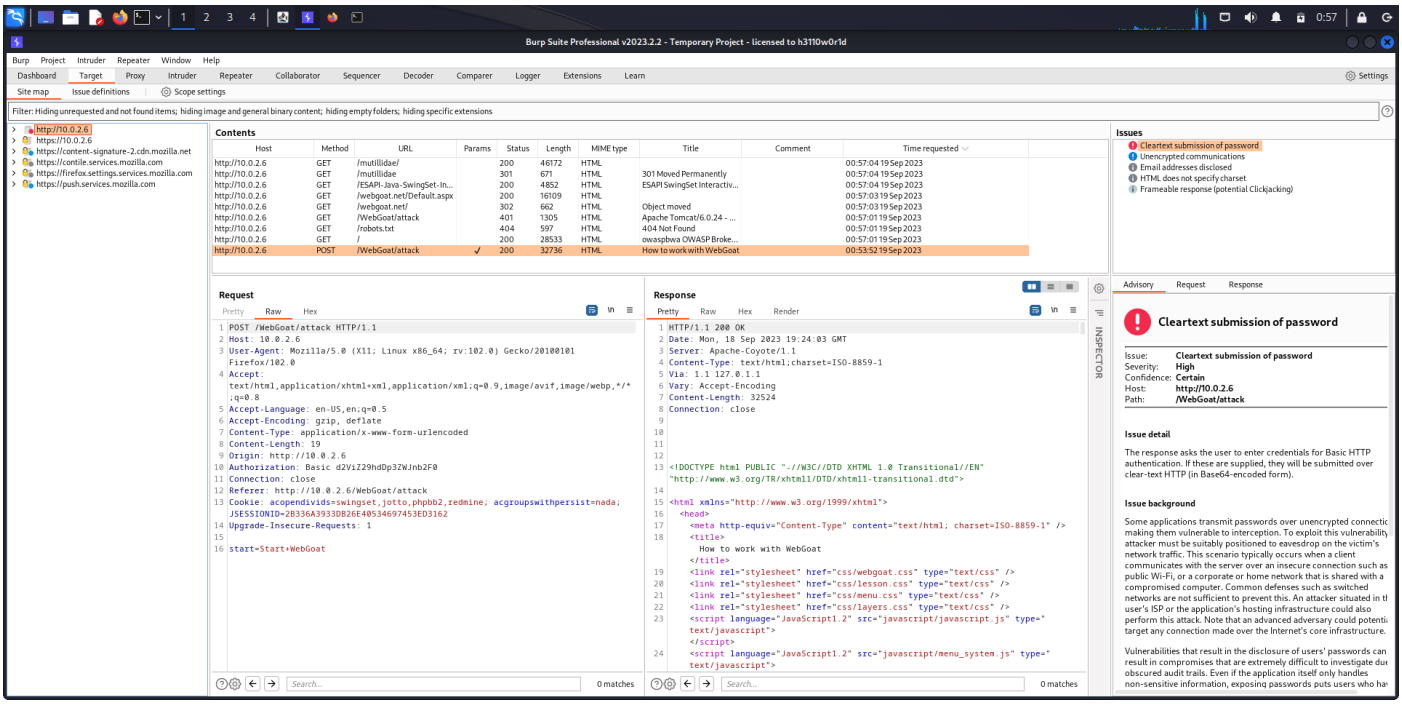
In Resource pool, you can configure how burp will make use of your network resources that you have.

You can configure the maximum number of concurrent requests or delay between requests which should be imposed.

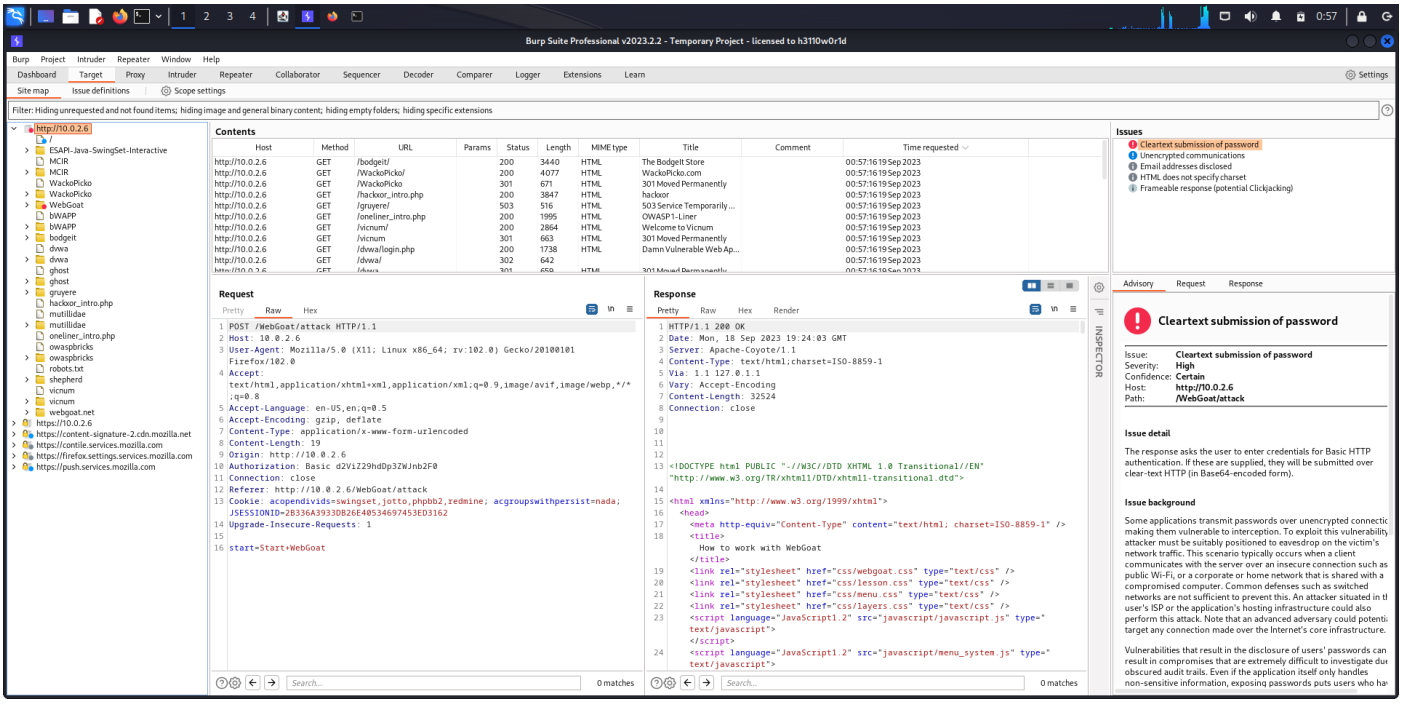
You can limit the total amount of traffic so as not to overwhelm the system.



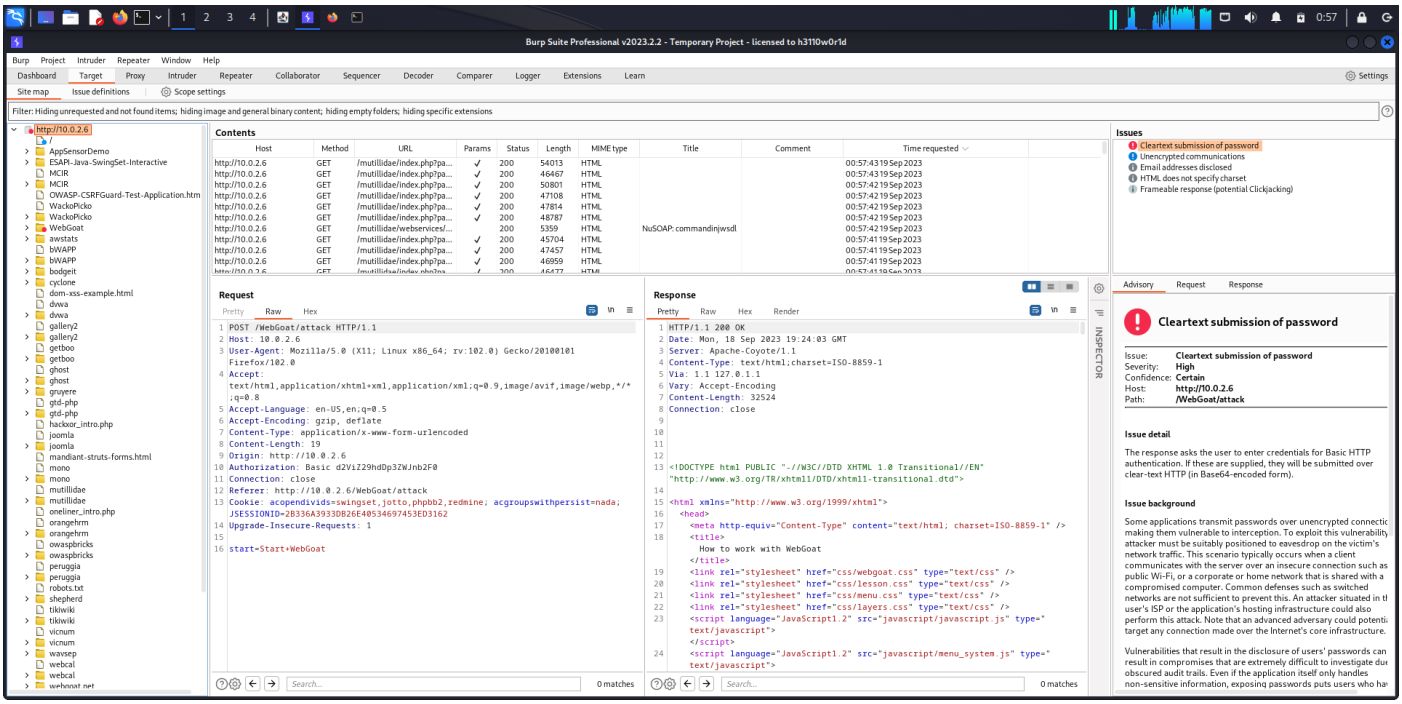
The scanning of the website has been started.



The scan displays all the directories and webpages that are present in the web server.

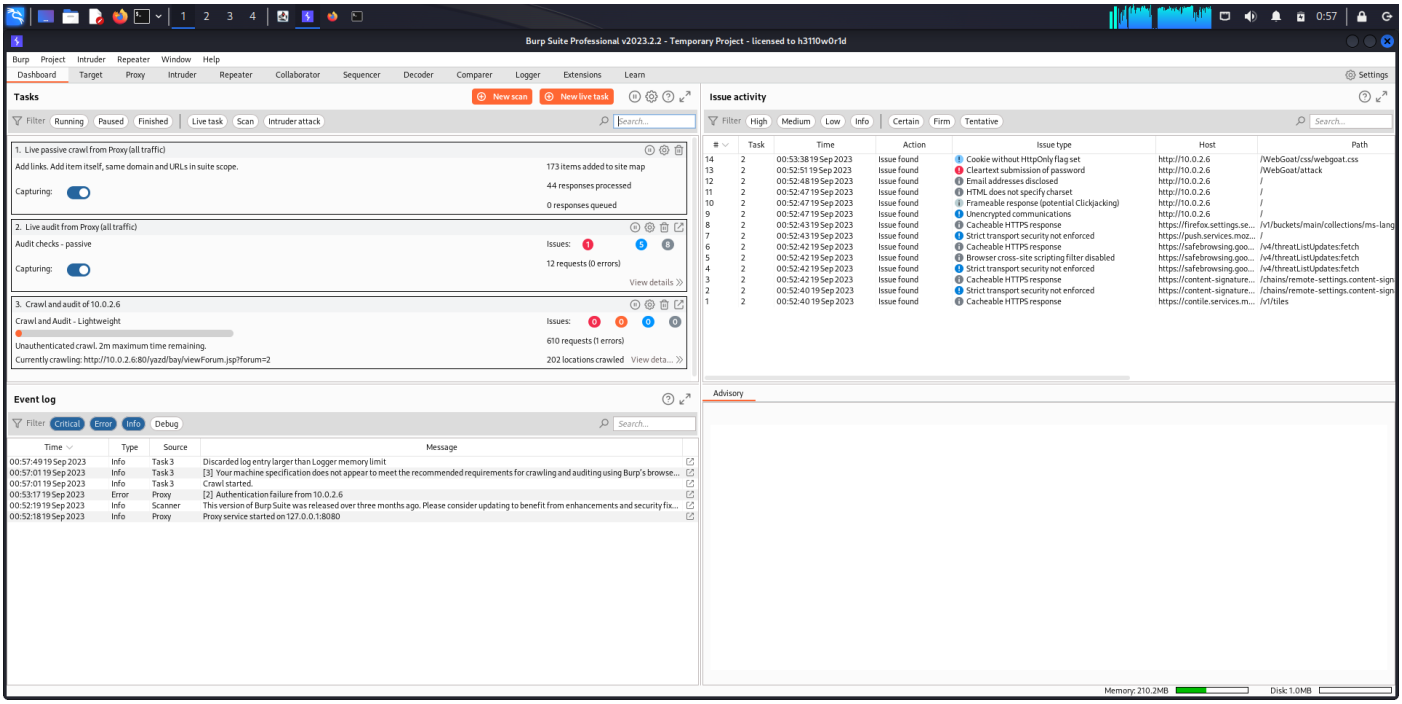


The scanning is still in progress.



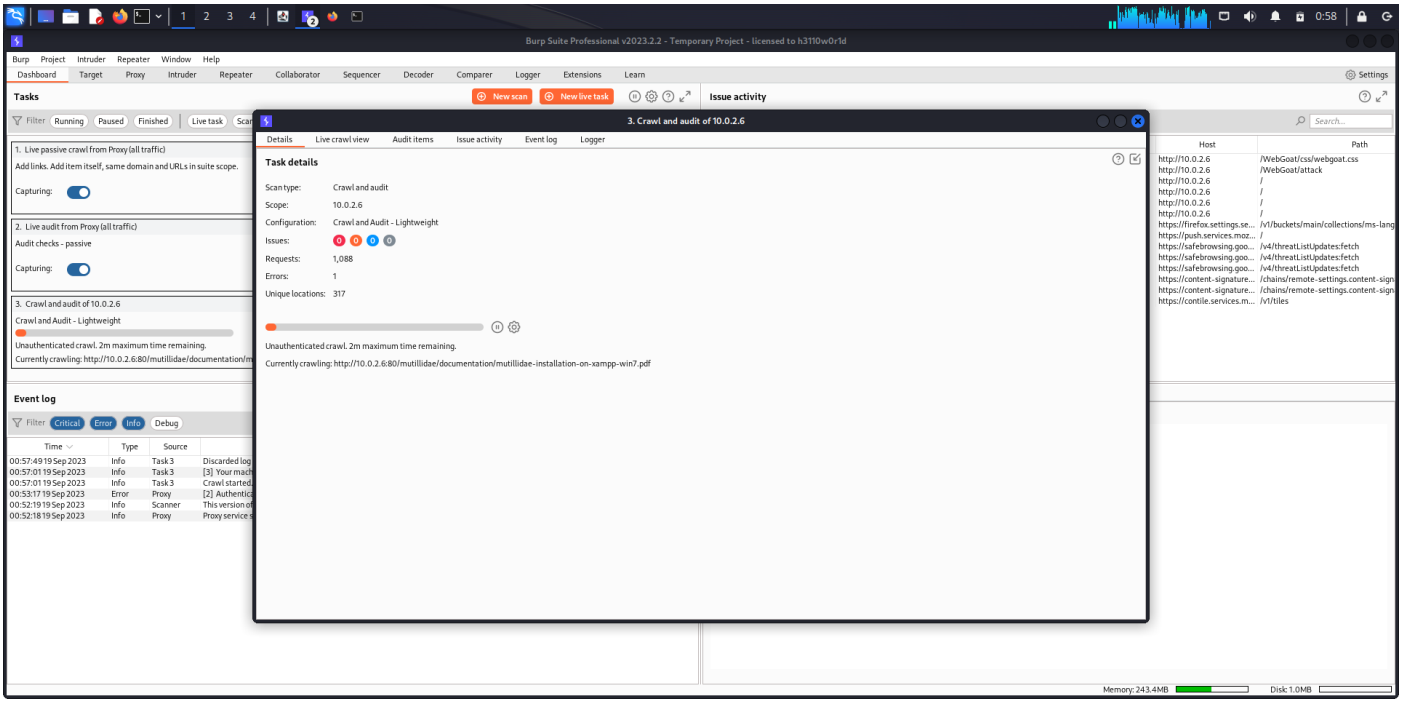
The dashboard displays all the progress of scanning.

The crawling phase displays all the request made. Later, the audit phase displays all the issues.



The progress of the scan can be viewed in the Details tab using the Progress Bar.

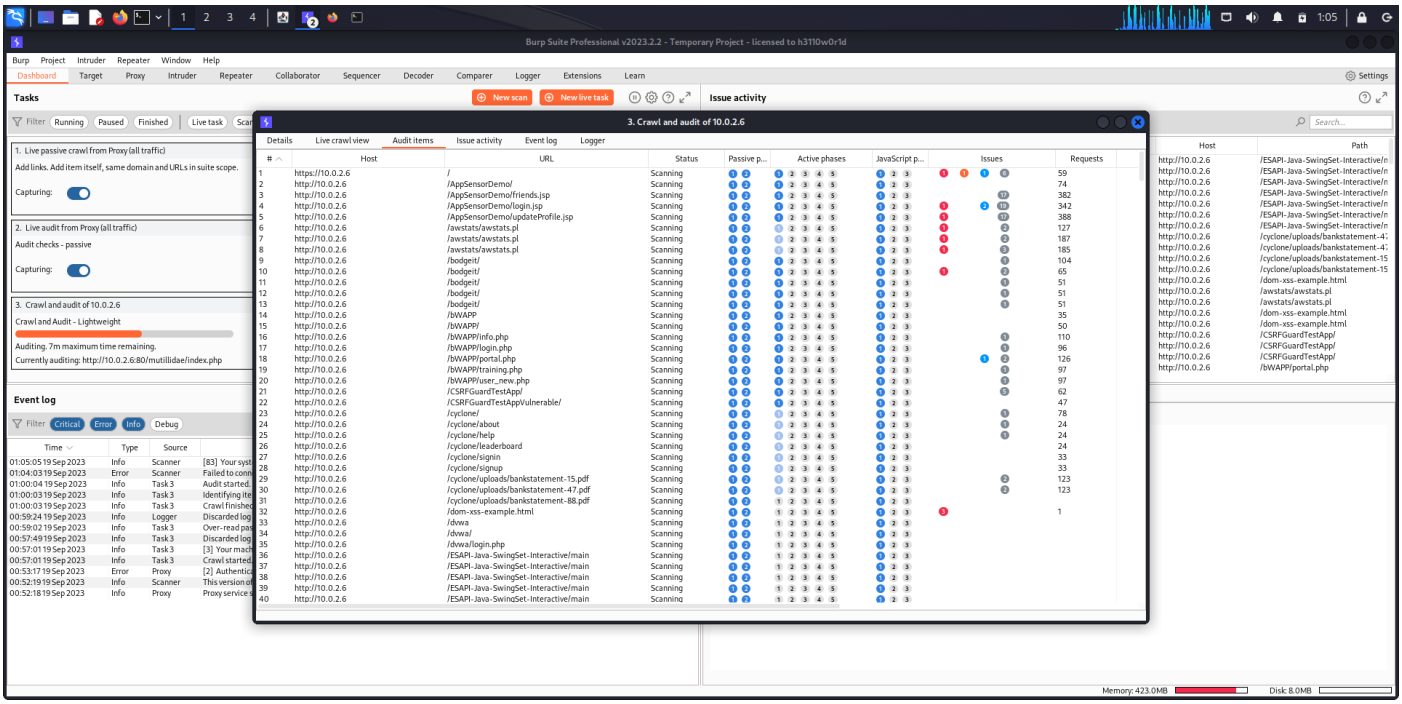
The settings can be changed in Details as they are in progress.



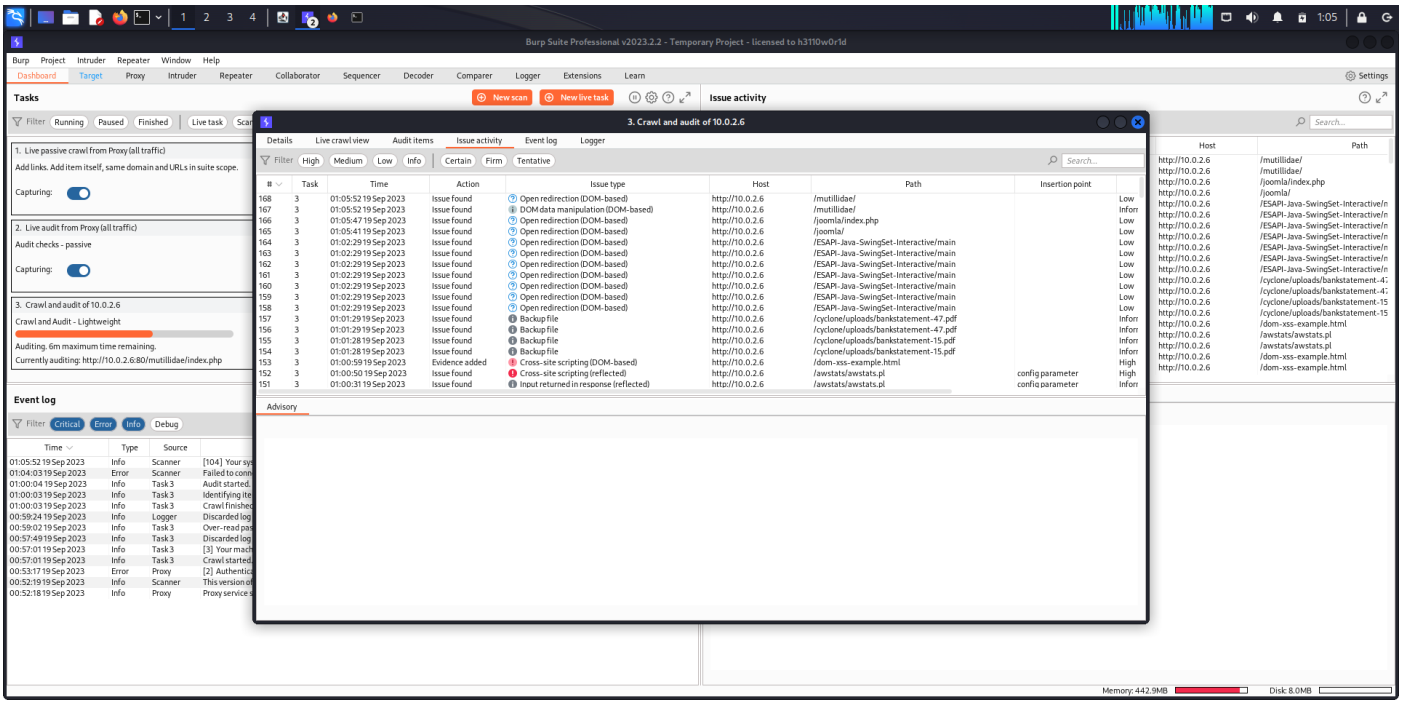
This shows you all of the items that have been discovered during the crawl and you can view their progress through the different phases of the audit.

You can see the Passive phases and Active phases, the JavaScript work, full URL, number of issues that have been reported for each item, number of requests and errors.

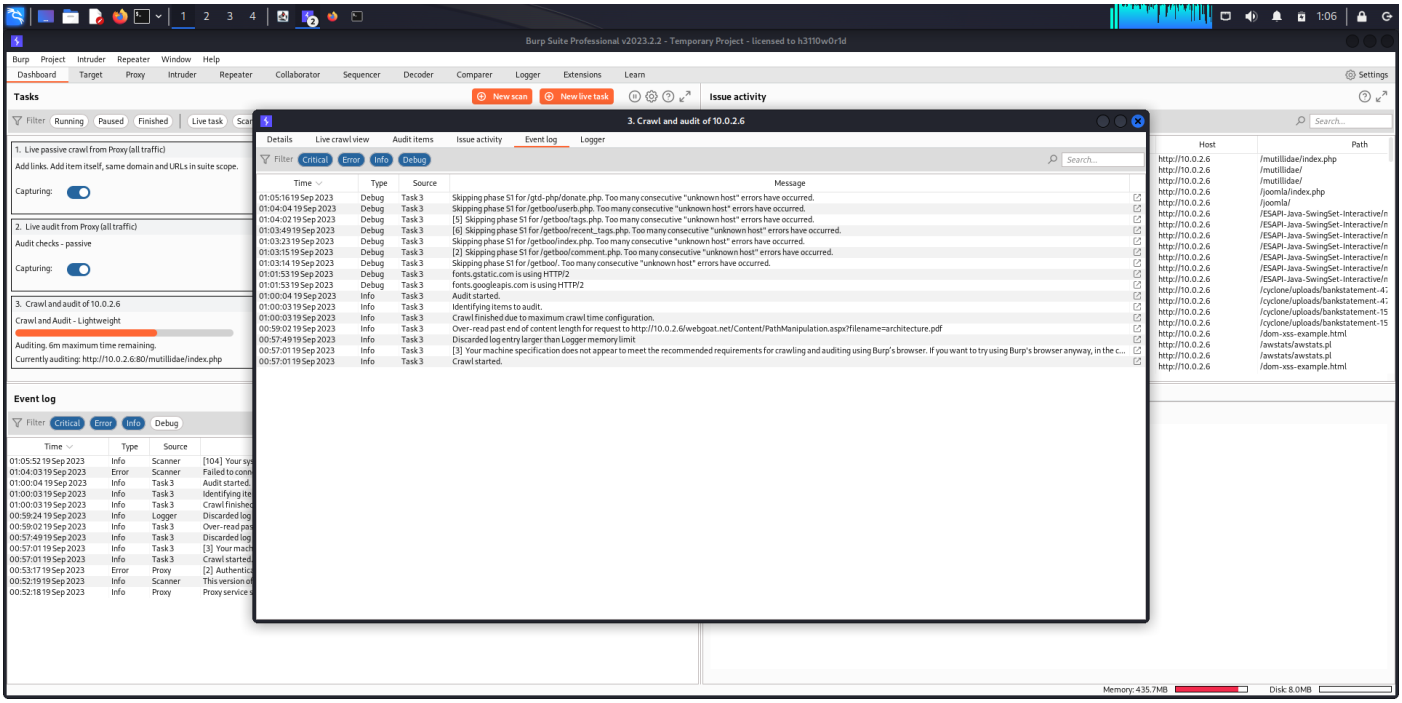
Provides complete visibility of the Burp scan.



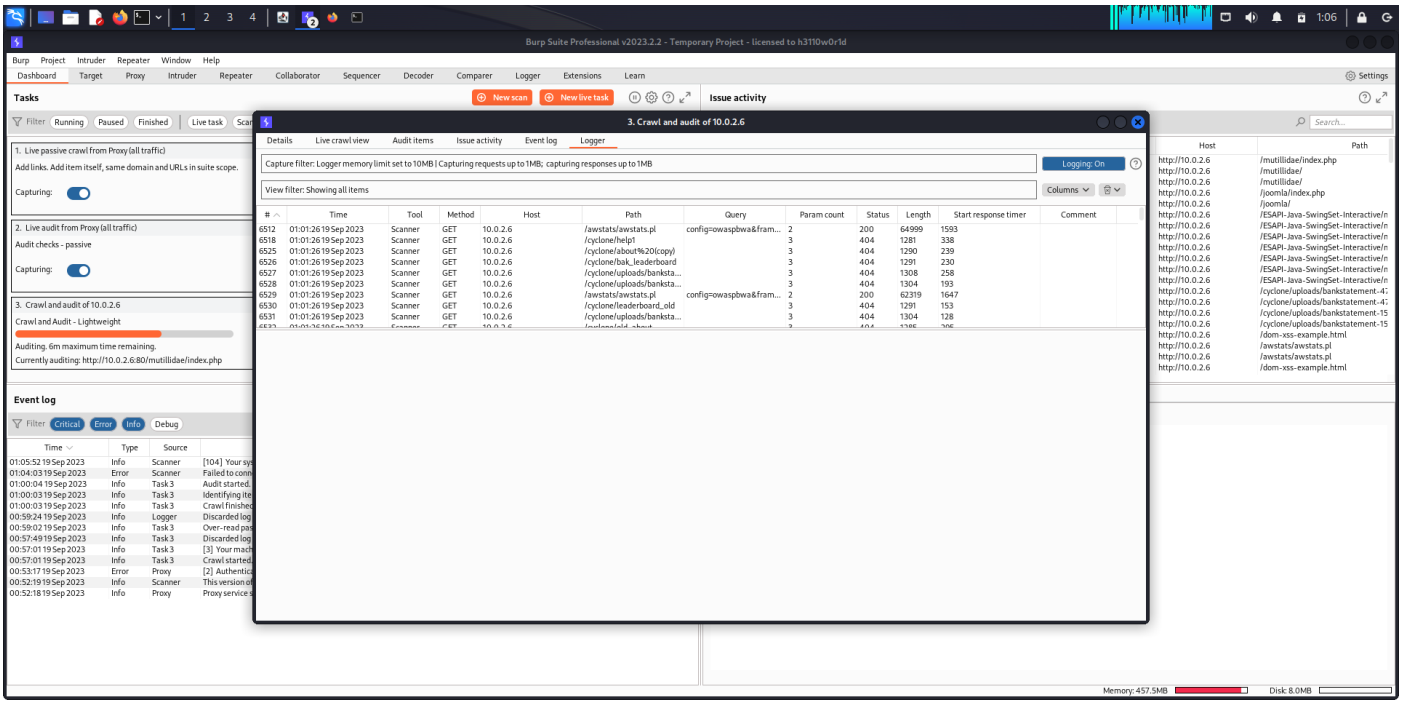
The Issue activity log displays the vulnerabilities which appear in real-time as they are discovered.



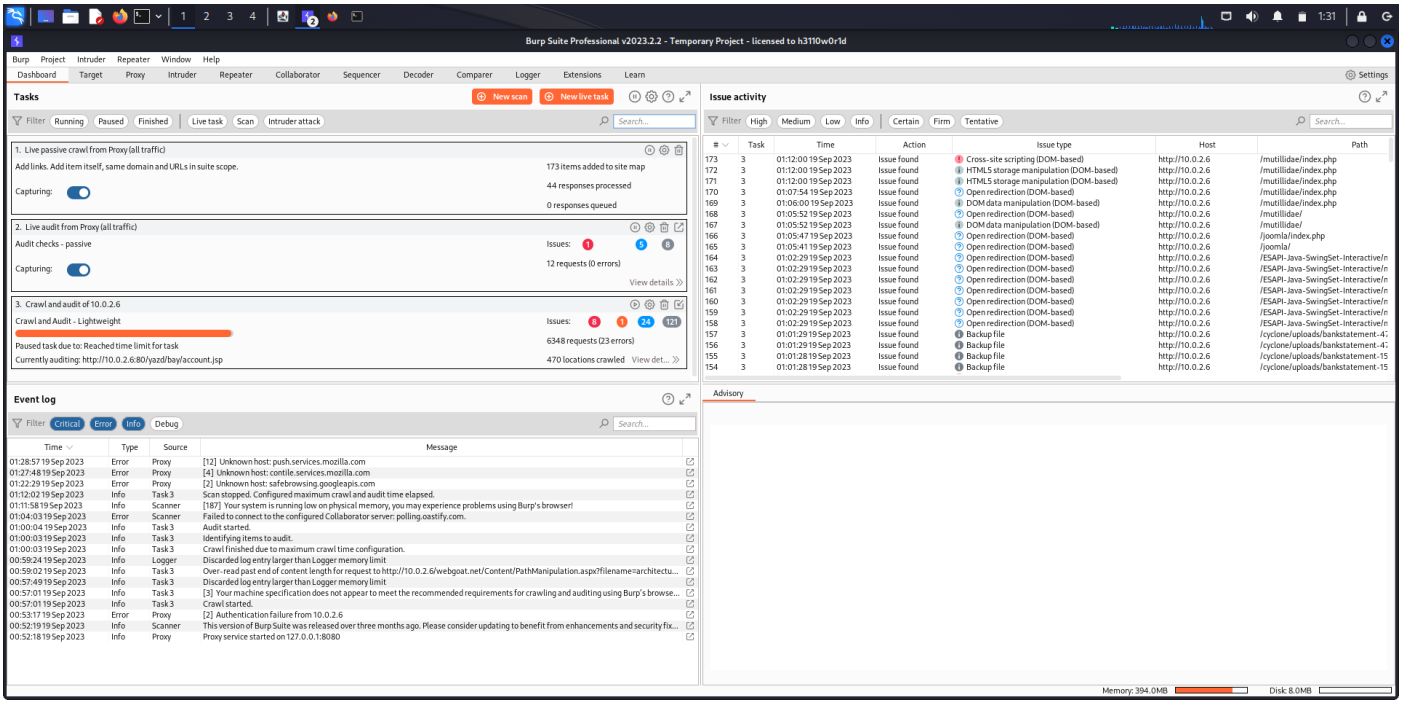
The Event log displays various information and errors and other details to be aware of.



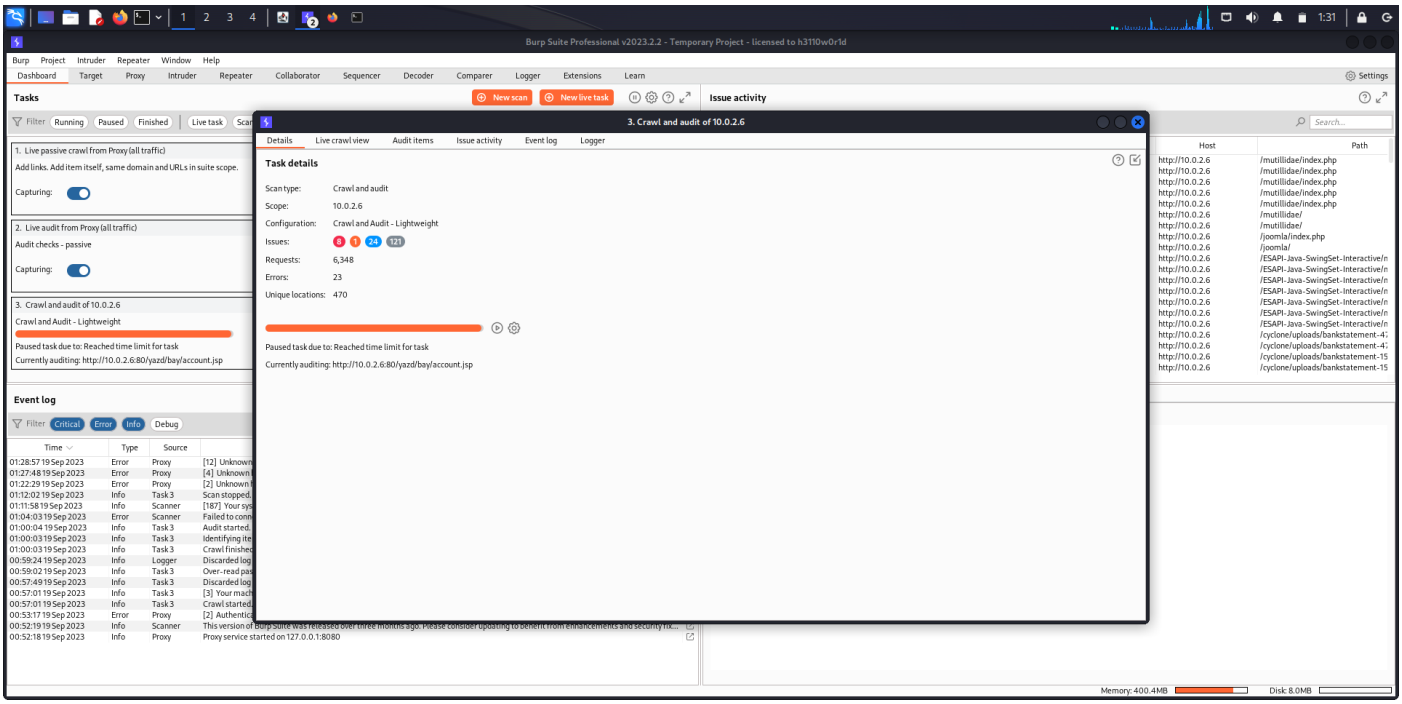
The Logger tab keeps track and logs all the activity performed during the Crawl and Audit.

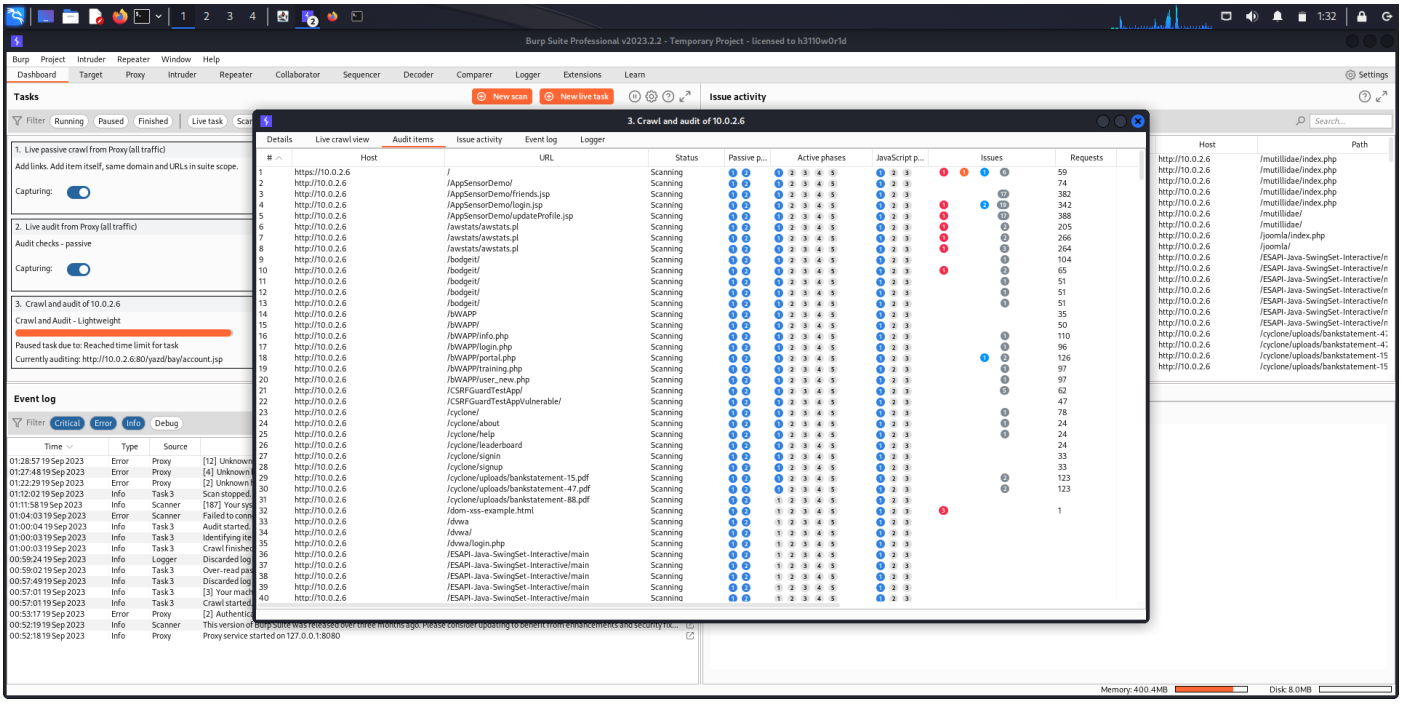


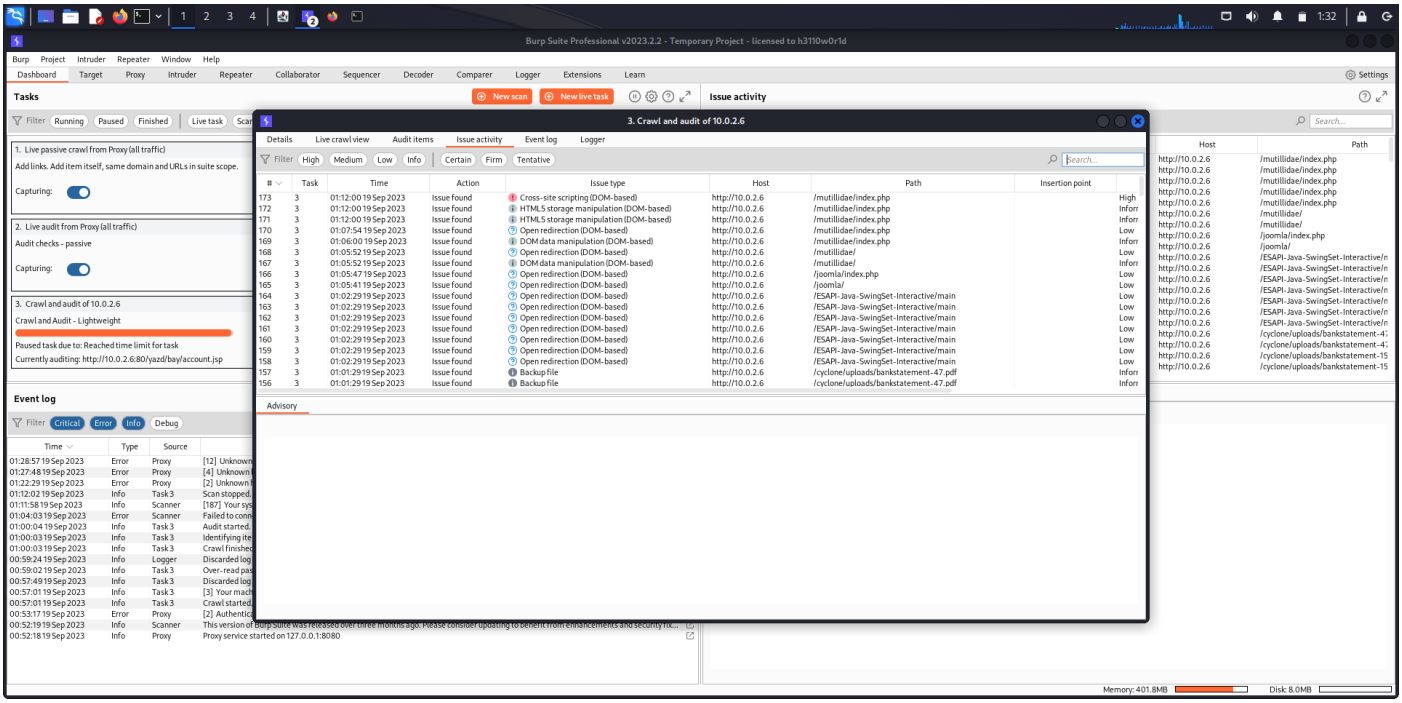
The complete scan of the target website is complete.



The progress bar shows the completion of the crawl and audit.





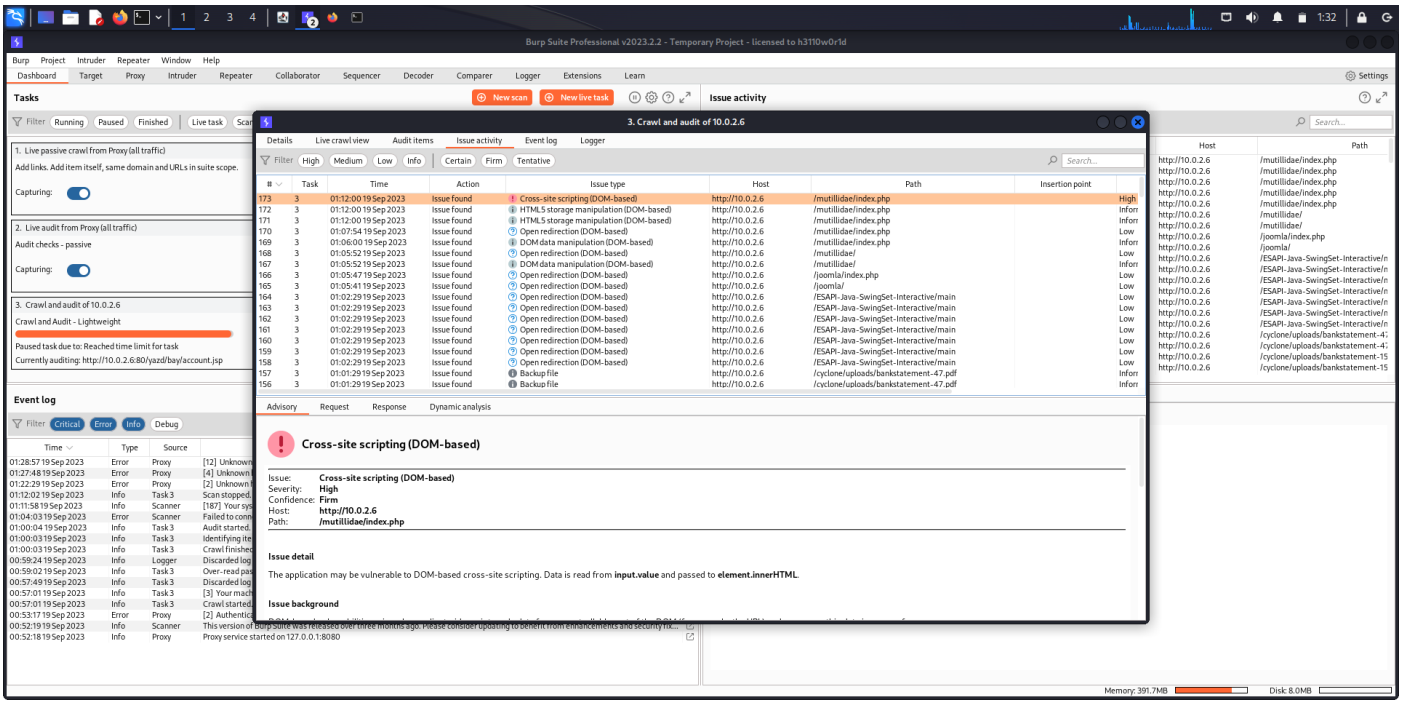


The Audit phase of the Crawl and Audit has detected many issues.

They are all displayed in the Issue Activity tab.

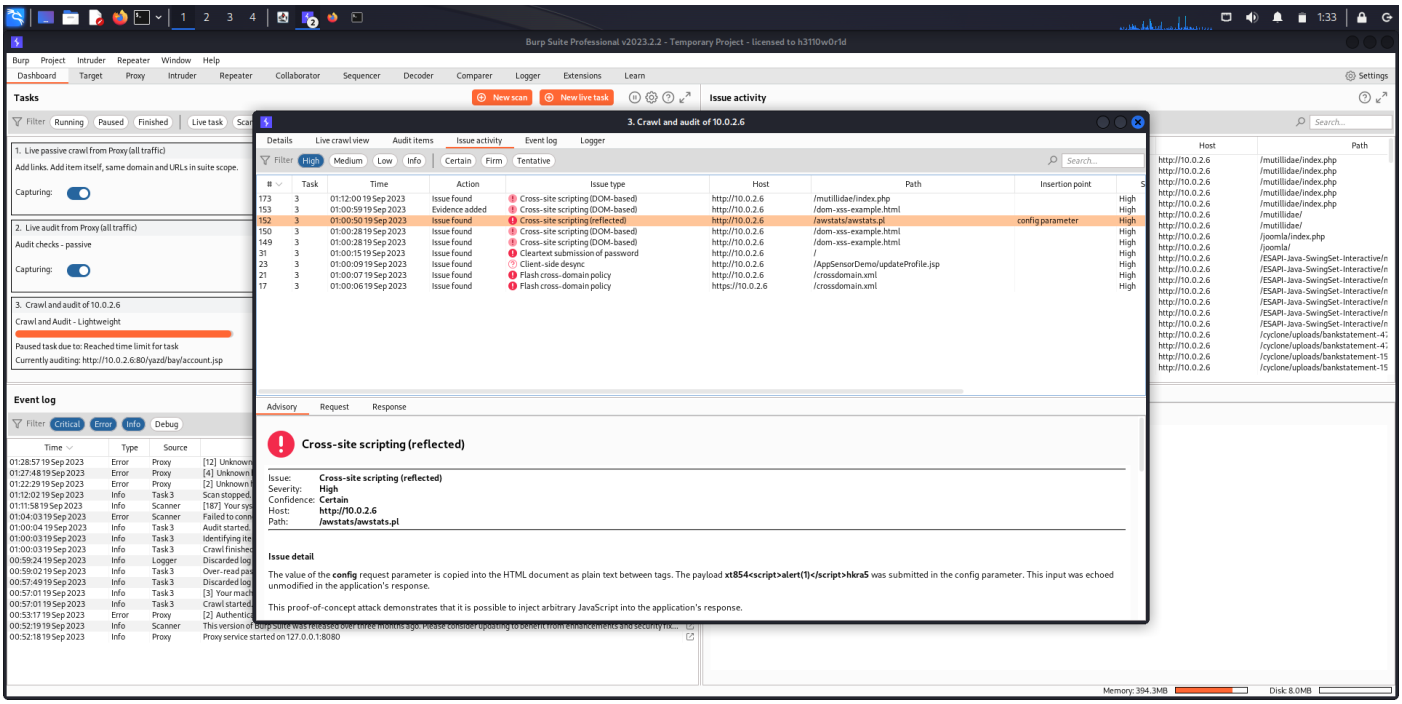
As we can see, a DOM-based Cross-Site Scripting vulnerability has been reported. It is a high-level threat.

The Report of the vulnerabilities can be extracted. The issue is has been notified to the auditor.



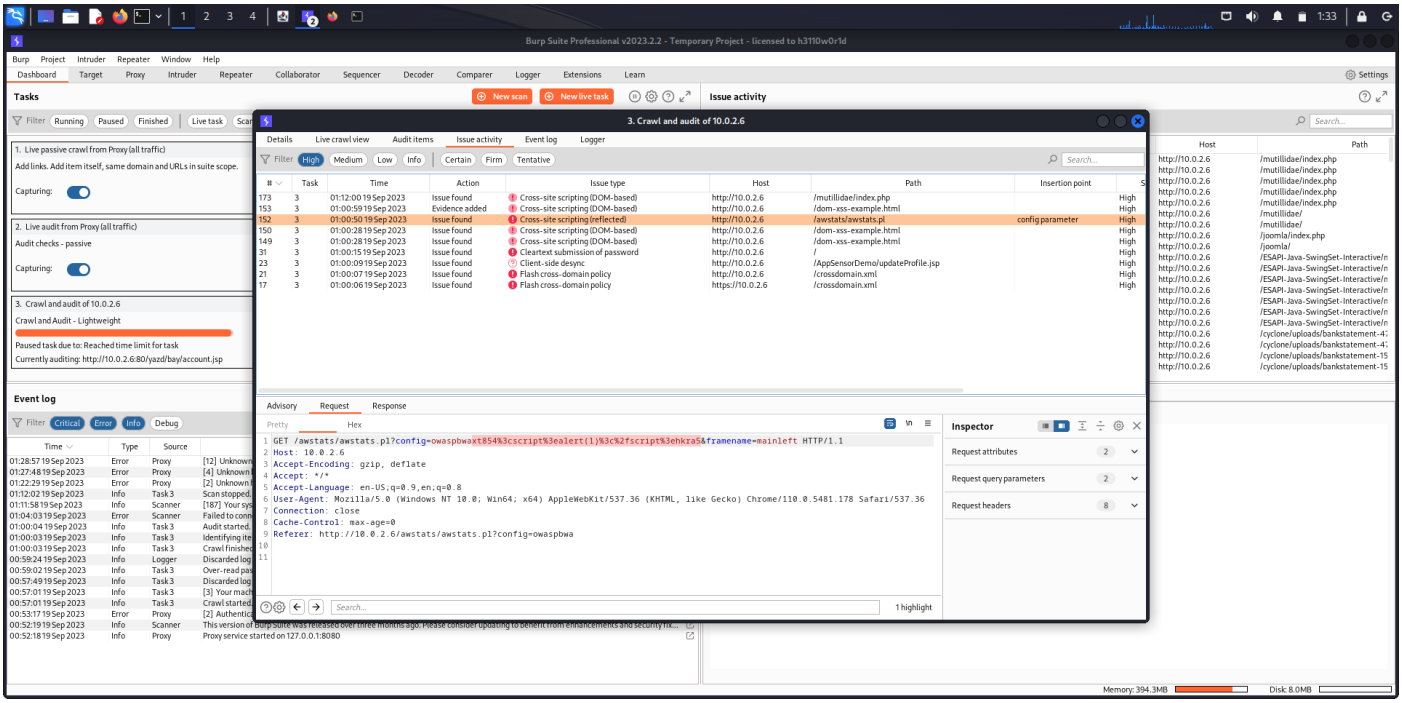
The types of issues can be filtered in the Issue activity tab.

Here, all the issues/vulnerabilities of high-level threat are displayed and all other threat levels are filtered out.

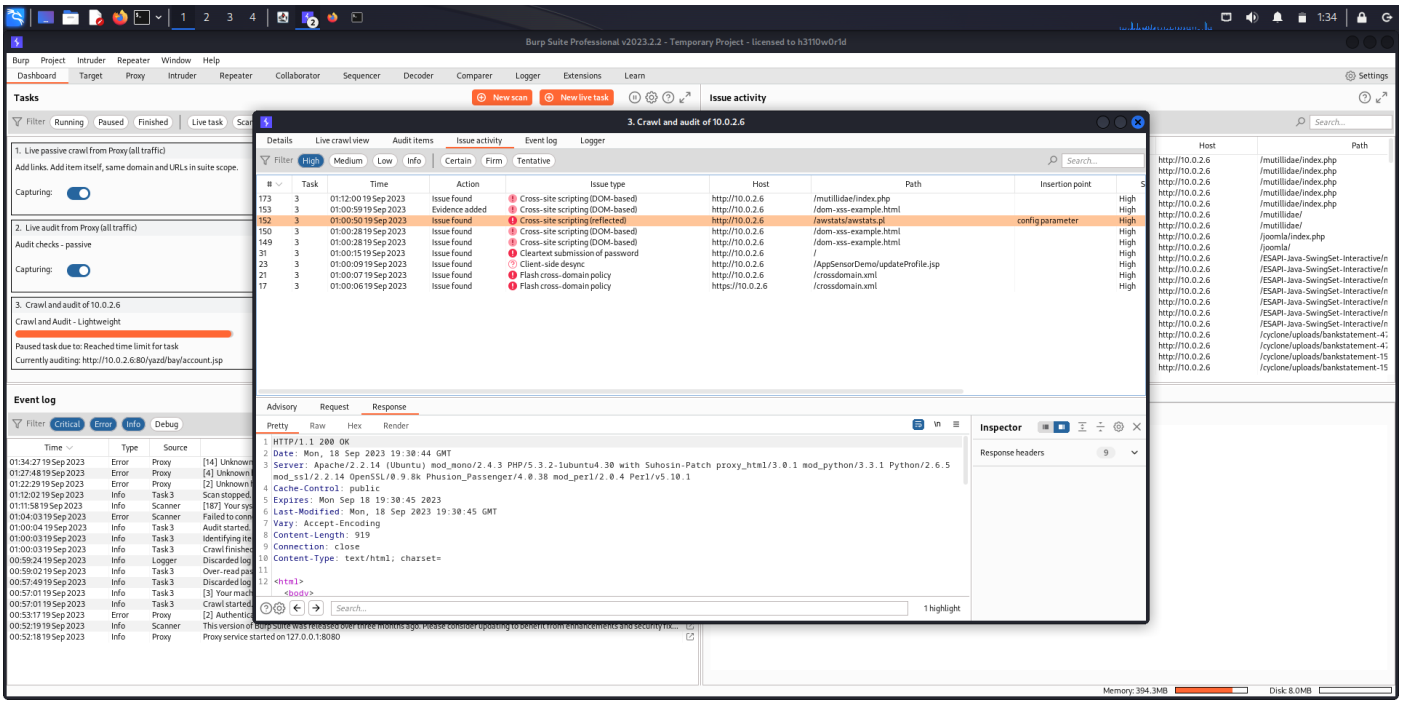


The HTTP Request message sent during the Crawling phase can be seen.

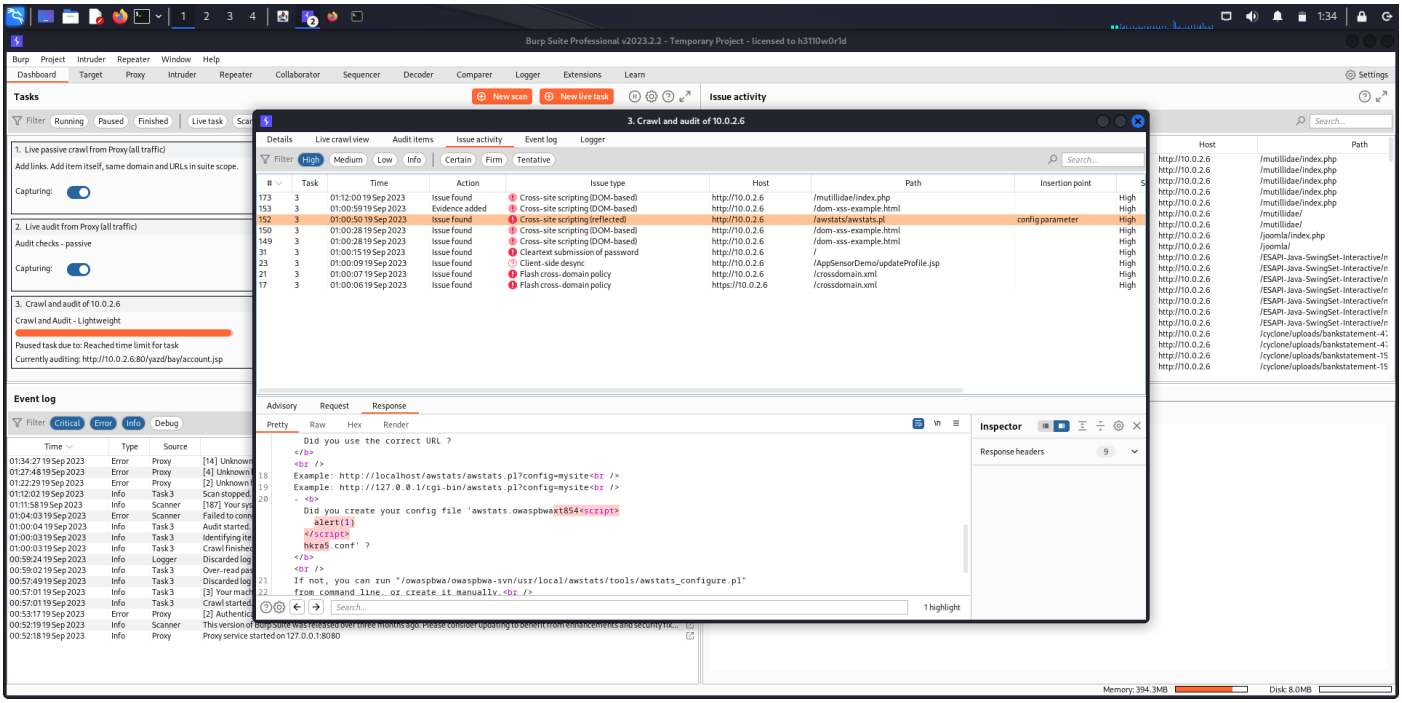
The highlighter specifically highlights the issue in the webpage.



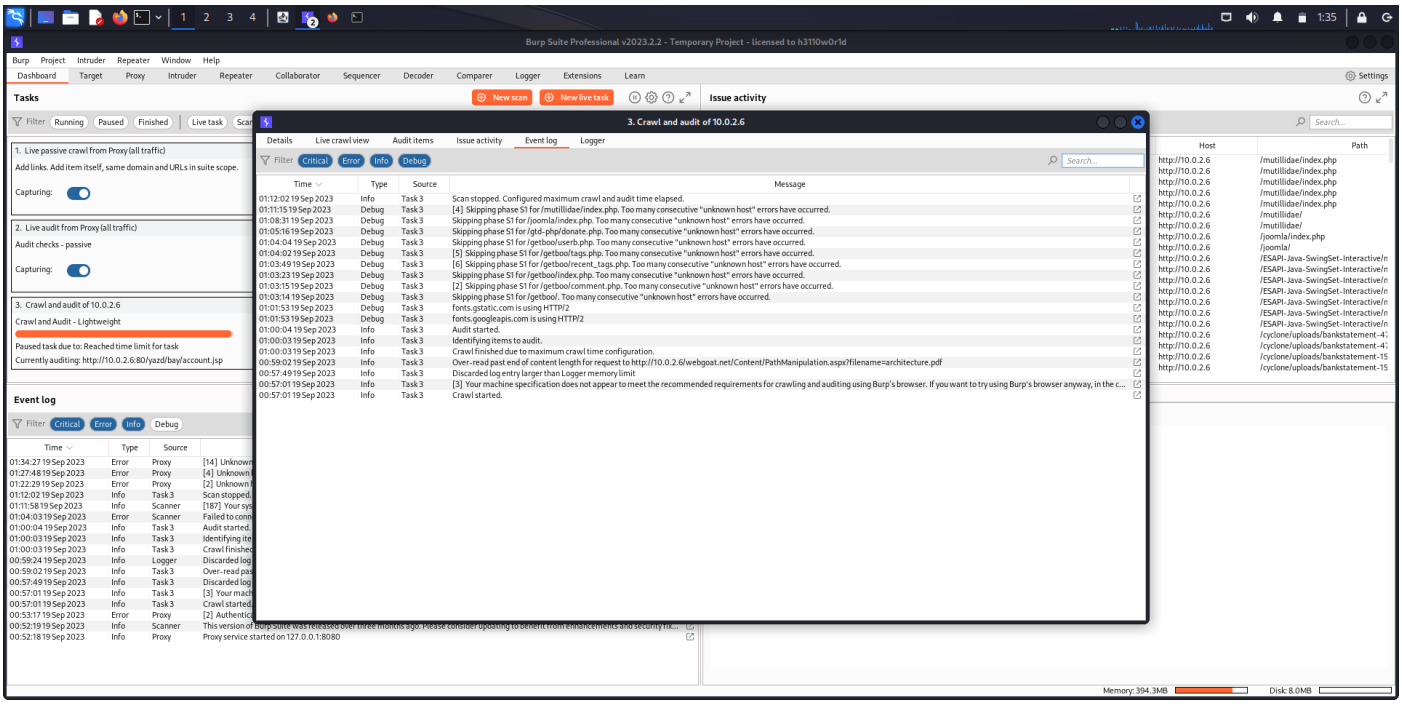
The HTTP Response message can be seen.

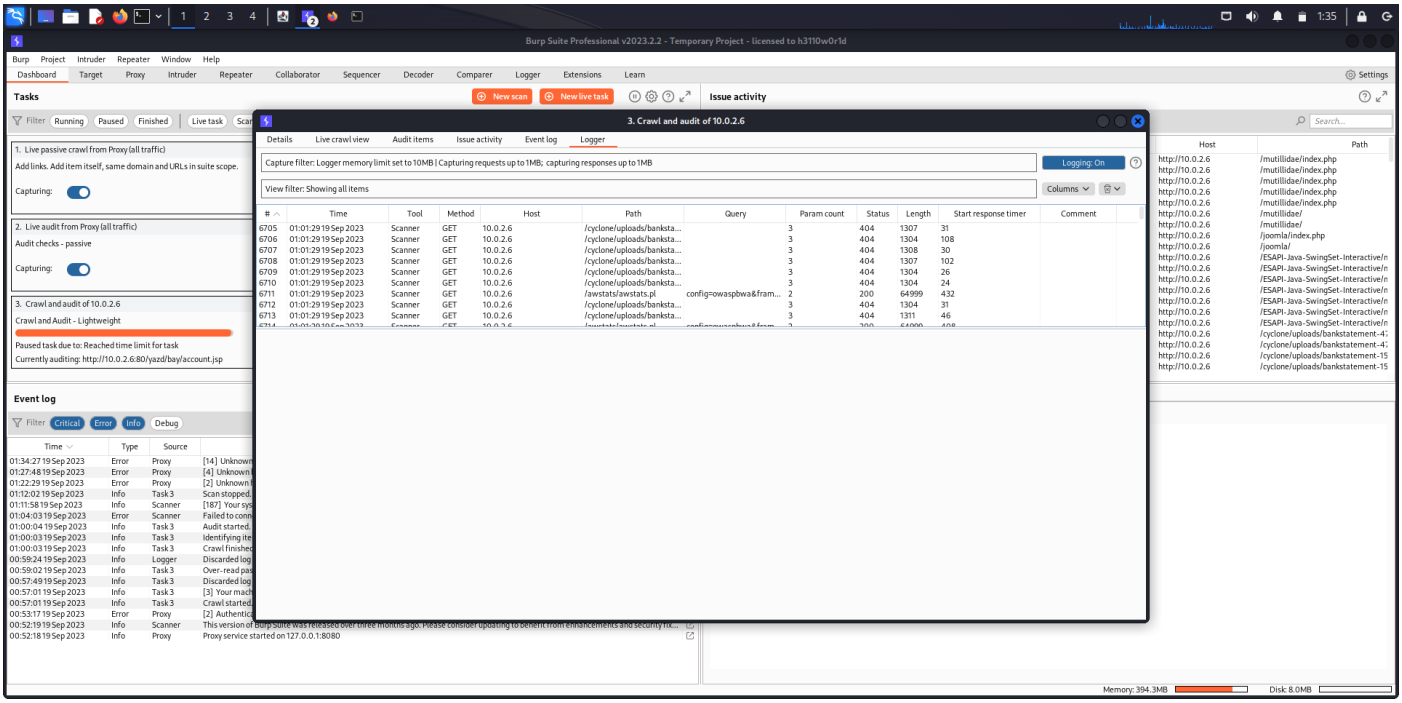


The highlighter specifically highlights the issue in the webpage.



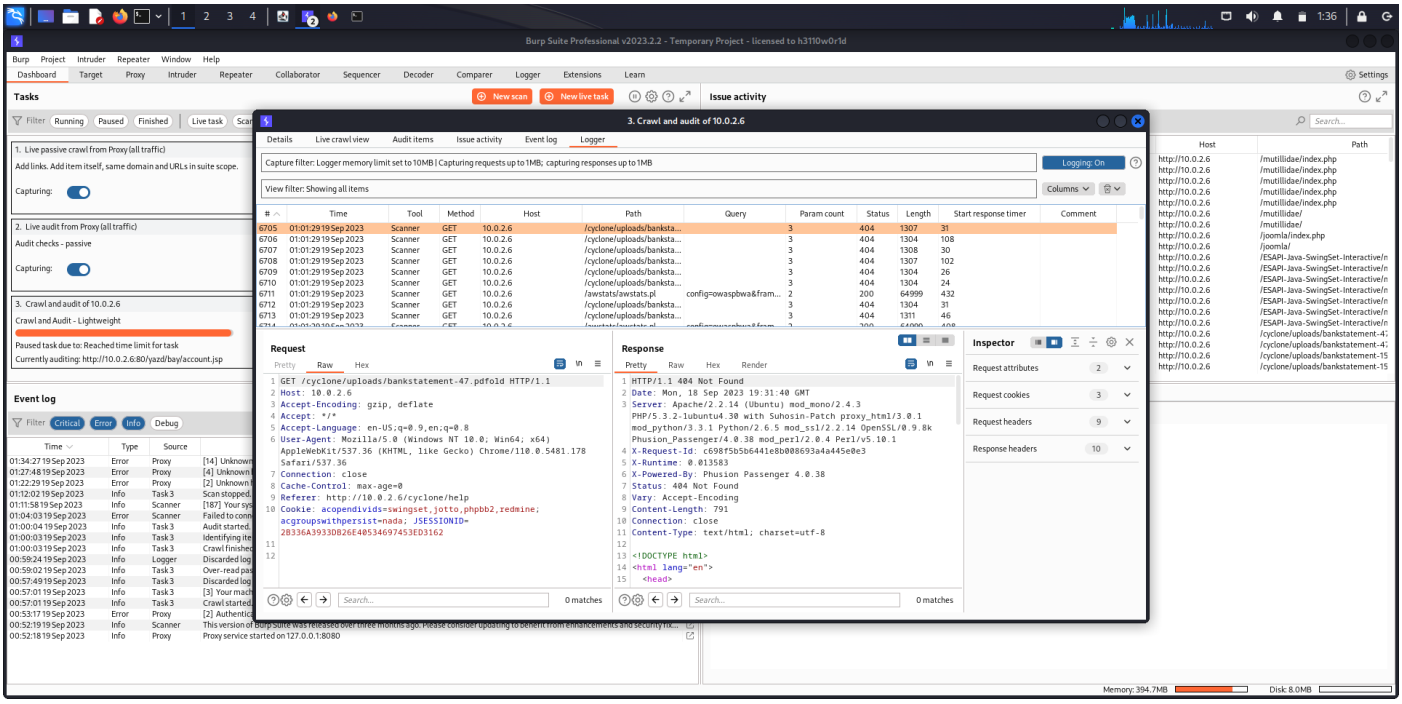
The Event log keeps track of all the events.



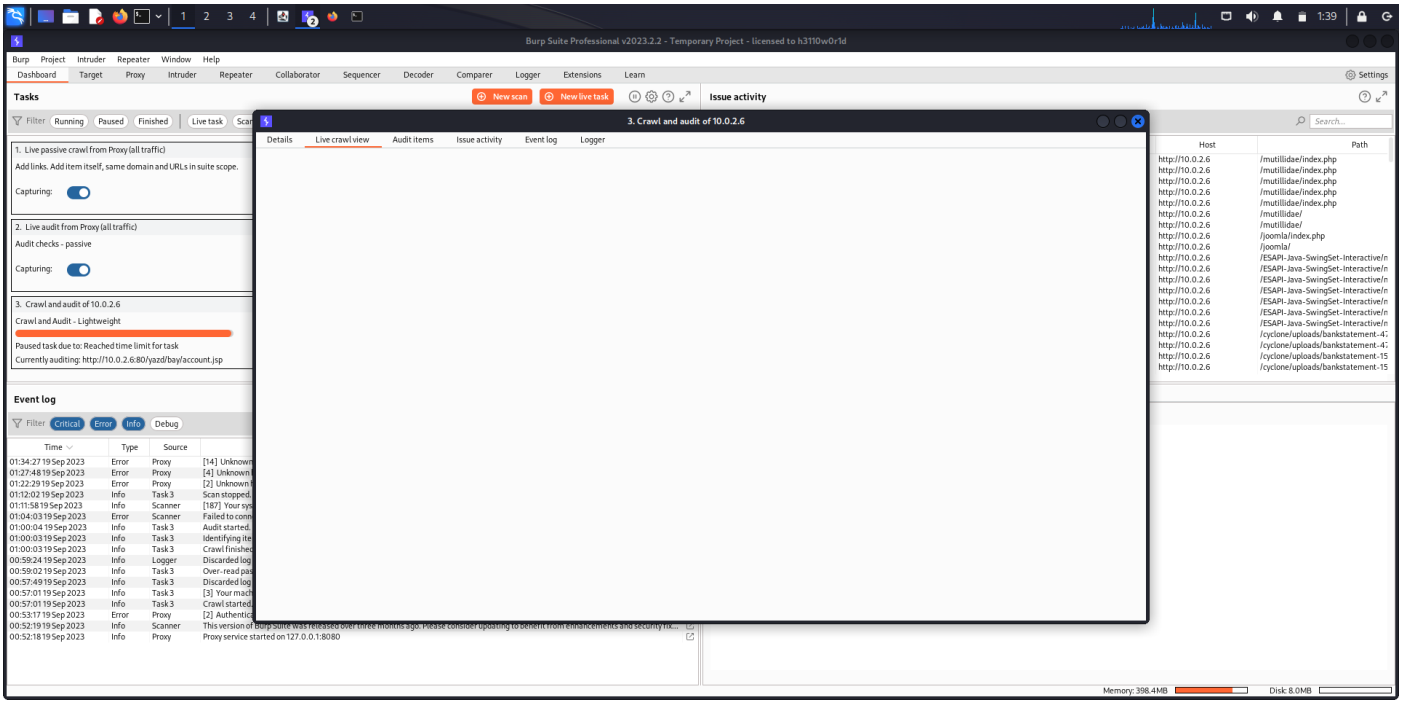


The Logger tab keeps all the HTTP Requests made and their HTTP Response messages.

The 6705th HTTP Request and it's consequent HTTP Response message is displayed below.



Live Crawl View tab.



Analysis

The analysis of spidering in our report highlights its critical role in web application assessment and information gathering. Spidering allows for the systematic exploration of a website's architecture, enabling us to map its structure and identify potential security vulnerabilities and weaknesses. By automating the process of following links and collecting data, spidering significantly enhances the efficiency of web security assessments. Furthermore, the integration of spidering tools like Burp Suite empowers cybersecurity professionals to conduct comprehensive audits, making it an indispensable component of modern web application security practices.

Conclusion

In conclusion, our report has shed light on the pivotal role of spidering in the realm of web application assessment and security. Spidering serves as a foundational step in understanding and analyzing the structure and content of websites. It enables efficient navigation and data collection, ultimately leading to the discovery of potential vulnerabilities and misconfigurations. When used in conjunction with specialized tools like Burp Suite, spidering becomes a powerful asset in the arsenal of cybersecurity professionals, offering comprehensive insights and facilitating robust security audits. Embracing spidering techniques is imperative for organizations seeking to enhance the resilience of their web applications in an ever-evolving threat landscape.

References

Burp Scanner - Web Vulnerability Scanner from PortSwigger

How to scan a website for vulnerabilities using Burp Scanner - YouTube