

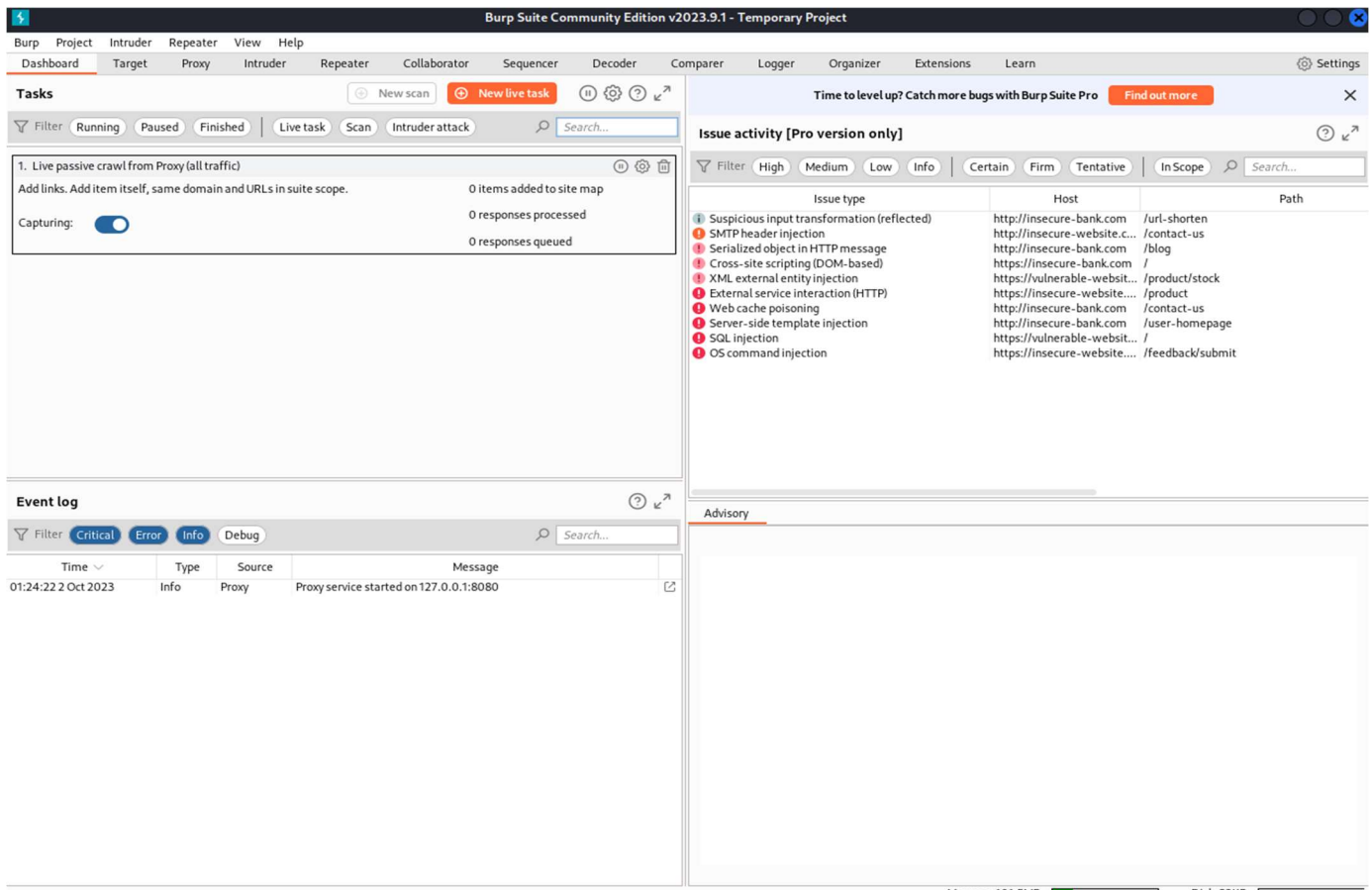
ASSIGNMENT-3

What is Burp suite ?

Burp Suite: PortSwigger created the well-known Burp Suite of web application security testing tools. Cybersecurity experts, such as penetration testers and ethical hackers, frequently utilise it to find weaknesses in web applications. The Burp Proxy, Burp Scanner, Burp Intruder, and Burp Repeater are some of the different parts of the Burp Suite that help with activities like intercepting and analysing web traffic, looking for security flaws, and evaluating the security of web applications.

Another popular cybersecurity tool that was created for network exploitation and penetration testing is called Metasploit. It gives security experts a platform for finding, using, and validating vulnerabilities in various systems and networks. The extensive library of exploits, payloads, and support modules in Metasploit enable testers to evaluate the security of target systems.

A penetration tester's capacity to find web application vulnerabilities and potentially exploit them for security testing and assessment purposes can be improved by combining the capabilities of these two tools, Burp Suite and Metasploit. This set of tools for thorough web application security testing and exploitation is sometimes referred to as "Burpsutie" in colloquial or inventive contexts.



Why Burp suite?

Burp Suite is a preferred option among penetration testers and cybersecurity experts for a number of reasons:

Comprehensive Web Application Testing: Burp Suite was created primarily to test the security of web applications. It offers a wide range of tools and functions, including as vulnerability scanning, online traffic analysis, and modifying requests and answers, that enable testers to completely evaluate the security of web applications.

User-Friendly GUI: Burp Suite has a user-friendly graphical user interface (GUI), which enables it to be used by people who may not have much command-line experience. Simple activities like intercepting and altering HTTP requests and answers are made easier by the GUI.

Burp Suite has a sizable and active user base, therefore there are many resources, tutorials, and discussion boards available for assistance and support. Burp Suite's developer, PortSwigger, also offers official guidance and assistance.

To stay up with new web application technologies and security risks, the tool is routinely updated. By doing this, testers are guaranteed access to the most recent features and security checks.

Burp Suite's extensibility enables users to customise and increase its functionality by supporting extensions and plugins. As a result, it can be modified to fit a variety of testing scenarios and requirements.

Burp Proxy is one of its key capabilities, allowing users to intercept and alter HTTP/S requests and responses sent back and forth between the client and the server. Understanding how a web application functions and spotting potential vulnerabilities depend on this.

Vulnerability detection and scanning are automated by Burp Suite's robust scanning engine (Burp Scanner), which can detect typical web application vulnerabilities like SQL injection, cross-site scripting (XSS), and more. This shortens testing time and speeds up the detection of security flaws.

Professional Edition: Burp Suite has a paid professional edition with more functionality in addition to its free community edition. The professional edition is ideal for doing more thorough security analyses because it comes with other tools like Burp Scanner.

Industry Standards Compliant: Security experts use Burp Suite to conduct security assessments that are compliant with numerous security standards and laws. Burp Suite is well known and recognised within the cybersecurity industry.

In conclusion, it is a flexible and strong tool that makes it easier to find and fix security flaws in online applications. Several cybersecurity professionals and organisations favour it because of its capabilities, ease of use, and community support.

Burp Suite is a popular cybersecurity tool used for web application security testing and vulnerability assessment. It offers a wide range of features to help security professionals identify and mitigate vulnerabilities in web applications. As of my last knowledge update in September 2021, here are some of the key features of Burp Suite:

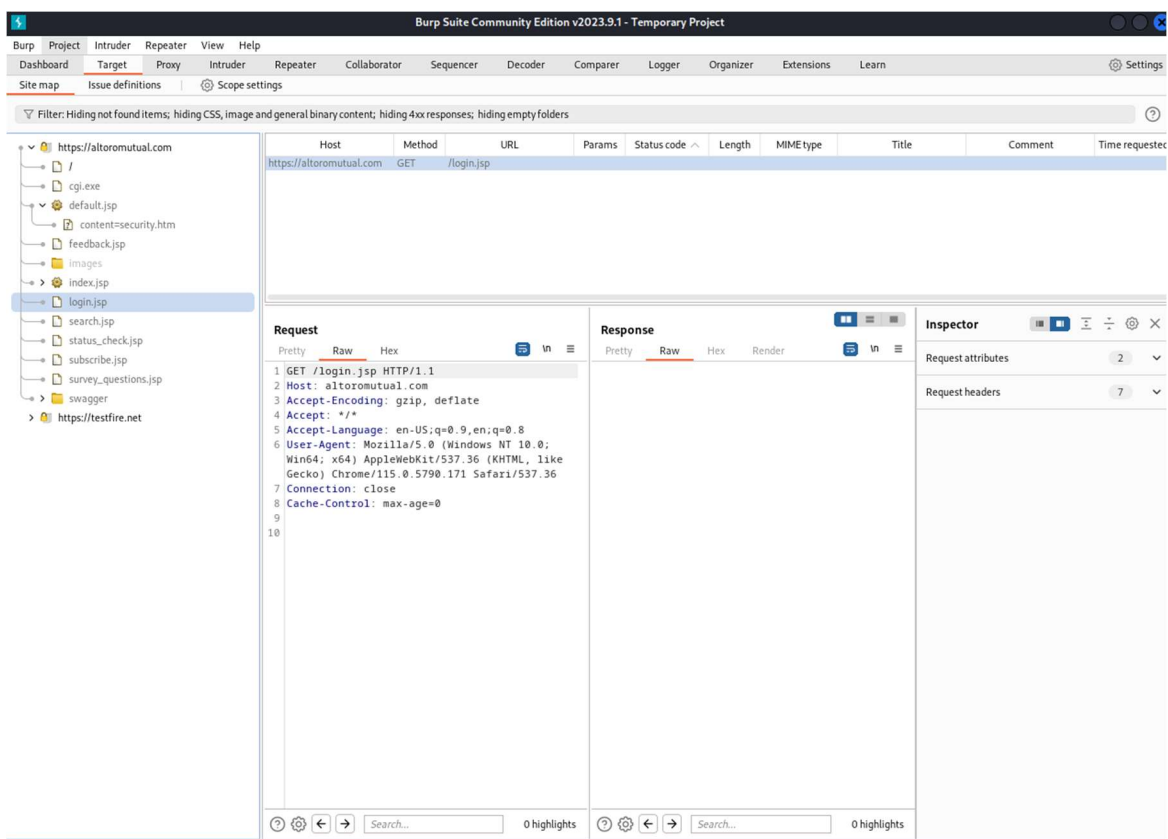
What are the features of Burp suite?

1. **Web Vulnerability Scanning:** Burp Suite allows users to scan web applications for common security vulnerabilities, including cross-site scripting (XSS), SQL injection, and more.
2. **Proxy:** The proxy feature enables users to intercept and manipulate HTTP requests and responses between the client and the web server. This helps in identifying security issues and testing the security of web applications.
3. **Spider:** Burp Suite includes a web spider that automatically crawls a website to discover and map its structure. This is useful for identifying hidden or undocumented parts of a web application.
4. **Intruder:** The Intruder tool lets users automate attacks on web applications, making it easier to identify vulnerabilities like brute force login, parameter manipulation, and more.
5. **Repeater:** Repeater allows users to manually modify and replay HTTP requests, making it a valuable tool for testing specific scenarios and analyzing the impact of changes on the web application.
6. **Sequencer:** This feature analyzes the randomness of tokens, such as session cookies, and helps identify weaknesses in token generation algorithms that could lead to session fixation attacks.
7. **Scanner:** Burp Scanner is a powerful automated scanner that can identify a wide range of vulnerabilities in web applications, including those mentioned earlier, as well as more complex issues like deserialization vulnerabilities and business logic flaws.
8. **Collaborator:** Burp Collaborator assists in detecting out-of-band vulnerabilities by providing a way to monitor interactions between the target application and external entities, such as DNS or HTTP requests.
9. **Extensibility:** Burp Suite is highly extensible through its support for plugins and extensions. Users can create custom extensions using Java to enhance its functionality or integrate it with other security tools.

10. Reporting: Burp Suite allows users to generate detailed reports of identified vulnerabilities, making it easier to communicate findings to development teams or stakeholders.
11. Session Handling: The tool can handle sessions and maintain state while testing web applications, which is crucial for testing authenticated parts of a website.
12. Target Scope: Users can define the scope of their testing by specifying the target URL or IP range, helping to focus testing efforts on specific parts of a web application.

Testing Burp suite on testfire.net

1.



Sir I am unable to scan in burp suite because it is asking to get paid scan I tried my best but unable to scan can you teach more about this.