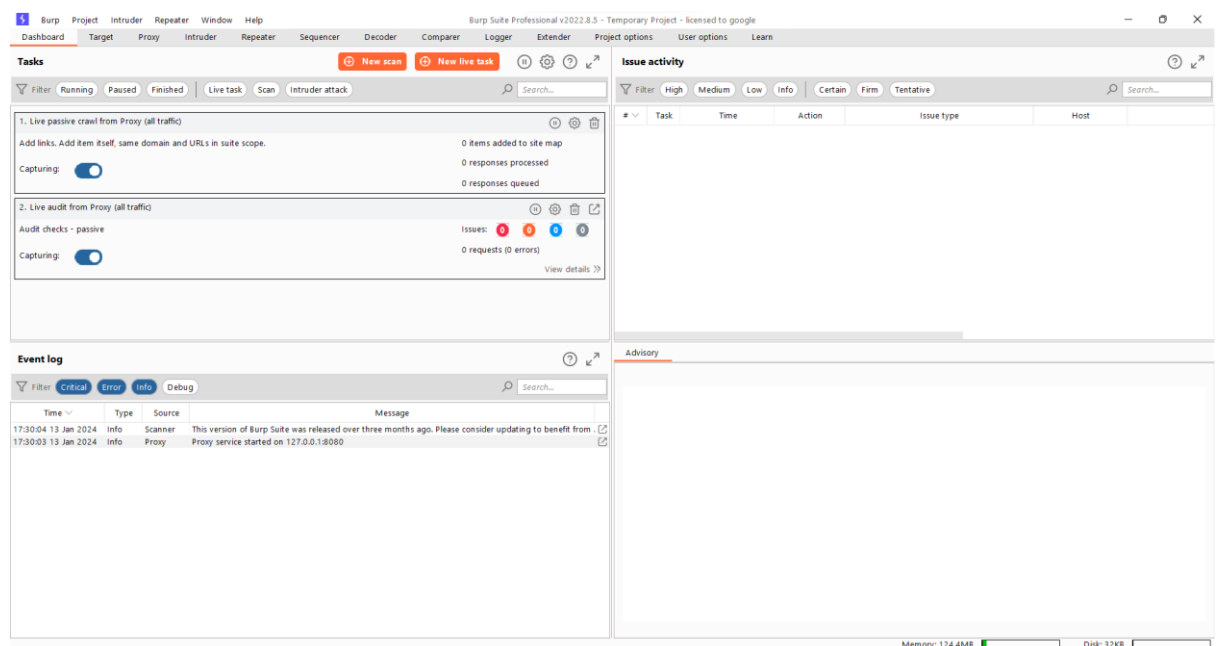# Burpsuite

1. What is burpsuite –

Burp Suite is a cybersecurity tool designed for testing web applications. It helps security professionals find potential vulnerabilities in the code of websites and web applications. It acts like a middleman between your browser and the target application, allowing you to intercept and inspect the data that goes back and forth.

The tool has various features like scanning, crawling, and analyzing web applications to identify security issues such as SQL injection, cross-site scripting (XSS), and other potential weaknesses. Ethical hackers and security experts often use Burp Suite to ensure that websites are robust and secure against malicious attacks.


2. Options in burpsuite –
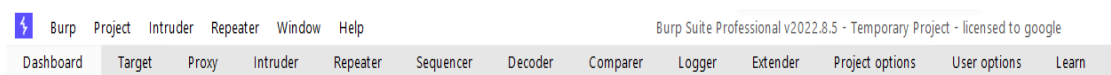
1. **Proxy**: The Proxy tool allows you to intercept and modify HTTP/S requests and responses between your browser and the target application. It's essential for understanding and manipulating the data flow during security testing.
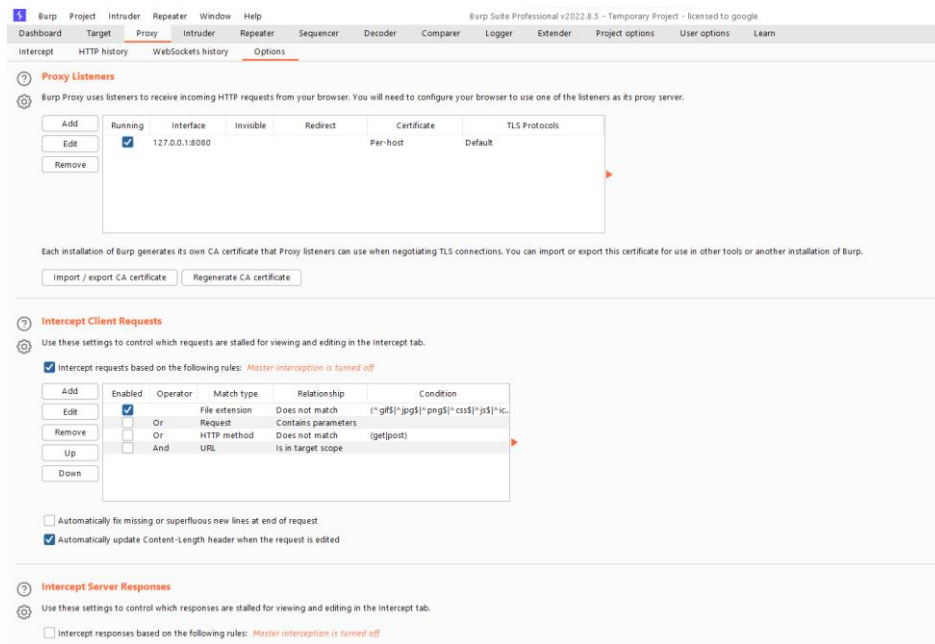
2. **Target:** The Target tool helps you manage and analyze the target scope of your testing. You can specify which applications you want to test, view site maps, and configure various target options.
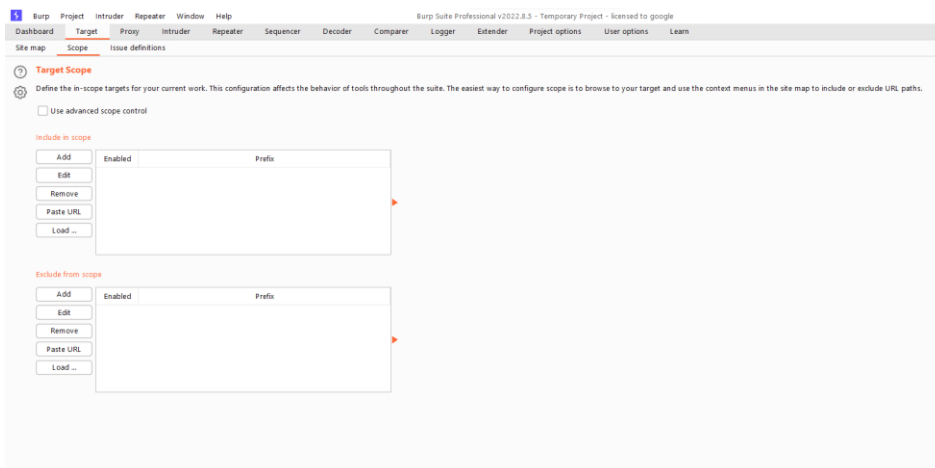

3. **Spider:** Burp Suite's Spider tool is a web crawler that navigates through the target application, mapping out its structure and identifying potential vulnerabilities. It helps in understanding the application's architecture.

4. **Scanner:** The Scanner tool automates the detection of common security issues in web applications. It scans for vulnerabilities such as SQL injection,

cross-site scripting (XSS), and more, providing a quick assessment of potential risks.

5. **Intruder:** The Intruder tool is used for automated attacks on web applications. It assists in identifying vulnerabilities related to input validation by sending multiple payloads to a target and analyzing the responses.
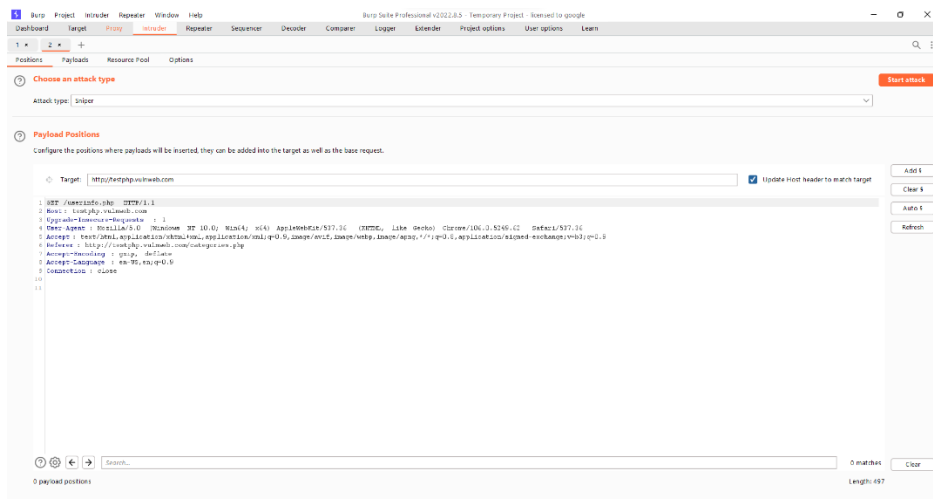

6. **Repeater**: The Repeater tool allows you to repeat and modify individual requests to the target application. It's useful for testing how the application responds to different inputs and for fine-tuning your testing approach.
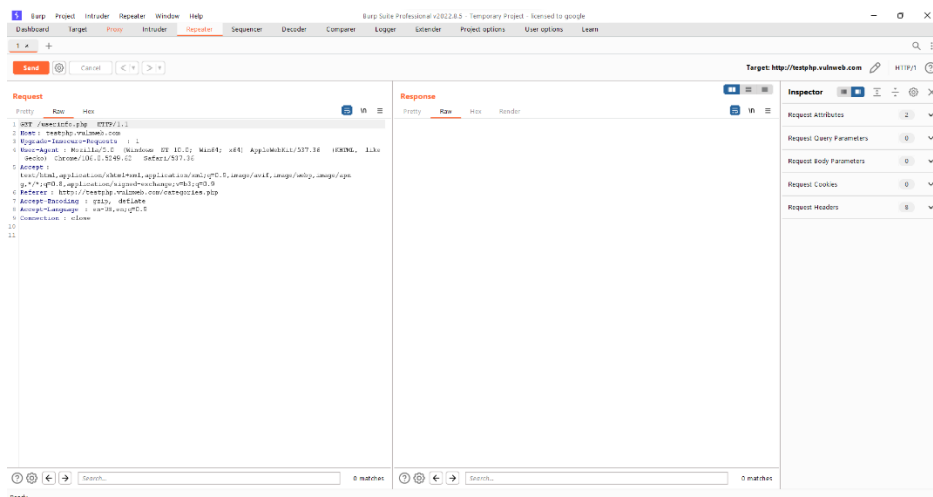

7. **Sequencer**: This tool analyzes the randomness and strength of tokens or session identifiers within the application. It helps in assessing the security of session management and token generation mechanisms.
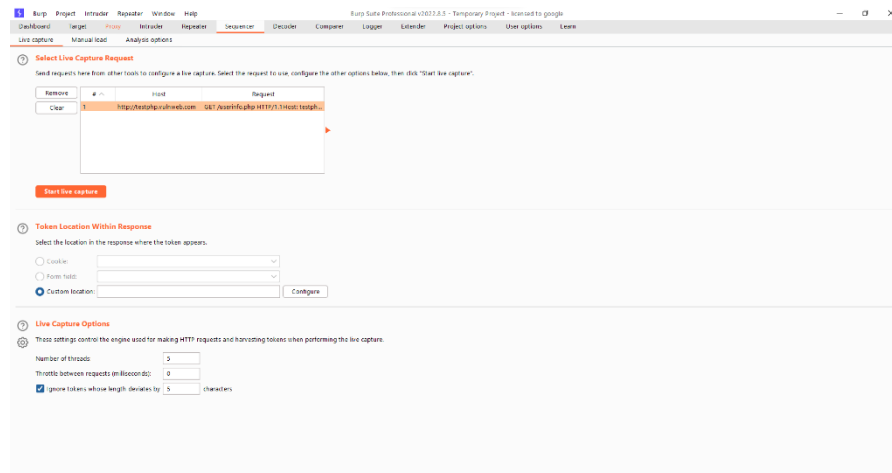
8. **Decoder:** The Decoder tool helps in decoding and encoding various types of data, such as URL parameters, base64, and more. It's useful for understanding how data is manipulated and for crafting specific payloads during testing.
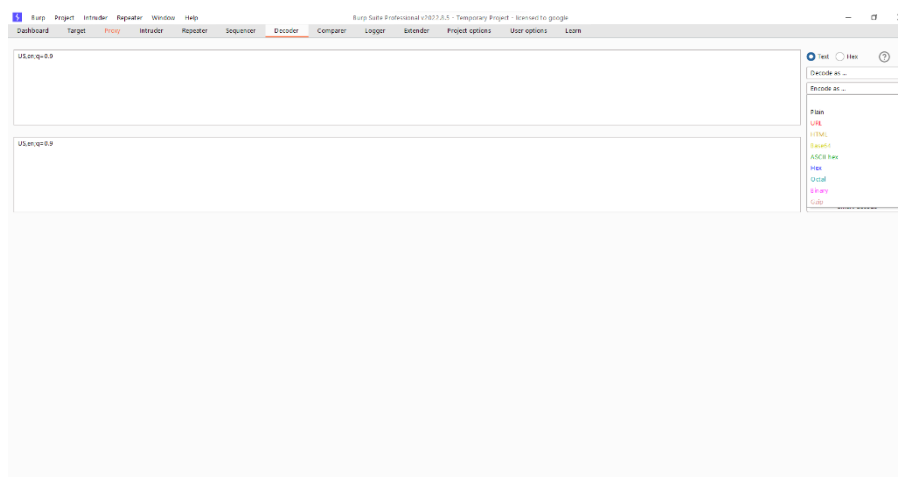

9. **Comparer:** Burp Suite's Comparer tool allows you to compare two pieces of data, such as requests or responses, to identify differences. This is helpful for finding anomalies and potential security issues.
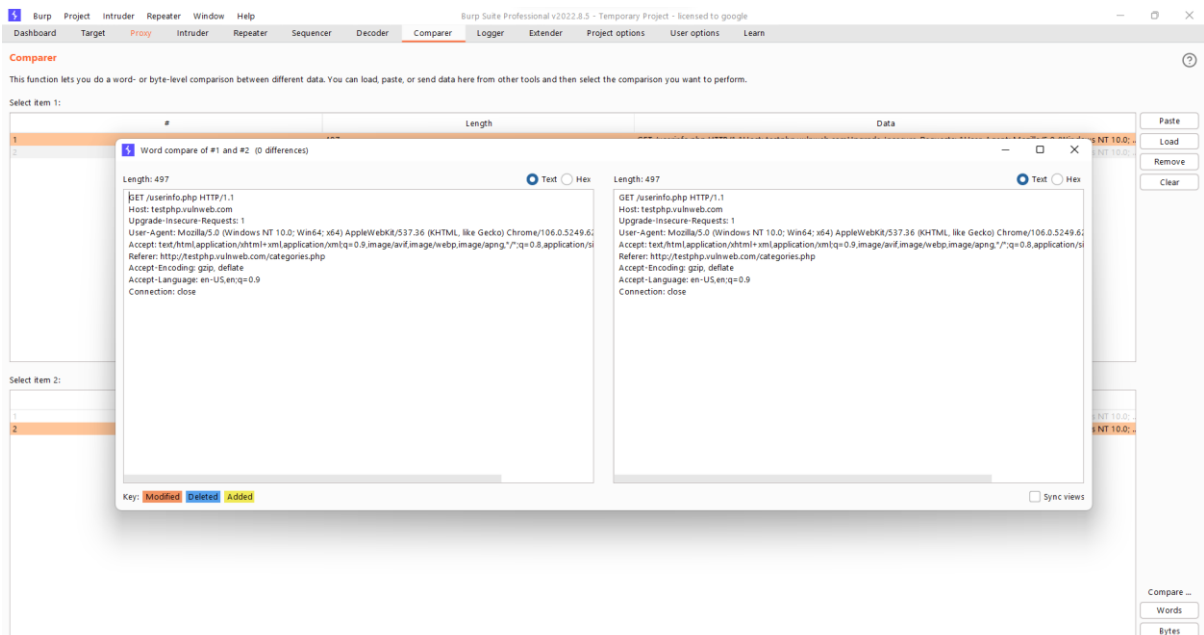
10. **Collaborator:** The Collaborator tool helps in detecting interactions between the target application and external systems. It's valuable for identifying potential security risks related to data leakage or unintended information disclosure.

11. **Extender:** The Extender tool allows you to enhance Burp Suite's functionality by adding extensions. Extensions can be custom scripts or plugins that provide additional features tailored to your testing needs.
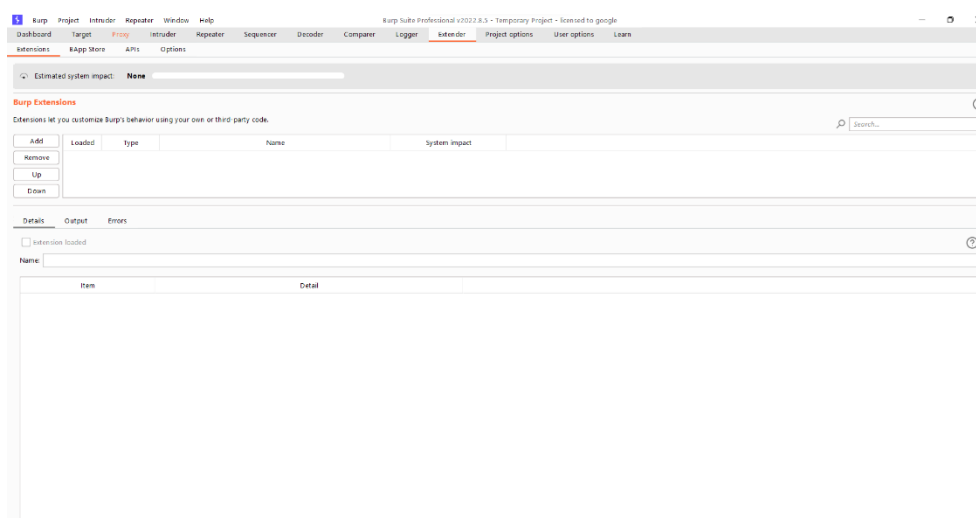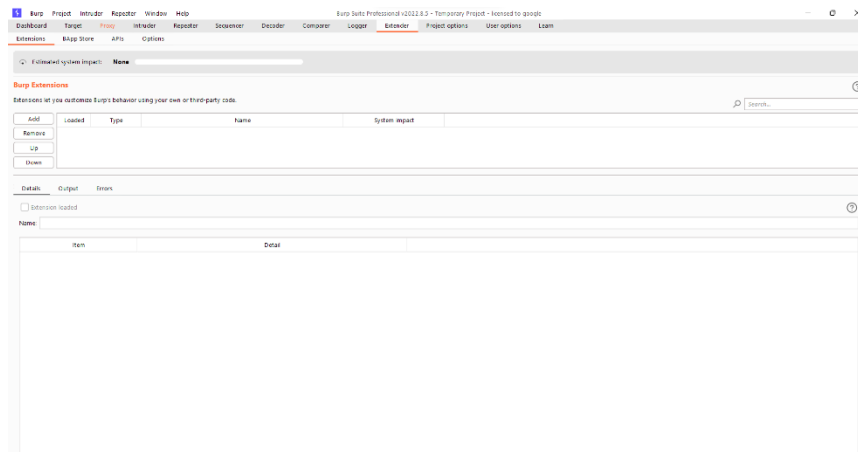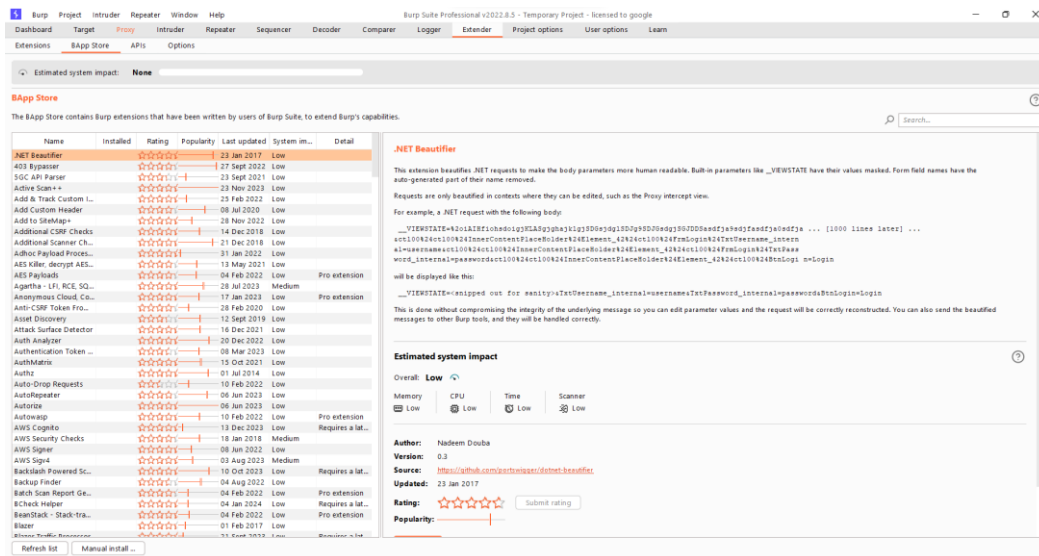
Room completed –
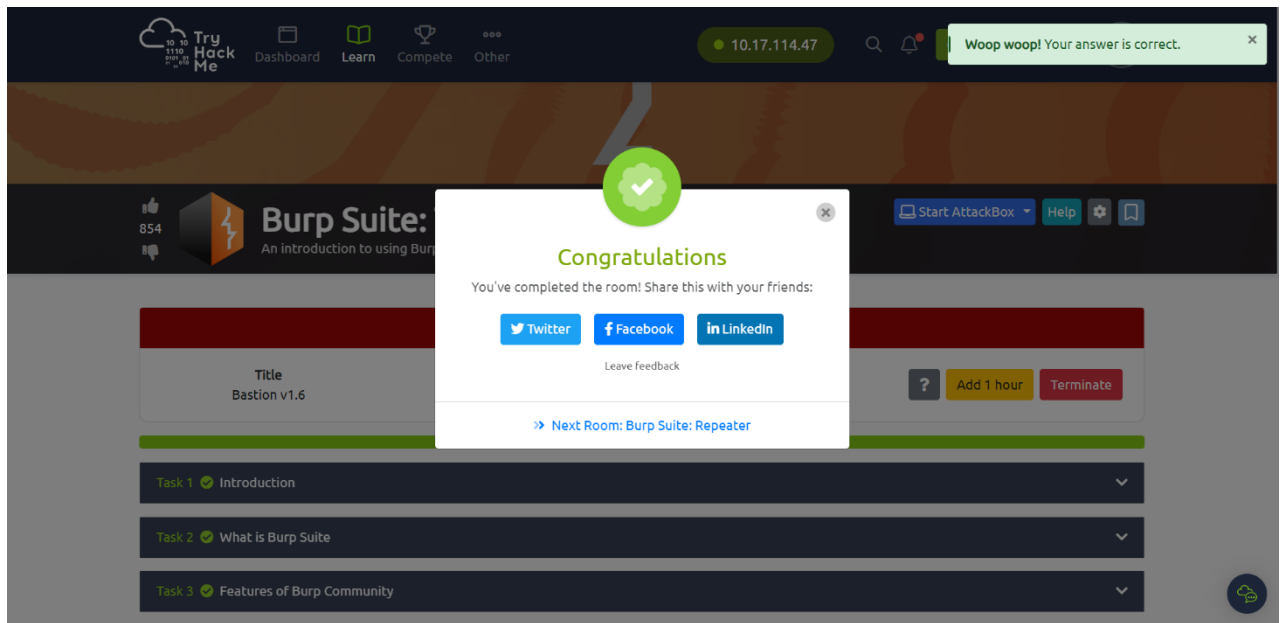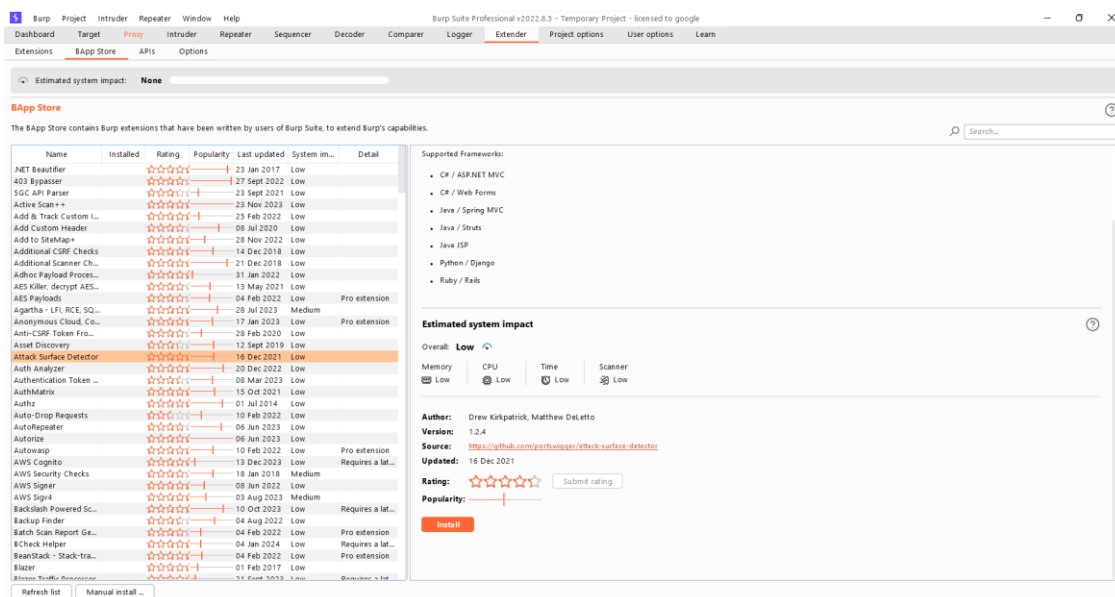

3. How to find and add Extensions in Burpsuite? –

Step 1 – open burpsuite and find extender tab

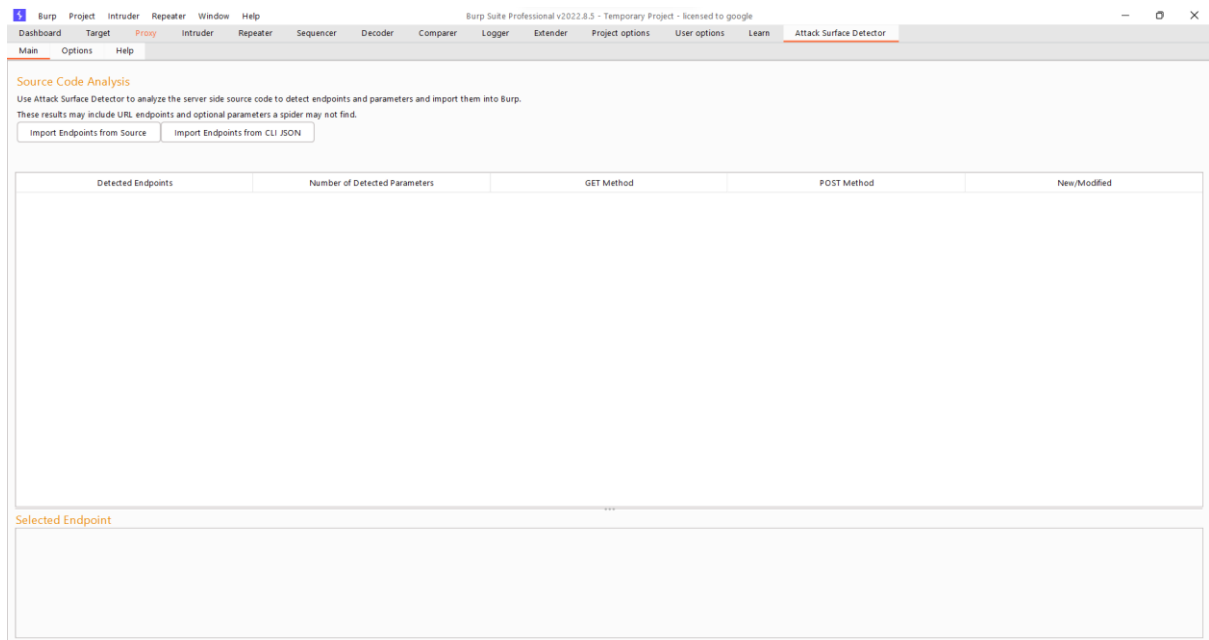**Step 2 –** go in subtab called **Bapp Store**

Step 3 – select extension you want and click for more details.

Step 4 – click on **install** button –

Step 5 – restart brave & navigate to that extension –

4. References –

https://www.geeksforgeeks.org/what-is-burp-suite/

https://blogs.perficient.com/2023/03/17/introduction-to-burp-suite-and-its-testing-features/

https://subscription.packtpub.com/book/web-development/9781783550111/9/ch09lvl1sec53/loading-and-installing-a-burp-extension-from-the-burp-app-store