EyeQ Dot Net Pvt. Ltd.

LEARN FROM REAL HACKERS

TASK 4: BURP SUITE

What is Burp Suite?

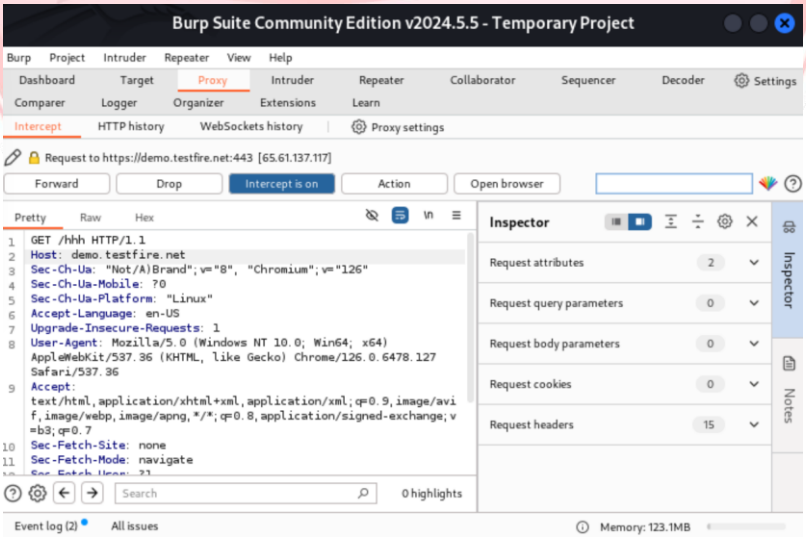
Burp Suite is a comprehensive security testing tool used to identify vulnerabilities in web applications. It offers various tools for scanning, crawling, and simulating attacks to analyze and strengthen application defenses. Widely used by penetration testers, Burp Suite provides an interactive platform to assess application security effectively.

What are the features available in Burp Suite?

Burp Suite includes several robust features for web application security:

1. Proxy:

The Proxy tool allows users to intercept and modify web traffic between the browser and target application, enabling detailed inspection and alteration of requests and responses in real-time.

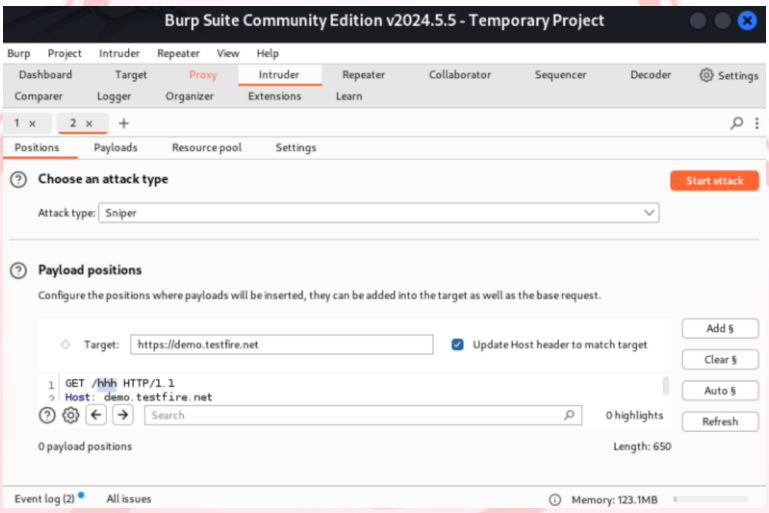


2. Scanner:

The Scanner automates the process of identifying vulnerabilities in web applications by performing comprehensive scans, detecting issues like SQL injection, cross-site scripting, and more, with detailed reporting.

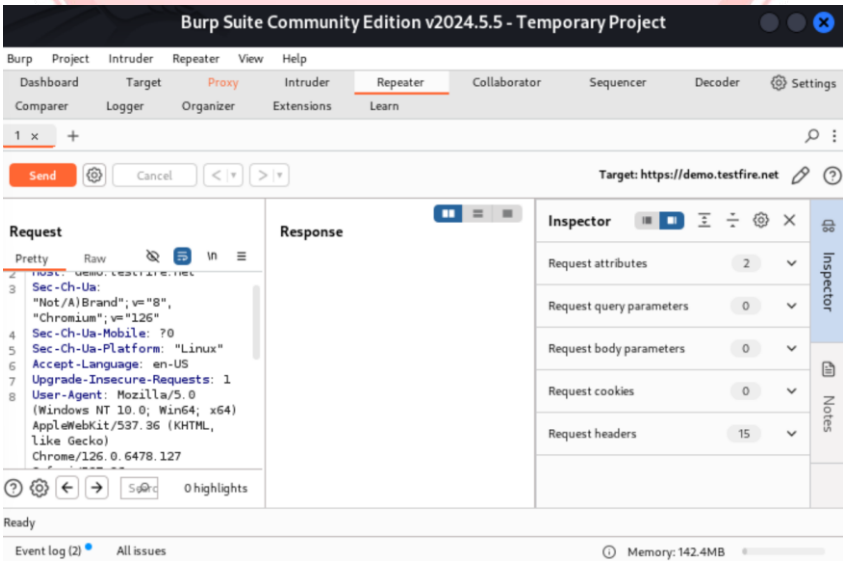
3. Intruder:

Intruder is used for automating customized attacks on web applications, allowing testers to conduct brute force attacks, enumerate users, and test various payloads to find weak points in the application's security.



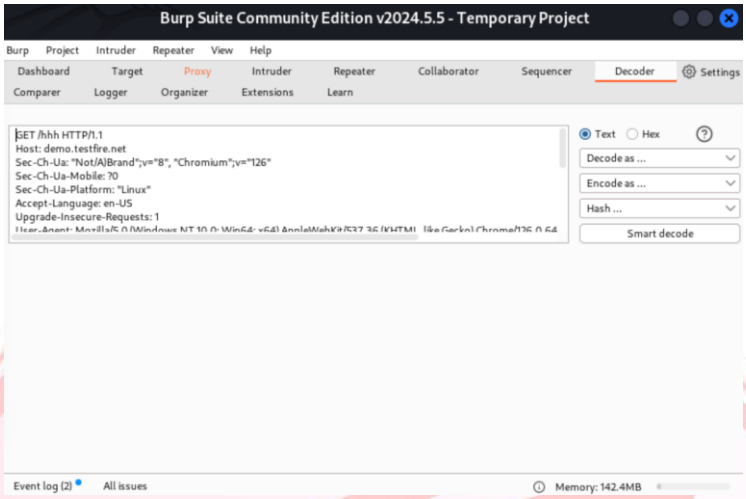
4. Repeater:

The Repeater tool allows testers to manually reissue HTTP requests with modifications, which is helpful for refining and verifying vulnerability exploitability.



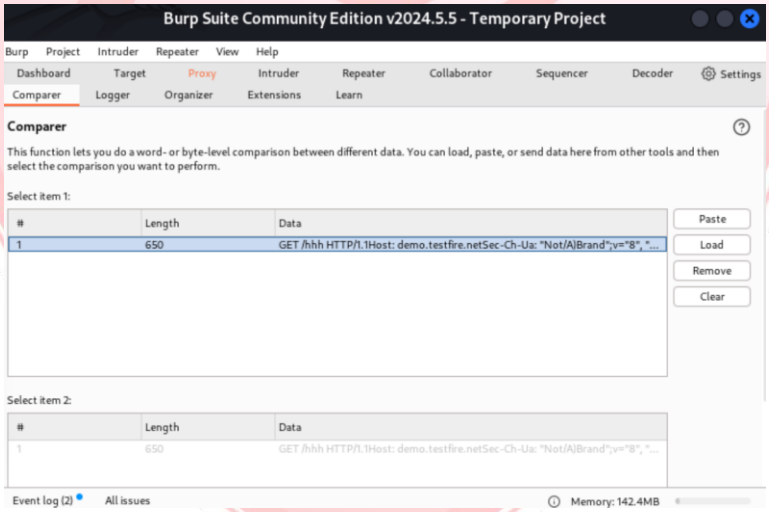
5. Decoder:

Decoder assists in encoding and decoding various data formats, making it easier to manipulate encoded data like URL, Base64, or hex formats during testing.



6. Comparer:

Comparer helps in analyzing differences between two items, such as requests or responses, making it easier to detect subtle changes that might indicate security issues.



7. Extensibility:

Burp Suite's extensibility feature supports plugins and custom scripts, allowing users to integrate additional tools or write custom scripts to enhance functionality tailored to specific testing needs.

What are the types of intruder attack in Burp Suite?

Burp Suite's Intruder tool supports various attack types for testing web application vulnerabilities:

1. Sniper:

This type targets one position in the request at a time, testing each payload individually, making it ideal for testing single parameters to identify potential injection points or vulnerabilities.

2. Battering Ram:

In Battering Ram attacks, the same payload is used across multiple positions in the request simultaneously, useful for identifying issues where the same input affects multiple parts of a request.

3. Pitchfork:

Pitchfork allows for synchronized payload lists to be used across multiple positions, testing each payload in parallel across the designated positions, which is efficient for testing coordinated input variations.

4. Cluster Bomb:

Cluster Bomb attacks use multiple payload sets in combination across positions, generating all possible permutations. This exhaustive approach is valuable for testing complex input dependencies in applications.

Here are scenario-based examples for each Burp Suite Intruder attack type:

1. Sniper:

If testing an input field for SQL injection, the Sniper attack inserts various payloads like ' OR '1'='1 to test the field one at a time, helping identify if any single input is vulnerable to SQL injection.

2. Battering Ram:

In a login form requiring a username and password, Battering Ram can insert the same payload, such as common usernames, across both fields to test if duplicate input triggers authentication vulnerabilities.

3. Pitchfork:

When testing a form with multiple parameters, such as `username` and `security_token`, Pitchfork can inject matching values like sequential IDs and corresponding tokens to assess if paired inputs bypass access controls.

4. Cluster Bomb:

For a multi-field form requiring combinations (e.g., username, password, and OTP), Cluster Bomb can try all permutations of usernames, passwords, and OTPs, revealing any bypass methods through unexpected combinations.

References:

https://portswigger.net/burp

https://chatgpt.com

https://www.google.co.in