Burp Suite Basics

Burp Suite is one of the most popular security testing tools. Burp Suite can be used to identify different types of vulnerabilities, such as SQL injection or cross-site scripting, by testing the web application beyond its graphical user interface (GUI). It is a type of proxy server, which means it sits between the user’s web browser and the web server to observe and manipulate all the data that is being sent back and forth.
Burp Suite has different features such as proxy, Repeater, intruder, scanner, decoder, and more.

Use case: -

1. **Web Application Vulnerability Scanning: -**
    - Burp Suite's scanner can automatically detect vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more.

2. **Intercepting and Modifying HTTP/S Traffic: -**

    - **Proxy**: Burp Suite functions as a proxy server, allowing testers to intercept, inspect, and modify HTTP/S requests and responses between the browser and the target application.

- **Repeater**: Allows testers to manually modify and resend individual HTTP requests to test how the application responds to different inputs.

3. Analyzing and Exploiting Vulnerabilities: -

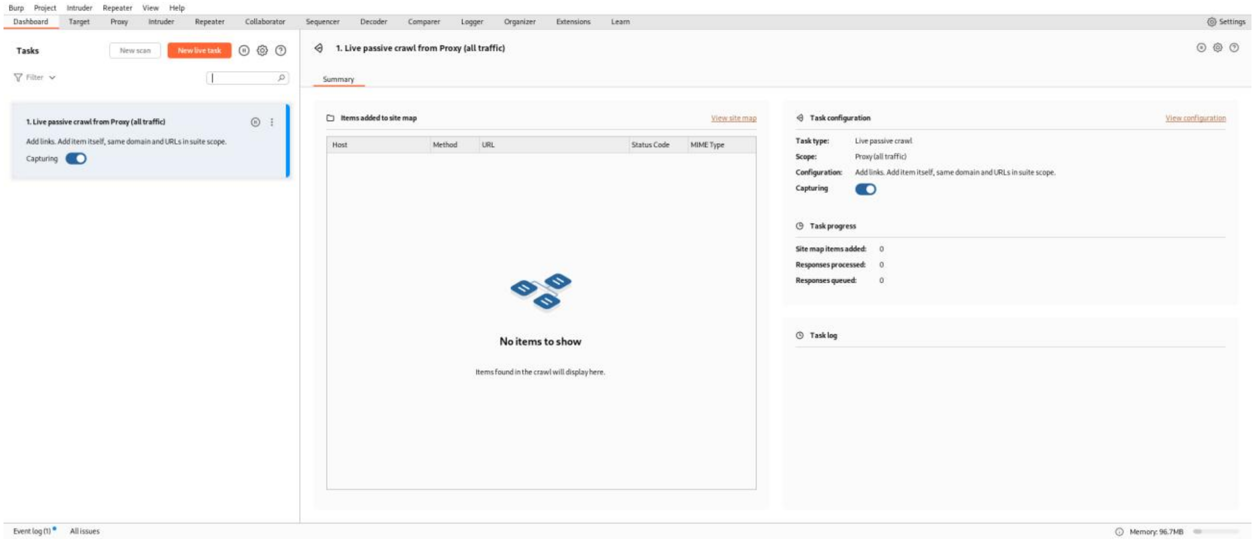
- **Intruder**: Allows for automated customized attacks, such as fuzzing, by iterating through payloads and monitoring responses to identify vulnerabilities.
- **Scanner**: Automated scanning to find vulnerabilities, including advanced scanning options for more in-depth analysis.
- **Extender**: Allows integration of third-party plugins and scripts to extend Burp Suite’s functionality, which can be used to exploit discovered vulnerabilities or enhance testing capabilities.

4. Spidering and Crawling: -

- **Enumeration**: Useful for enumerating directories, files, and parameters within the web application to ensure all possible attack surfaces are identified.

Tab Overview: -

1. The Dashboard tab in Burp Suite provides a centralized view of all ongoing and completed tasks, making it easier to manage the workflow during a security assessment. It includes an event log that tracks significant events and notifications, ensuring that testers are aware of any important developments. The issues section lists discovered vulnerabilities, providing a quick overview of potential security problems that need to be addressed. The activity map offers a visual representation of the application's activity, helping testers understand the interactions and flow of data within the application.



1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

Items added to site map

Host	Method	URL	Status Code	MIME Type

No items to show

Items found in the crawl will display here.

Task configuration

Task type:	Live passive crawl
Scope:	Proxy (all traffic)
Configuration:	Add links. Add item itself, same domain and URLs in suite scope.
Capturing	

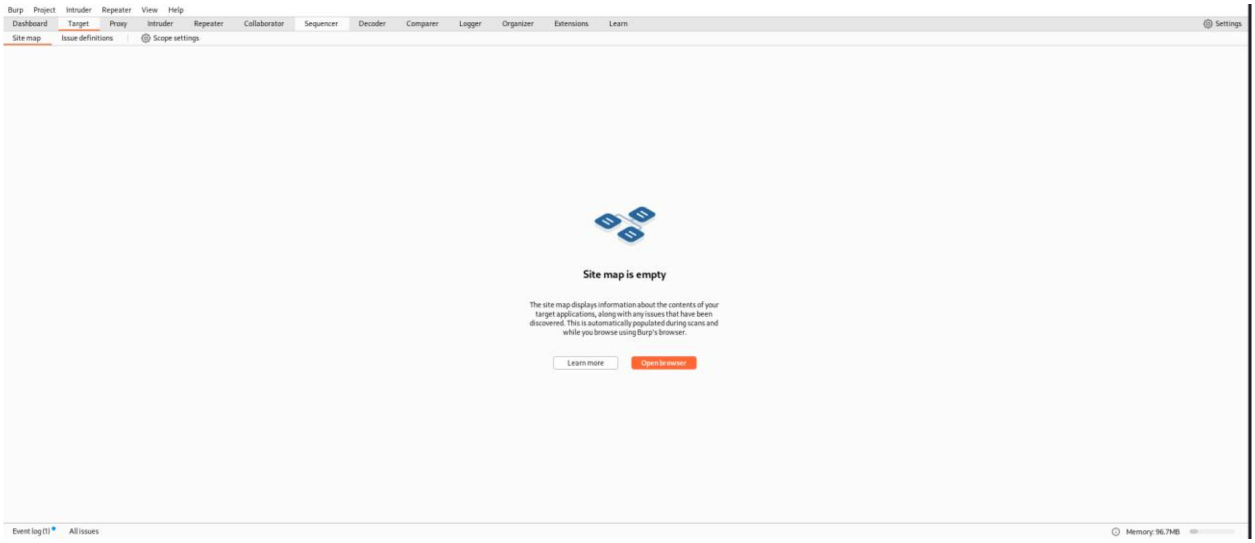
Task progress

Site map items added:	0
Responses processed:	0
Responses queued:	0

Task log

Memory: 96.7MB

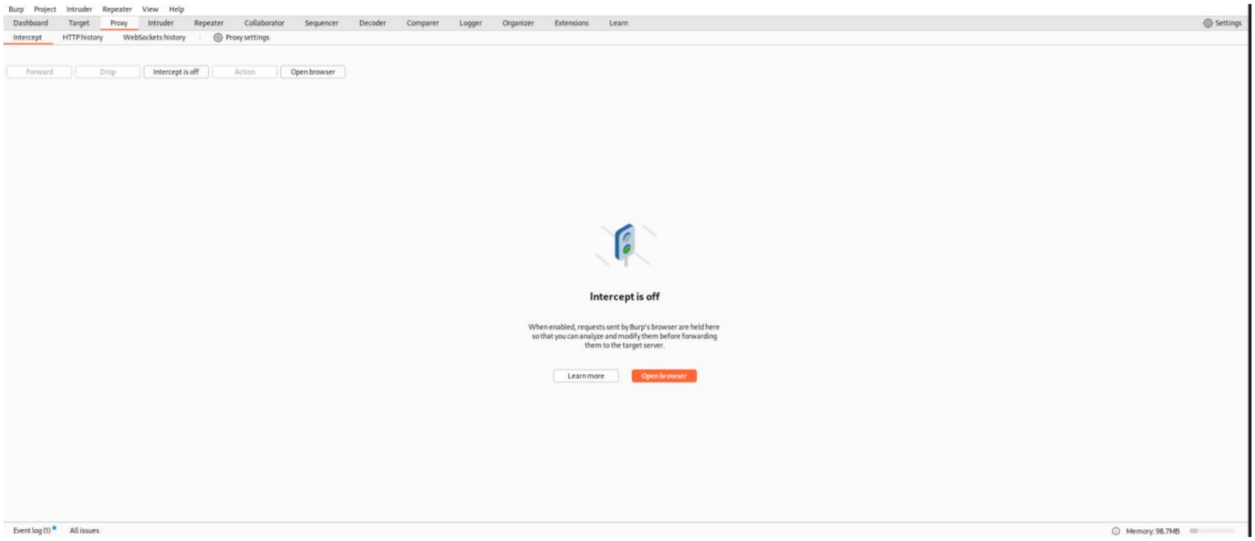
2. The Target tab is crucial for setting the scope and structure of the web application under test. It displays a hierarchical site map that shows all discovered URLs and endpoints, allowing testers to navigate the application's structure easily. Users can define the scope, specifying which parts of the application are included in the testing process. This tab also includes issue definitions, providing detailed descriptions of various security issues that Burp Suite can detect, helping testers understand the potential risks and remediation steps.



Site map is empty

The site map displays information about the contents of your target applications, along with any issues that have been discovered. This is automatically populated during scans and while you browse using Burp's browser.

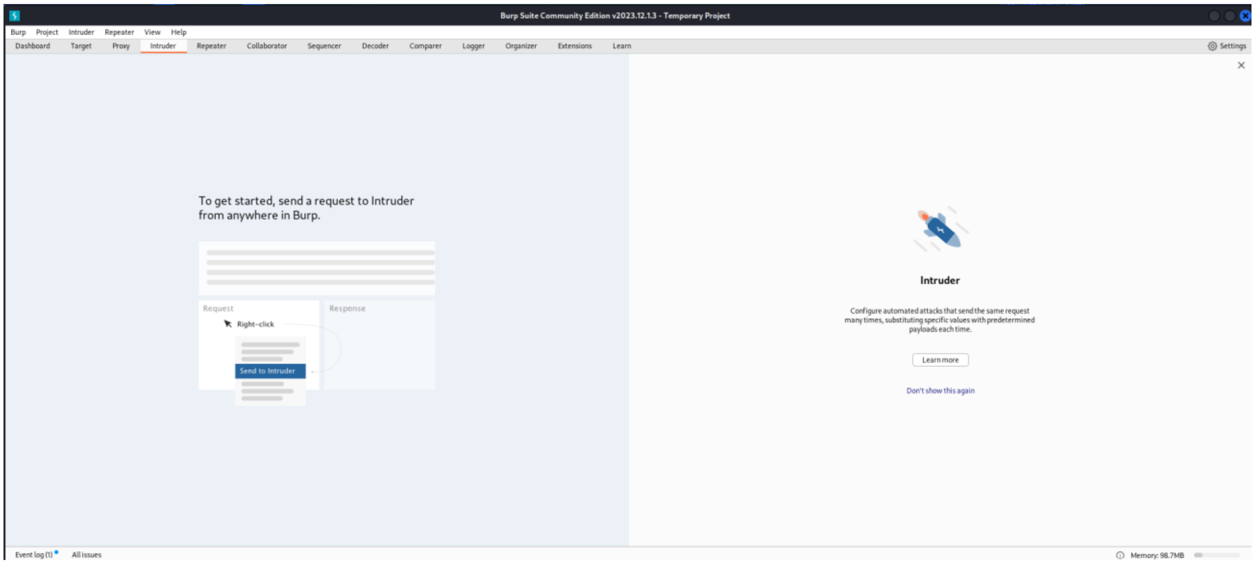
3. Burp Suite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in Burp Suite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back IP and a port. The proxy can also be configured to filter out specific types of request-response pairs.



Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

4. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. Burp Suite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:
    - Brute-force attacks on password forms, pin forms, and other such forms.
    - The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
    - Testing and attacking rate limiting on the web-app.



Burp Suite Community Edition v2023.12.1.3 - Temporary Project

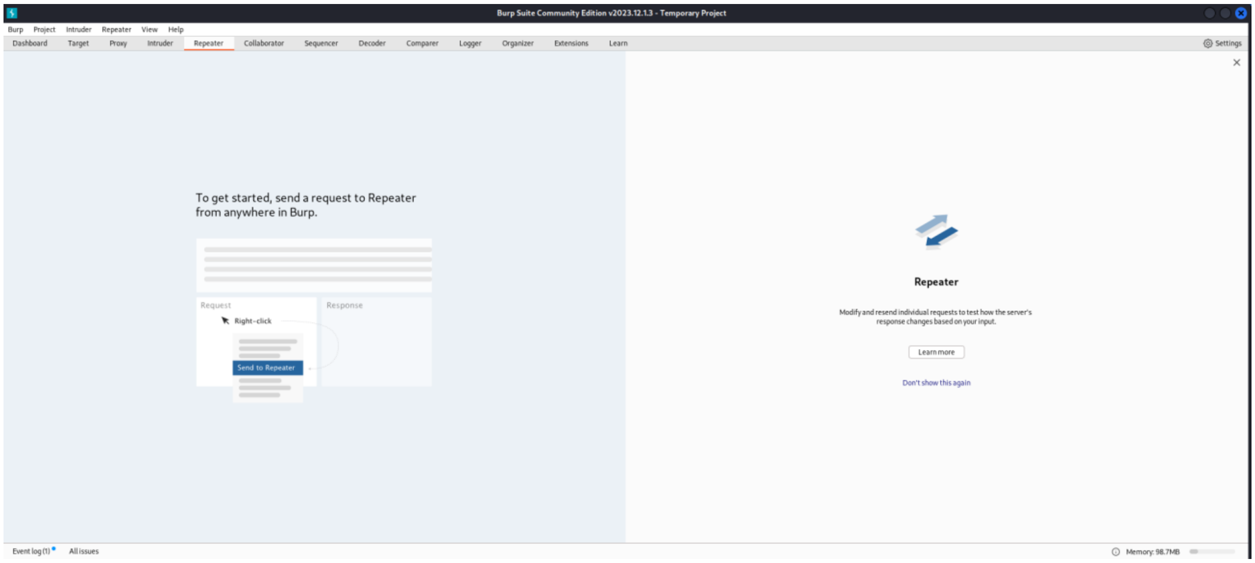
To get started, send a request to Intruder from anywhere in Burp.

Intruder

Configure automated attacks that send the same request many times, substituting specific values with predetermined payloads each time.

Memory: 98.7MB

5. The **Repeater** tab is used for manual testing of HTTP/S requests. It provides a Request/Response Editor where testers can manually modify and resend requests to observe how the application responds. This tab is particularly useful for verifying vulnerabilities discovered during automated scanning or exploring potential security issues in greater detail. The History sub-tab tracks and reviews all repeated requests and responses, allowing testers to keep a record of their manual testing efforts.

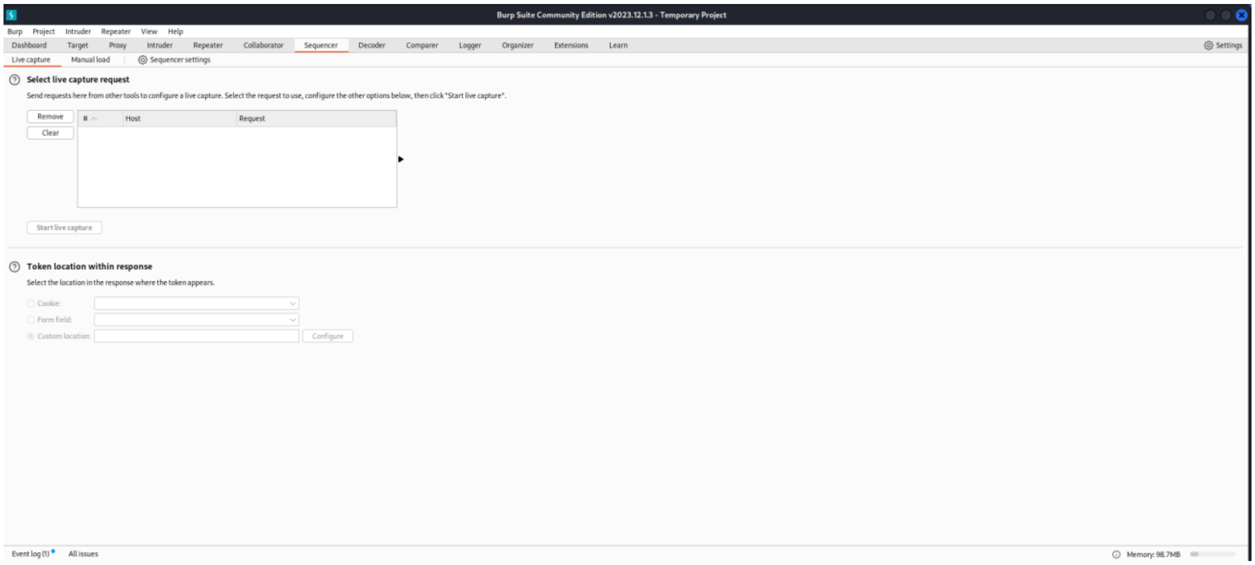


To get started, send a request to Repeater from anywhere in Burp.

Repeater

Modify and resend individual requests to test how the server's response changes based on your input.

6. The **Sequencer** tab is dedicated to analyzing the randomness of session tokens and other data. The Live Capture sub-tab allows real-time capture of tokens, while the Manual Load sub-tab enables manual loading of captured data for analysis. The Analysis sub-tab performs statistical analysis to evaluate the quality of randomness, which is crucial for ensuring the security of session management mechanisms in the web application.


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Live capture Manual load Sequencer settings
Remove
Clear
# Host Request
Start live capture
Cookie:
Form field:
Custom location:
Configure
Event log (1) All issues
Memory: 98.7MB

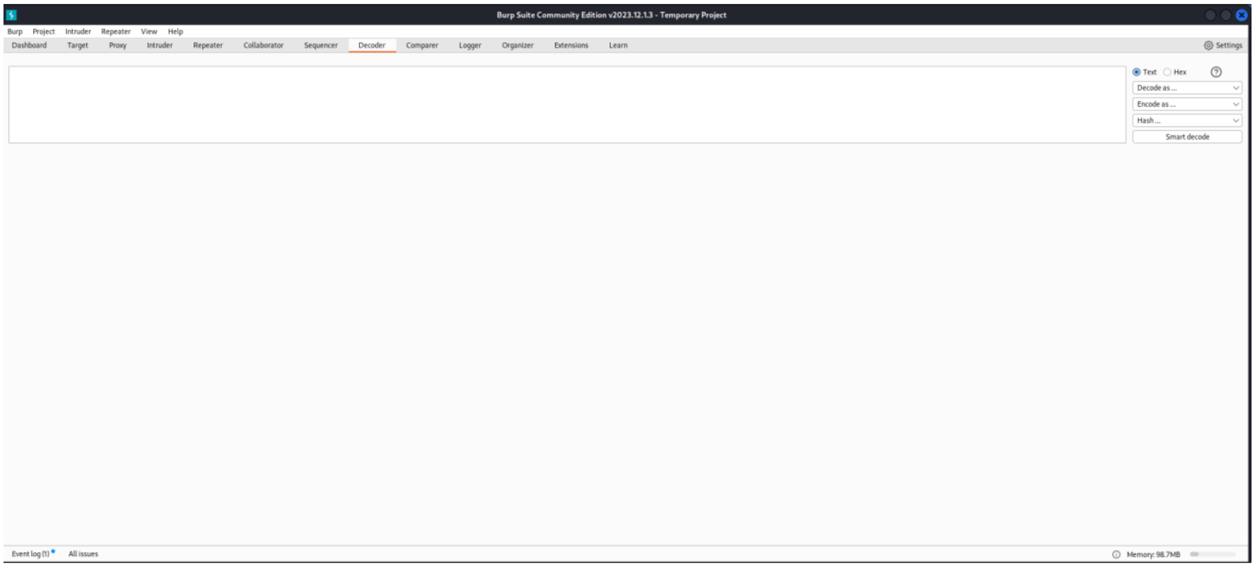
Select live capture request

Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".

Token location within response

Select the location in the response where the token appears.

7. The Decoder tab provides tools for encoding and decoding data using various schemes, such as Base64, URL, and HTML encoding. The Input/Output sub-tab allows testers to quickly encode or decode data, which is useful for analyzing and manipulating encoded payloads or responses. The History sub-tab tracks encoding and decoding operations, providing a record of transformations performed during testing.


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp
Project
Intruder
Repeater
View
Help
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Settings
● Text
○ Hex
?
Decode as ...
Encode as ...
Hash ...
Smart decode
Event log (1)
All issues
Memory: 98.7MB