Name of Capstone Project : -
Burp-Suite

- By Vikram Singh

Agenda

- Introduction of Burp-Suite.
  - Types of Burp Suite
  - Module of Burp suite
    1. Dashboard
    2. Target
    3. Proxy
    4. Repeater
    5. Intruder
    6. Sequencer
    7. Decoder
    8. Comparer

Introduction of Burp-Suite

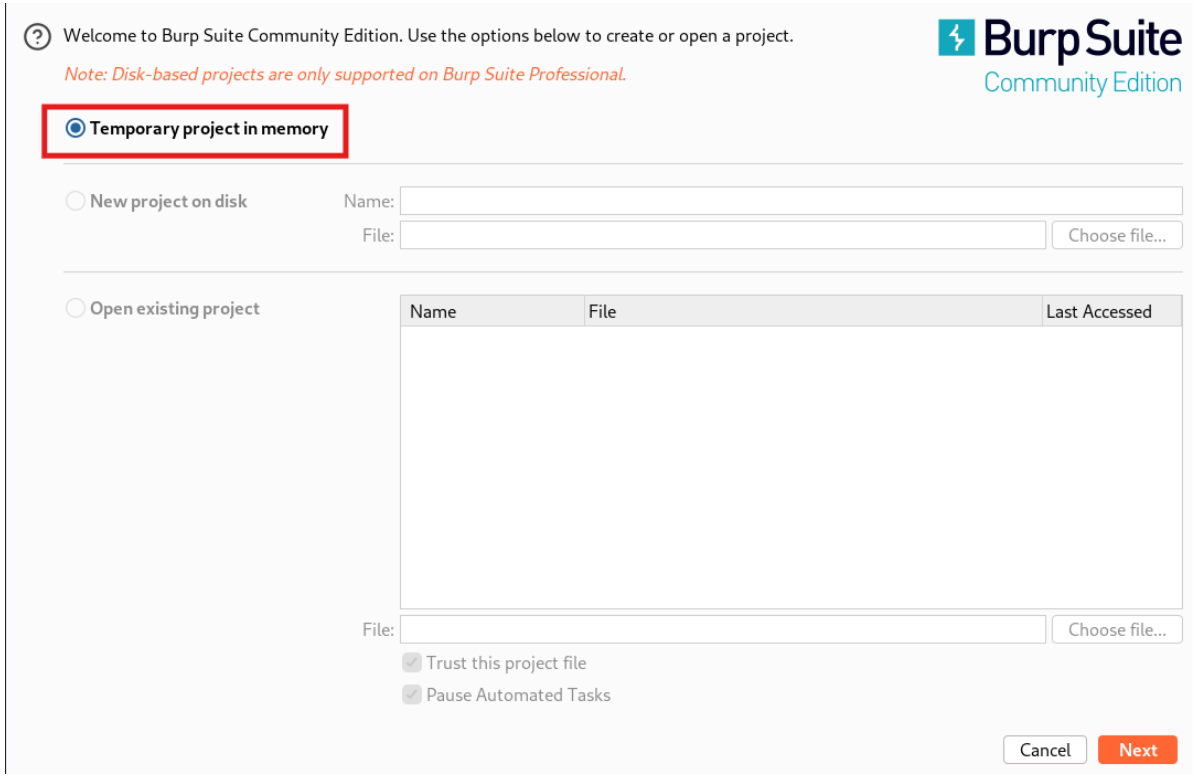
- What is Burp-Suite ?
  - Burp-Suite is a popular cybersecurity tool use for web application testing and find the vulnerability and exploit it.
  - Burp-Suite is known as a Proxy tool its intercept the request between client and server PCs, and It manipulate the request and response by capturing the packet.
  - It is written in Java and Developed by PortSwigger Security.
  - It is available for all Operation Systems like : - Windows, Linux, MacOS.

  - **Burp-Suite has three version:**
    1. **Community Edition (Free)** : Basic manual testing tools, includes an Intercepting proxy, repeater, decoder, and comparer.. NO automated scanning or advance tools. Suitable for beginners and learning purpose.
    2. **Professional Edition (Paid)** : Includes everything in the Community Edition, Automated vulnerability scanner for finding security flaws. Intruder tool for brute force, fuzzing, and parameter testing. Pricing : $449 usd per user/year
    3. **Enterprise Edition** : It Designed for large-scale automated security testing. Role based access control for teams. **Pricing** : $6995 per year, depending on the number of users.

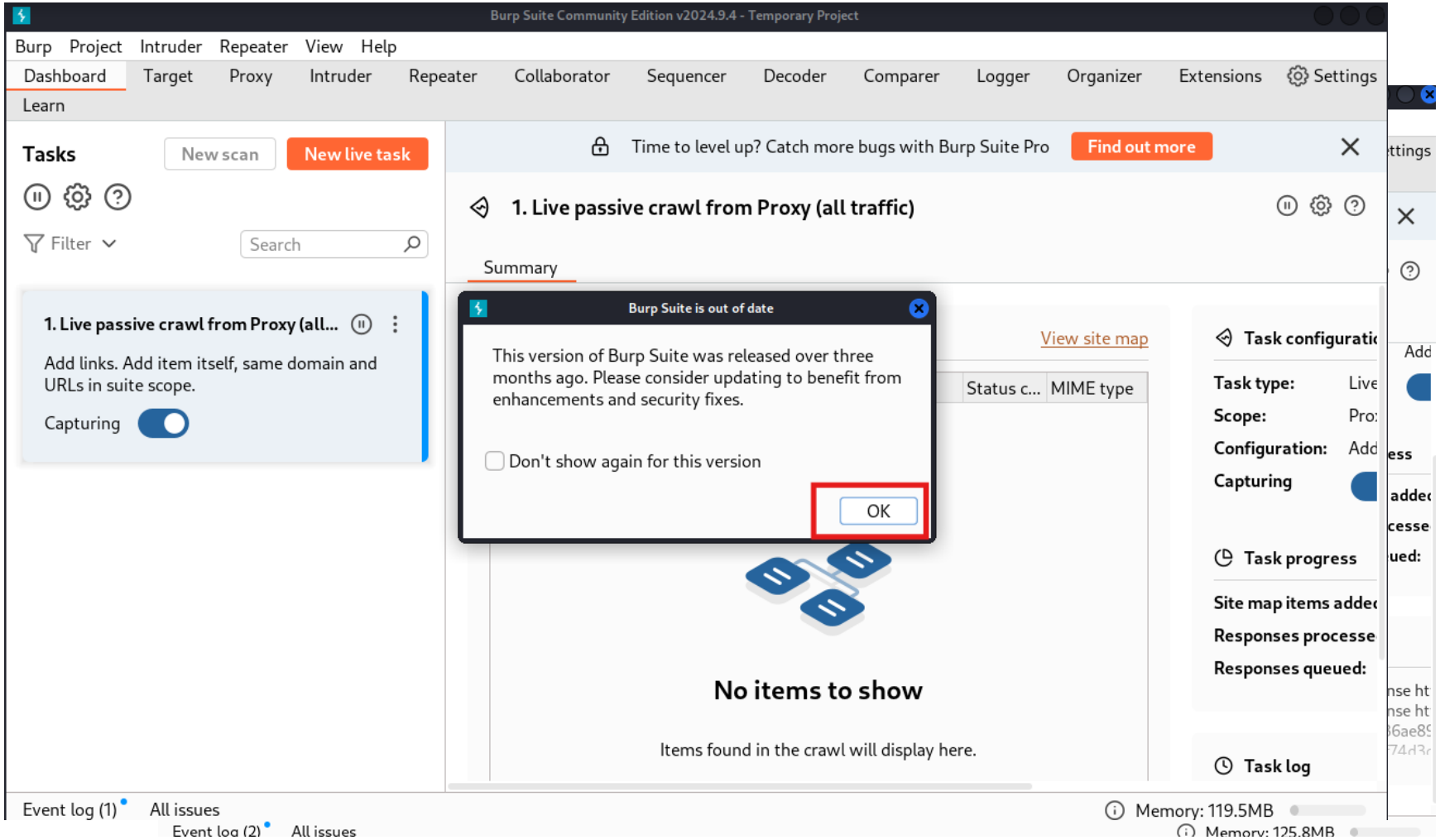
    - **Download links : -**
      - Burp-Suite Community Edition : https://portswigger.net/burp/releases/professional-community-2025-1-1
      - Burp-Suite Professional Edition : https://portswigger.net/burp/releases/professional-community-2025-1-1
      - Burp-Suite Enterprise Edition : https://portswigger.net/burp/releases/enterprise-edition-2025-1-1

I am using Burp-suit Community edition in this Project.

- Temporary project in memory : It create a temporary project in the Community edition Disk based project support in professional edition.

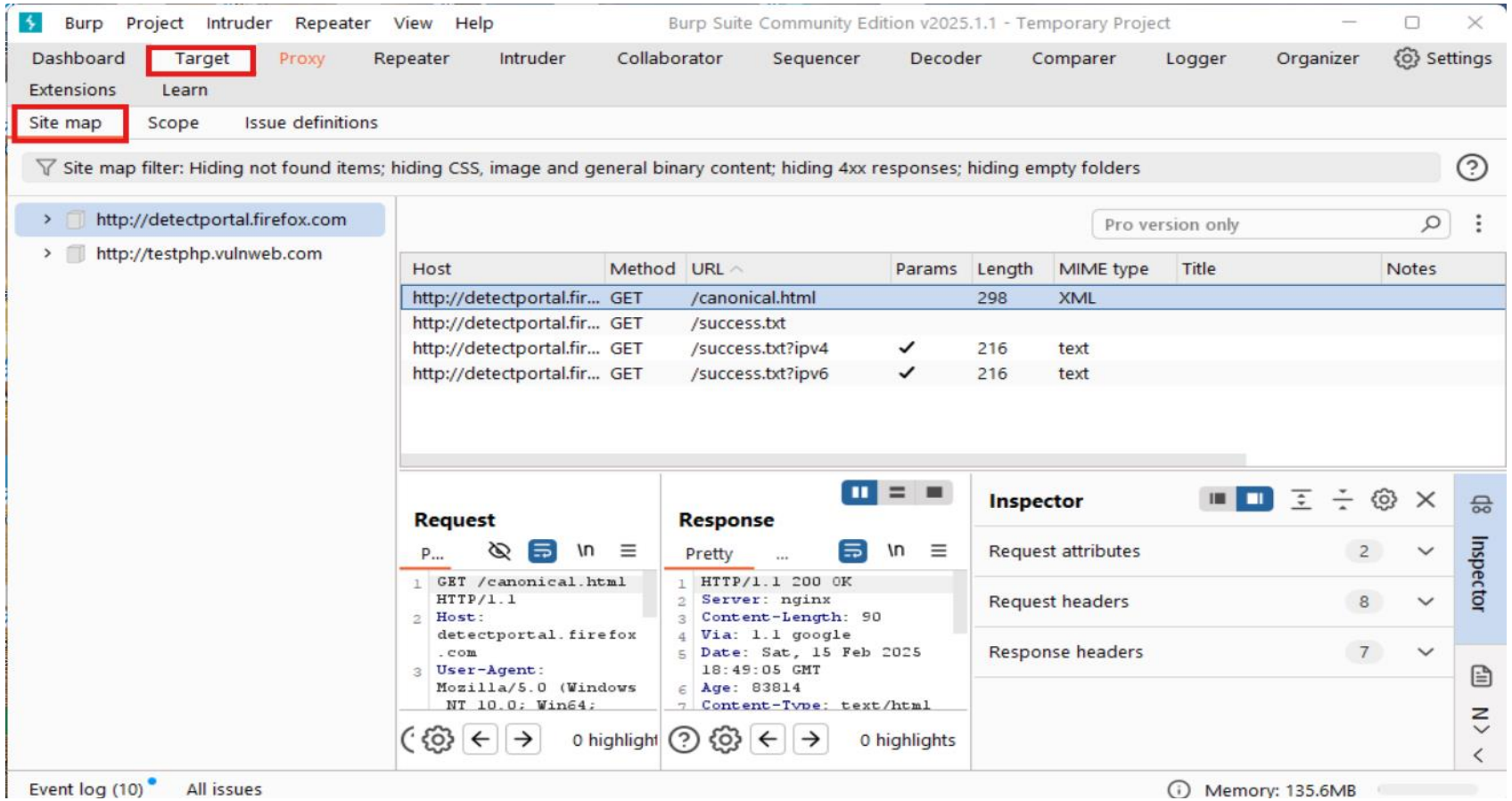


1. Dashboard :- It provides an overview of running tasks, scan results, and vulnerability findings.

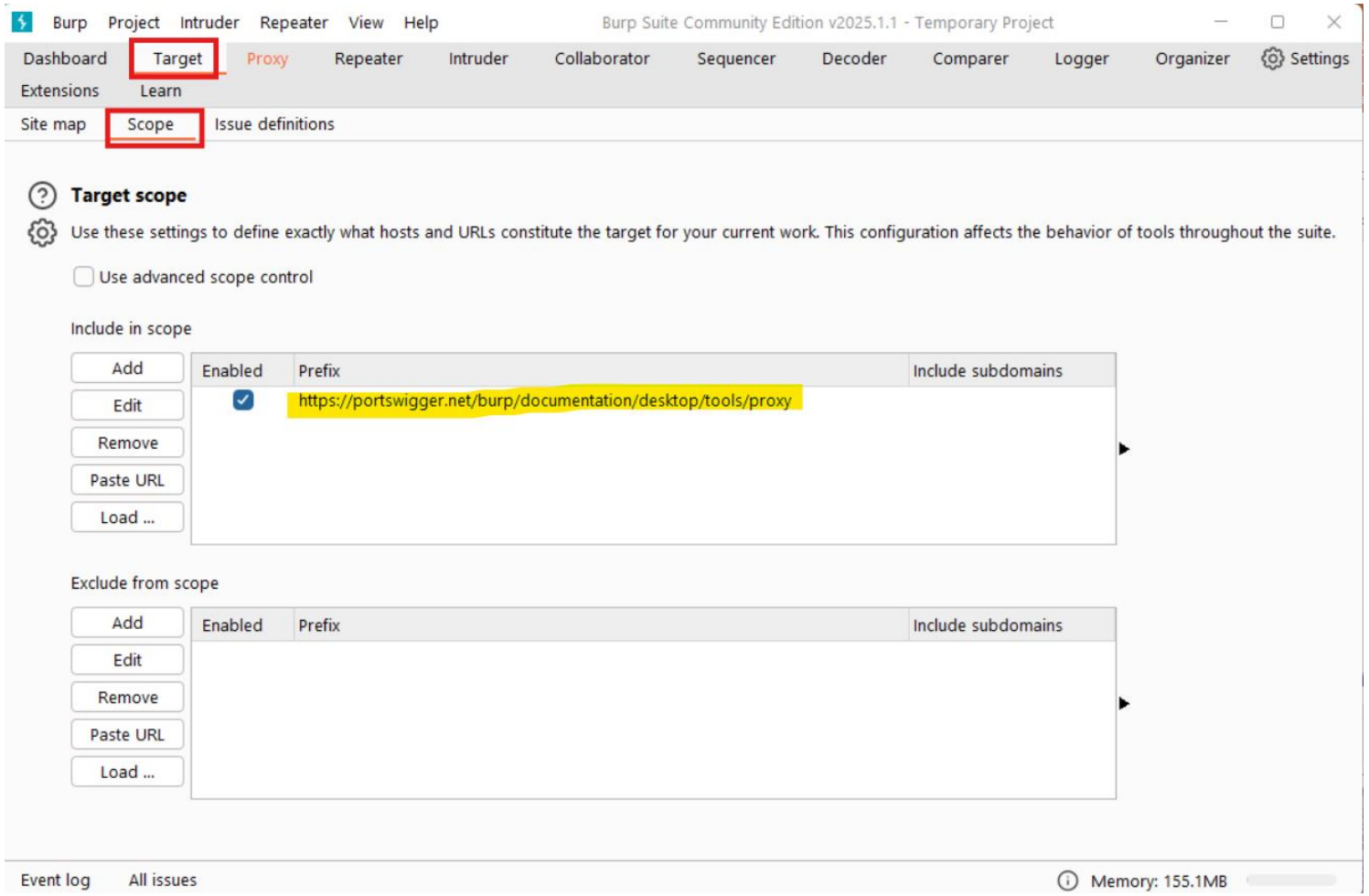


2. Target : - The Target tab gives a overview of the target.

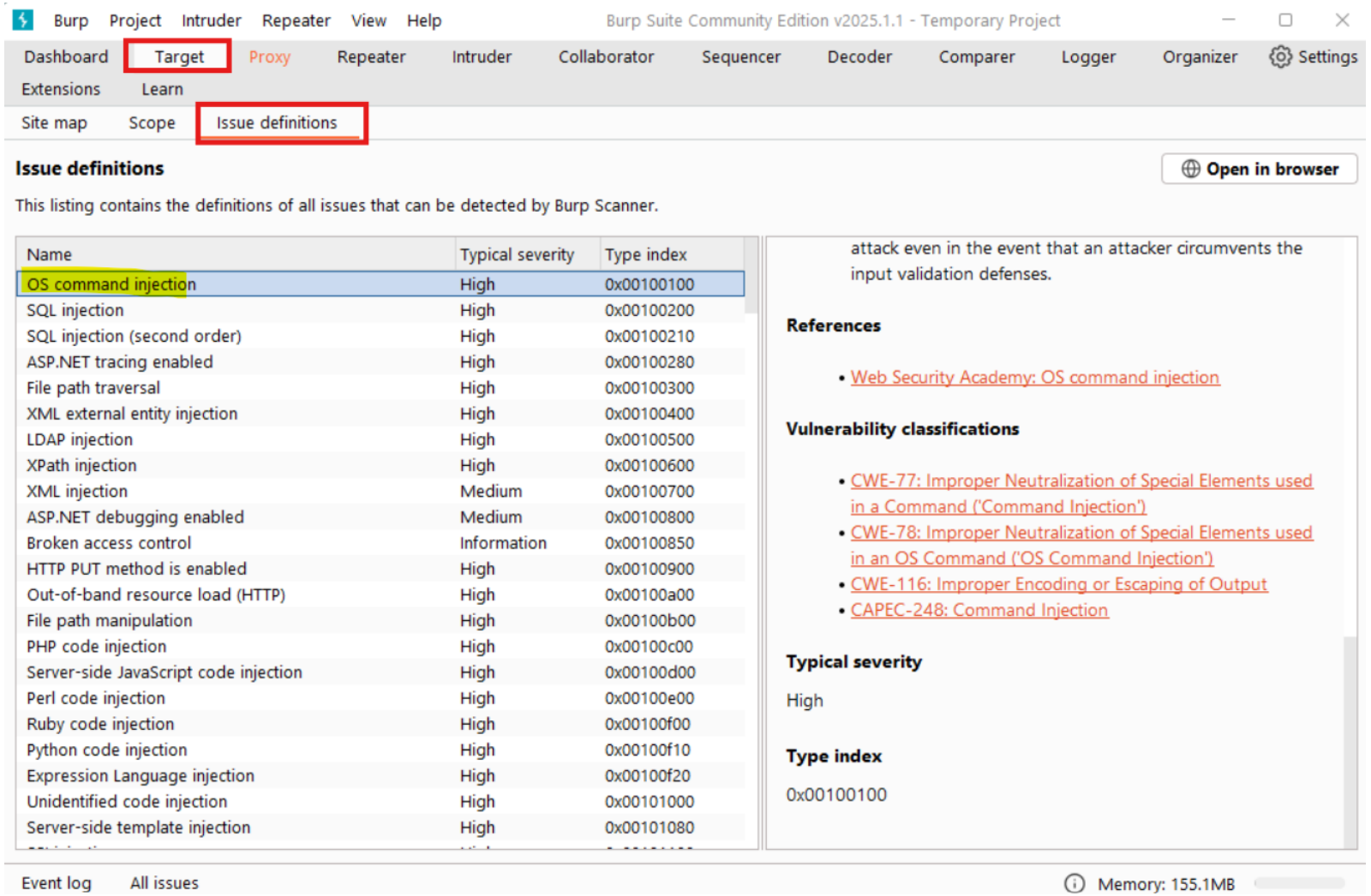
- **Site map : -** Its displays a hierarchical view of all domains and endpoints discovered during testing. Allow users to analyze request/response structures, parameters, and vulnerabilities and helps in identifying attack surfaces.



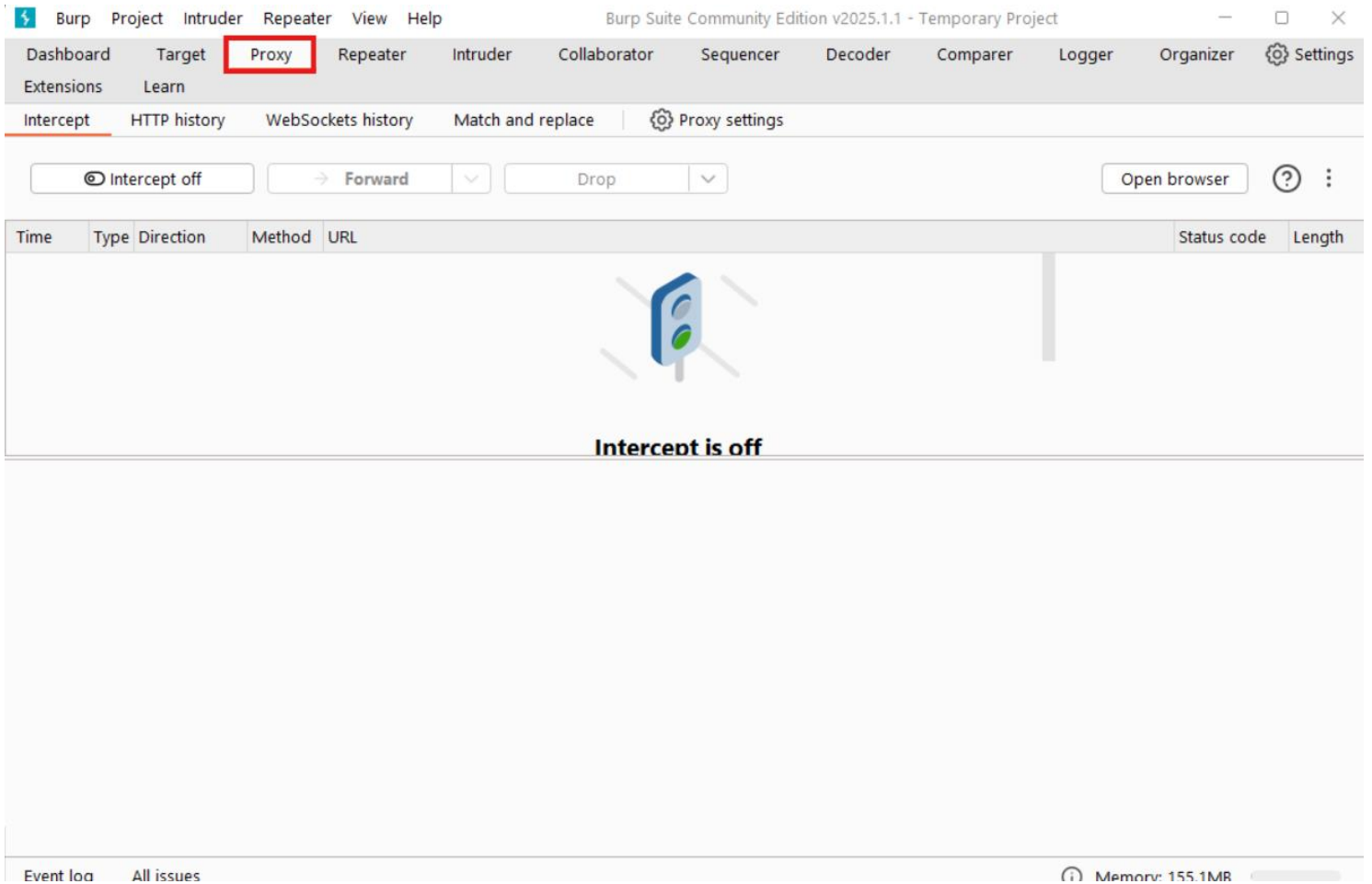
- **Scope : -** In the scope management define which URLs should be included or excluded from testing. Avoid unnecessary or out-of-scope endpoints (t3rd party services). Prevents accidental testing of production environments.



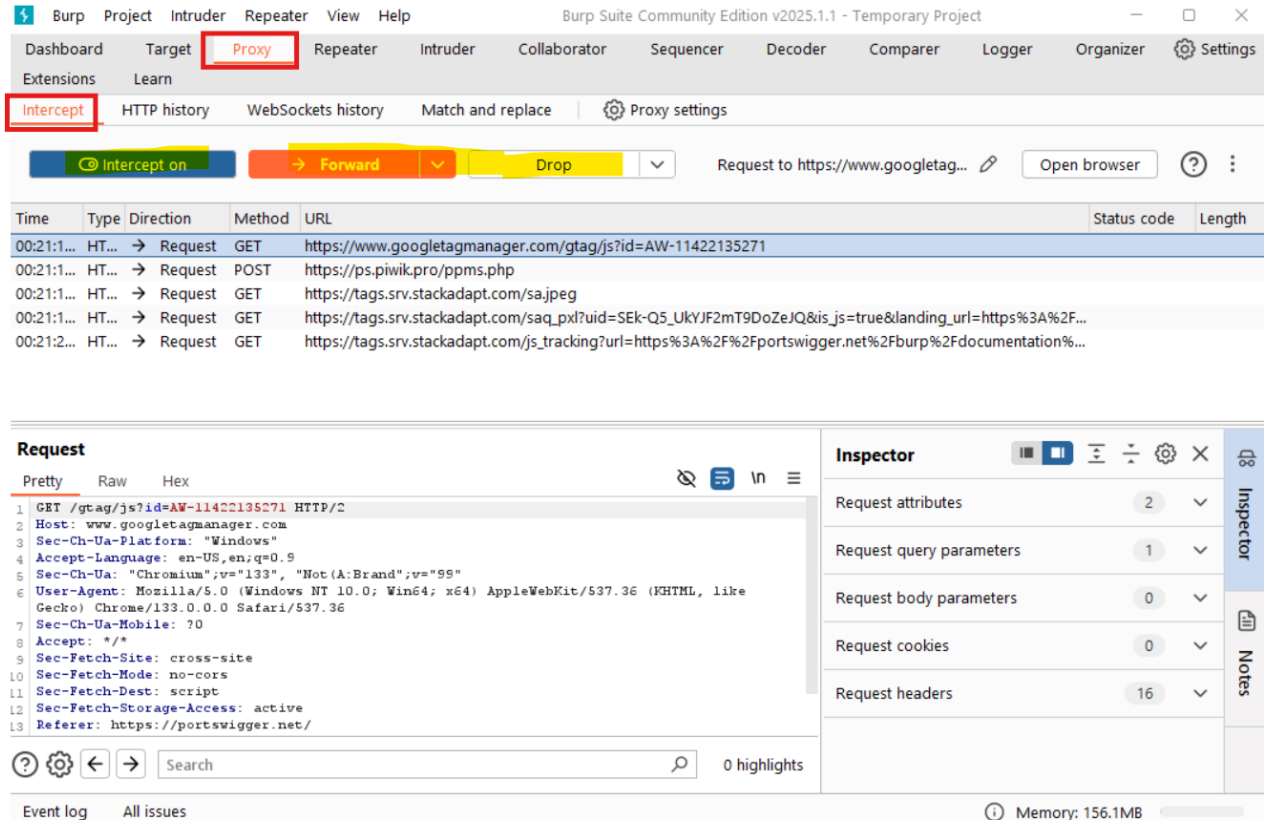
- **Scope Definitions : -** It marks security issues like XSS, SQL injection, Broken Authentication etc.



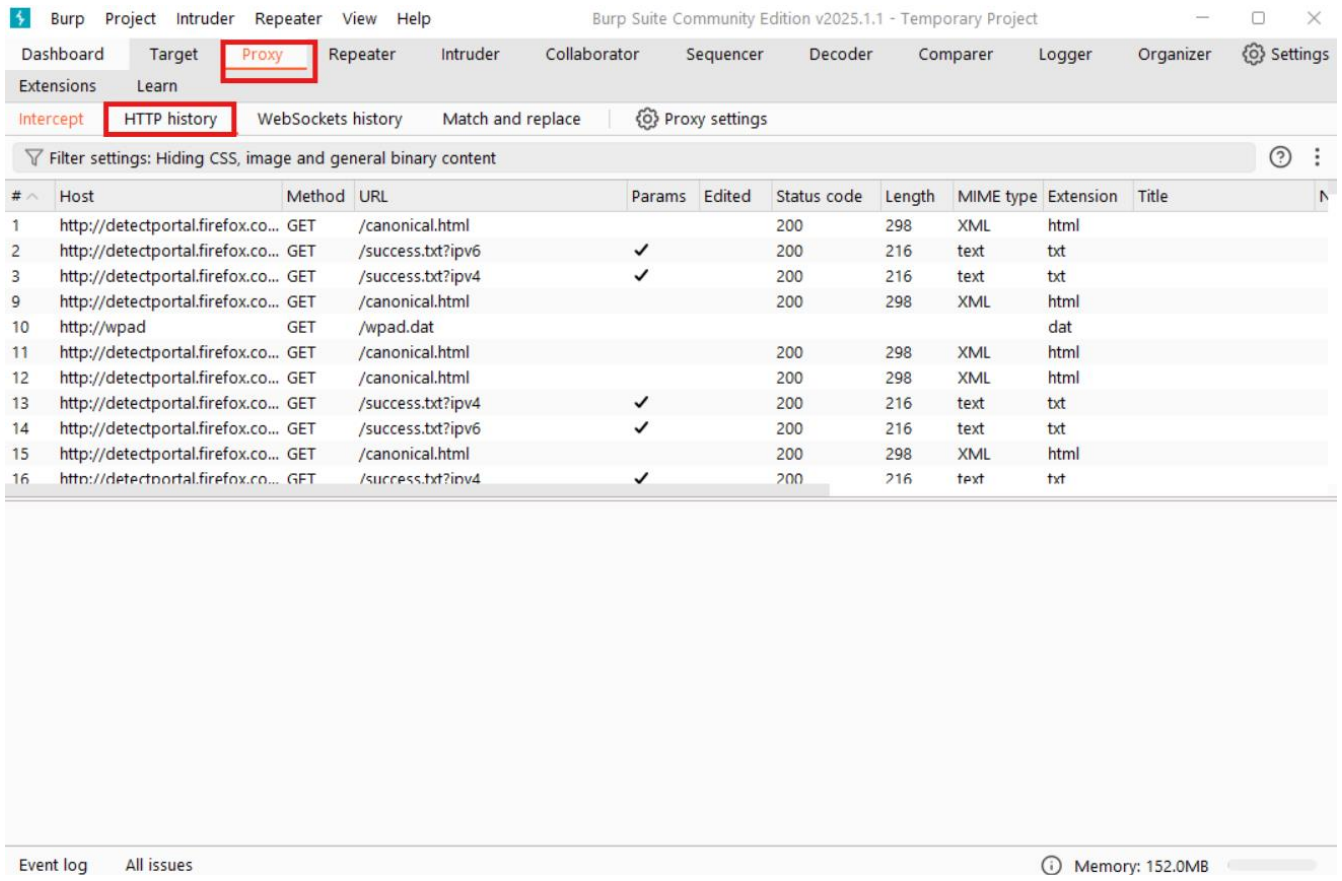
3. Proxy : - The Proxy is core feature of the burp-suite. It operates as a web proxy server, and sits as a man-in-the-middle between your browser and destination web servers. Its intercept, modify and anlayze HTTP(s) traffic between the browser and the server.



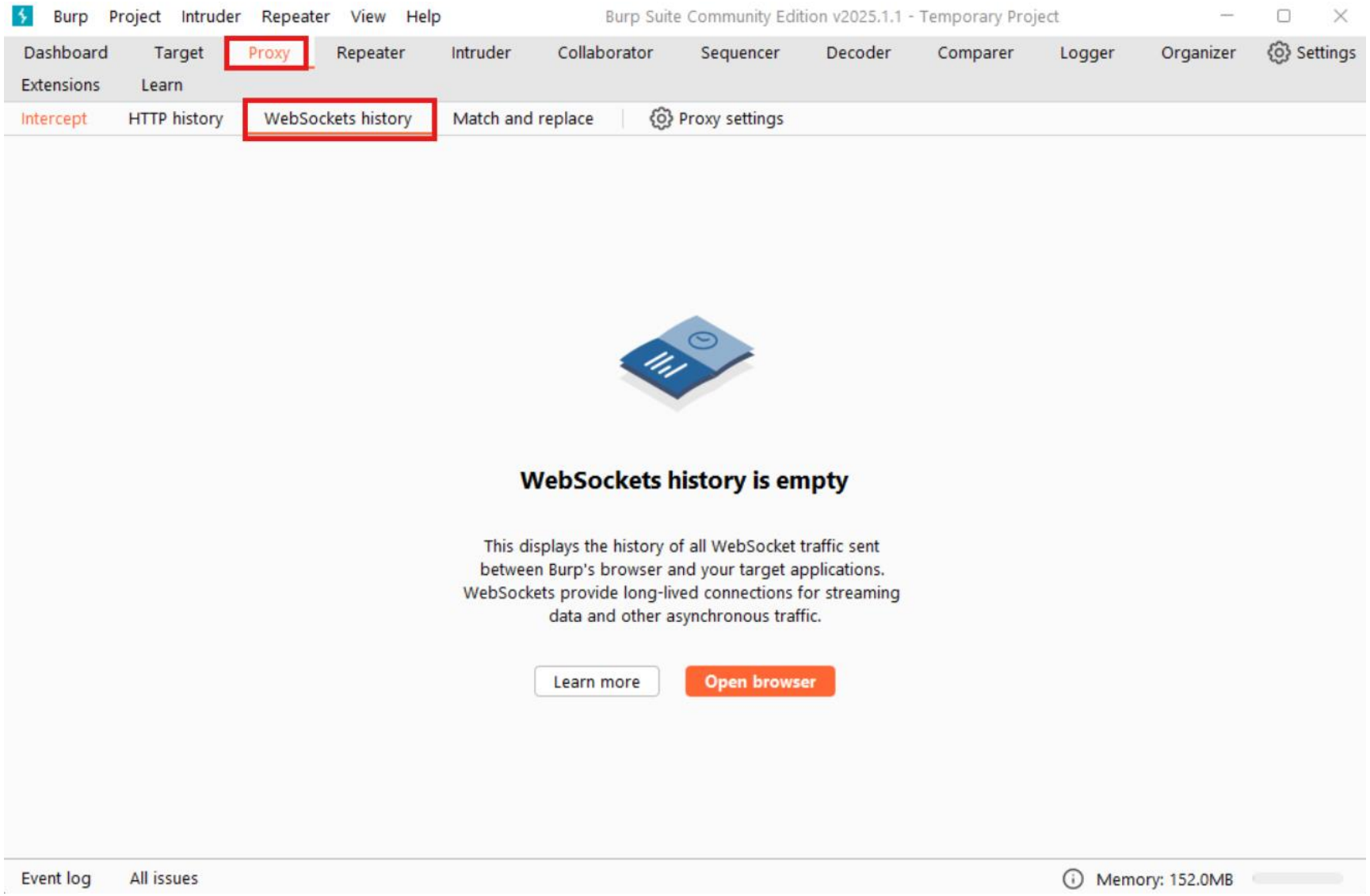
- **Intercept : -** It intercept HTTP(s) Request & Response.
  - Captures traffic between the browser and web server.
  - Allows manual modification before forwarding the request/response.



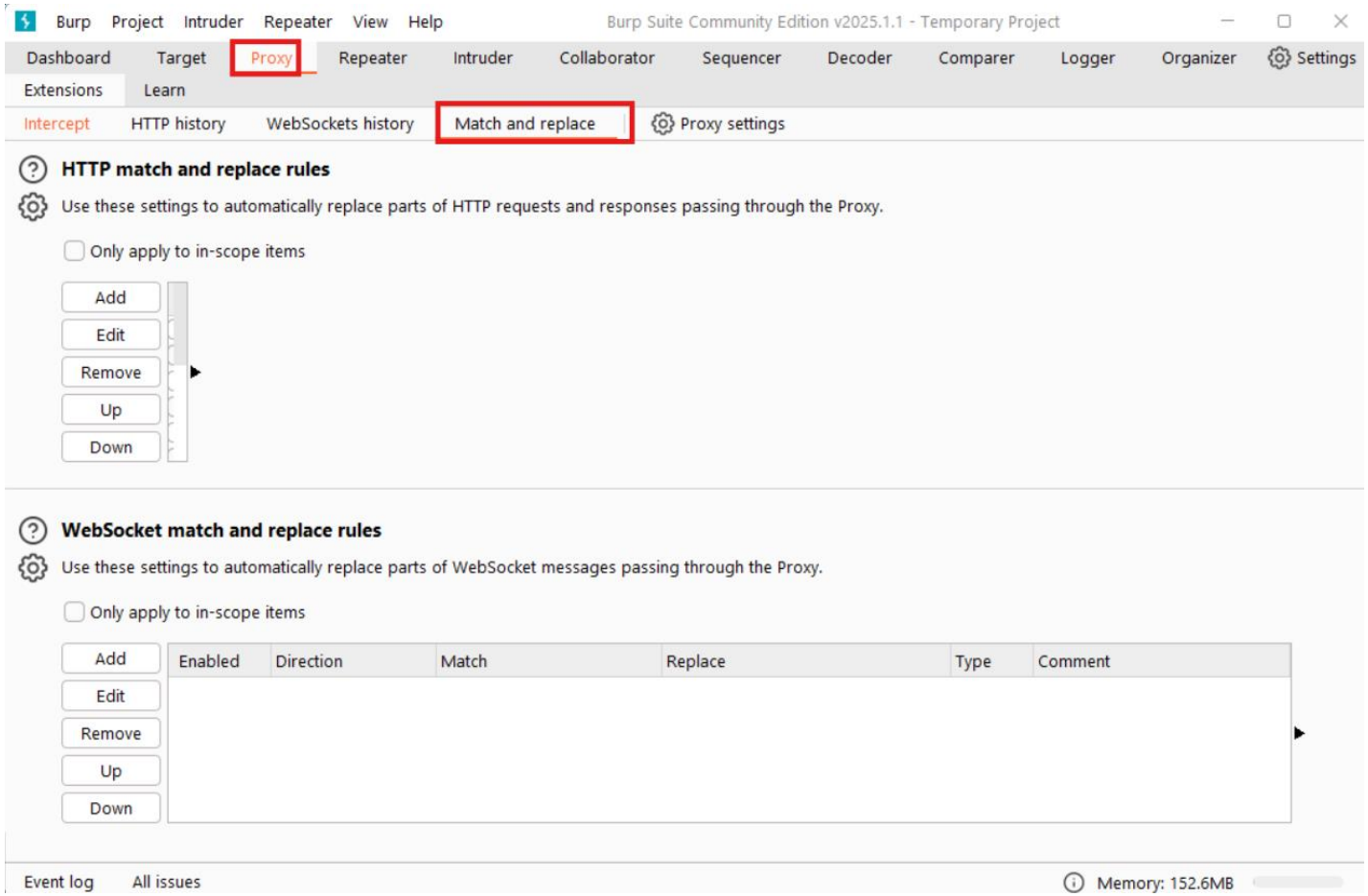
- **HTTP history : -** It contain the history of the web application.
    - It stores all captured request and response for the later analyze.
    - Helps track user interactions, authentication tokens, and API requests.



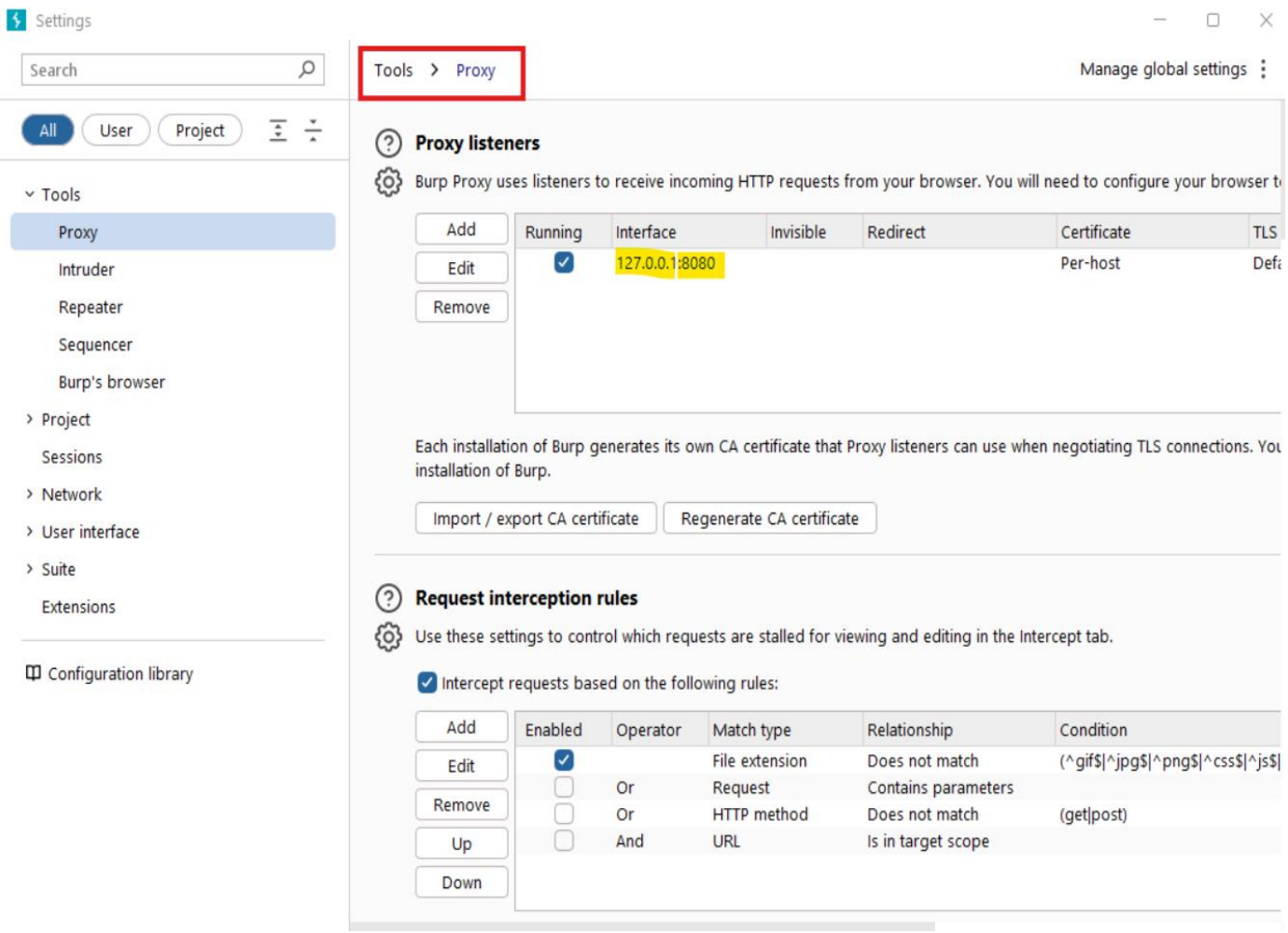
- WebSockets History : - Intercept WebSocket messages in real-time.
  - Useful for testing real-time application(e.g., chat apps, live notifications).



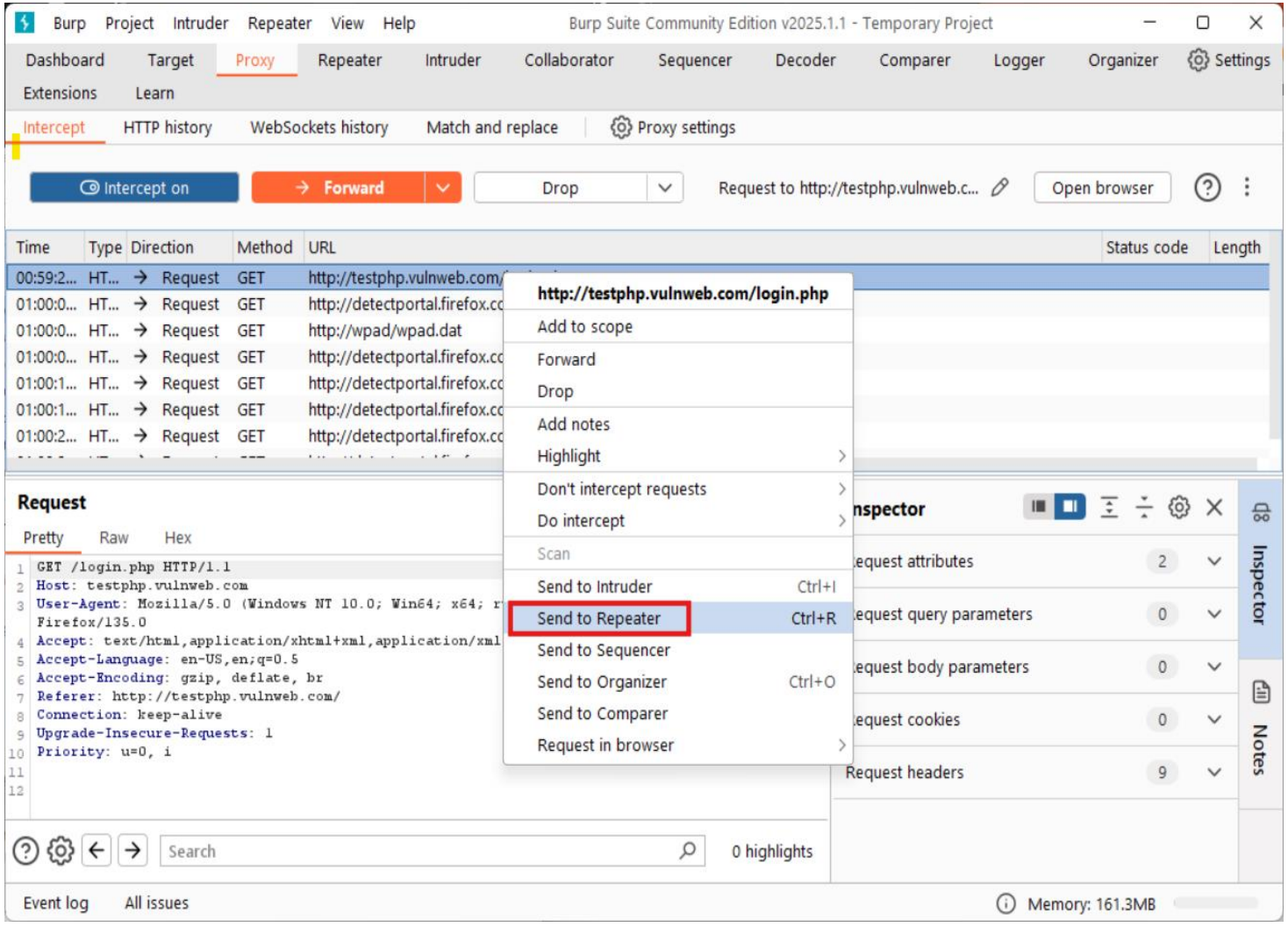
- Match and replace : -
  - It automatically modify headers, cookies, or request parameters.
  - Example: replace User-Agent heaters for user-agent spoofing.



- **Proxy Settings : -** In the proxy setting we can add, edit and remove the particular interface which is necessary to intercept the traffic.
    - In this tab we can Import/export CA certificate. CA certificate that proxy listenrs can use negotiating TLS (Transport layer security) connection.



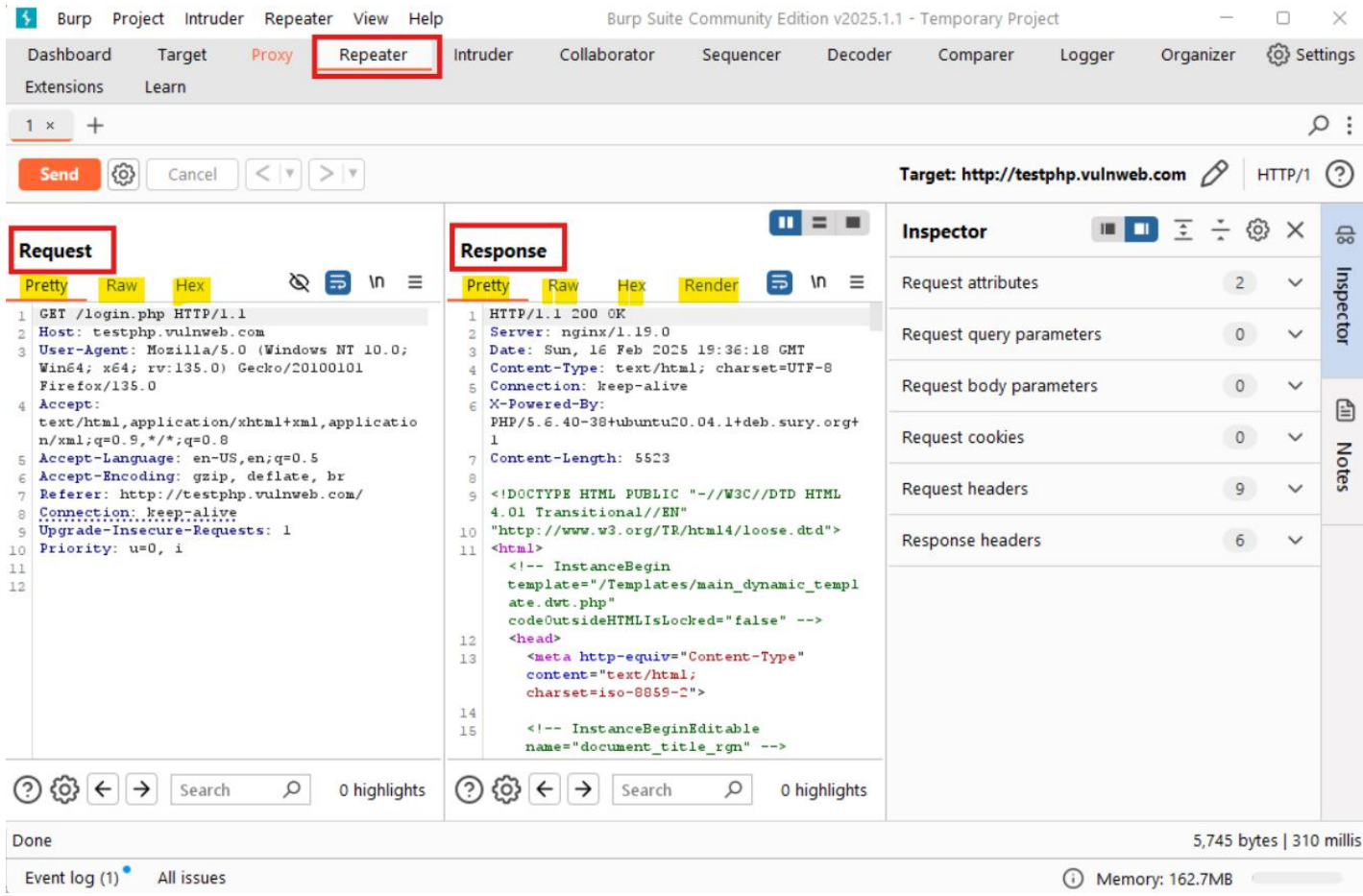
- Send request to the Repeater to the proxy.



4. Repeater : - The Repeater tool in Burp-suite is used for manual testing of HTTP(s) requests. It allows security testers to modify and resend individual requests multiple times to anlayze how a web application responds.

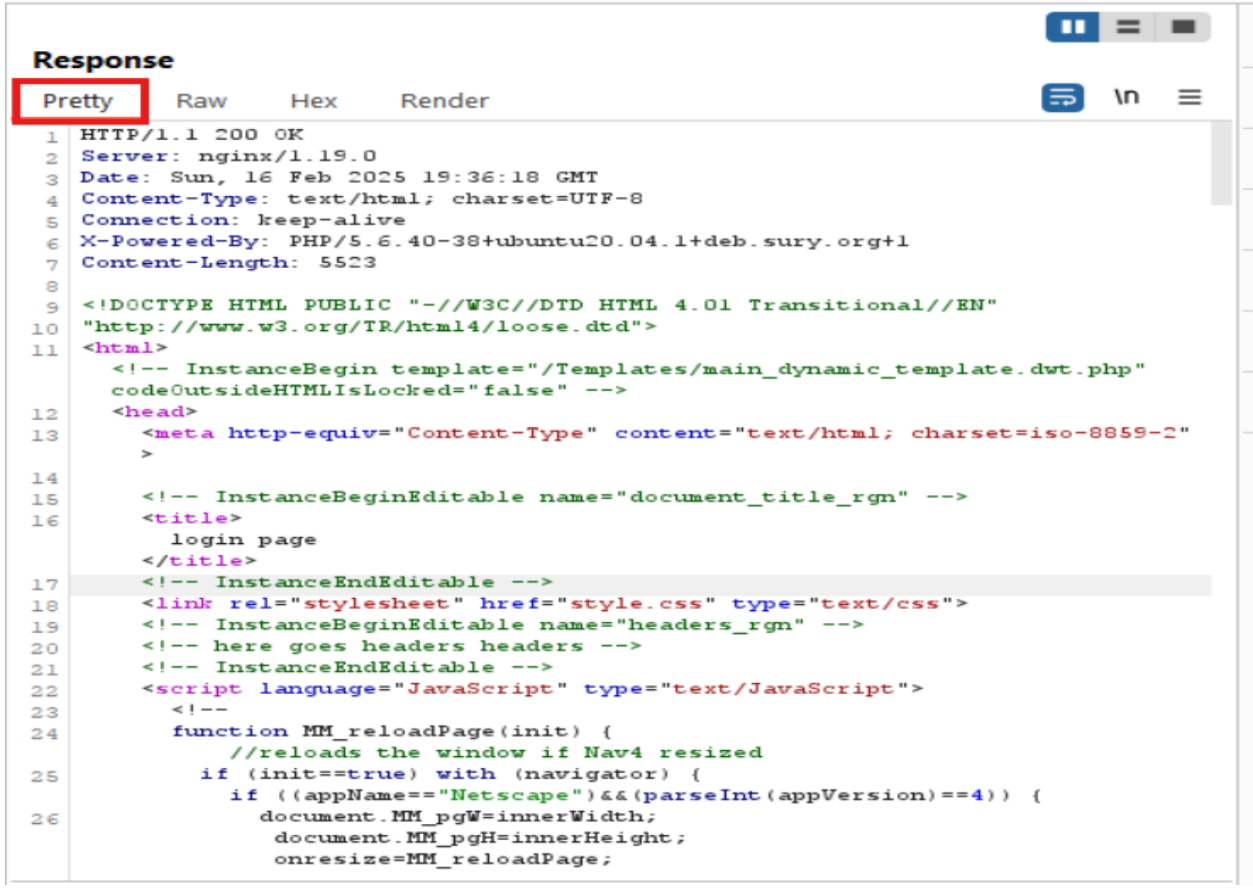
Key features : -

- **Modify and resend Requests –** Edit HTTP headers, parameters, cookies, or body contents.
- **Compare Responses –** View differences between multiple request attempts.
- **Support for WebSockets-** Modify and resend WebSocket messages.
- **Raw, Hex, and Render Views –** Anlayze responses in different formats, including rendering as a web page.



➢ Pretty view : -

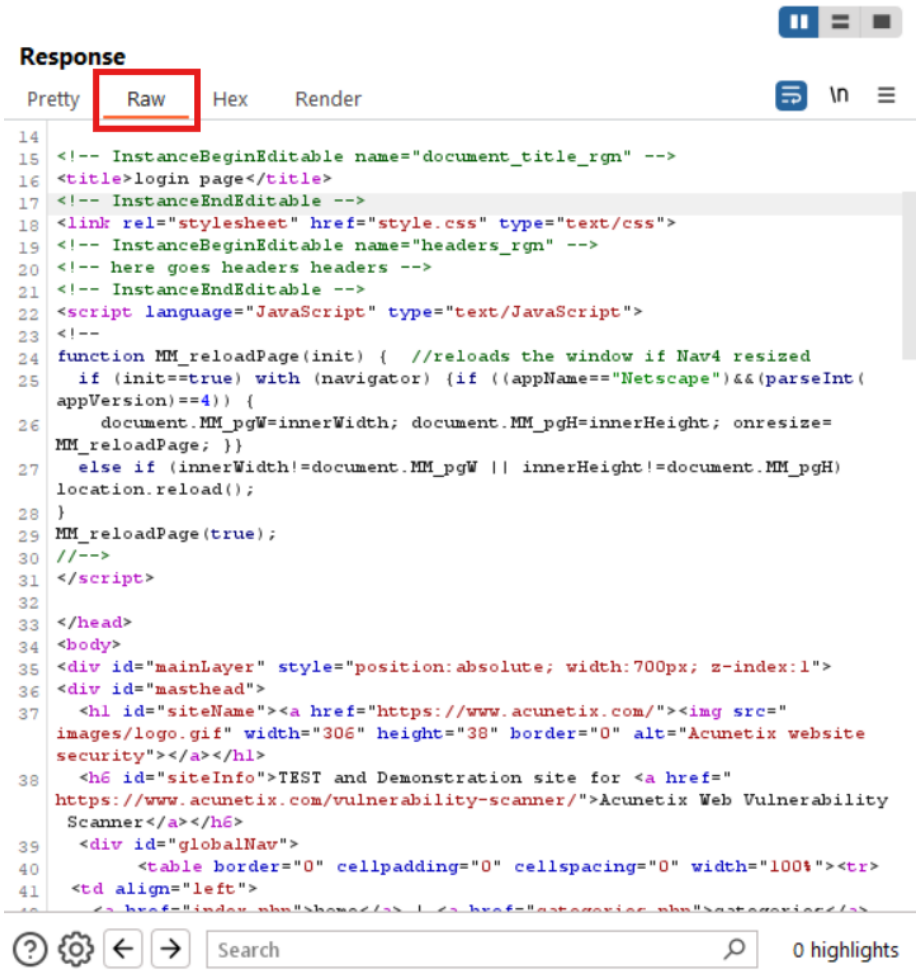
- ➢ Formats and color-codes the response for better readability.
- ➢ Works best for JSON (JavaScript object notation), XML (Extensible markup Language) , HTML (Hyper Text Markup Language).
- ➢ Helps in quickly understanding API (Application Programming Interface) response and error messages.
- ➢ Example: A JSON response will be properly indented with syntax highlighting.



➢ Raw View : -

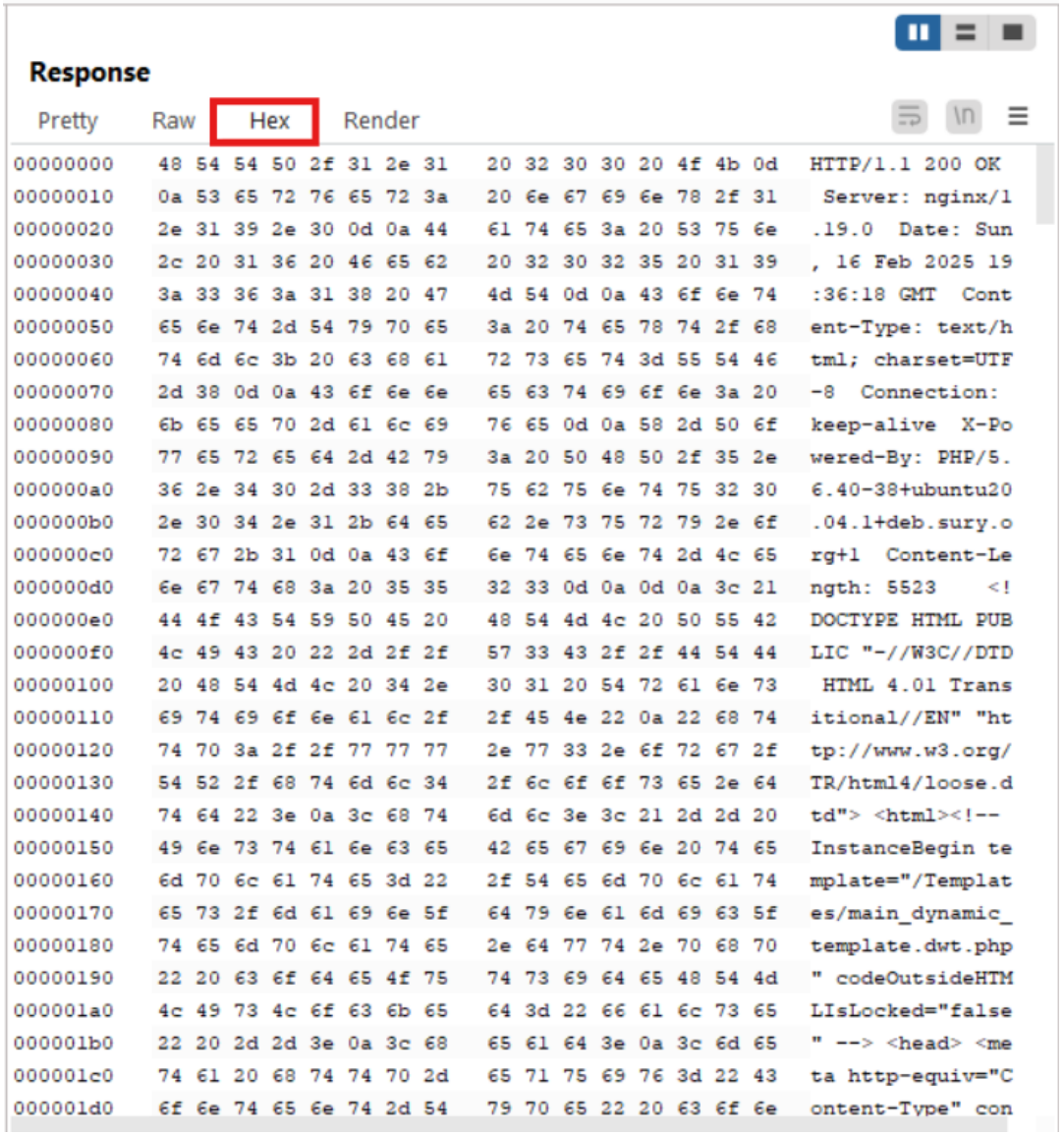
- ➢ Displays the response exactly as received from the server.
- ➢ Shows full HTTP Headers, response body, an status codes.
- ➢ Useful for debugging HTTp headers, cookies, and redirection.

Use case: Checking for security Headers (e.g., CSP (Content Security Policy), CORS (Cross Origin Resource Sharing), HSTS (HTTP Strict Transfer Security) and debugging raw HTTP response.



- Hex View : -
  - Shows the response in hexadecimal format (useful for binary data).
  - Displays both hex values and ASCII (American Standard Code for Information Interchange) representations side by side.
  - Useful for inspecting file downloads, encryption, and encoding issues.

Use case : Analyzing binary responses like images, compressed files, or encrypted data.



- Render View :-
  - Renders the response as a web page (if it's HTML-based).
  - Helps in tesing HTML injection, XSS, and DOM-bases vulnerabilities.
  - Sometime, contain may not load properly if external resources are blocked.

Use case : Verifying if XSS payloads successfully execute in a browser-like envireoment.

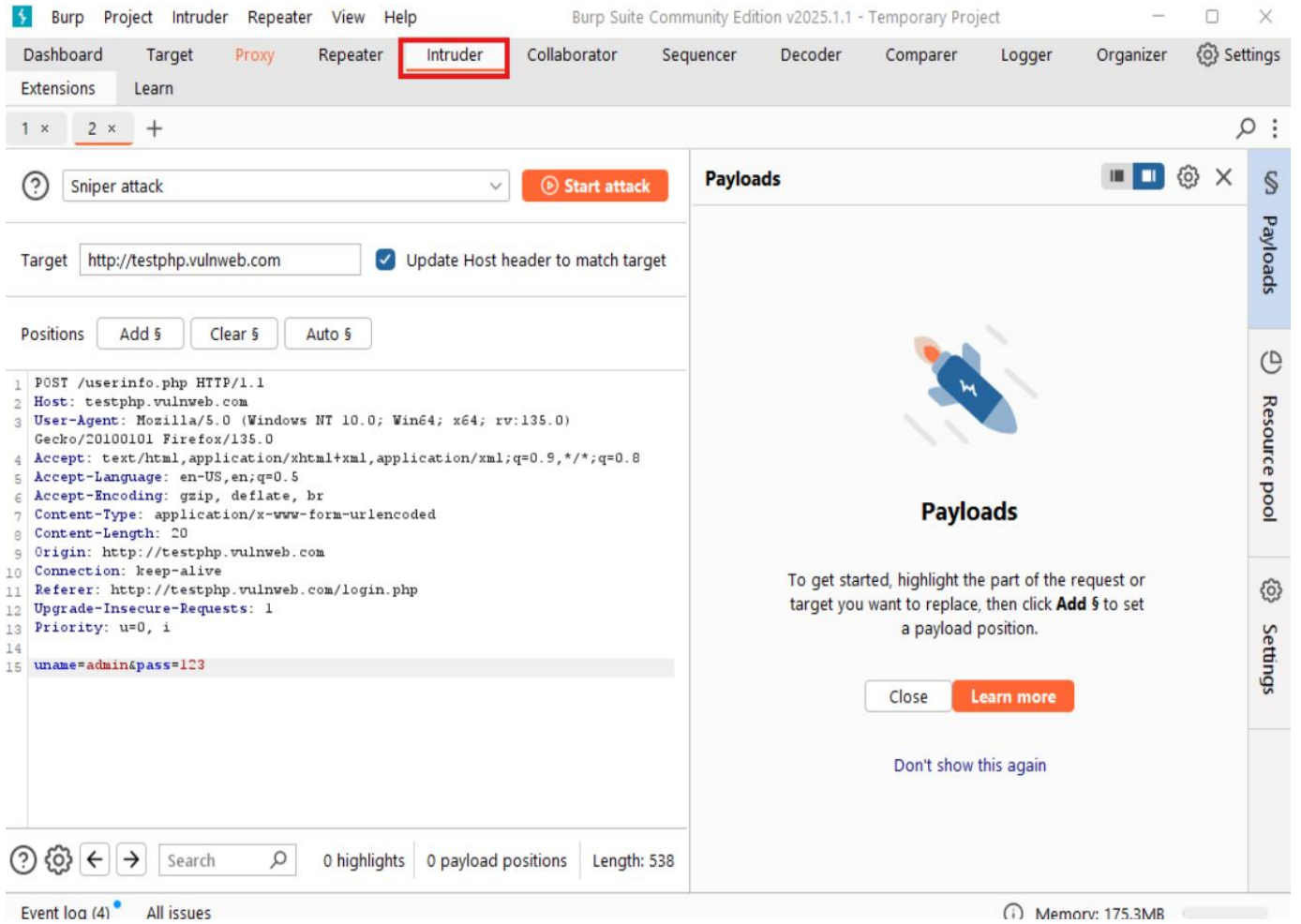
5. Intruder : - The Intruder tool in Burp-Suite is used for automated attacks on web applications. It allows security testers to send multiple requests with different inpts to test for vulnerabilities like Brute Force, SQL Injection, and Parameter fuzzing.

Key Features Of Intruder:-

- **Automated Attacks –** Send multiple payloads to test for vulnerabilities.
- **Four Attack Modes –** Control how inputs are inserted into request.
- **Custom Payloads –** Use wordlists, numbers, or custom payload generators.
- **Results Analysis –** View response status codes, response length, and patterns.
- **Grep Match/Extract –** Find specific keywords or extract data from responses.

In the Intruder we have 4 types of payloads.

i. Sniper Attack
ii. Bettering Ram Attack
iii. Pitchfork Attack
iv. Cluster Bomb Attack

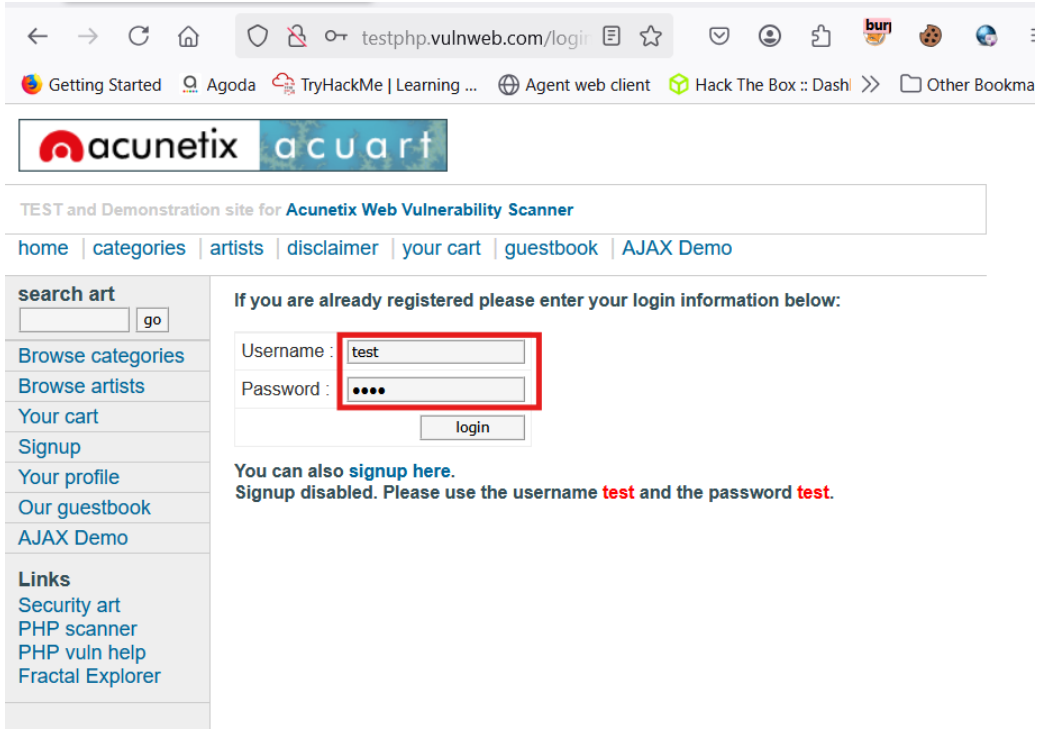


i. **Sniper Attack : -** The Sniper attack is a simplest mode in Busp Suite Intruder. It tests one input parameter at a time, replacing the marked position with different payloads from a list. This is useful for Fuzzing, testing SQL injection, XSS, and brute-force attacks.

Performing a Brute force attack on Login parameter using sniper attack.

- Lets suppose I have a username and I need to brute-force the Password to get login.
  - Username = test
  - Password = ?
  - Website = http://testphp.vulnweb.com/login.php

Step 1 : go to the website : - http://testphp.vulnweb.com/login.php



Step 2 : On burp-suite capture the request and send it to the Intruder.

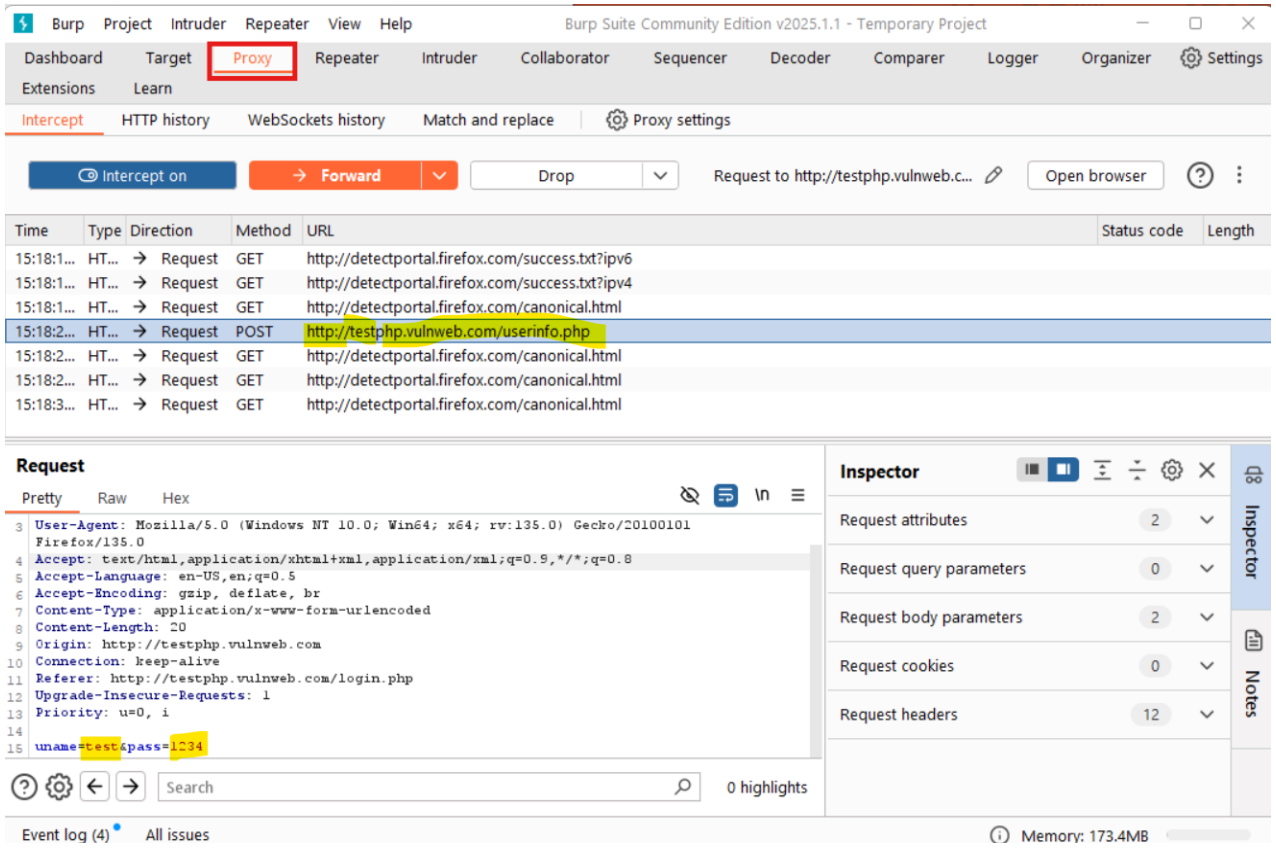


Image **1**

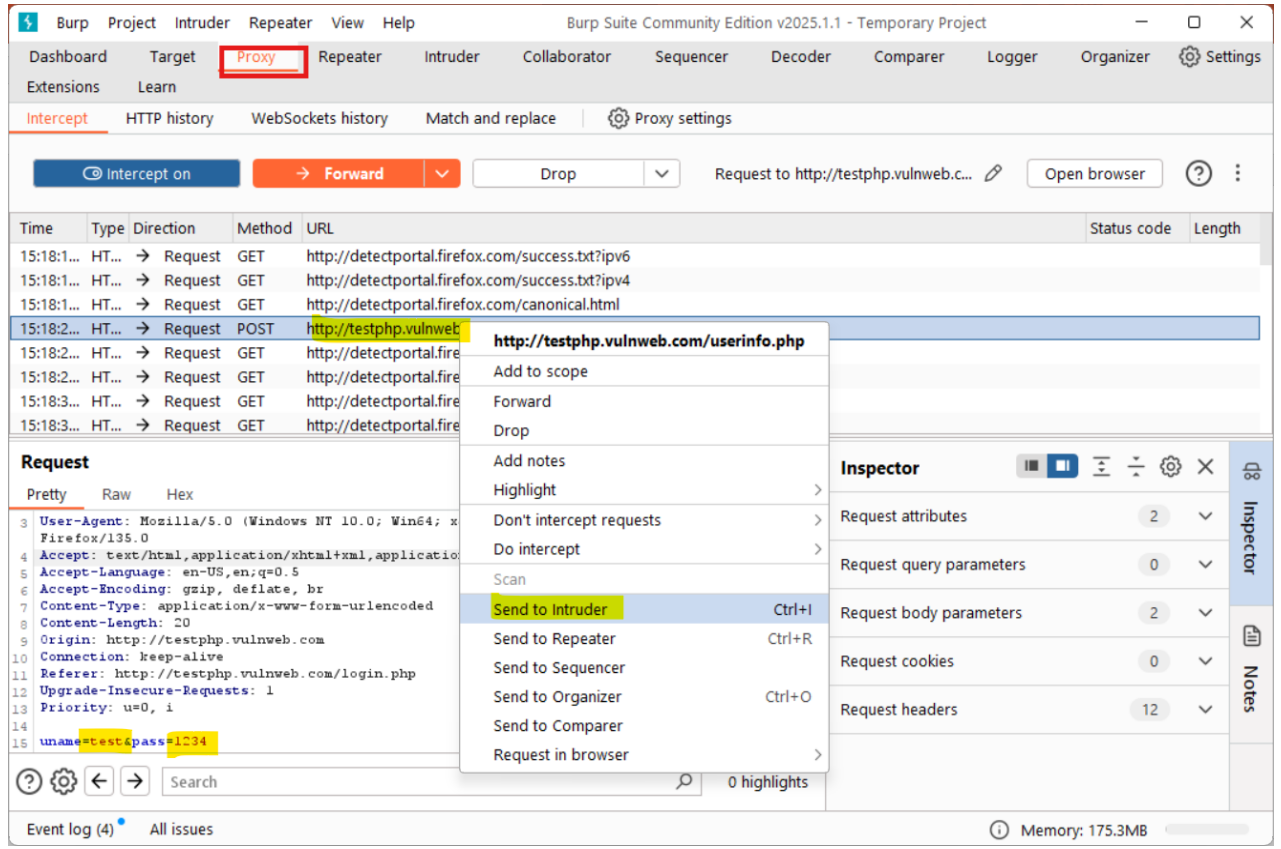


Image **2**

Step 3 : Click on Intruder tab.

=> Select the Password position where we attempt brute-force.

=> Click on add

=> payload type = simple list

=> Past the guessable password in like in image 4

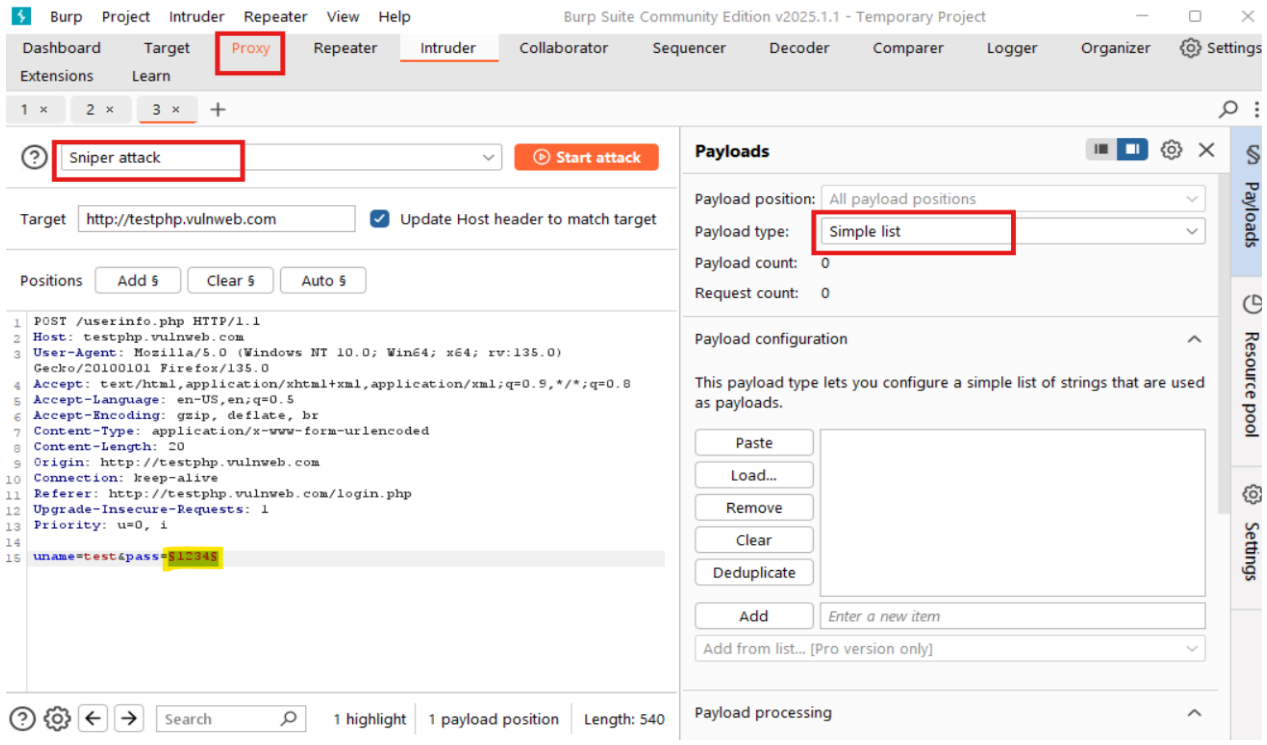


Image 3

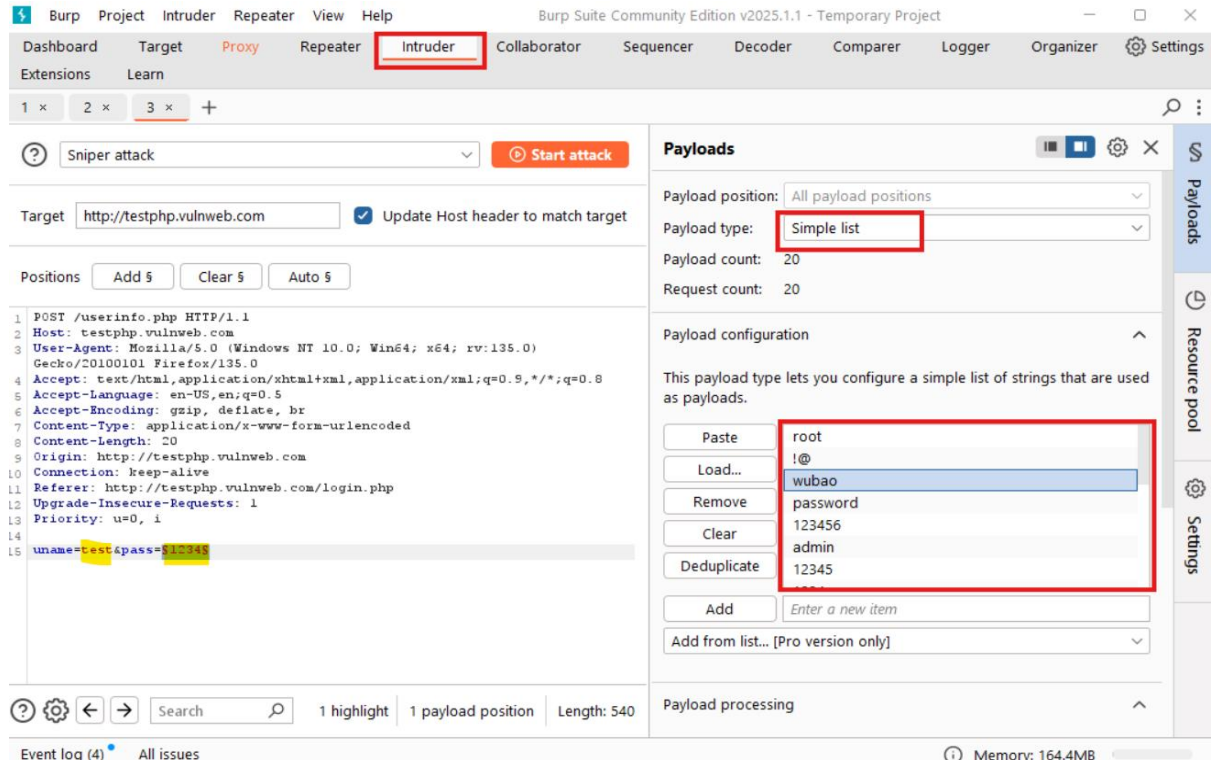


Image 4

Step 4 : Click on Start attack and its appears a new window like image 5

=>After the complete attack.

=> check Status-code, and Length if the Status-code or length is change so check the response of the parameter.

=> Like image 6 checking response.

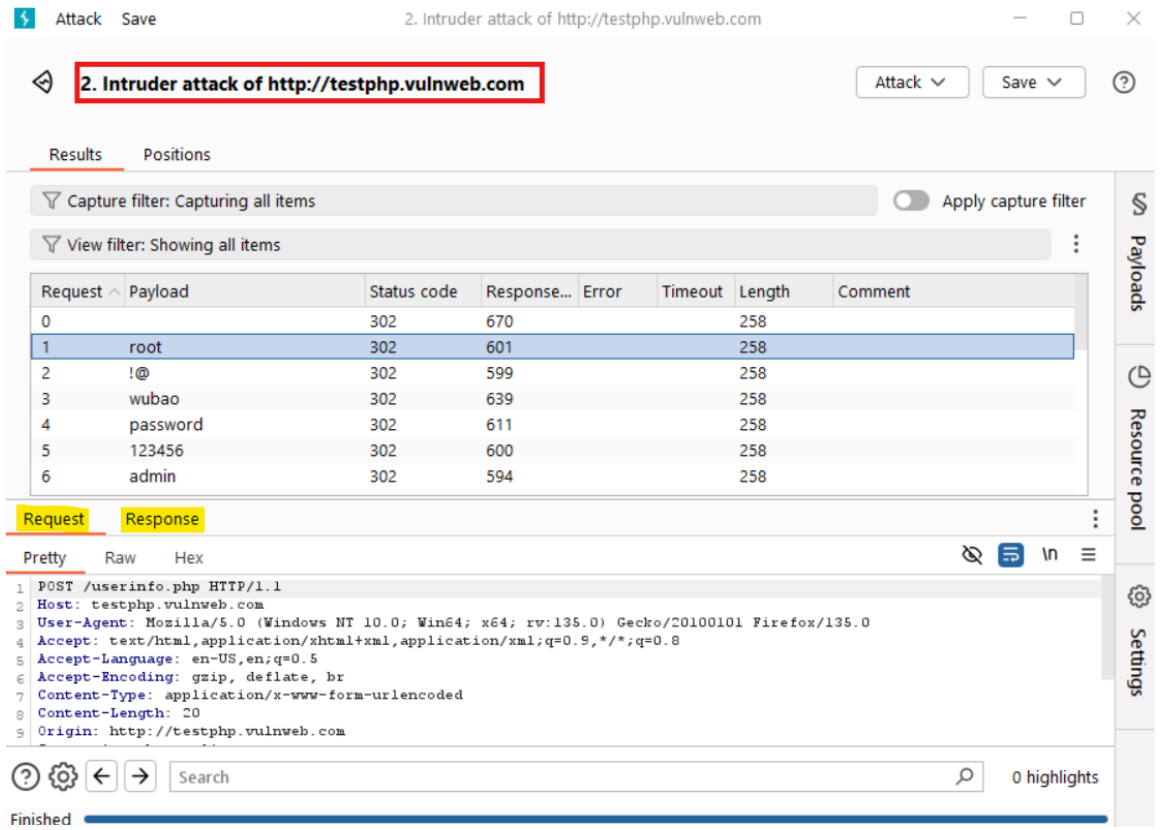


Image 5

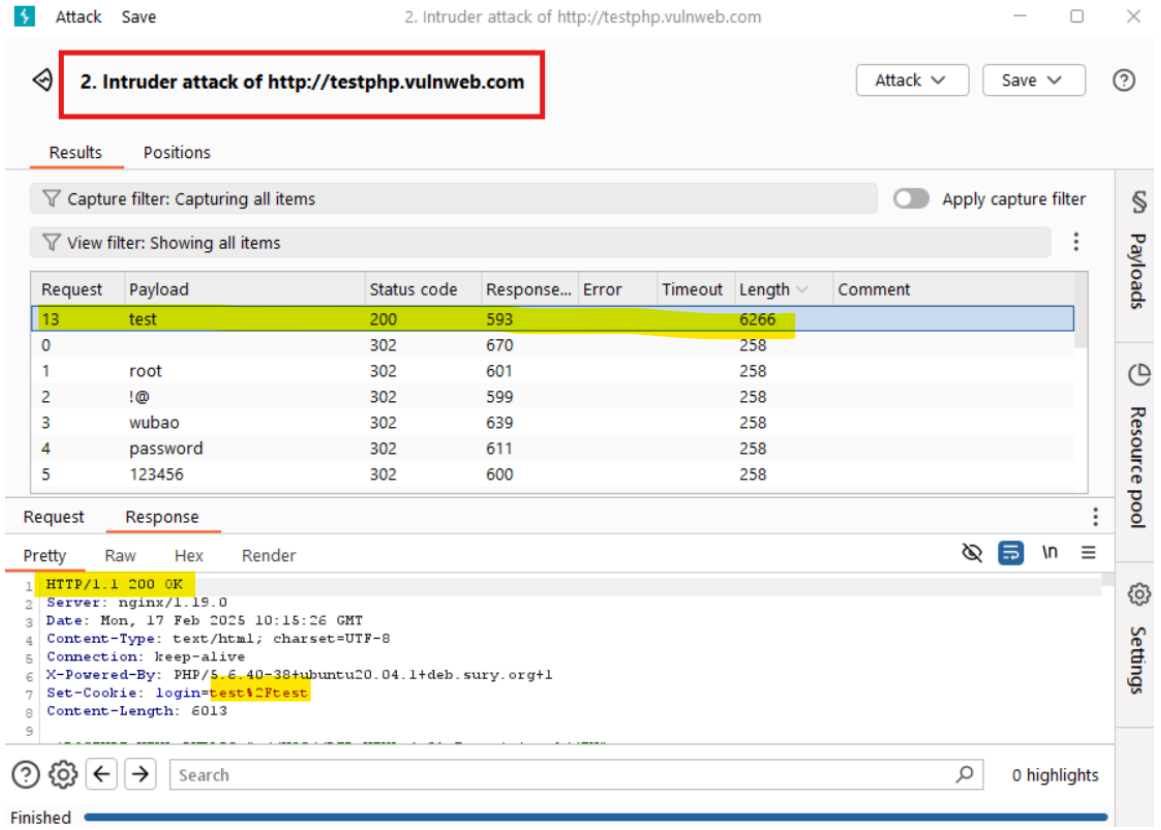


Image 6

Step 5 : Username = test, Password = test

Image 7

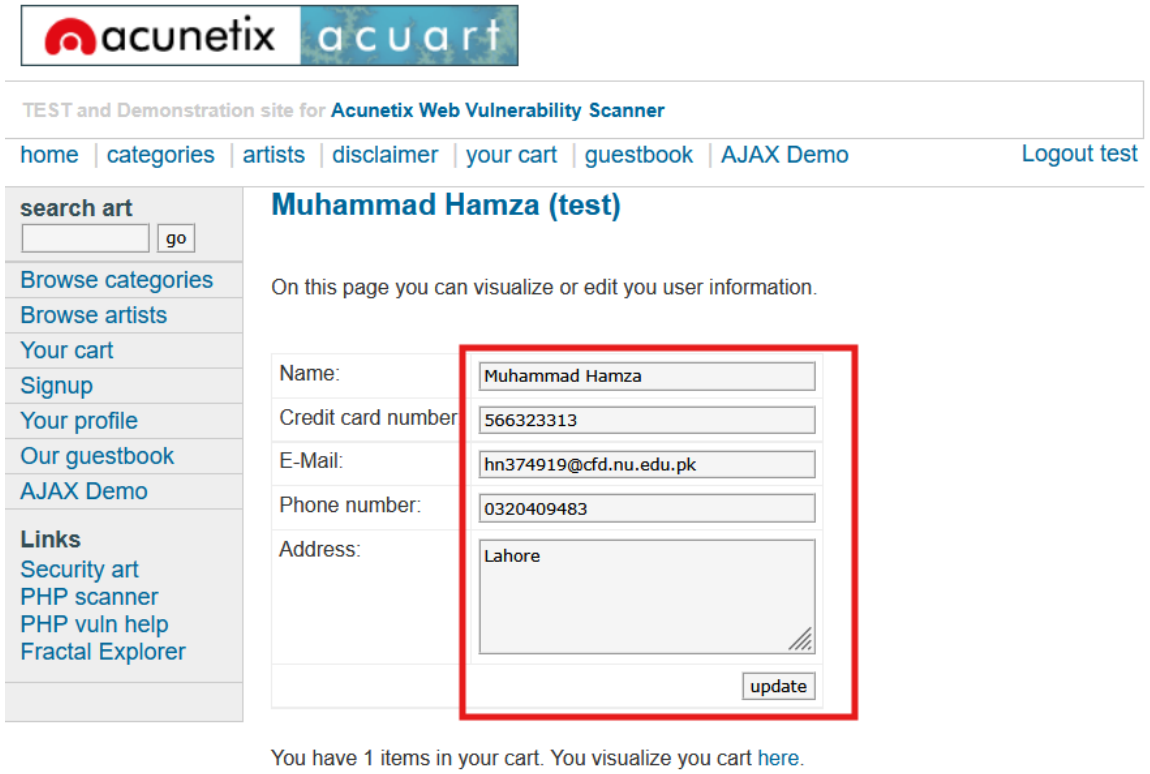


Image 8

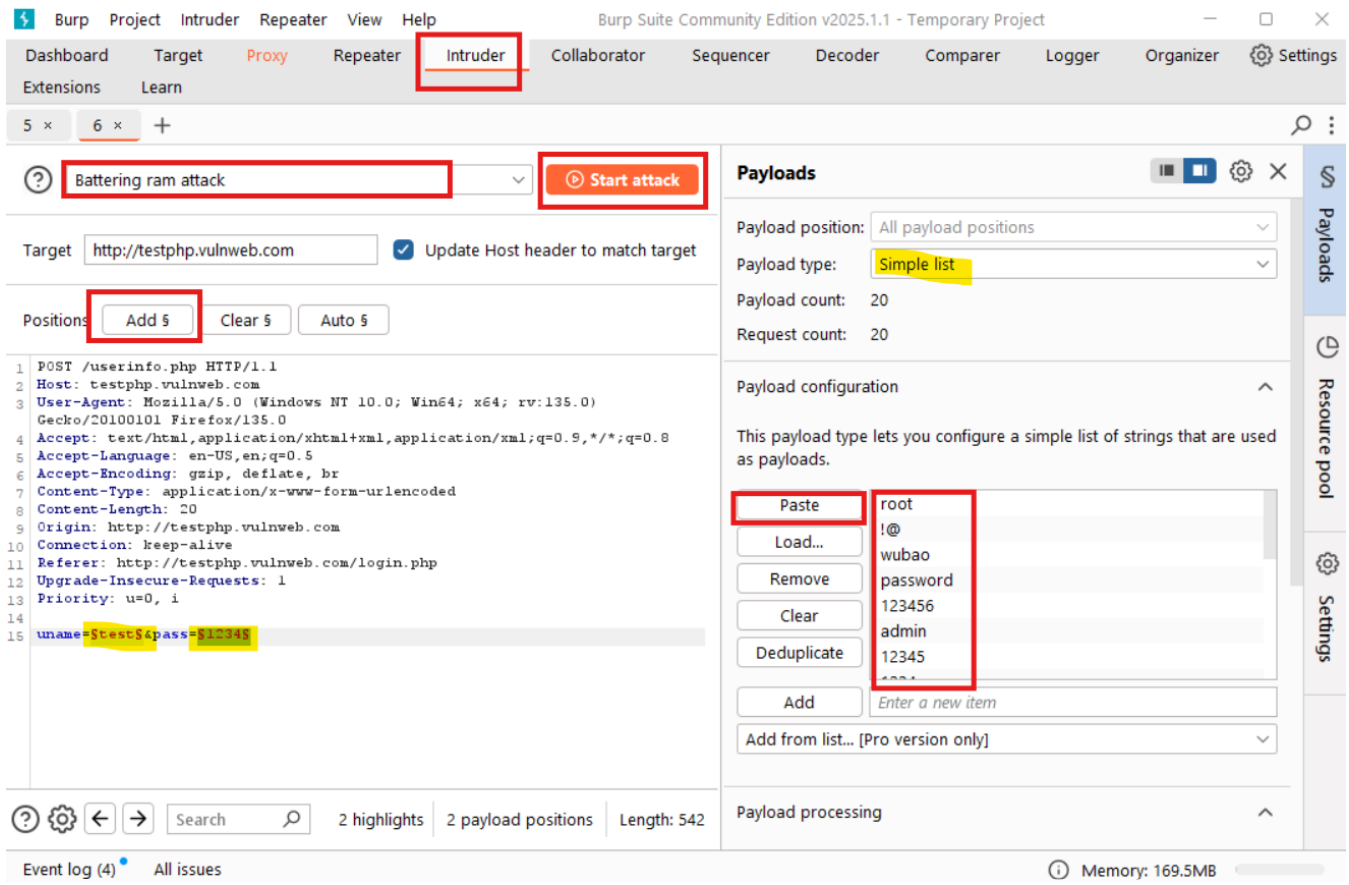
II. Battering Ram Attack : -

- It replaces all marked positions in the request with the same payload in each request.
- Useful for testing repeated tokens, session IDs, or authentication fields where the same values is used in multiple places.
- In this we can choose multiple position.

Step 1 : select the Battering ram attack

⇒ Select the position

⇒ Add Password list.



Step 2 : Click on Start attack

⇒ Once the attack completed

⇒ Check the Status-code, and length if the Status-code or length is change check the response.

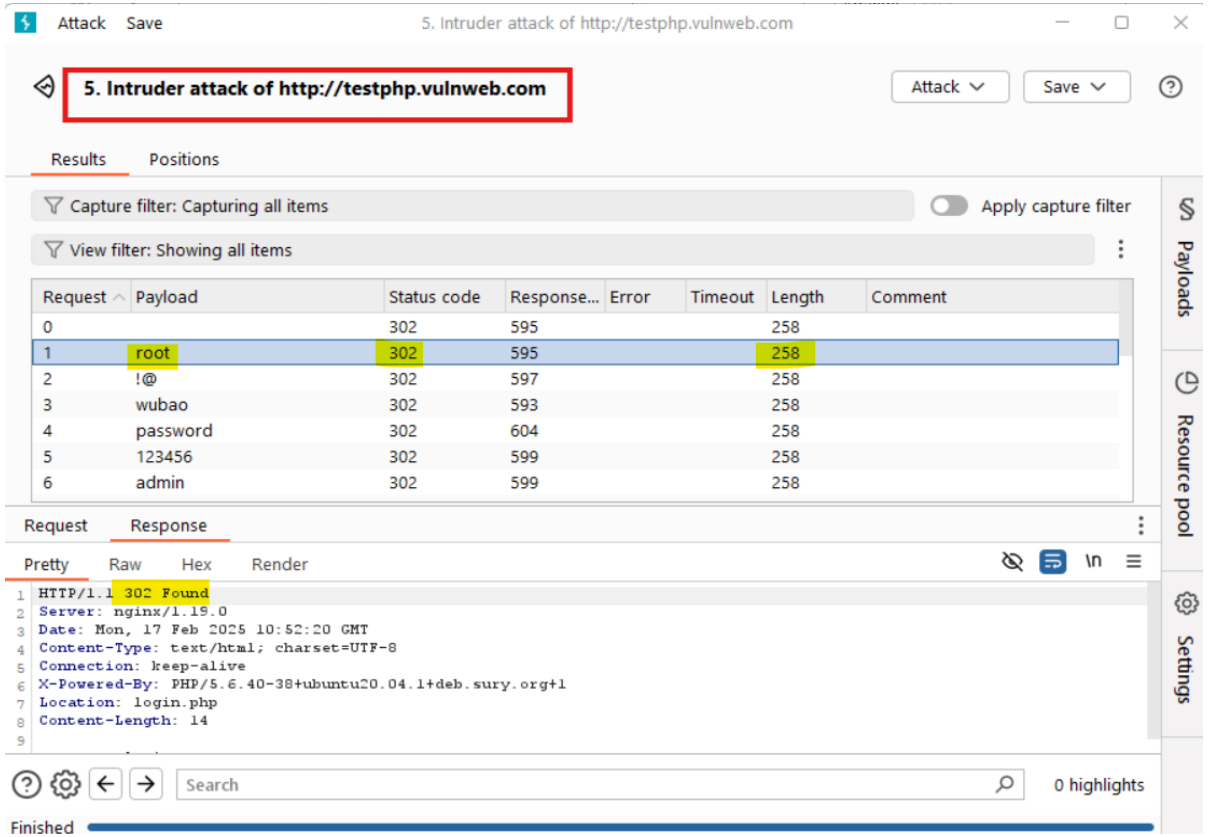


Image 1

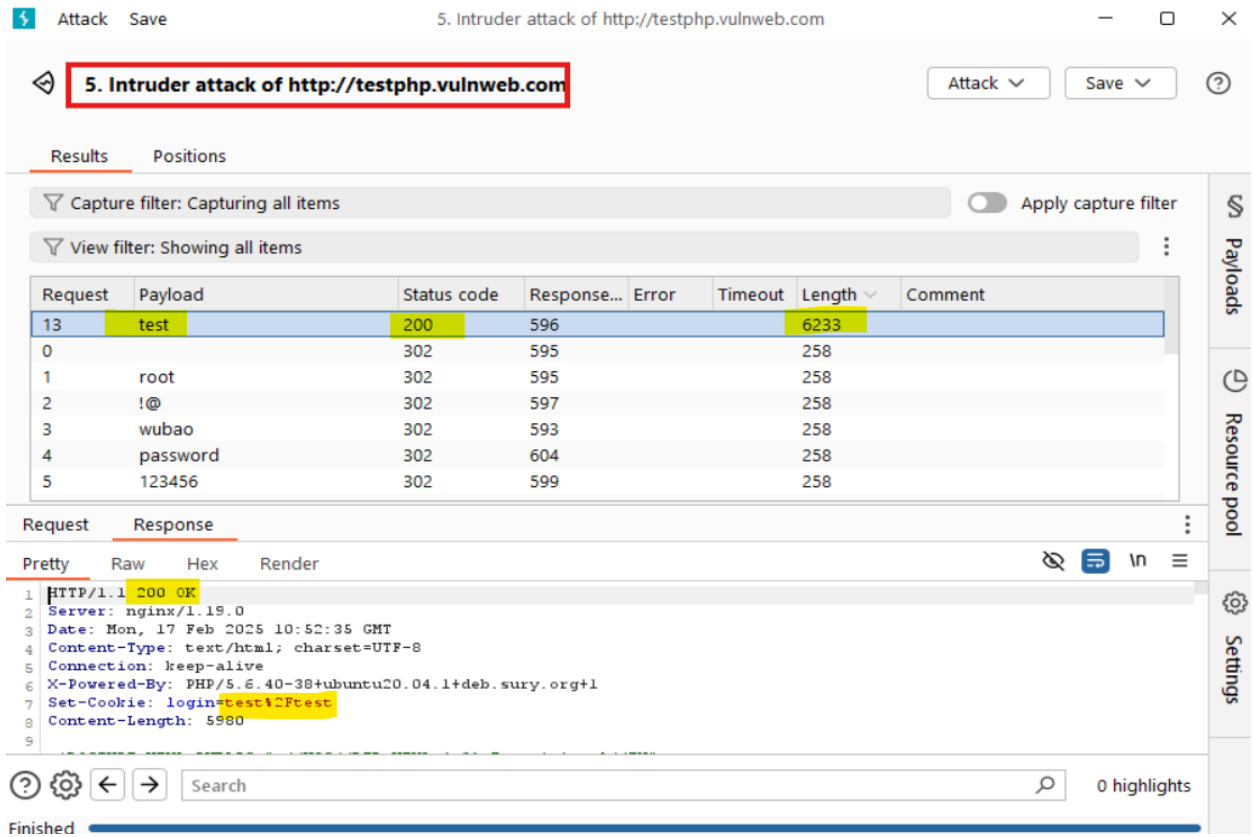


Image 2

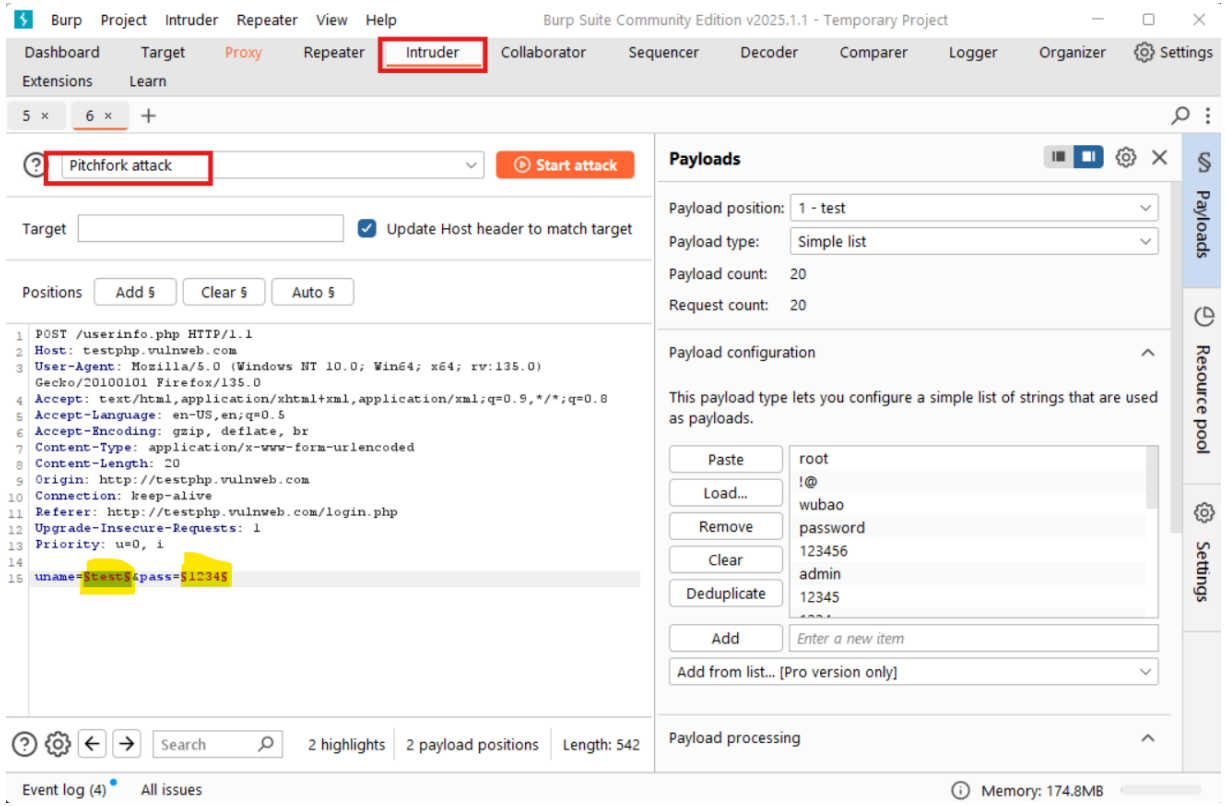
III. Pitchfork Attack : - The pitchfork attack type to allows you to test multiple paratemeters simultaneously, but with different values for each parameter. Unlike Sniper (Which terst one position at a time) and Battering Ram (which sends the same value to multiple positions), pitchfork runs Parallel payload lists, assigning a unique value from each list to its corresponding position.

How Pitchfork Works :

⇒ Each payload position gets its own separate lists of test values.

⇒ Burp takes one value from each list and sends them together in a single request.

⇒ The number of requests equals the length of the shortest payload list (unlike Cluster Bomb, which test all combinations)



- How Pitchfork Attack Works : -

Step 1 :

⇒Capture the request on burp sent it to the intruder.

⇒Select attack type : Pitchfork attack

⇒Select positions uname, pass, => Click on Add$

⇒ Select Payload position and add wordlist in both position. E.g. : image 2, and image 3

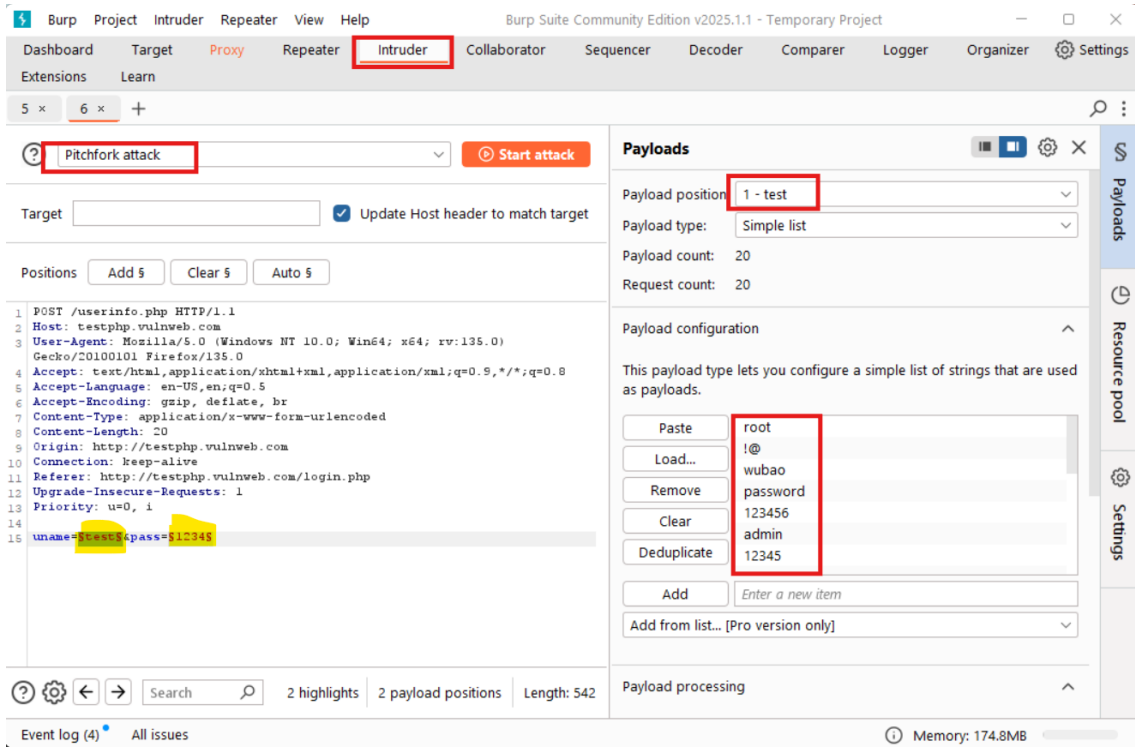


Image 2

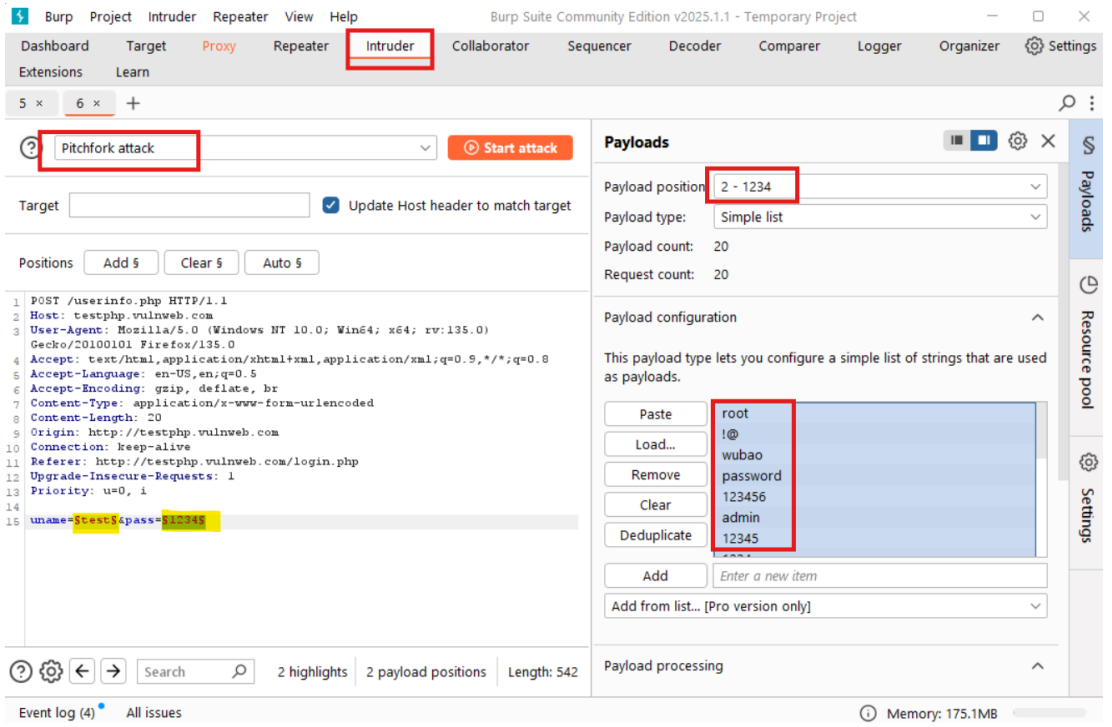


Image 3

- Step 2 :

⇒Click Start attack

⇒ Image 4 has 302 status code and image 5 has 200 ok status code :

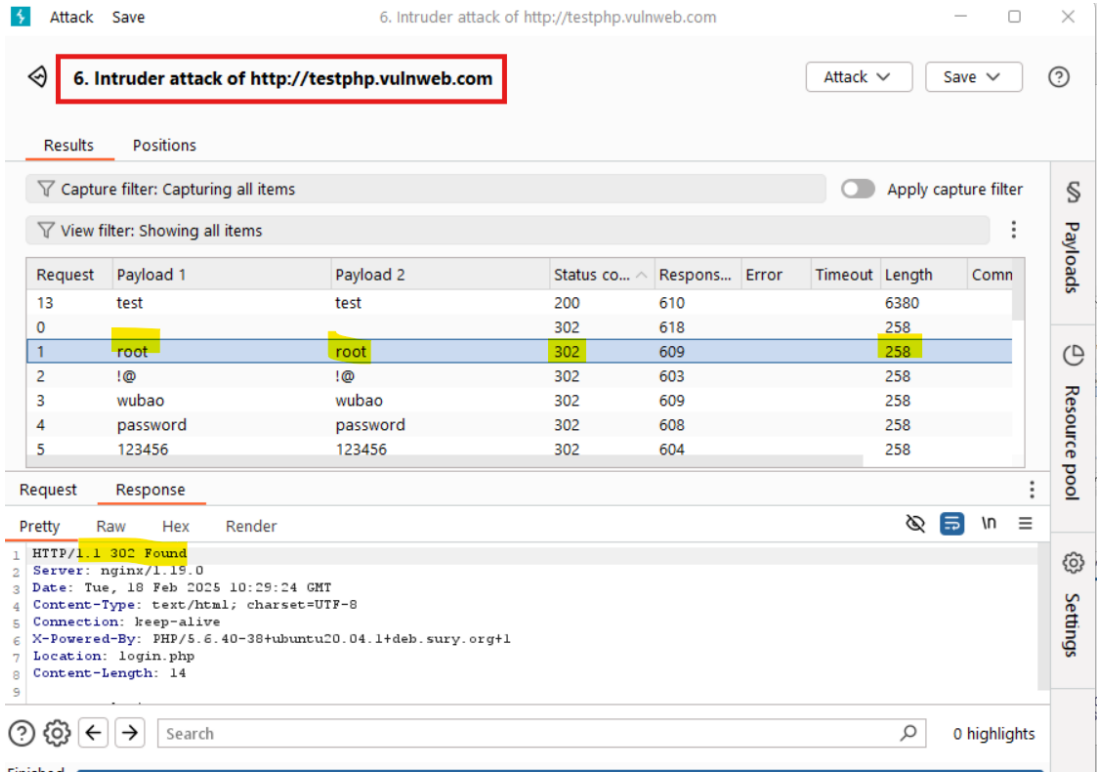


Image 4

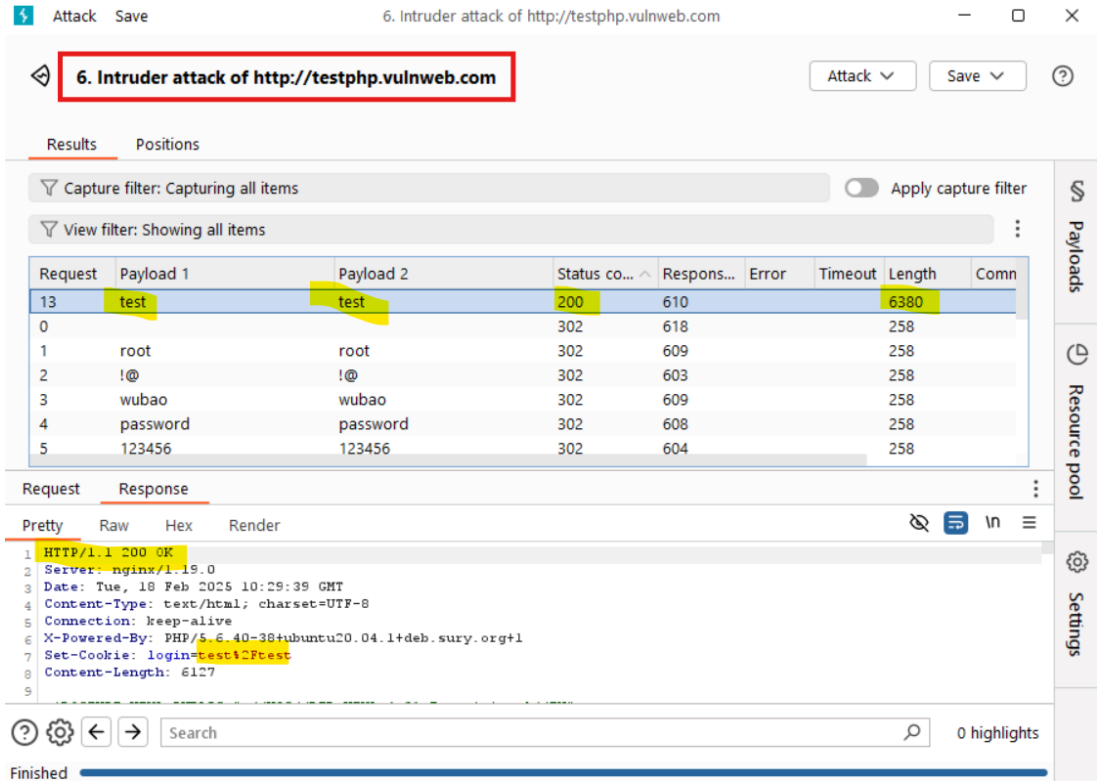


Image 5

IV. Cluster Bomb Attack :- A Cluster Bomb attack in Burp Suite Intruder is an advance brute-force attack that tests all possible combinations of multiple payloads. Unlike Pitchfork Attack (which runs payload lsts in parallel), Cluster Bomb tests every value in one list against every value in another list.

Note :- In the Cluster bomb Attack I am using 20 payload for each position and it make 400 combination to start brut force attack.

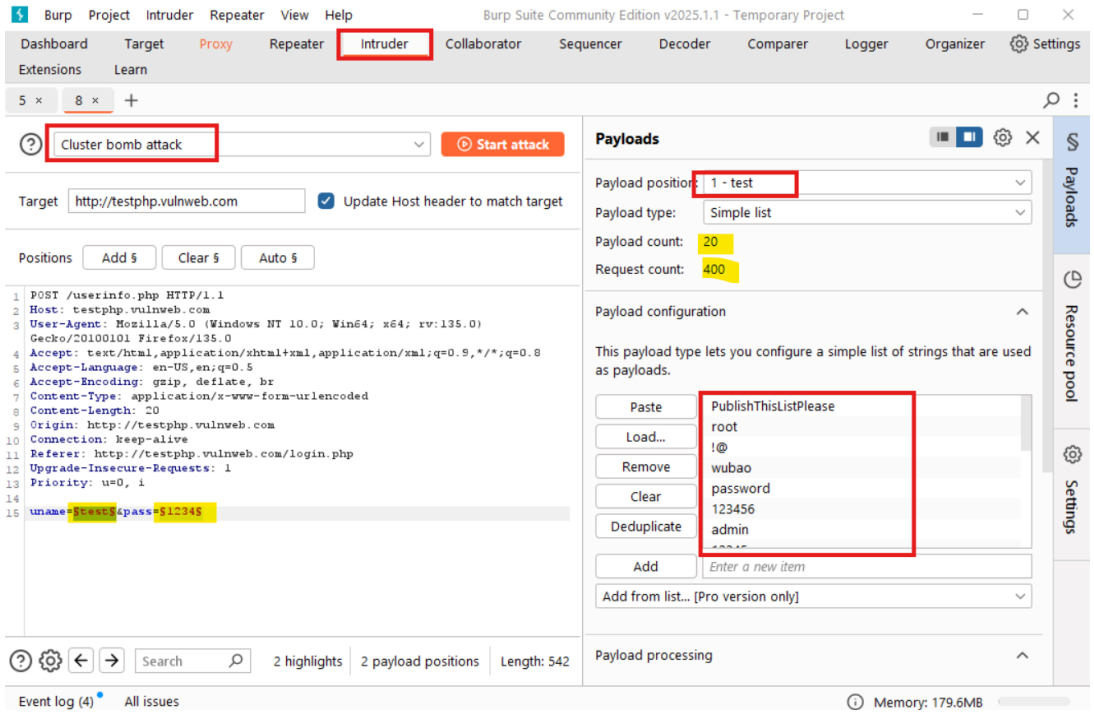


Image 1

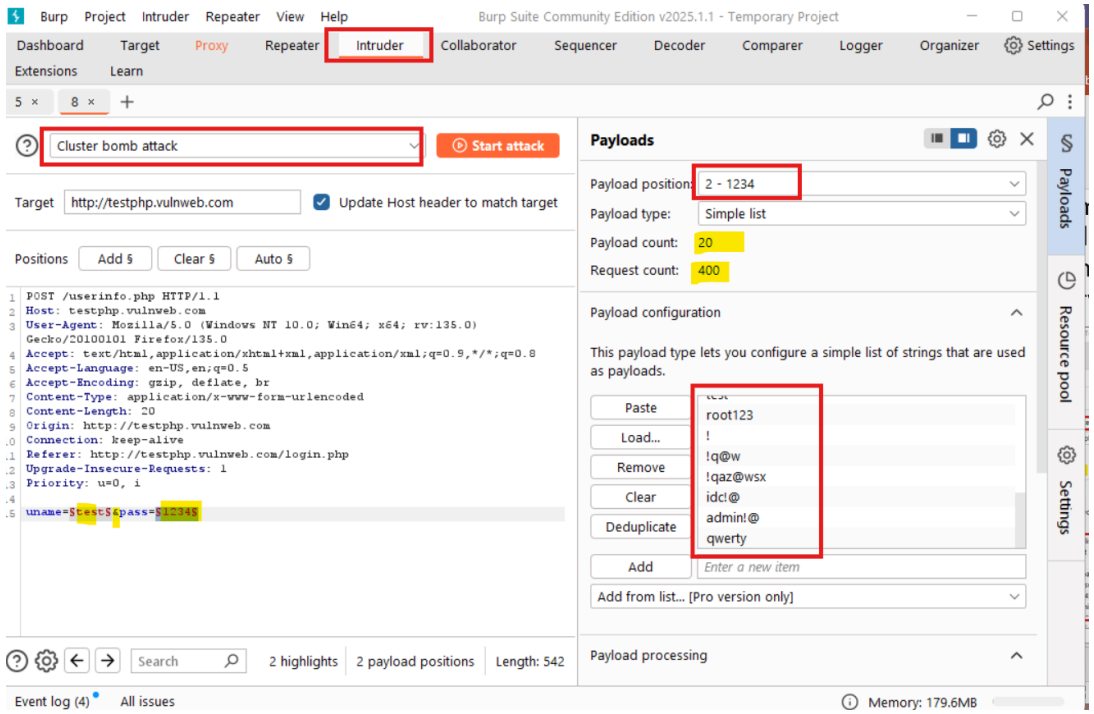


Image 1

6. Sequencer : - Burp Suite Sequencer is a tool to analyze the randomness (entropy) of the session tokens, CSRF tokens, an other pseudo-random values used in web applications. It helps determine whether an application's tokens are predictable and venerable to attacks.

- **How to use Burp Suite Sequencer :-**

Website = https://ginandjuice.shop
Creds = carlos/hunter2
Taks = capture tokens

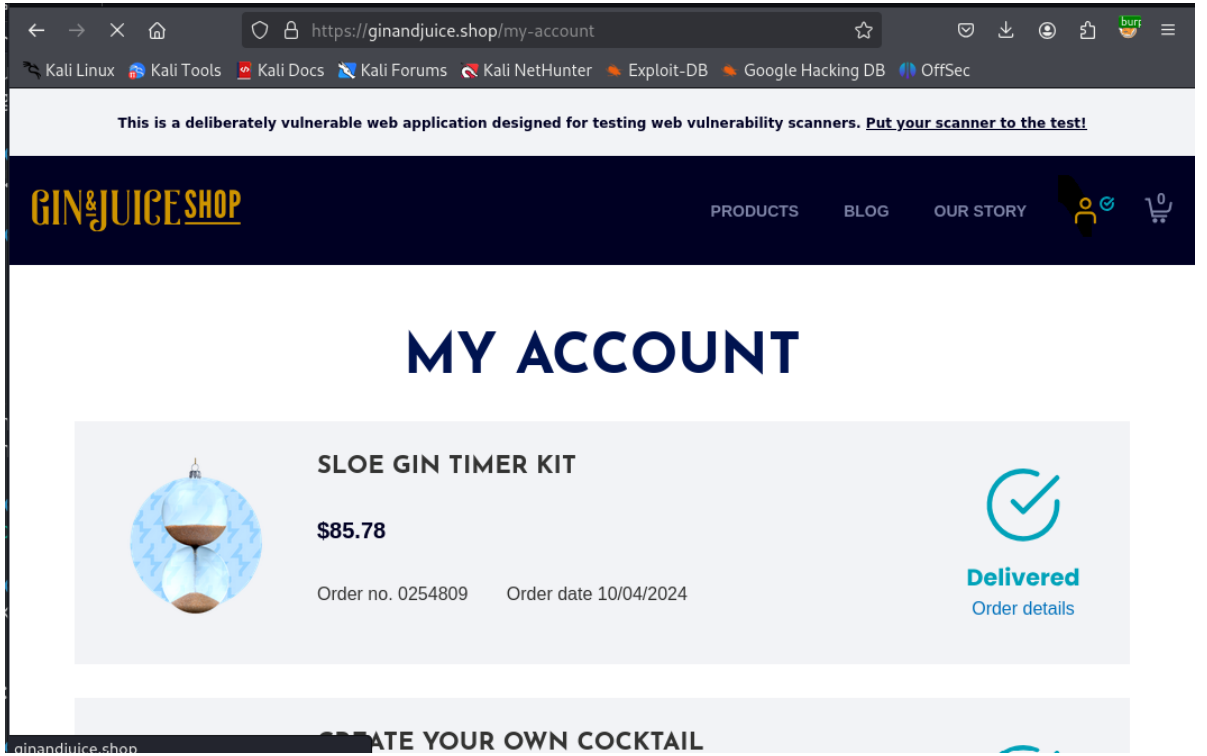


Image 1

Step 1 : Capture Tokens

=> Open Burp suite and go to the Sequencer tab.

=> Click "start Capture" and select where to capture randomness from:

- Live Interception (capturing session tokens from request).
- Manual input (copy-pasting a set of tokens).
- From a Request (capturing tokens via automated request).

Step 2 : Capture cookie and sending towards sequencer.

In image 2

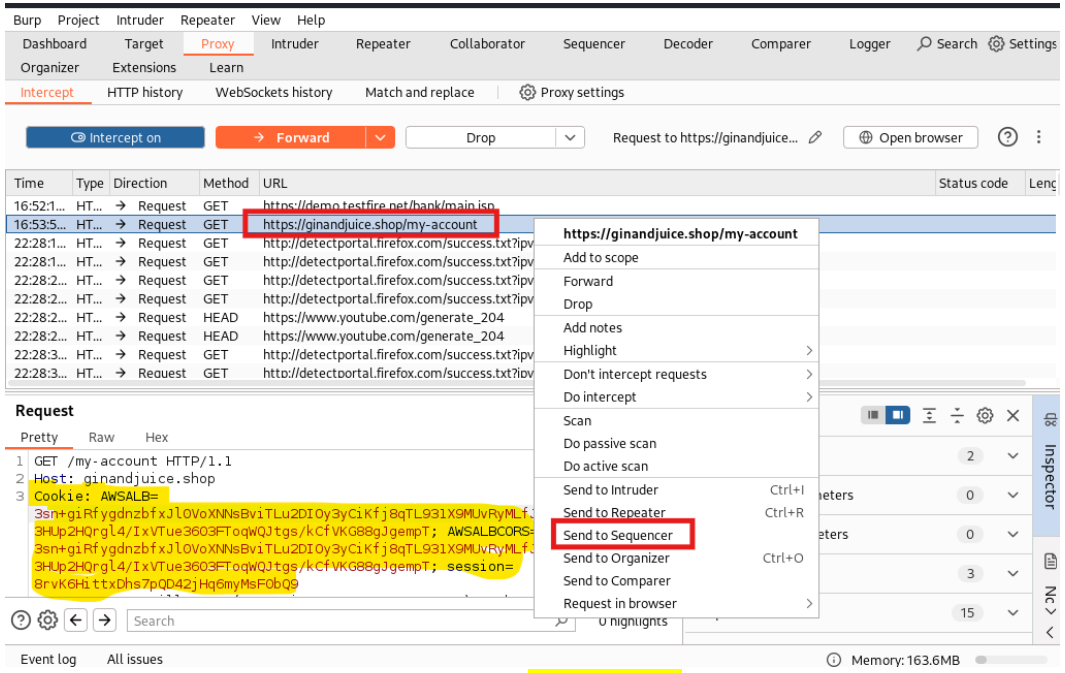


image 2

Step 3 : click on Sequencer tab (image 3)

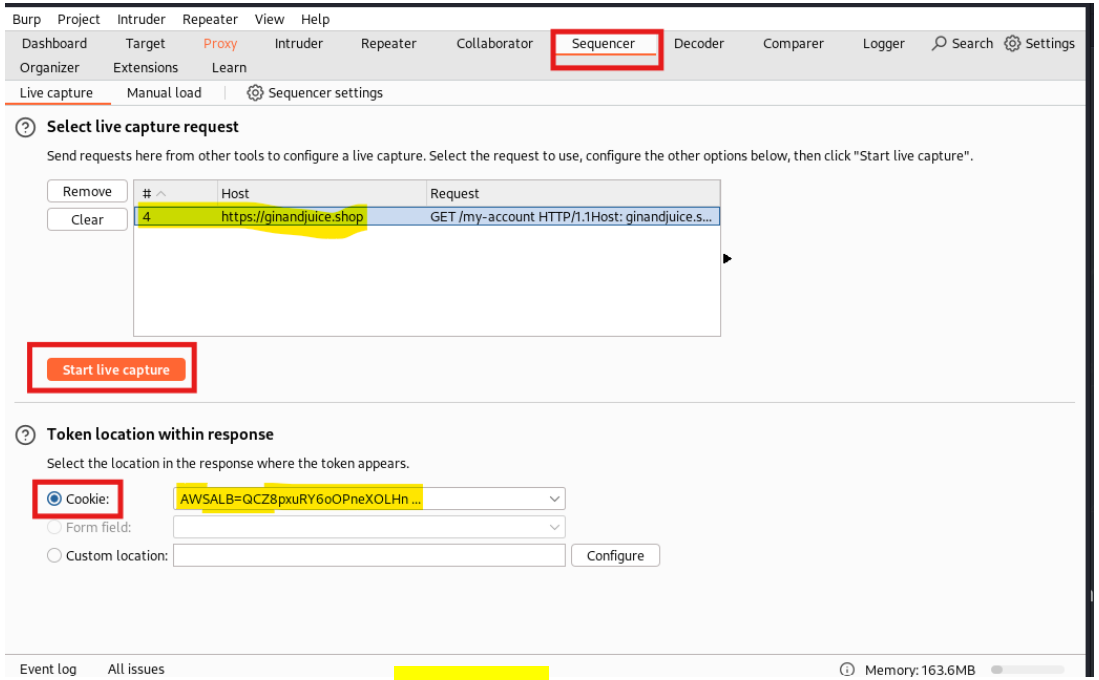


Image 3

Step 4 : click on start live capture (image 4)

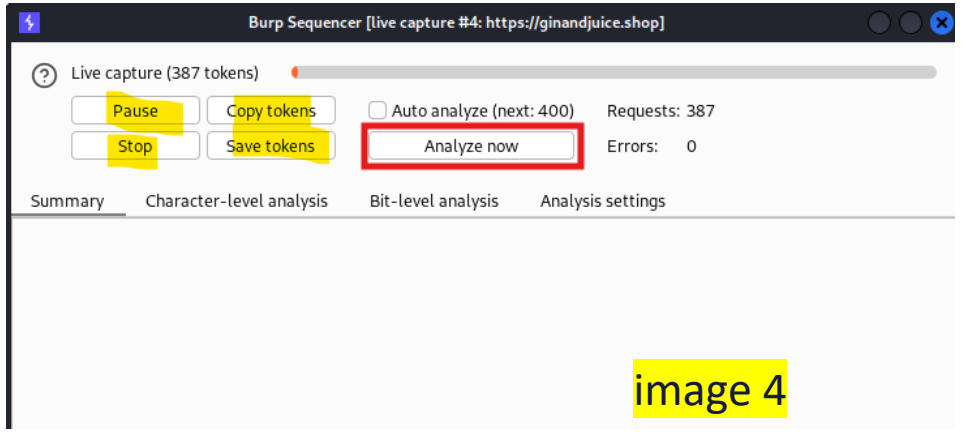
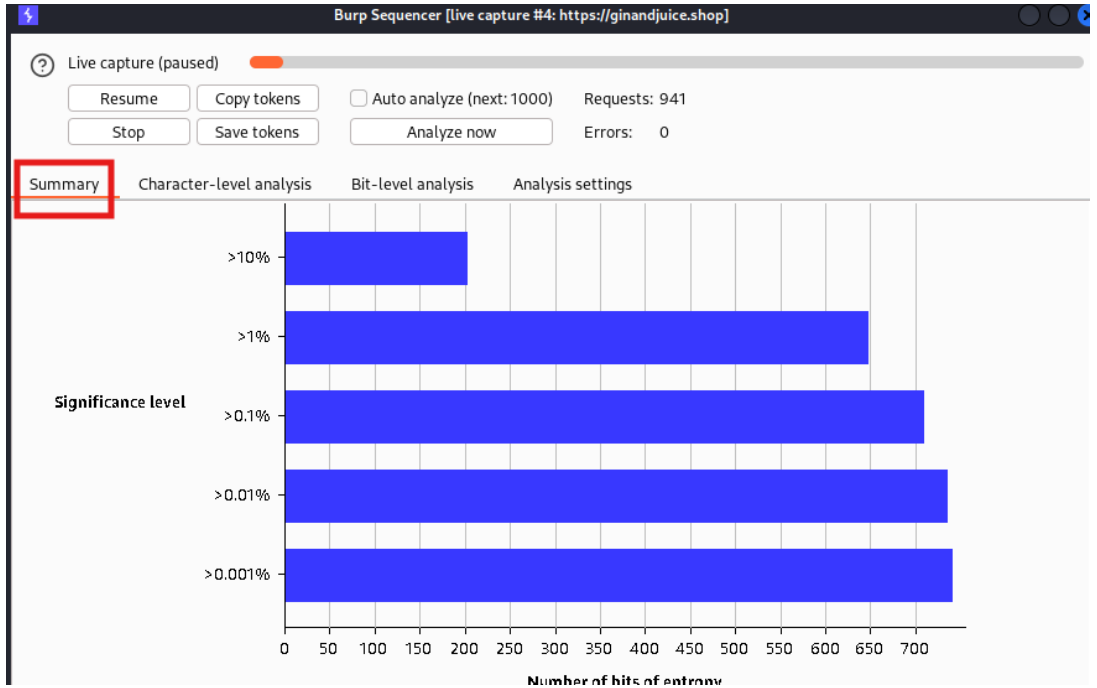


image 4

Step 5 : click on analyze now and see (image 4)



(image 4)

7. Decoder : -

- Burp suite Decoder is a tool used to encode, decode, and transform data between different formats. It helps penetration testers analyze encoded payloads, obfuscated data, and encrypted values used in web applications.
- It can encode and decode format like : URL, HTML, Base64, ASCII hex, Hex, Octal, Binary, and Gzip.

⇒Encoded to URL <script>alert(1)</script> Image 7.1

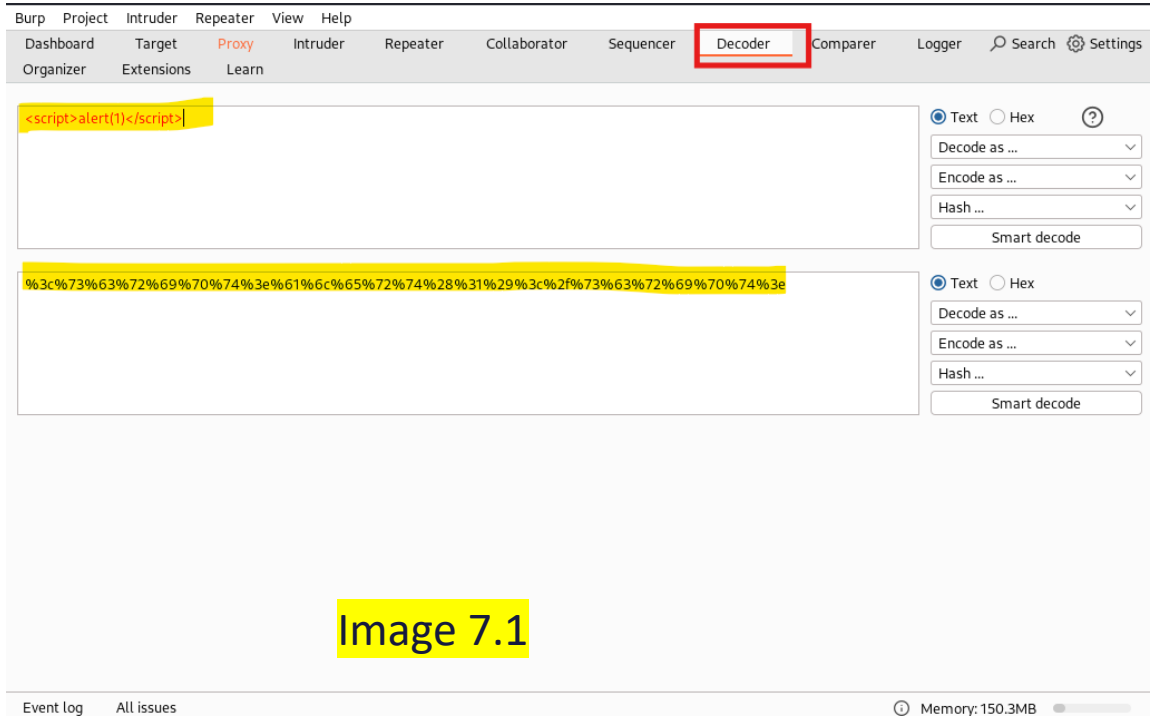


Image 7.1

8. Comparer :- Burp Suite Comparer is a tool used to compare two pieces of data (request. Response, tokens, etc) to identify differences and similarities. It is helpful for analyzing session tokens authentication responses, and code changes in web applications.

How to use Comparer :-

Step 1: Capture the request in Proxy, then send it to the repeater.

see image 1 and 2

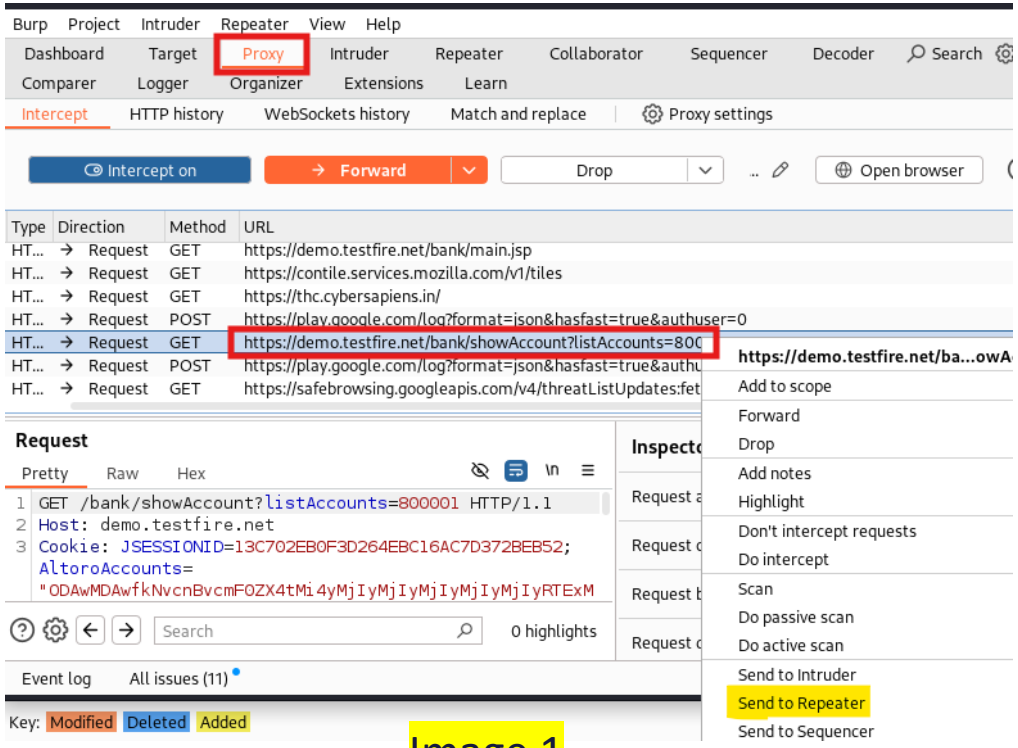


Image 1

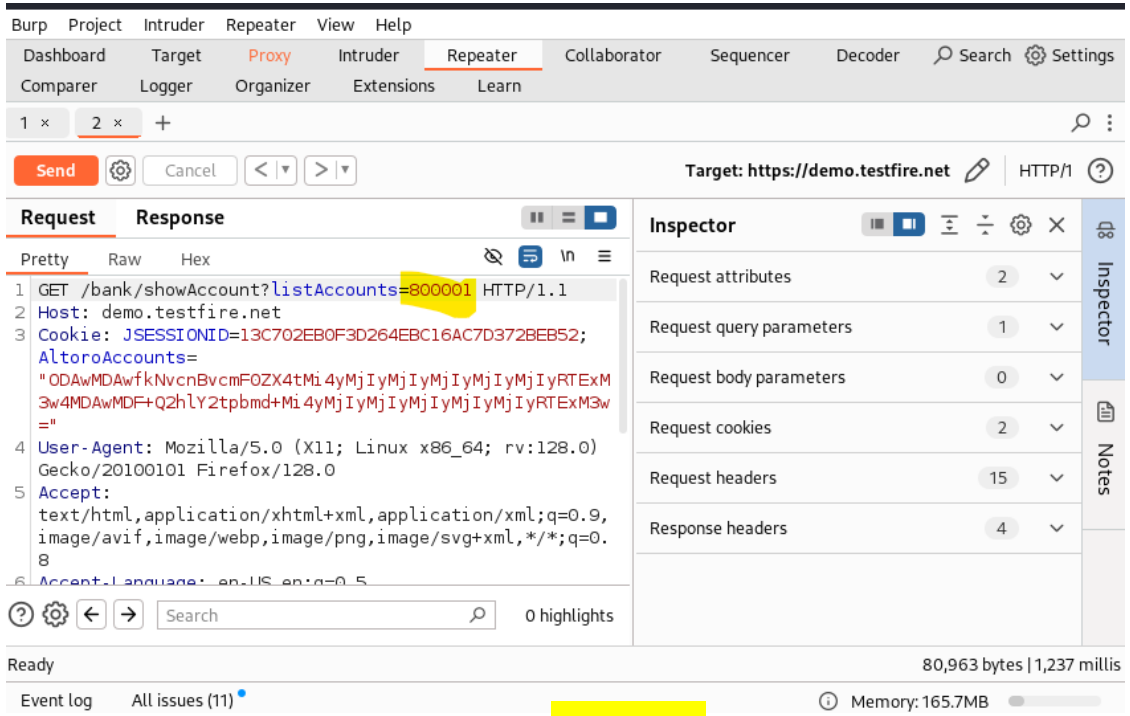


Image 1

Step 2 : then send the request to the repeater after that modify some content and send again to the comparer to compare both request.

=> we can compare in words and Bytes

Note : If have change 800001 to 899999999

you can see the comparison in image 4

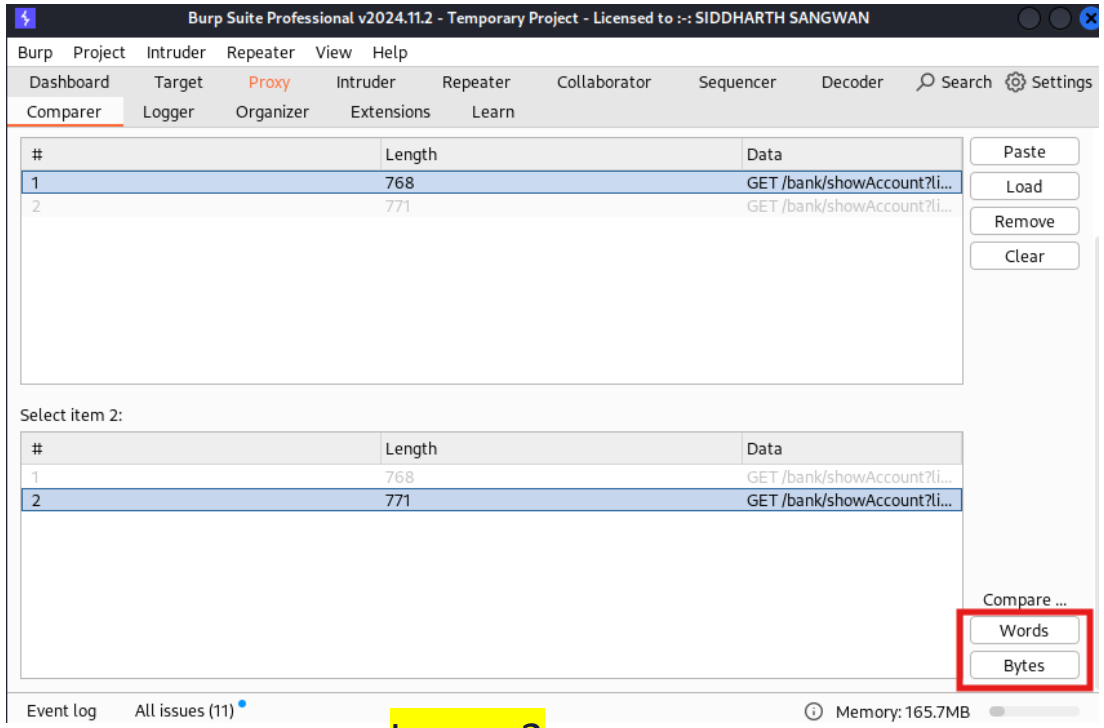


Image 3

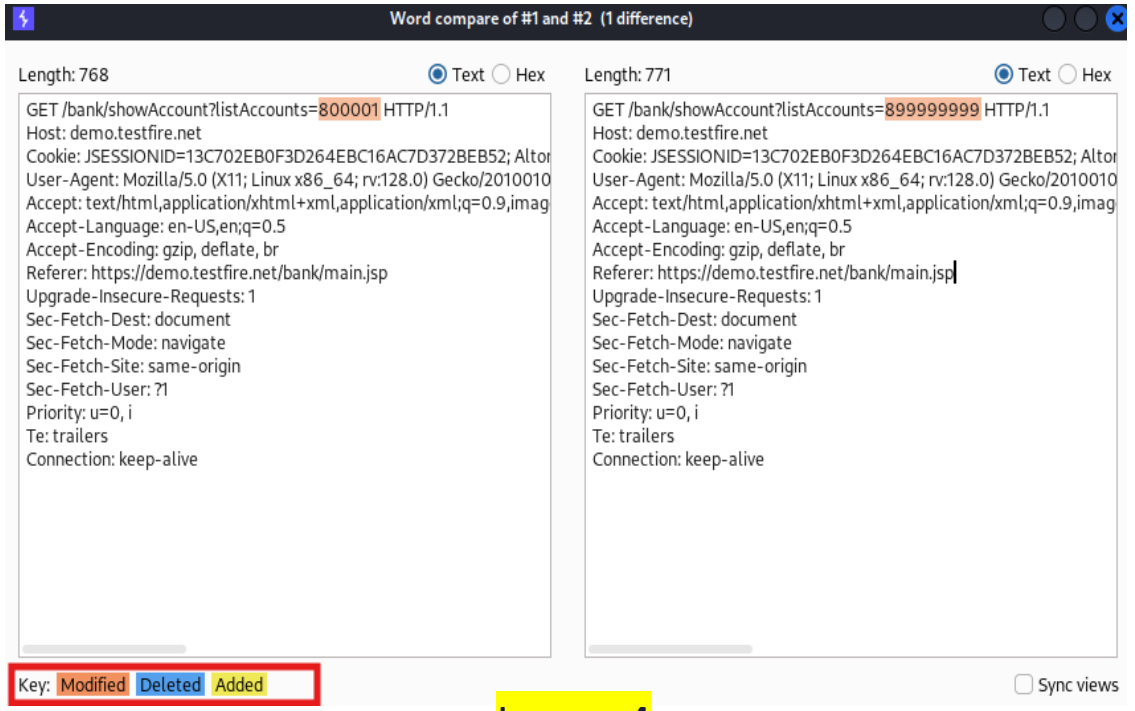


Image 4

Questions ?


Thank You!