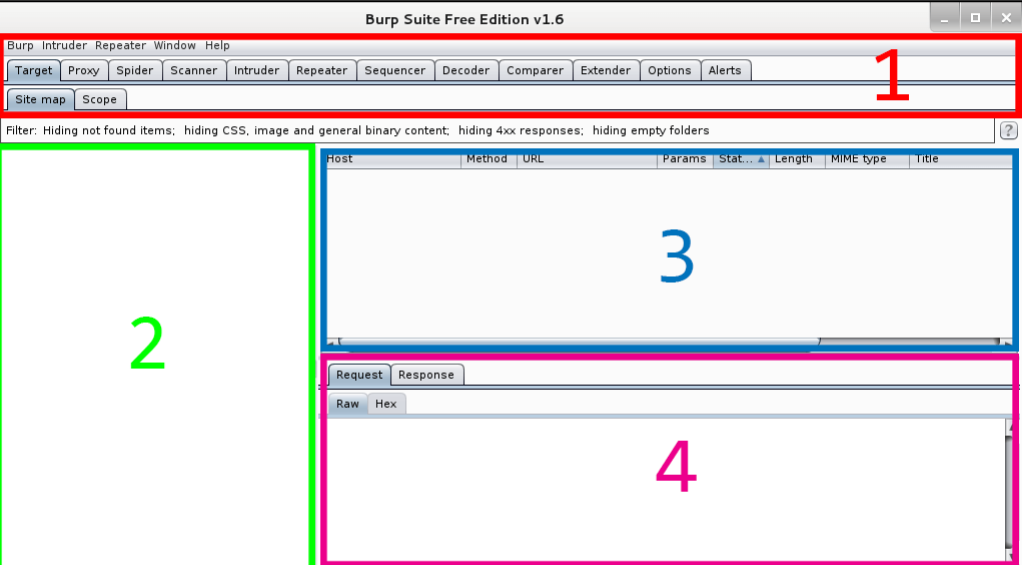
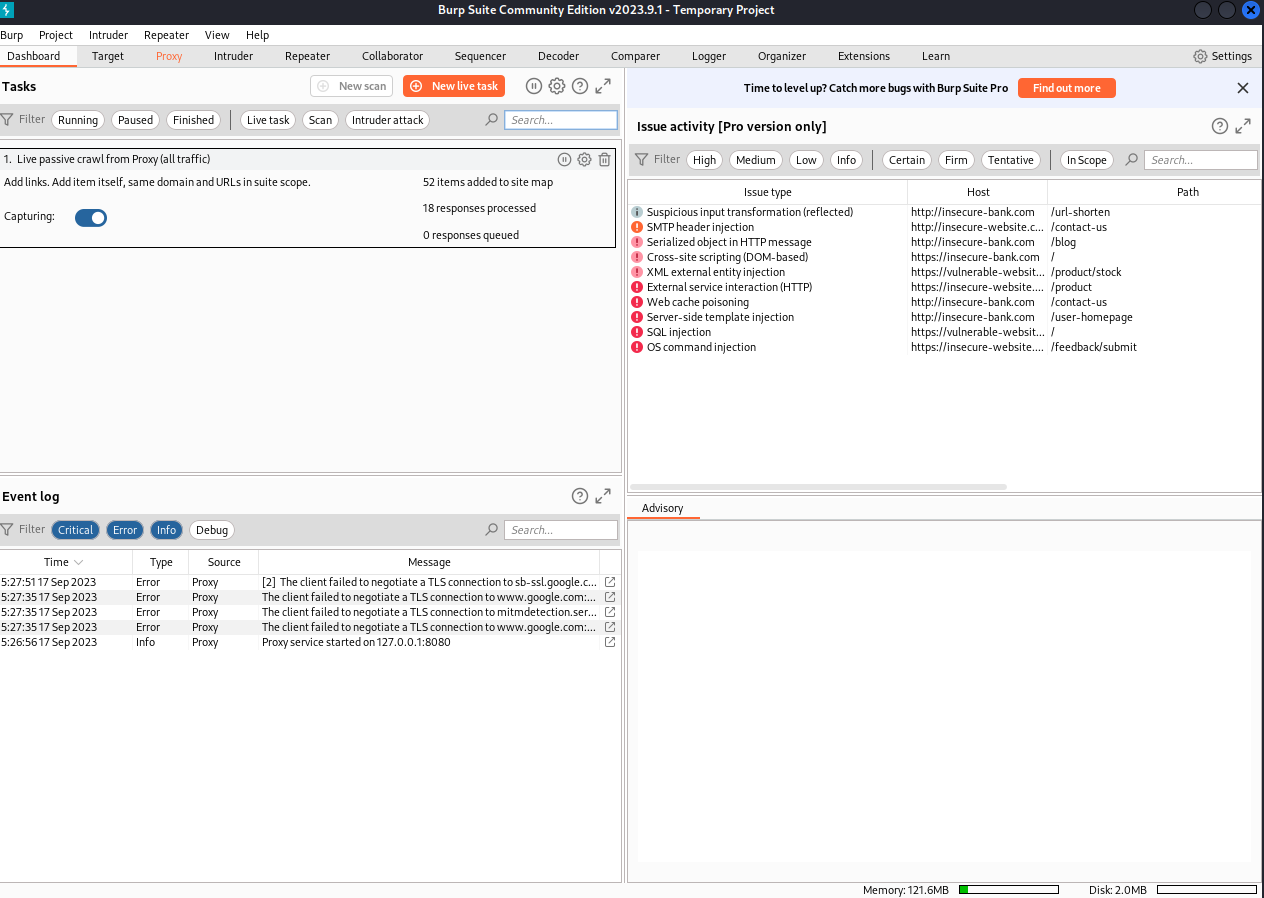
**SAMEER CHAUHAN 21BCE0999 ASSIGNMENT-4**

Aim- We have to prepare a document about usage and exploration of various features of burp suite tool.

Burp suite community edition- Burp Suite is a popular cybersecurity tool used for web application security testing and vulnerability assessment. It provides a wide range of features and capabilities to help security professionals identify and mitigate vulnerabilities in web applications.





**Here we can see the burp suite community edition dashboard interface-**

**Proxy**: Burp Suite acts as a proxy server that intercepts and logs HTTP and HTTPS traffic between a web browser and a web server. This allows users to inspect and modify requests and responses, making it a valuable tool for manual testing and analysis.

**Scanner:** Burp includes an automated scanner that can identify various vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and more. It can help automate the vulnerability assessment process.

**Spider:** The spider tool can crawl a website to discover and map out its content and functionality. This is useful for identifying hidden pages and potential attack surfaces.

**Intruder:** Burp Intruder is a powerful tool for performing automated attacks on web applications, such as brute-force attacks, fuzzing, and payload manipulation. It helps identify vulnerabilities that may not be apparent through manual testing.

**Repeater:** This tool allows security professionals to manually modify and replay HTTP requests to observe how a web application responds. It's helpful for identifying vulnerabilities and testing the impact of different inputs.

**Sequencer:** Burp Sequencer analyses the quality of randomness in tokens and session identifiers, which can help identify potential session management vulnerabilities.

**Decoder:** It provides various encoding and decoding tools for working with different data formats, such as URL encoding, Base64, and more.

**Comparer:** Burp Suite's comparer helps identify differences between two HTTP responses or requests, which can be useful for detecting potential security issues.

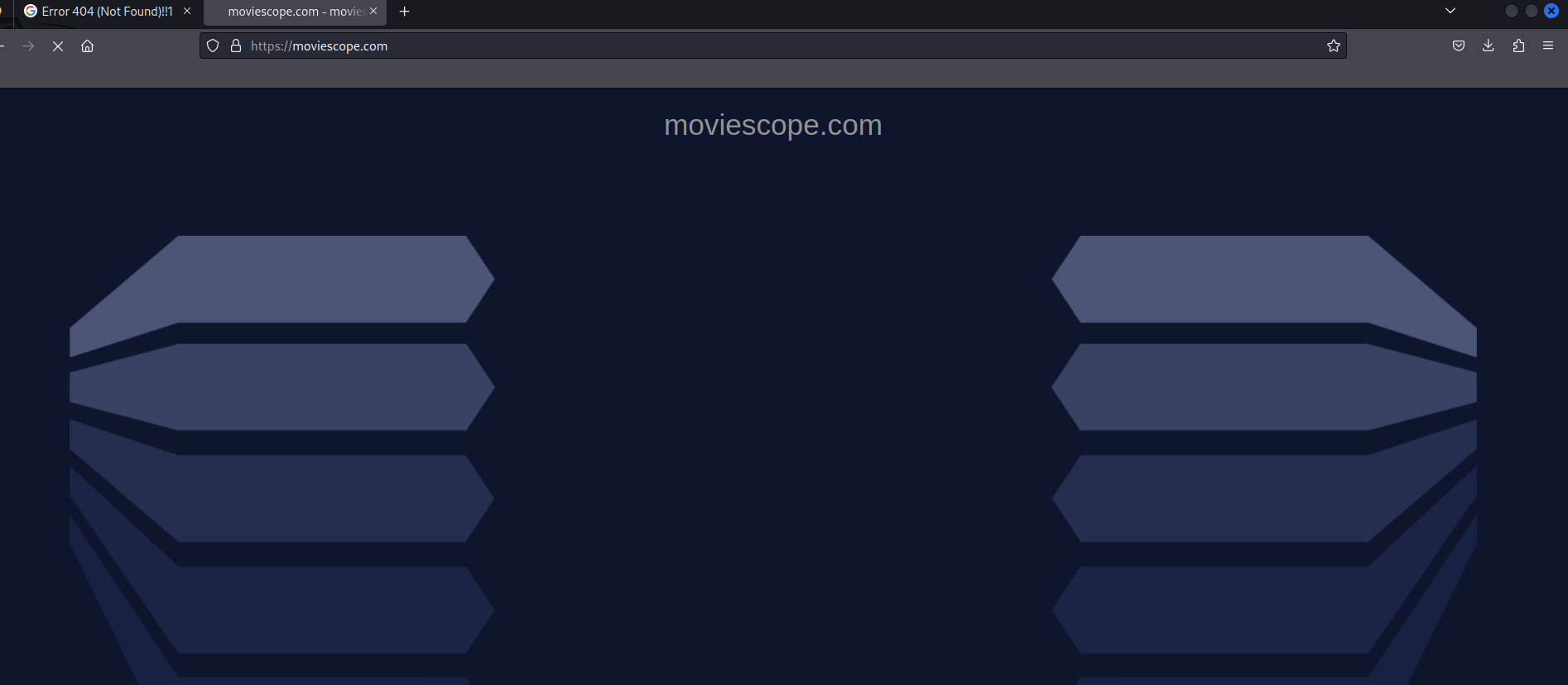
**Extensibility:** Burp Suite can be extended using its extensive API. Security professionals and developers can create custom extensions, plugins, and scripts to enhance its functionality and integrate it with other tools and systems.

**Target Scope:** Users can define the scope of their testing by specifying which parts of a website or web application should be included or excluded from the scan or testing.

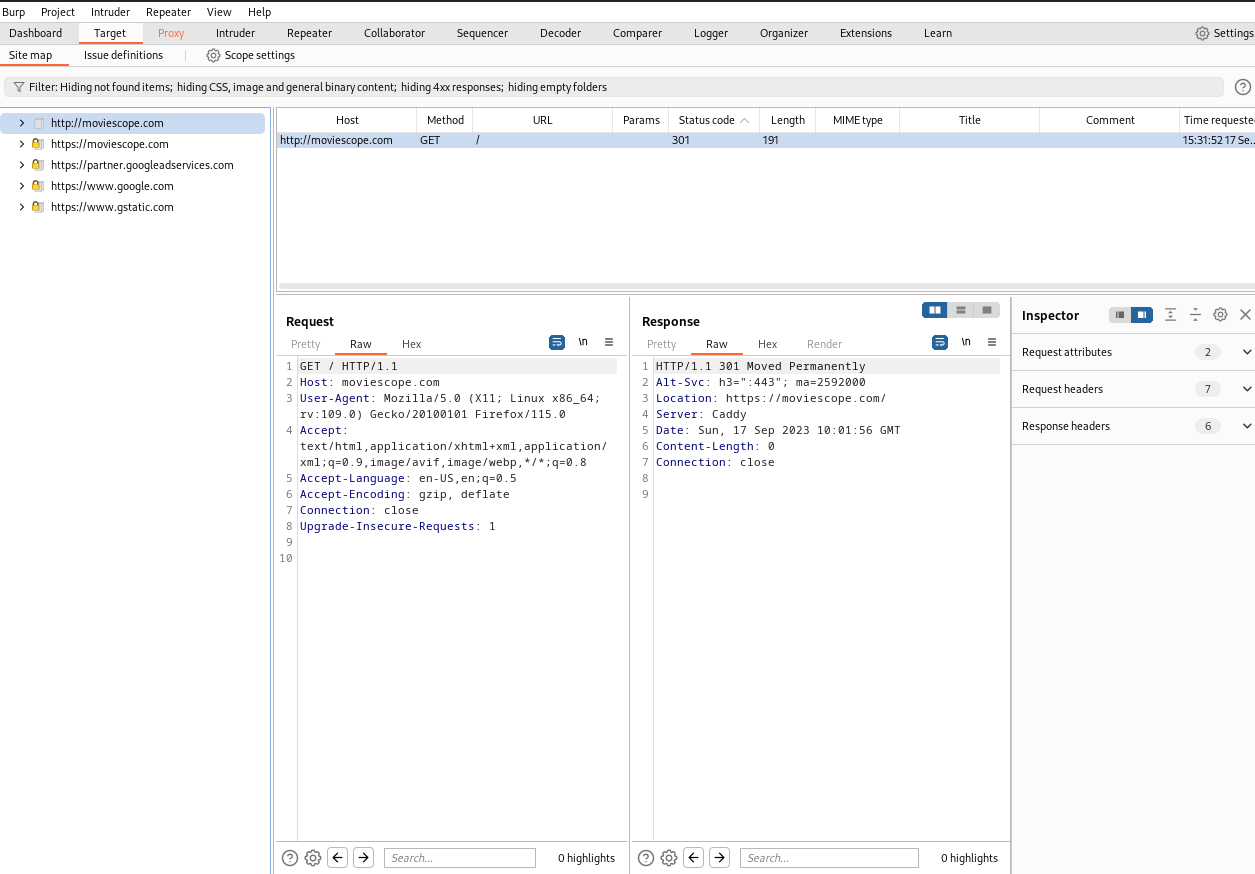
**Collaborator:** Burp Collaborator helps detect out-of-band vulnerabilities by providing a unique domain that can be used to trigger interactions with the target application, revealing potential security weaknesses.

**Session Handling:** Burp Suite allows you to manage and manipulate sessions, cookies, and authentication tokens during testing, enabling a more comprehensive assessment of web application security.

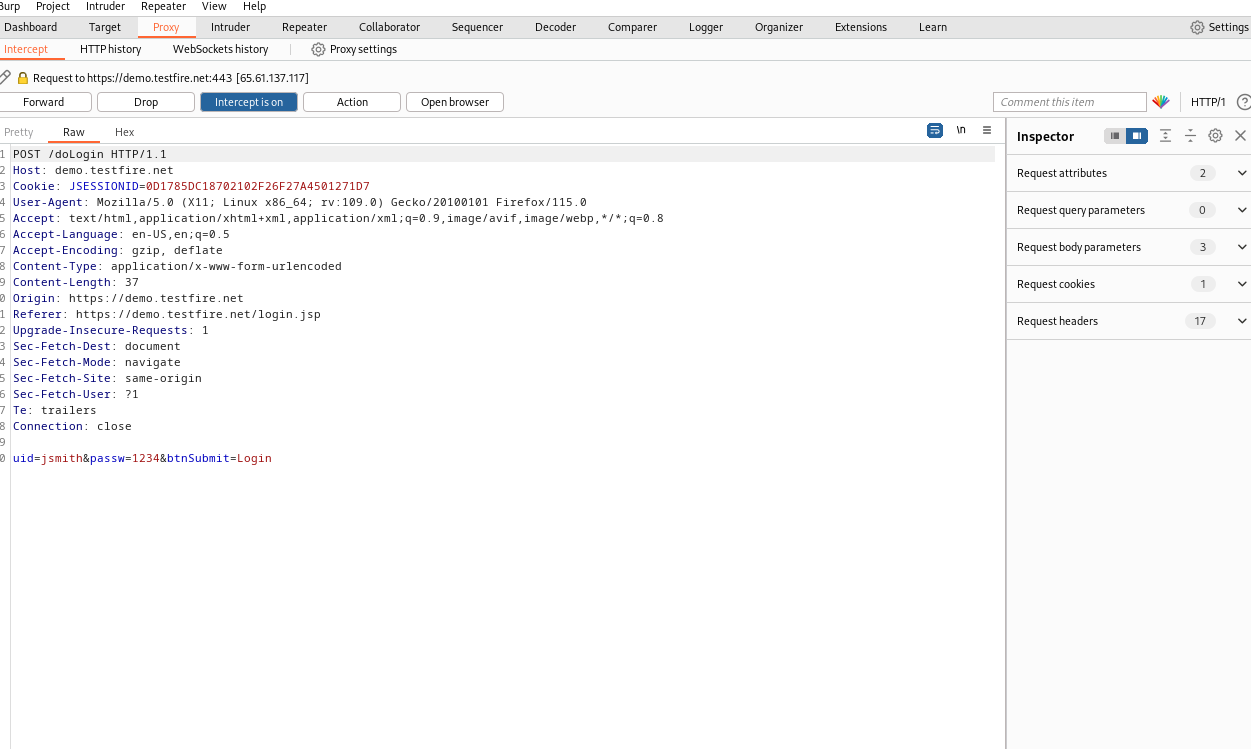
**Reporting:** It offers customizable reporting capabilities to generate detailed reports of identified vulnerabilities and testing results.



Here we can see that www.moviescope.com website is opened in our web browser

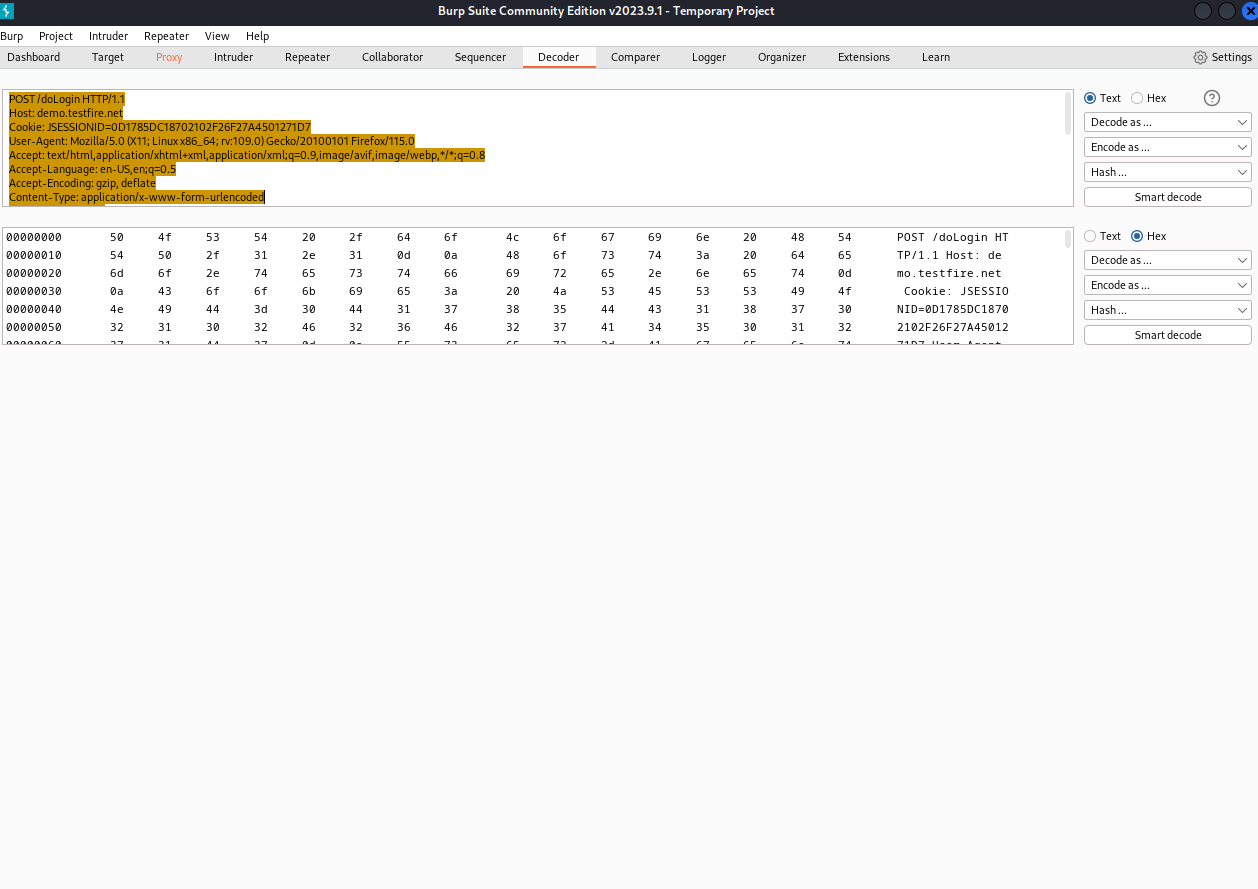


Here we can see our website our web browser and burp suite are linked with manual proxy 127.0.0.1 and port 8080 we can see the websites incoming requests get and post, in this way we can intercept the following websites and perform man in the middle attack.

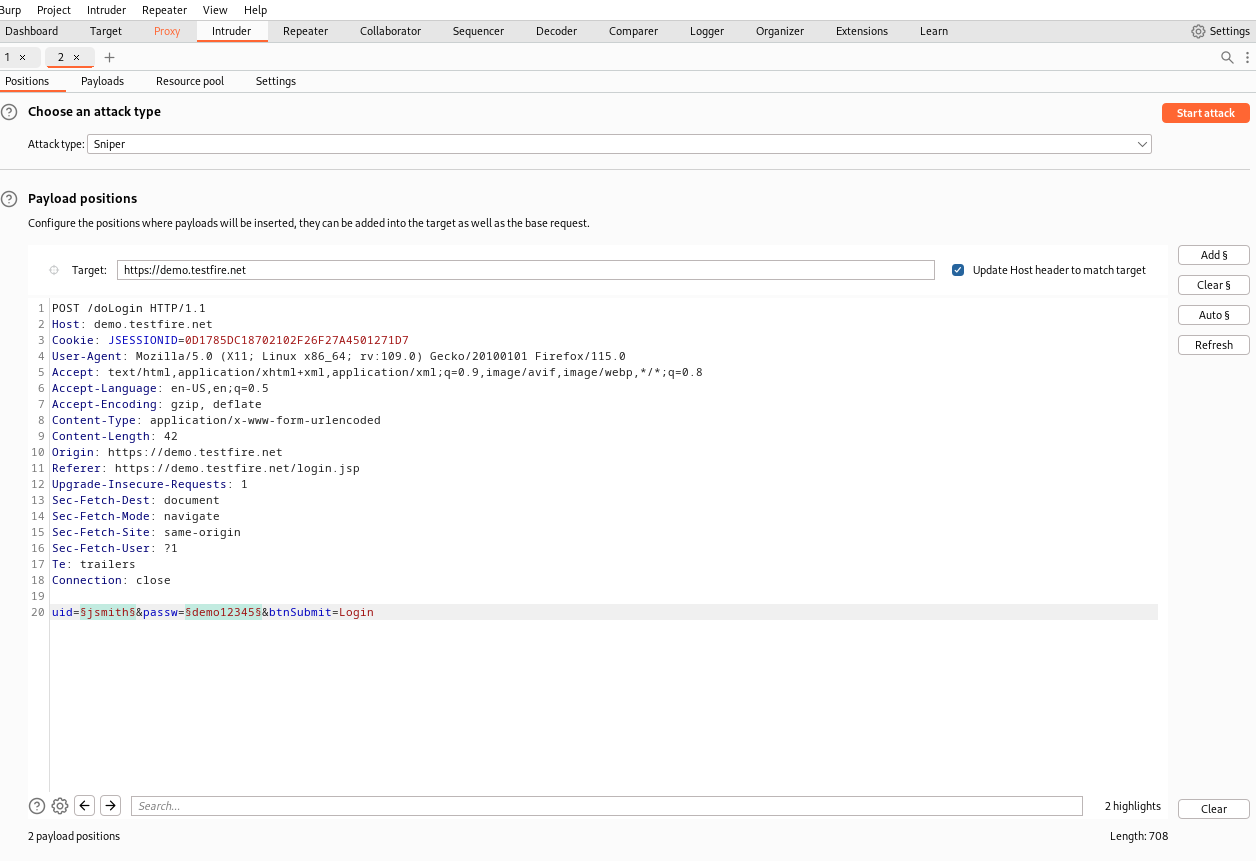


Here we can see that when we login in our website, burp suite has captured the login details ,it has also captured cookie id, j session id,

By poisoning them we can perform session hijacking attack as well as man in the middle attack.



We can see decoder section which helps us to decode our back end code, we can decode it in many forms and in hex format as well.



By sending our captured data to intruder we can perform brute force attack, we have four types of options as attack in this:

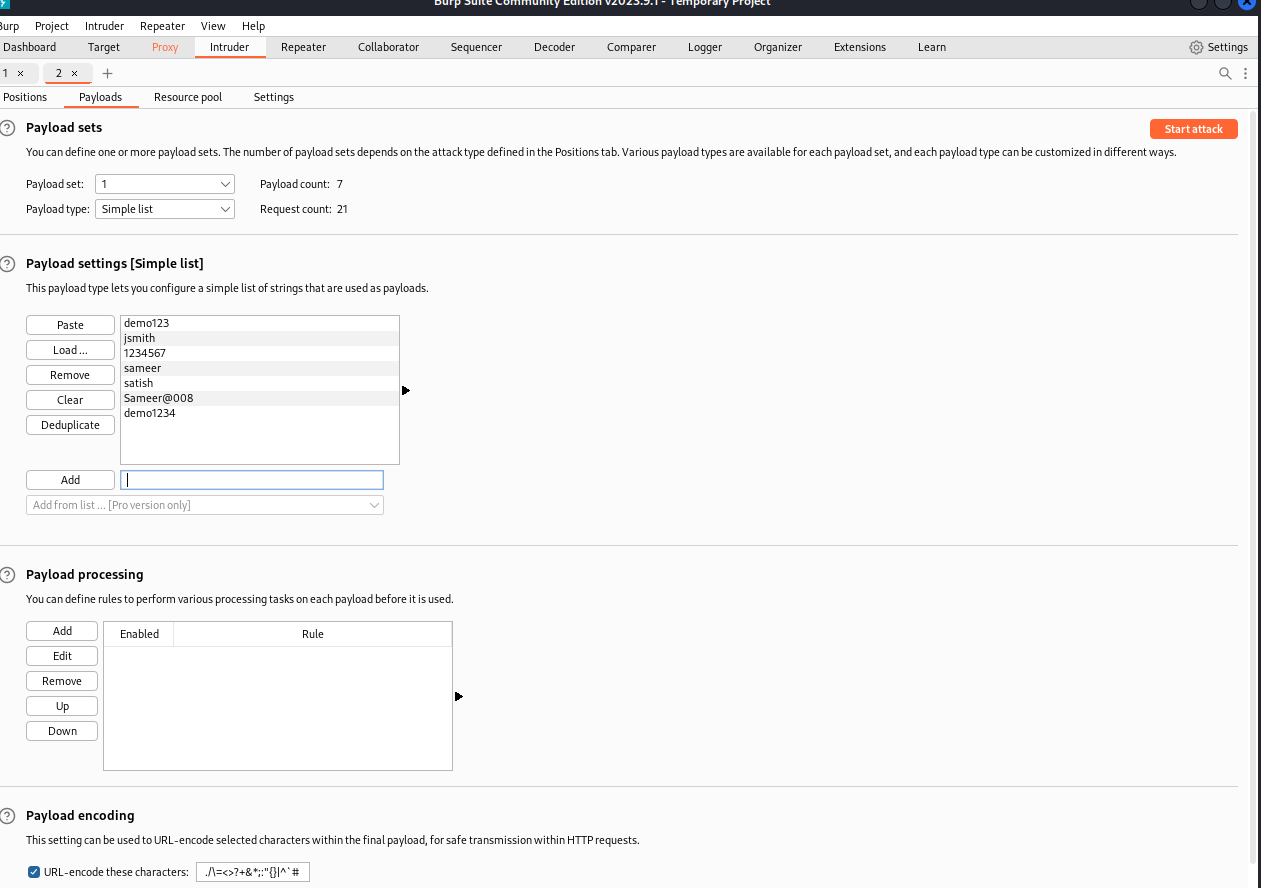
1-Sniper attack-it is used when there is generally one payloads.

2-battering ram-it used single set of payloads which iterates all the payloads while interchanging the payloads.

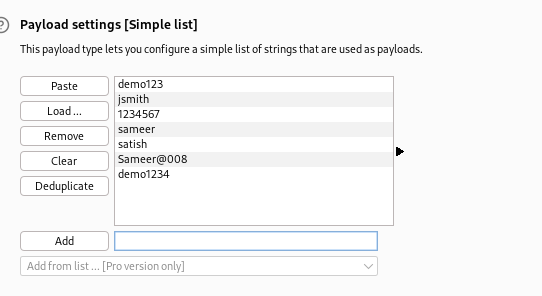
3-Pitch forks-this type of attack use multiple sets of payloads

Attacker iterate through each set of payloads simultaneously.

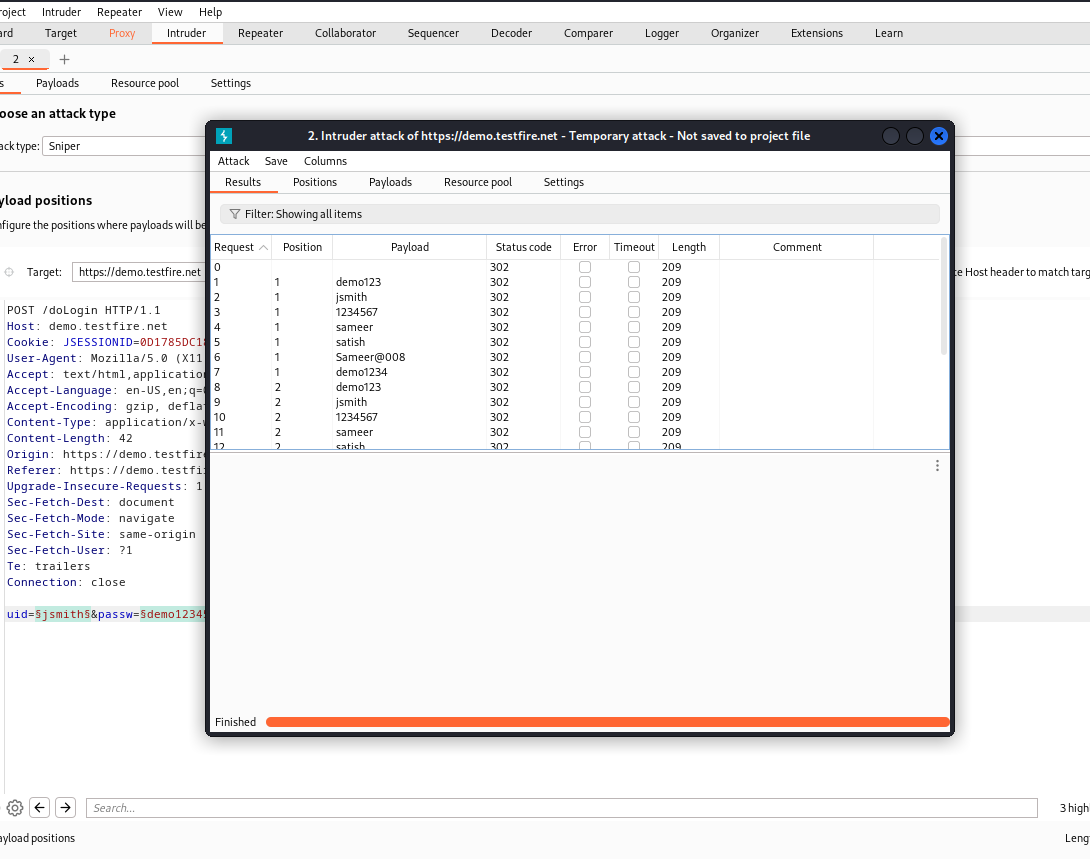
4-Cluster bomb-This attack iterates through a different payload set for each defined position. Payloads are placed from each set in turn, so that all payload combinations are tested.



In this section we can set payloads and add customize dictionary for password attacks



Here we can see I added some wordlists to my payload in burp suite manually:



As we can see our brute force attack is going on with the help of burp suite tool.

Spoofing your IP address using Burp Proxy match and replace:

Burp suite allows you to configure [match and replace rules](https://portswigger.net/burp/documentation/desktop/settings/tools/proxy#match-and-replace-rules) that automatically modify your requests and responses while you explore the target application as normal using Burp's browser. This enables you to add, remove, or modify headers in requests or responses, for example.

There are a number of uses for this, including potentially spoofing your IP address. In some cases, this may allow you to trick a server into believing that you belong to its local network, which could enable you to communicate with internal infrastructure that is otherwise inaccessible.

Burp Suite: Good Tool For Vulnerability Scanning:

It is a very good tool that you we can use to carry out vulnerability scanning on your web applications or websites.

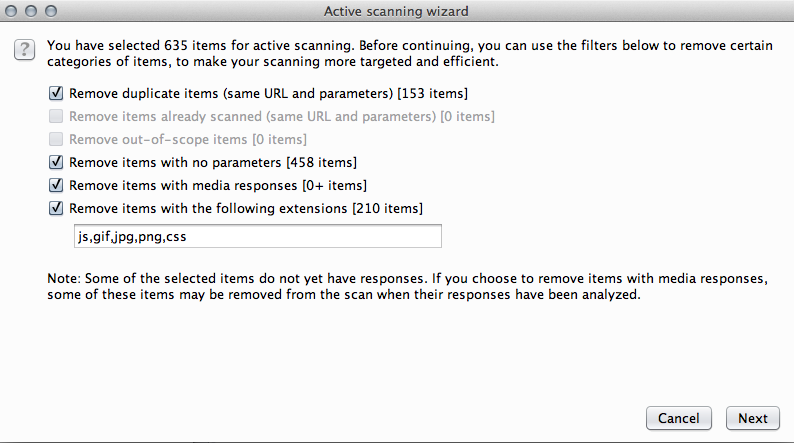
This is an automation process that helps the pen-tester to finish a testing task because sometimes the pen-tester may not have enough time to test all parameters of a web request. This will invariably make the pen-tester to be effective and efficient in achieving his target after going through a rigorous process of penetration testing.

It has the capacity to analyse every detail during the scanning process and it will notify you when a vulnerability has been discover.

Automated Scanning:

I like to do the passive scan first because it doesn’t send any traffic to the target server. Alternatively you can configure [Burp Suite](https://www.pentestgeek.com/what-is-burpsuite) to passively analyse requests and responses automatically in the “Live scanning” sub-tab. You can also do this for Active Scanning but I do not recommend it.

When doing an active scan I like to use the following settings.

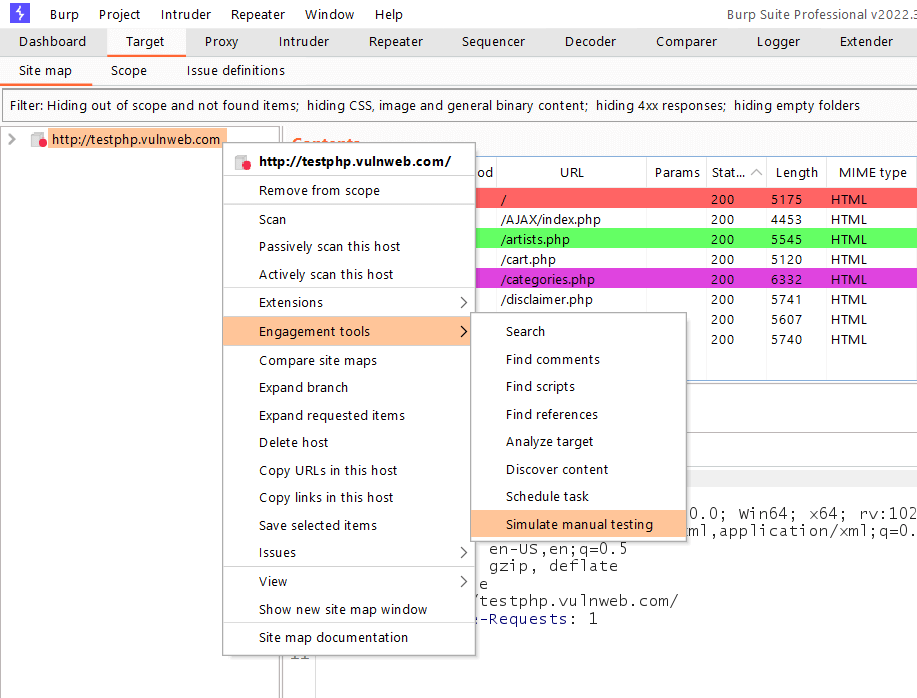
[](https://www.pentestgeek.com/wp-content/uploads/2014/07/10-Active-Scan-Settings.png)

Spidering a Website:

A web crawler is a bot program that systematically browses the pages of a website for the purpose of indexing. Precisely a web crawler maps the structure of a website by browsing all its inner pages. The crawler is also referred to as a spider or automatic indexer.

Burp Suite has got its own spider called the burp spider. The burp spider is a program that crawls into all the pages of a target specified in the scope. Before starting the burp spider, the Burp suite has to be configured to intercept the HTTP traffic.

### **Simulate Manual Testing:** **To simulate manual penetration testing traffic, the function sends common test payloads to random URLs and parameters at irregular intervals. Its sole purpose is to allow you to take a break from testing while remaining active in the server’s logs. Only the items from the site map that you selected will be requested.**



Conclusion: We noted the use of burp suite and explored different features of the tool