# **ASSIGNMENT - 4**

K. Naveen Abhiram

21BCE7357

**EXPLORING BURP SUITE**

**BRUP SUITE**

The Java-based Burp Suite framework aspires to provide a one-stop shop for online application penetration testing. Burp is essentially the industry standard tool for performing hands-on web app security evaluations, therefore in many ways this objective is accomplished. The same characteristics that make Burp Suite so appealing for web app testing also make it very popular when evaluating mobile applications, since it almost perfectly translates into testing the APIs (Application Programming Interfaces) that power most mobile apps.

The foundation of the system is Burp, which can at its most basic level intercept and modify any traffic between an attacker and a web server. We can select to send requests to different Burp Suite components after capturing them. Burp Suite is ideal for any form of manual web app testing since it has the capacity to intercept, examine, and edit web requests before they are delivered to the target server (or, in certain situations, the responses before they are received by our browser).

Burp Suite is offered in a number of different editions. Since the Burp Suite Community edition is free to use for any (legal) non-commercial use, that is what we will be using. Both the Burp Suite Professional and Enterprise editions have pricey license fees but also have strong added features:

* Burp Suite Professional is a version of Burp Suite Community that is unrestricted. A vulnerability scanner that runs automatically is one of its characteristics.
* A rate-unlimited fuzzer / brute force.
* Creating reports and saving projects for later use.
* A built-in API that enables tool integration.
* Complete freedom to incorporate new extensions for increased functionality.
* Access to the Burp Suite Collaborator, which serves as a self-hosted or server controlled by Portswigger unique request catcher.
* The little difference is in Burp Suite Enterprise. Burp Enterprise, in contrast to the community and professional editions, is used for continuous scanning. Similar to Nessus, it offers an automated scanner that can routinely check webapps for vulnerabilities. Burp Suite Enterprise sits on a server and continuously checks target web apps for vulnerabilities, in contrast to the other editions of the software that let you launch manual assaults from your personal computer.

**Features of Brup Suite:**

Although Burp Community offers fewer features than the Professional edition, it still provides access to several excellent tools. These consist of:

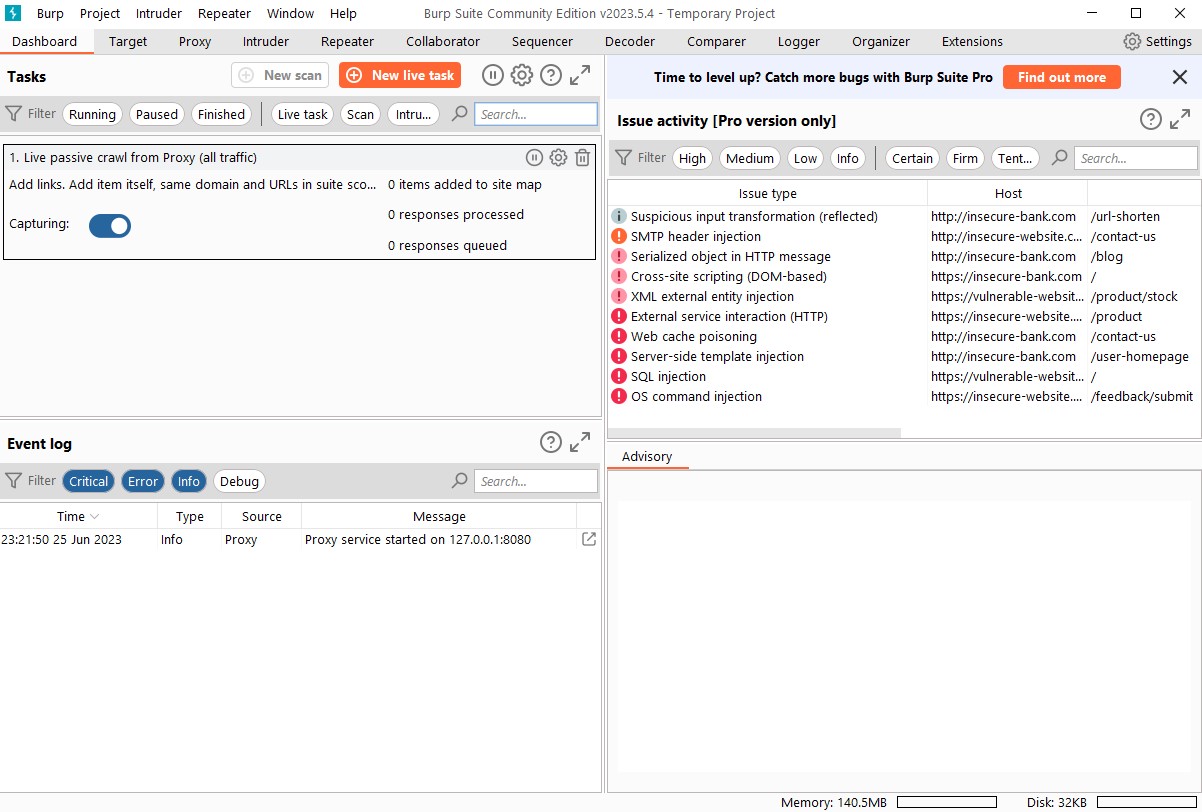
* Burp Proxy, the feature of Burp Suite that is most well-known, enables us to intercept and change requests and responses while dealing with online applications.
* Despite being severely rate-limited in the Burp Community, Intruder enables us to bombard an endpoint with queries. This is frequently used for endpoint fuzzing or brute force attacks.
* Repeater enables us to repeatedly capture, alter, and deliver the same request. When creating a payload by trial and error (as in a SQLi -- Structured Query Language Injection) or testing an endpoint's functionality for faults, this feature can be incredibly helpful.
* The Comparer program lets us compare two sets of data at the word or byte level, as the name suggests. Again, this is not a feature exclusive to Burp Suite, but it can significantly speed up operations to be able to transfer (perhaps very huge) amounts of data into a comparison tool with a single keyboard press.
* Although less frequently used than the characteristics listed above, decoder nonetheless offers a useful function when transforming data, such as when decoding information that has been captured or encoding a payload before delivering it to the target. While there are other services that can do the same function, Burp Suite has the potential to be a very effective option.

**Burp Suite installation and setup:**

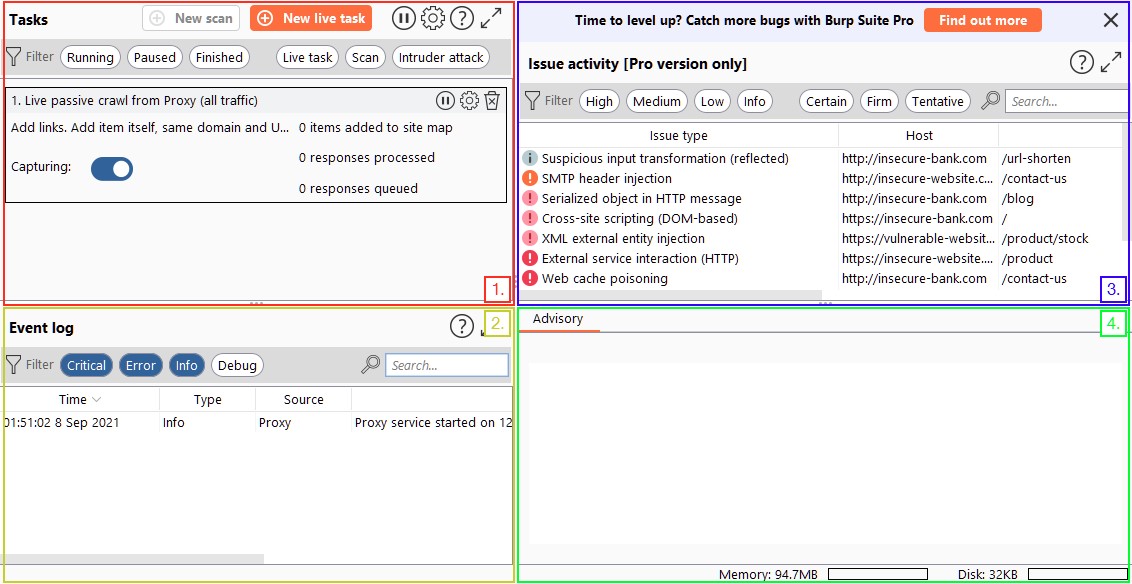
After accepting the terms and conditions and opening Burp Suite, a dialog asking us to choose the project type greets us. All we have to do is press "Next" here.

The primary Burp Suite interface will appear after clicking "Start Burp"!

There's a BURP Dashboard now!



The Dashboard interface is divided into four quadrants, which are as follows:

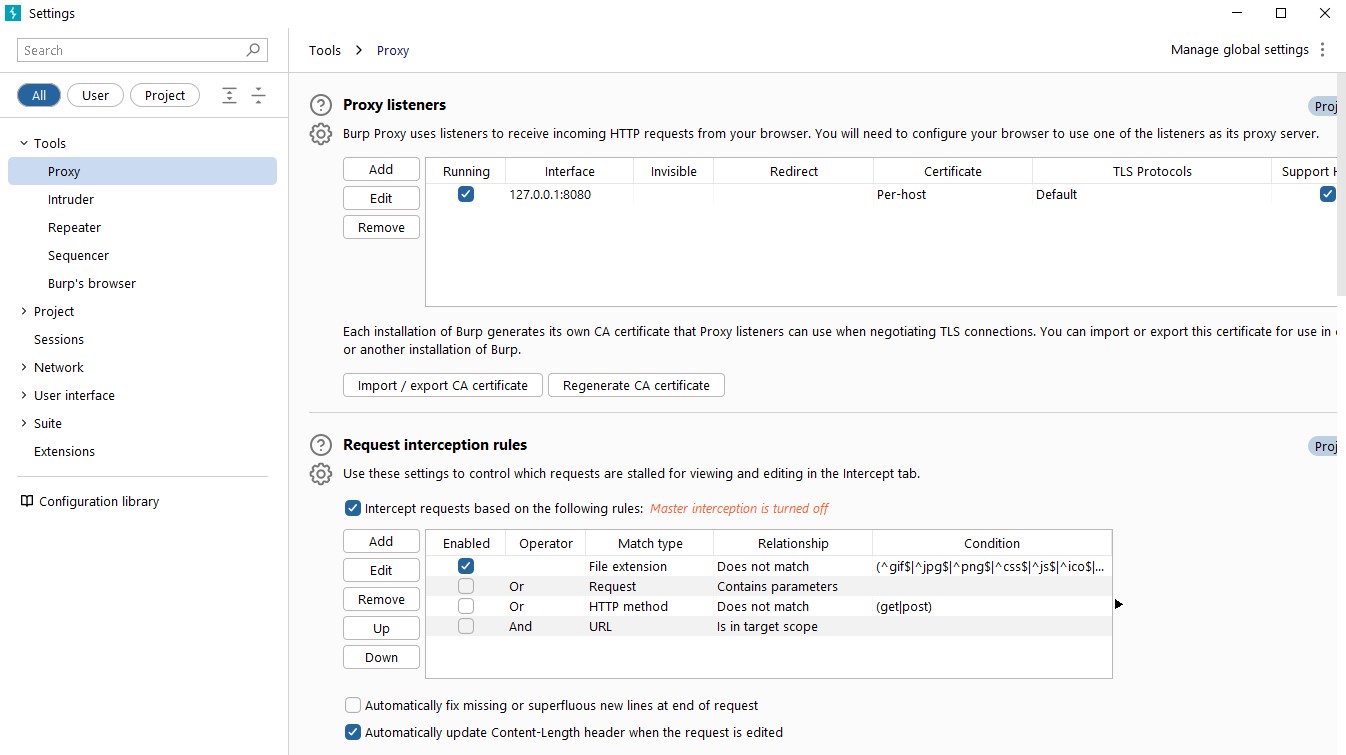


* We can specify the background tasks that Burp Suite will carry out while we use the program using the **Tasks** option.
* The **Event log** provides details about any connections we make using Burp Suite as well as information about what Burp Suite is doing (such as establishing the Proxy).
* Only **Issue Activity** is available in Burp Pro. Burp Community won't provide any information, however Burp Professional would list all vulnerabilities discovered by the automated scanner. These would be sorted according to how serious they are and how confidently Burp believes the component is vulnerable.
* More details regarding the vulnerabilities discovered are provided in the **Advisory** section, along with references and possible fixes. Then, a report might be created using these.

It should be noted that a lot of the tools in Burp Suite provide shortcuts to particular settings categories. As an illustration, the "Proxy settings" button on the Proxy tool will open the Settings window to the part relevant to the proxy.



The ability to search for settings using keywords is a relatively recent addition to the settings page, but it is of the utmost importance.



**Brup Proxy:**

The Burp Proxy is the most fundamental (and crucial!) of the Burp Suite's utilities. It enables us to record the requests and answers we exchange with our target. Before being permitted to proceed to their destination, they can then be altered or routed to other tools for additional processing.

For instance, if we send a request to https://tryhackme.com using the Burp Proxy, it will be intercepted and held until we expressly permit it to go to the TryHackMe servers. Although this is not enabled by default, we may opt to do the same with the server's reply. When it comes to testing online apps, the ability to completely manage our web traffic is made possible by our capacity to intercept requests.

Burp provides us with a ton of background reading and helpful information when we first access the Proxy page. Although going through this material is highly recommended, the actual magic comes once we have captured a request:



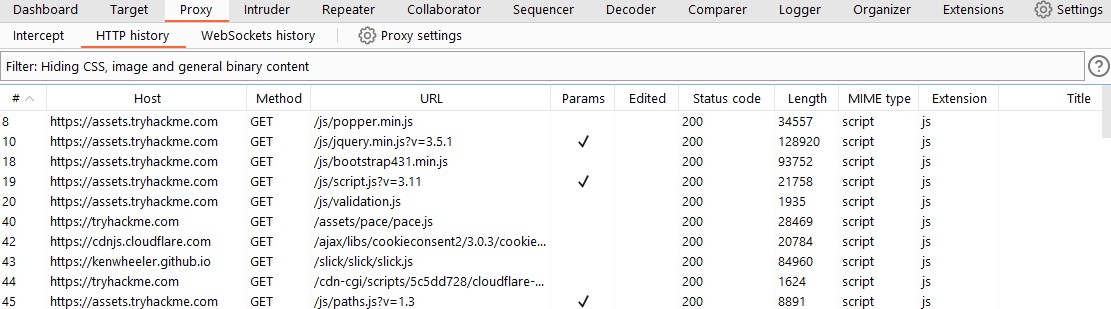
A request was made to the TryHackMe website while the proxy was running. The request will now display in the Proxy tab, giving us the view seen in the above picture, and the browser making the request will halt at this point. The request can then be sent or rejected (perhaps after being edited). Other options include storing the request to a file, transferring it to another Burp module, copying it as a CURL command, and a number of others.

Clicking the "Intercept is on" button will turn off the Intercept after we are done using the proxy, allowing requests to proceed via the proxy without being halted.

When the intercept is off, Burp Suite will continue by default be logging requests that go via the proxy. Even if we didn't expressly collect previous requests when they were made, this may be incredibly helpful for looking back and analysing them.

Burp will also record and log WebSocket communication, which is yet another extremely useful feature when examining a web application.

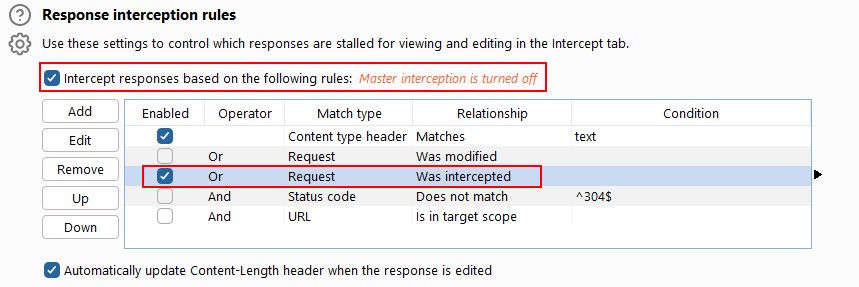
The "HTTP history" and "WebSocket history" sub-tabs can be used to inspect the logs:



It's important to note that you can send any requests you record here to other framework tools by right-clicking and selecting "Send to..." For instance, we may send Repeater a previous HTTP request that has already been proxied to the target.

In the Proxy Settings, you may access the Proxy-specific options by choosing the "Proxy Settings" button.

It is a good idea to become familiar with these settings because they provide us a lot of control over how the proxy behaves.



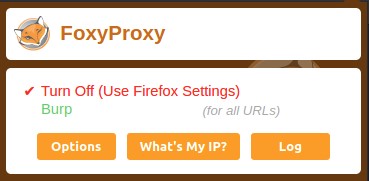
Most Proxy choices allow you to create your own rules, so here is one place were exploring and trying things out can be quite helpful.

There are two ways to use Burp Suite to proxy our traffic.

1. The embedded browser might be used.

2. We may set up our local web browser to use Burp as a proxy for our traffic.

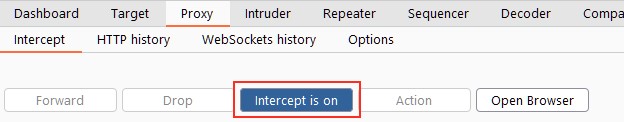
There is a configuration for Burp available when you click on the Foxy Proxy icon at the top of the screen:



Our browser will start sending all of our traffic to 127.0.0.1:8080 if we click on the "Burp" setting!

Activate this configuration right away, and the icon in the menu should change to show that a proxy is active.

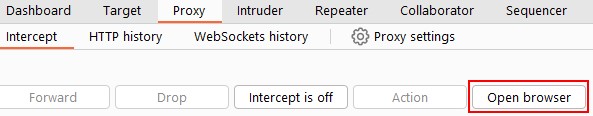
After that, switch to Burp Suite and confirm that the Intercept is turned on:



Try now opening Firefox and going to https://www.google.com. Your browser should freeze, and the request headers will appear in your proxy.

You can now decide whether to move the request forward or not. Alternatively, you may right-click the request and choose an item from the right-click menu to transfer it to another tool or carry out a variety of additional tasks.

With the "Open Browser" button selected in the proxy tab, we can launch the Burp Browser:



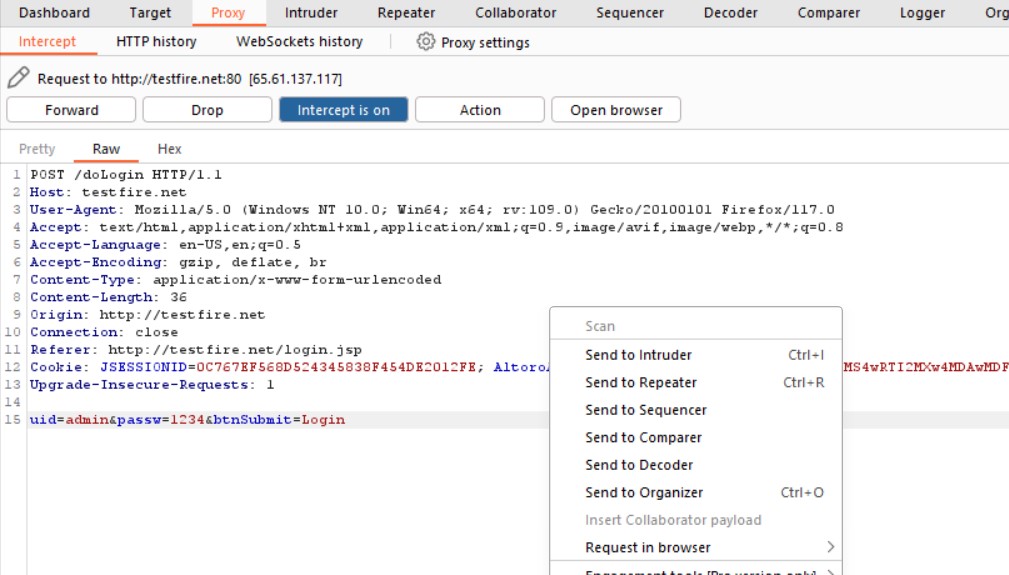
**Intruder:**

This is an incredibly strong tool that can be used to launch various assaults against web applications. It is quite simple to set up, and you can use it to quickly and efficiently do a variety of testing jobs. It is the ideal tool for both brute-force attacks and extremely challenging blind SQL injection operations.

Burp Suite Intruder typically operates by sending HTTP requests, which you may customize to your preferences. The study of application answers to queries may be done using this tool.

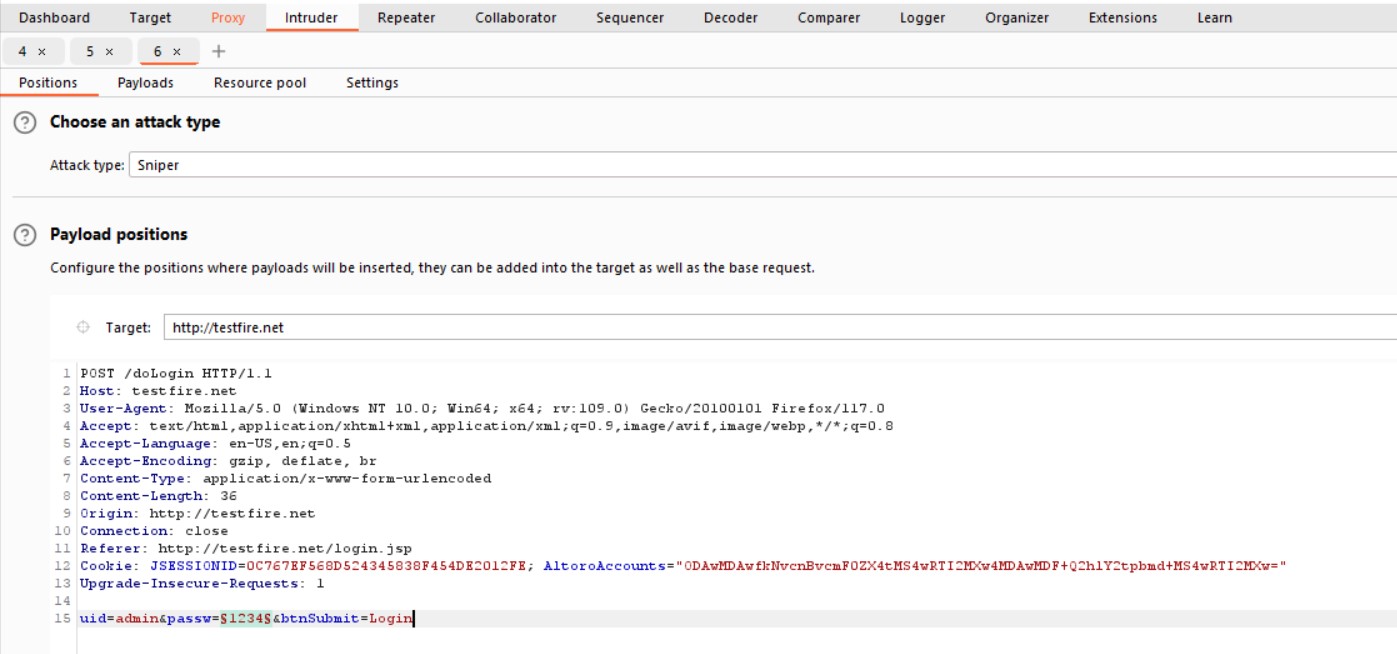
You must specify specific payloads for each assault, as well as the precise area in the base request where the payloads are to be inserted or released. Today, we offer several alternative methods for creating or producing your payloads. A basic list, a username generator, numbers, a brute force attack, a runtime file, a bit flipper, and many others are among our payloads.

Different algorithms used by the Burp Suite intruder aid in the precise placement of these payloads. Intruders from the Burp Suite may be used to extract relevant data, enumerate IDs, and do fuzzing operations to check for vulnerabilities.

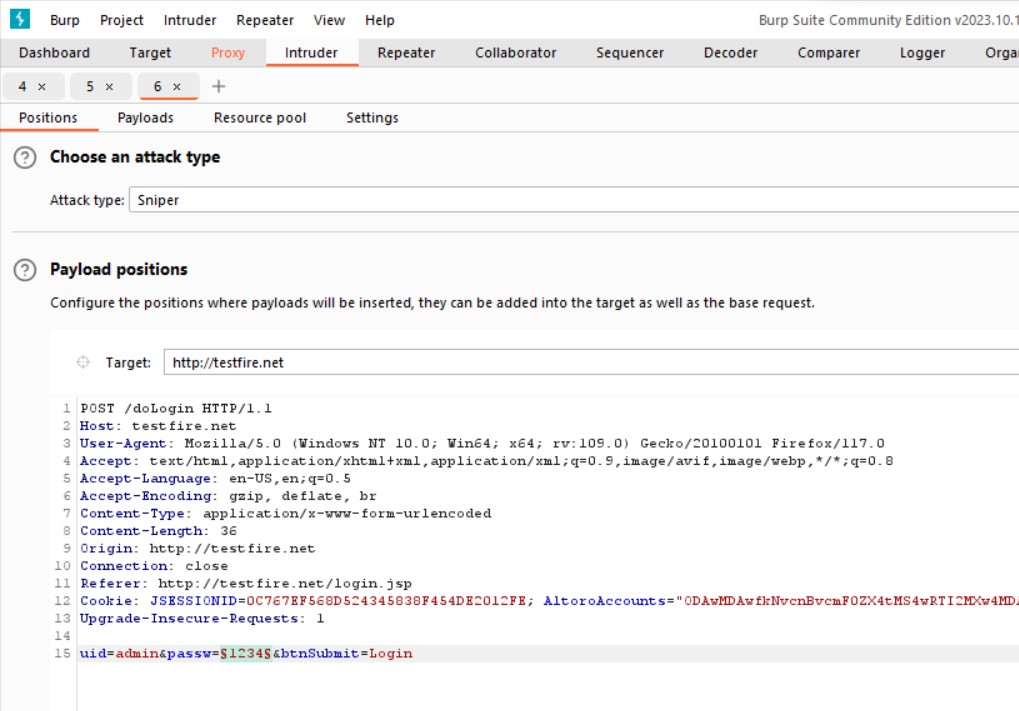


Follow these steps to successfully launch an attack using Burp suite Intruder:

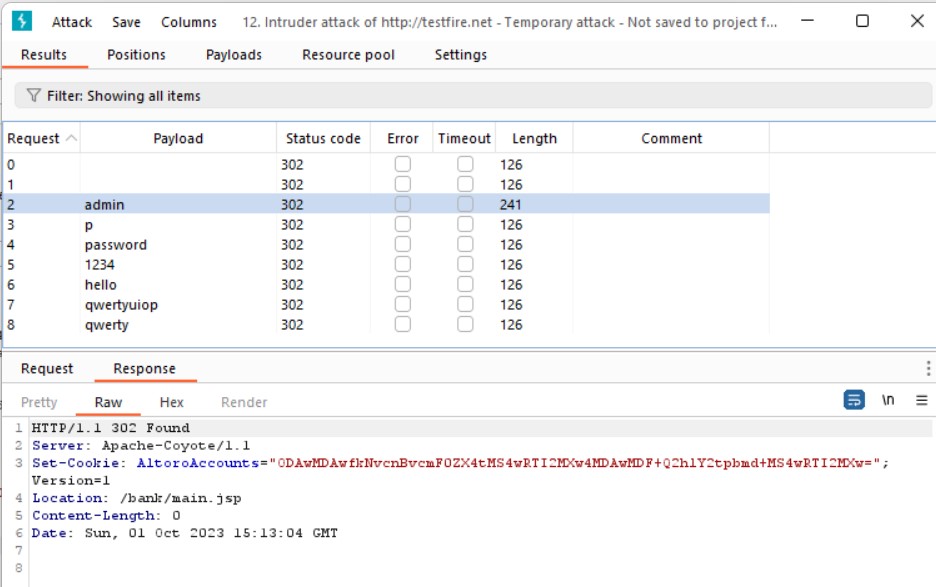
* Find the identification, which is frequently underlined in the request as well as the confirmation from the answer that it is legitimate.
* Then set up one payload position that is sufficient for the assault.



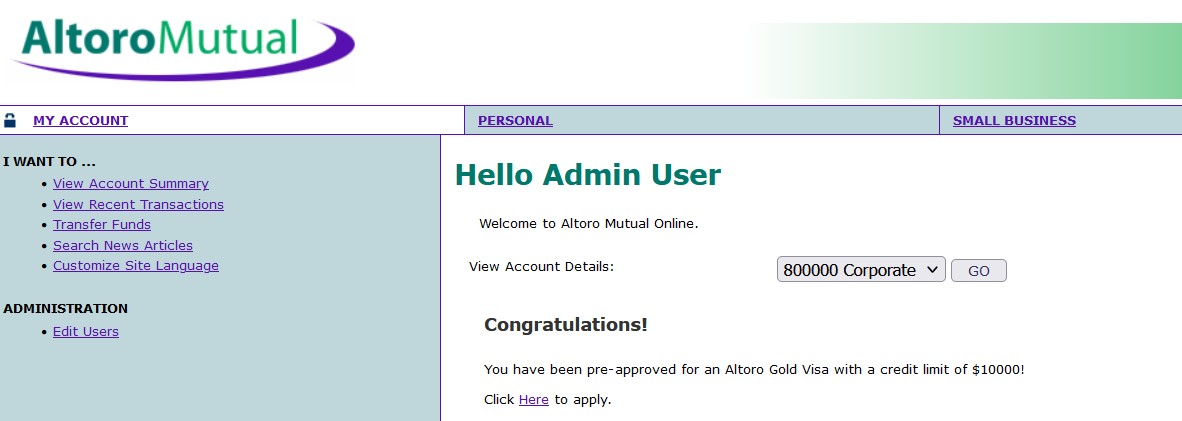
To create all of the IDs required for testing in the right format, use the Payload type drop-down.



You can click Start attack after inputting some of these crucial parameters to launch an assault. The result page will appear as the following pop-up page, which you must examine.



The proper password is the one that provides a different HTTP status code or response length from the others. If you use it, you will be allowed to log in. If you look at the image above, you can see that one identifier gives a different HTTP status code or response length.

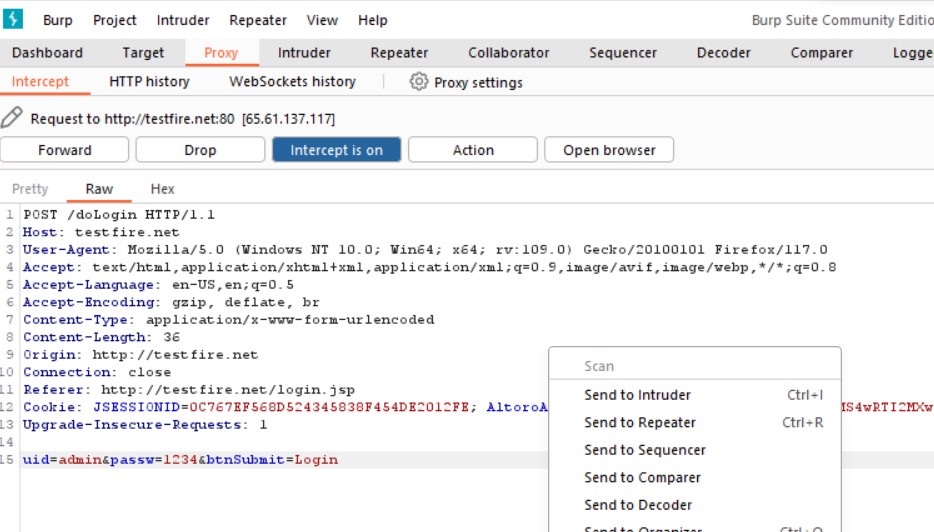


**Repeater:**

Burp Suite Repeater is made to manually alter and resend certain HTTP requests, allowing for deeper analysis of the answer. It is a multi-tasking tool used to test for input-based problems by modifying parameter details.

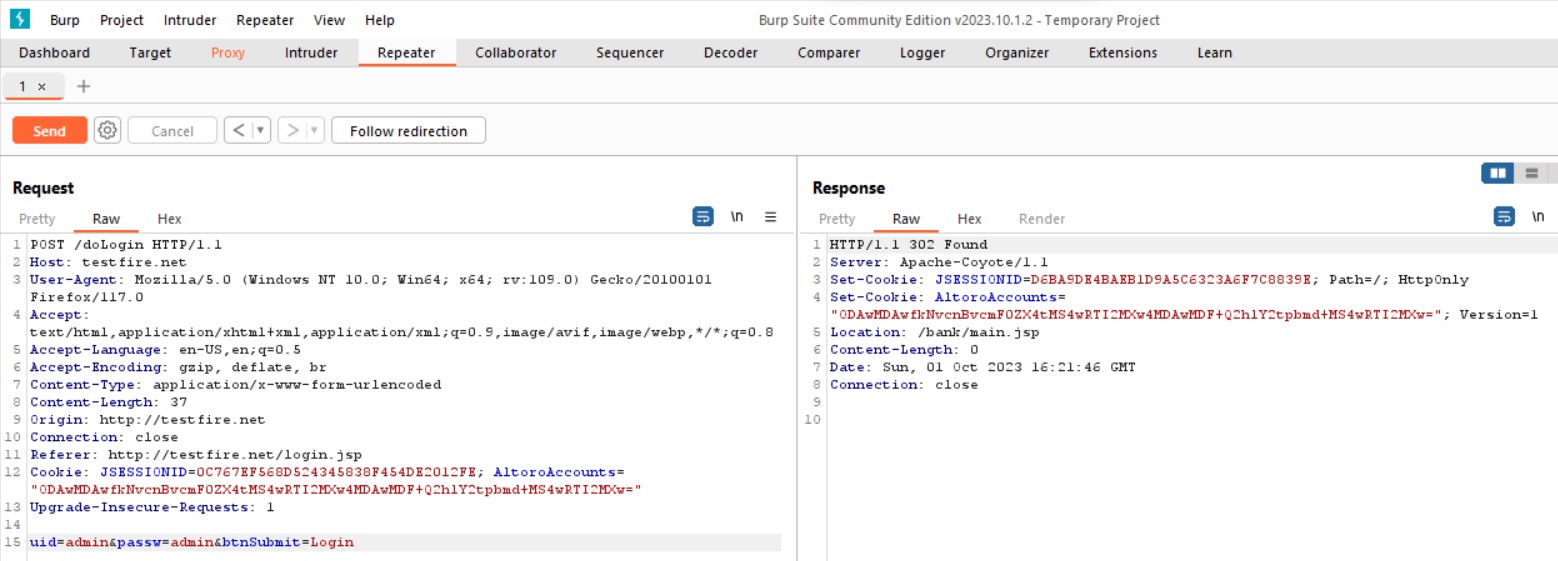
**Using Brup Repeater with HTTP Request:**

Simply choose Send to Repeater from the context menu when right-clicking on an HTTP request to utilize Burp Suite Repeater. The Repeater immediately creates a new request tab, and you can also view all the pertinent information in the message editor for future editing. Additionally, you may manually start a new Repeater tab and use the HTTP option.



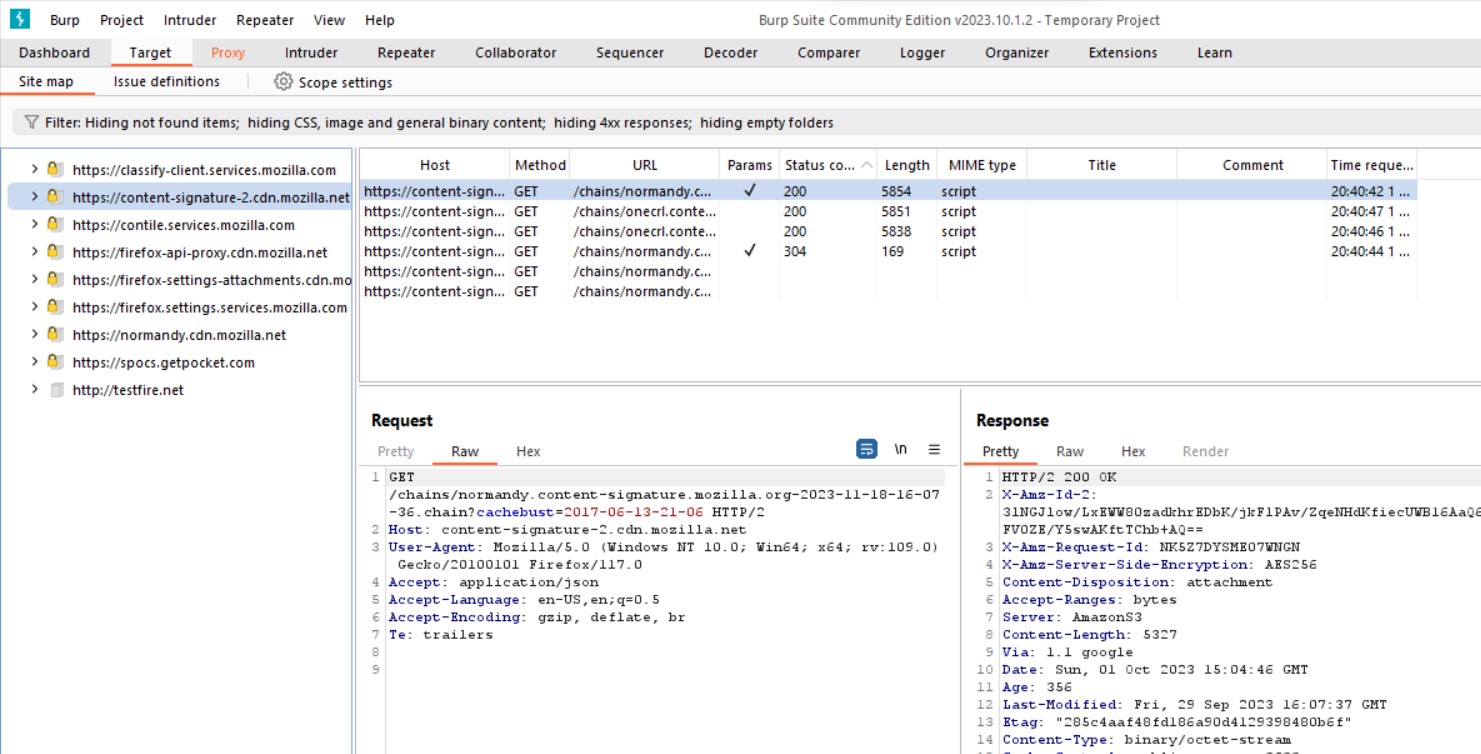
**Sending HTTP Requests:**

Simply click the Send or Go button to submit your request to the server after doing any necessary modifications. On the response panel at the right's side, the answer is shown. Additionally, you'll see that the answer message cannot be modified.



**Target:**

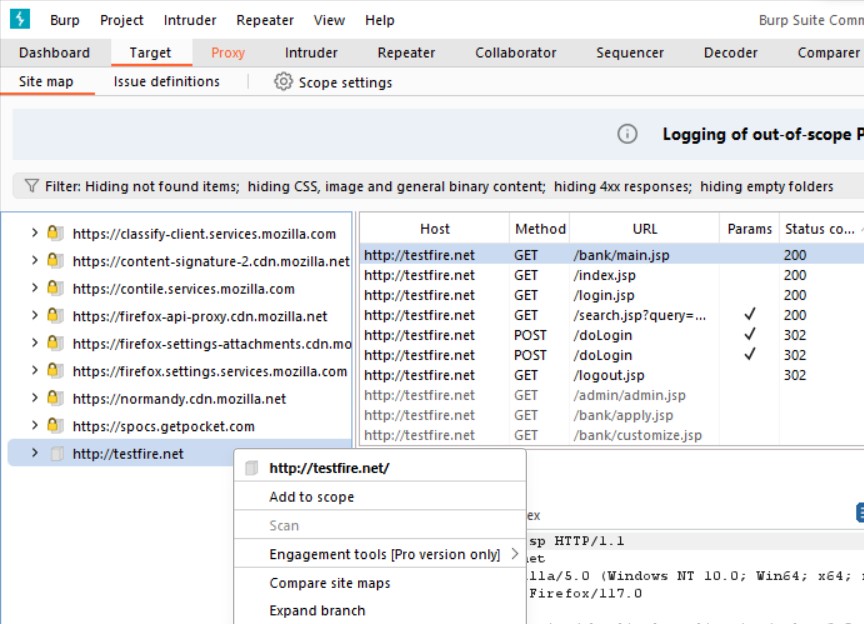
You may receive a complete overview of the functionality and content of your target application using the Burp Suite Target tab > Site map tool. The content of a URL is organized hierarchically on the left side of the page in a tree view, which is divided into domains, directories, folders, and files.



By starting the Burp suite browser—either the internal or external browser—and making sure the proxy interception is set OFF while you manually explore the full application, you may manually map your target application.

**Target Scope:**

By choosing any branch on the Site map, you may adjust your target scope. From the menu, choose Add to scope or remove from scope. You may set your Site map display filters to only display the items you wish to view and remove.



**Sequencer:**

You may use Burp Sequencer to examine the level of unpredictability in a sample of tokens. Any tokens meant to be unexpected may be tested using Sequencer, including:

* Session tokens
* Anti-CSRF tokens
* Password reset tokens

To give you an idea of the level of unpredictability in the sample, Sequencer performs many randomness checks on a sample of tokens before compiling the findings.

**Decoder:**

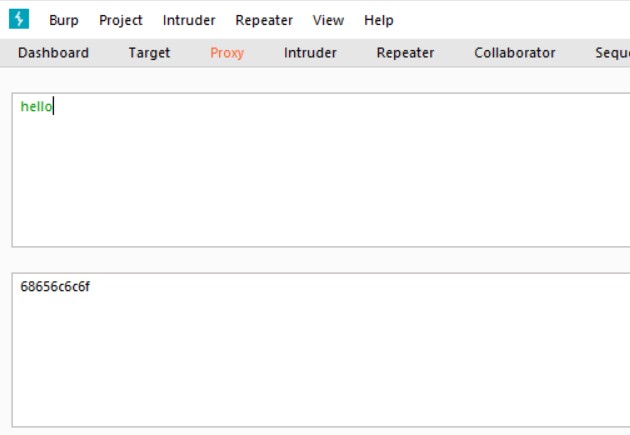
Data transformation utilizing popular encoding and decoding formats is possible with Burp Decoder. Decoder can be used for:

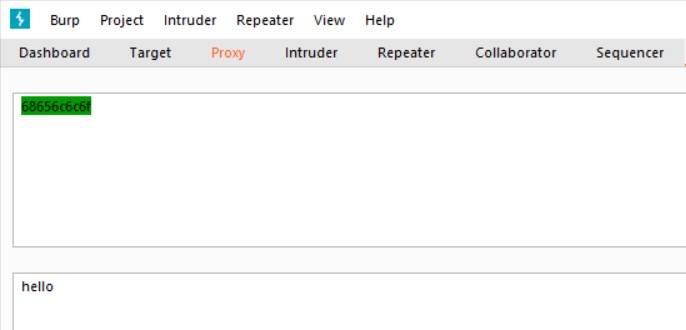
* data manually decoded
* recognize and decode recognised encoding types, including URL-encoding, automatically
* Transform unprocessed data into a variety of hashed and encoded representations

Applying many layers of alterations to the same input is possible with a decoder. This makes it possible for you to decode or use intricate encoding systems.

From the message editor in many Burp tools, such as HTTP history, you may transmit information to Burp Decoder. Using Burp Decoder, do a data transformation like follows:

* Find the data you wish to examine.
* Send to Decoder can be chosen by right-clicking the data in the message editor.
* Select the Decoder tab. The top panel contains the data.
* From the controls next to the data panel, choose the action you wish to carry out on the data. Encode as or Smart decode, for instance.



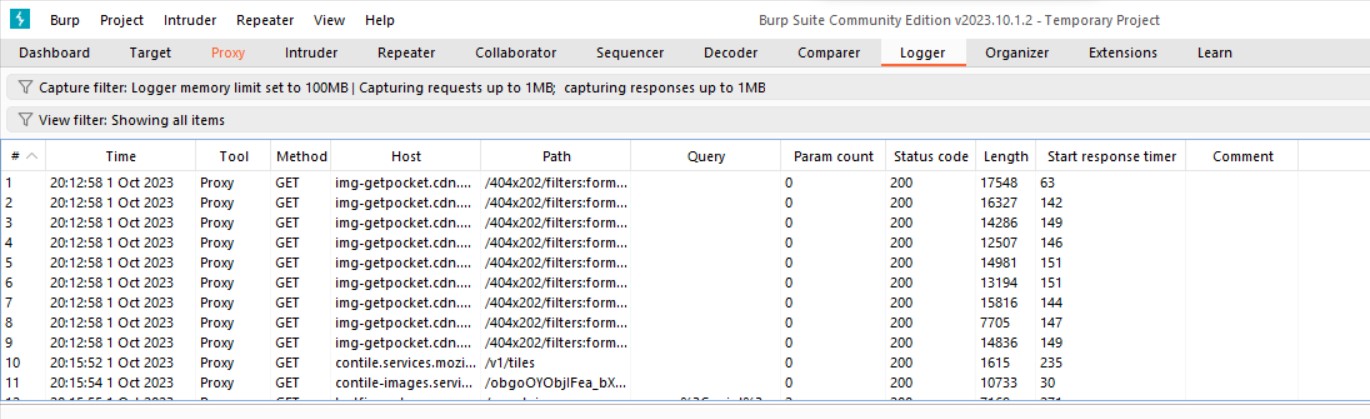


**Logger:**

Burp Logger captures all of the real-time HTTP traffic that Burp Suite creates. Logger is useful for:

* Analyse the requests that any extension or tool of Burp sends.
* View in real-time the queries made by Burp Scanner.
* Check out how extensions behave.
* Examine the requests that were issued after modifying the session handling rule.

By default, Logger shows all of the Burp Suite tools' traffic. Modified requests and requests delivered via extensions fall under this category. The HTTP history, on the other hand, only shows traffic coming from a browser that is using Burp as a proxy.



**Conclusion:**

Cybersecurity experts evaluate the security of online apps using Burp Suite, a well-liked and potent web security testing tool. It is a crucial tool for finding and reducing security risks in online applications since it offers a variety of functionality, such as web vulnerability scanning, intercepting and modifying web traffic, and automated testing.