Burp Suite is a comprehensive suite of tools used for web application security testing and penetration testing. It's designed to help security professionals identify vulnerabilities in web applications by intercepting, inspecting, and manipulating HTTP/HTTPS traffic. Key tools include the Proxy, Repeater, Intruder, Scanner, & Sequencer, among others. Burp also has features like the Collaborator, Decoder, and extensions for customization.

**Tools of burp suite :**

**PROXY**

**Function:** Acts as an intercepting proxy server, allowing you to inspect and modify HTTP/S traffic between your browser and the target application.

**Use Cases:** Intercepting requests and responses, modifying data, and testing various attack scenarios.

**Features:** HTTP history, WebSocket history, match and replace rules, and settings for managing CA certificates.

**REPEATER**

**Function:** Allows you to resend individual HTTP requests, modifying them as needed.

**Use Cases:** Testing specific requests, manually verifying vulnerabilities, and fine-tuning attacks.

**Features:** Multiple tabs for managing different requests, built-in editor for request modification, and the ability to save and load requests.

**INTRUDER**

**Function:** Automates customized attacks against web applications.

**Use Cases:** Fuzzing, parameter manipulation, and brute-force attacks.

**Features:** Payload generation, attack types (sniper, battering ram, pitchfork, cluster bomb), and customizable payload positions.

**SCANNER**

**Function:** Performs automated vulnerability scanning of web applications.

**Use Cases:** Discovering common vulnerabilities like XSS, SQL injection, and CSRF.

**Features:** Active and passive scanning, vulnerability reports, and scan configuration options.

**SEQUENCER**

**Function:** Analyzes the randomness of session tokens and other security-sensitive data.

**Use Cases:** Identifying predictable session tokens, which could lead to account takeover vulnerabilities.

**Features:** Token analysis, statistical tests, and pattern detection.

**BURP COLLABORATOR**

**Function:** A tool for detecting out-of-band vulnerabilities, often used with the Scanner or Intruder.

**Use Cases:** Detecting vulnerabilities that don't produce visible errors, like blind SQL injection or out-of-band XXE.

**EXTENSIONS**

**Function:** Burp Suite allows you to extend its functionality with custom extensions.

**Use Cases:** Adding custom scanning rules, automating tasks, and integrating with other tools.

**Features:** Python and Java scripting, a library of community-created extensions, and the ability to create your own.

**Notable Tools:**

**Decoder:** Used for decoding and encoding data.

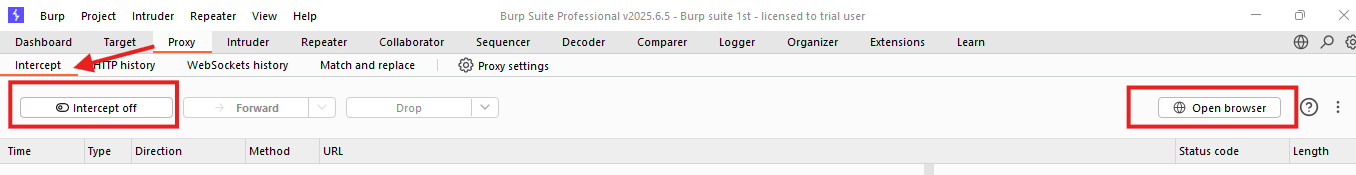
**Comparer:** Compares two sets of data.

**Extender:** Manages extensions.

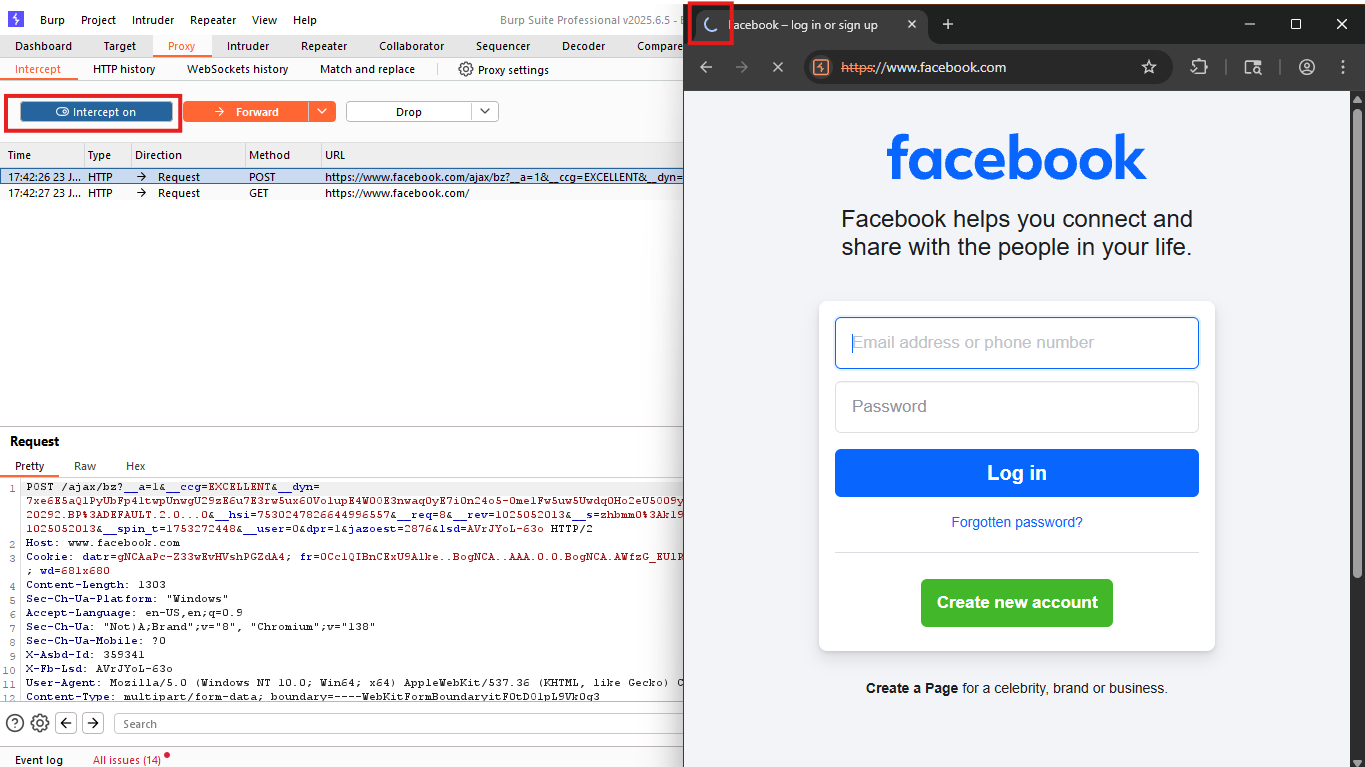
**Target:** Provides information about the target application.

**Intercept the http traffic on burp suite**

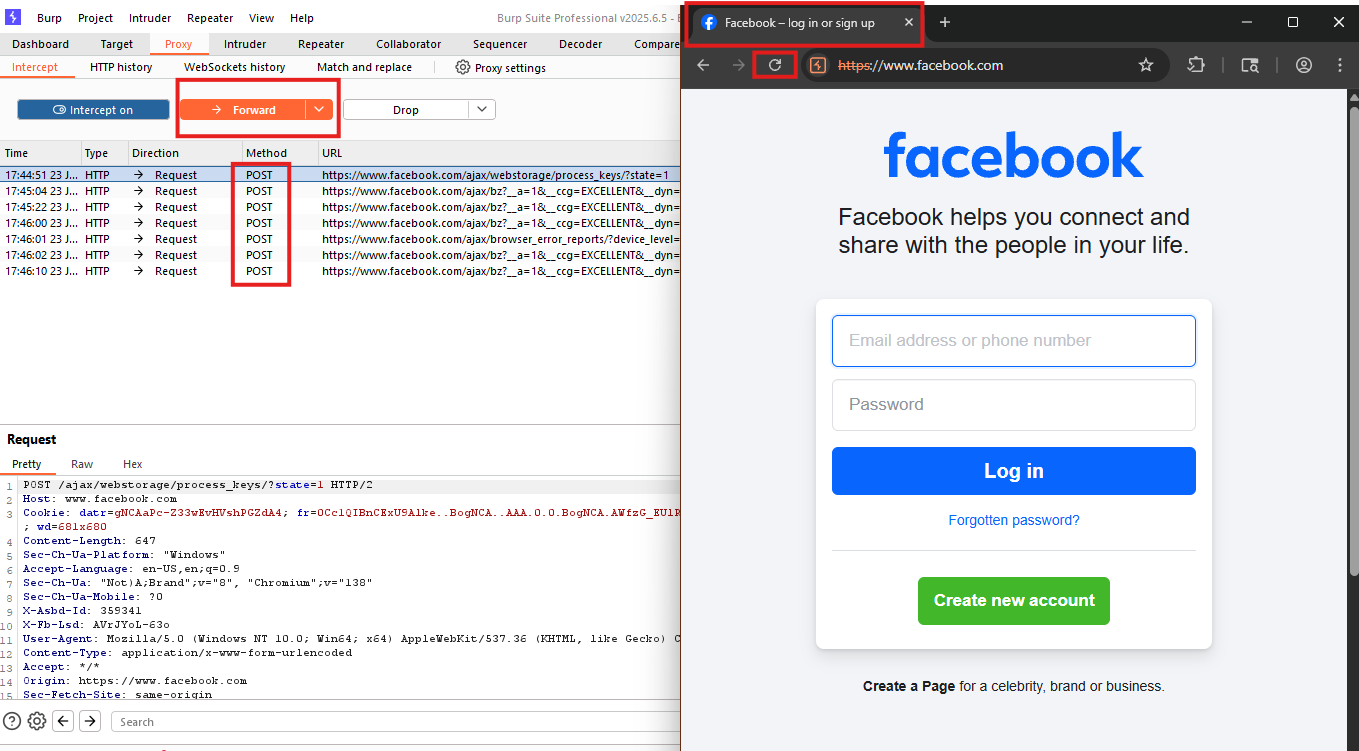
Here we are trying to intercept the http traffic using burp suite lets navigate to proxy in brup suite then to intercept turn the service “on” and open the in built browser as shown in the snap shot.



Search for a site for example facebook.com, the page will be in the loading session as we have interrupted the services between client and server using intercept the traffic will flow from client browser to interceptor then to the destination server. As shown in the snapshot.



Now will hit the forward button on burpsuite to run the services between them until the page gets loaded, once it got loaded we can see **post method** it will send data to server where we input the data for authentication, As shown in below snapshot.



Here in the below snapshot we are using repeater to resend HTTP requests individually to server and to modify it request accordingly. Its is used for manual testing to know the vulnerabilities manually.

