**What is burp suite?**

Burp Suite is a comprehensive set of tools that provides a range of functions for assessing the security of web applications. It is used for tasks such as web application scanning, automated and manual testing of web application vulnerabilities, and analyzing web traffic for security issues. Some of the key functions it offers include web vulnerability scanning, web proxying, crawling and scanning of web applications, and the ability to manipulate and intercept HTTP requests and responses.

**Why burp suite?**

Burp Suite is chosen for web application security testing for several reasons:

* **Comprehensive Toolset:** Burp Suite provides a wide range of features and tools, making it a one-stop solution for many web application security testing needs.
* **Flexibility:** Security professionals can perform both automated and manual testing, giving them control over the testing process.
* **Proxy Capabilities:** It offers a powerful web proxy that allows users to intercept and manipulate HTTP requests and responses, making it useful for understanding and testing web applications.
* **Actively Developed:** Burp Suite is actively maintained and updated, which ensures it can adapt to new web application technologies and security threats.

**What are the features of burp suite?**

Burp Suite is feature-rich and includes a variety of tools and capabilities. Some of the notable features include:

* **Proxy:** Intercept and modify HTTP requests and responses, allowing for detailed analysis and testing of web applications.
* **Scanner:** Automated web vulnerability scanner to discover and report security issues like SQL injection, XSS (Cross-Site Scripting), and more.
* **Spider:** Crawls websites to discover and map the application's structure and potential attack surface.
* **Repeater:** Manually modify and send individual HTTP requests to the application to test for vulnerabilities or analyze behaviour.
* **Intruder:** Perform automated attacks, such as brute-force, fuzzing, and parameter manipulation, to identify vulnerabilities.
* **Sequencer:** Analyze the randomness of tokens or session identifiers to identify potential weaknesses in session management.
* **Decoder:** Encode/decode data, such as URL encoding, base64 encoding, and hashing, for testing and analysis.
* **Collaborator:** Identify interactions between the application and external entities to detect blind vulnerabilities.
* **Extensibility:** Burp Suite supports extensions and customizations, allowing users to add functionality or integrate with other tools.

These features make Burp Suite a valuable tool for security professionals seeking to identify and address security vulnerabilities in web applications, ultimately enhancing the security of online systems and data.

**Brute force Login using Proxy:**



