**Burp Suite**

Burp Suite is a popular tool used by security professionals for web application security testing. It includes a variety of tools for testing web applications, including a scanner, intruder, repeater, and more, which can help find vulnerabilities like XSS, SQL injection, and others.

### Key Features of Burp Suite:

1. **Proxy:** Intercepts traffic between your browser and the target application, allowing you to inspect and modify requests and responses.
2. **Scanner:** Automatically crawls the web application and scans for vulnerabilities like XSS, SQLi, etc.
3. **Intruder:** Automates customized attacks on web applications, useful for brute force attacks, fuzzing, etc.
4. **Repeater:** Manually modify and re-send individual requests to test how the application responds.
5. **Sequencer:** Analyzes the randomness of tokens in the web application, such as session IDs or anti-CSRF tokens.
6. **Extender:** Allows you to add extensions and customize Burp Suite to meet specific needs.

### Learning Resources for Burp Suite:

* **Official Documentation:** Burp Suite Documentation.

### Tools & Extensions:

* **Burp Suite Community Edition:** Free version with limited features.
* **Burp Suite Professional:** Paid version with advanced scanning and automation tools.
* **Extensions:** Burp Suite has a robust marketplace where you can find extensions for tasks like fuzzing, SQL injection detection, and more.

### Example Scenarios:

* Use Burp Suite to intercept requests and manually inject malicious scripts to see if the web application is vulnerable to XSS.