NAME: MUNGILI CHETAN SAI RAJU

ASSIGNMENT 4

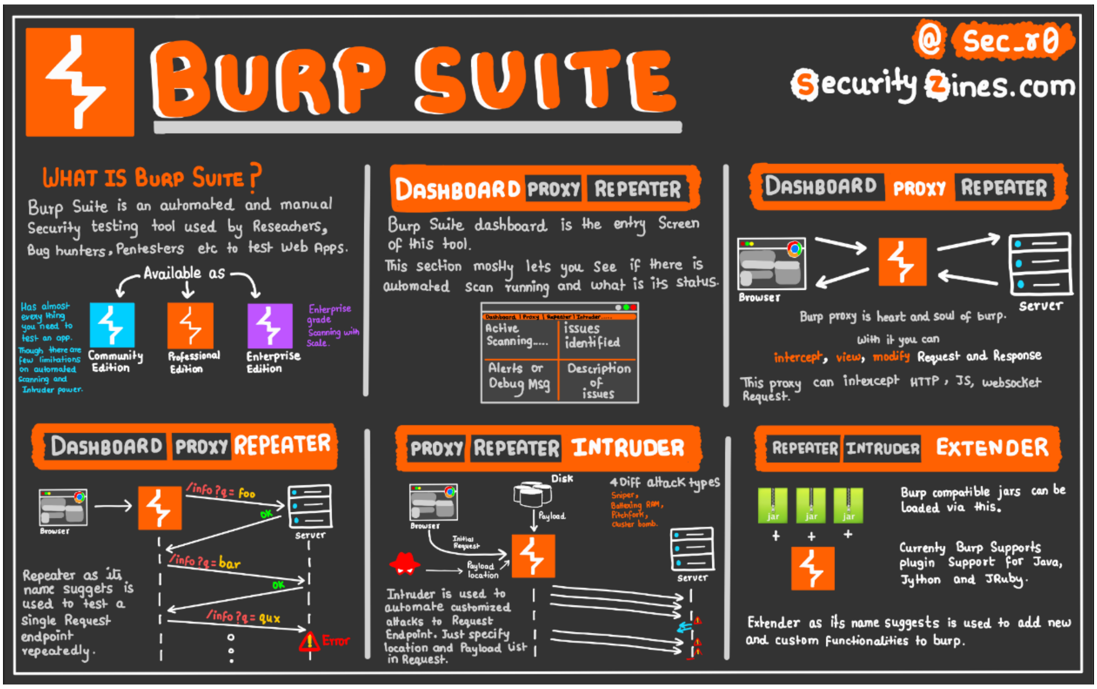
Understanding Burp suite and it's features

- **BURP SUITE:**

Burp Suite is an integrated platform for performing web application security testing. It is a popular tool among security professionals and bug bounty hunters, and is available in both free and paid versions.

Burp Suite consists of a number of tools that can be used to manually or automatically test web applications for vulnerabilities. These tools include:

- **Proxy:** Burp Suite includes a proxy server that can be used to intercept and inspect all HTTP traffic between the browser and the web application. This allows the tester to see and modify requests and responses, and to send them to other tools in Burp Suite for further analysis.
- **Spider:** The spider tool can be used to automatically discover all of the pages in a web application. This can be useful for identifying hidden pages or pages that are not linked from other pages.
- **Scanner:** The scanner tool can be used to automatically scan a web application for common vulnerabilities, such as SQL injection, cross-site scripting, and insecure direct object references.
- **Intruder:** The intruder tool can be used to perform brute-force attacks against web applications. This can be useful for testing password strength or for finding hidden functionality.
- **Repeater:** The repeater tool can be used to replay individual requests and responses. This can be useful for testing different inputs to a web application or for debugging problems.



Burp Suite is an automated and manual Security testing tool used by Reseachers, Bug hunters, Pentesters etc to test web Apps.

Has almost every thing you need to test an app. Though there are few limitations on automated Scanning and Intruder power.

Enterprise grade Scanning with Scale.

Burp Suite dashboard is the entry Screen of this tool. This section mostly lets you See if there is automated scan running and what is its status.

Burp proxy is heart and soul of burp. with it you can intercept, view, modify Request and Response

This proxy can intercept HTTP, JS, websocket Request.

Repeater as its name suggets is used to test a single Request endpoint repeatedly.

Intruder is used to automate customized attacks to Request Endpoint. Just specify location and Payload list in Request.

Burp compatible jars can be loaded via this.

Currenty Burp Supports plugin Support for Java, Jython and JRuby.

Extender as its name suggests is used to add new and custom functionalities to burp.

➢ **Why we use burp suite**:

There are many reasons why we use Burp Suite, including:

- Comprehensive: Burp Suite is a comprehensive platform for performing web application security testing. It includes a wide range of tools for manual and automated testing, as well as tools for intercepting and modifying HTTP traffic, fuzzing, and exploiting vulnerabilities.
- Powerful: Burp Suite is a powerful tool that can be used to find and exploit a wide range of vulnerabilities. It is used by security professionals and bug bounty hunters alike to find and report vulnerabilities in web applications.
- Flexible: Burp Suite can be used to test a wide range of web applications, regardless of their size or complexity. It can be used to test web applications that are hosted on-premises or in the cloud, and it can be used to test web applications that are built using a variety of different technologies.
- Extensible: Burp Suite can be extended with third-party plugins, or BApps. This allows users to add new features and functionality to Burp Suite, such as support for new technologies or new types of vulnerabilities.

Here are some specific examples of how Burp Suite can be used:

- To identify vulnerabilities in a web application: Burp Suite's scanner tool can be used to automatically scan a web application for common vulnerabilities, such as SQL injection, cross-site scripting, and insecure direct object references. Burp Suite's proxy tool can also be used to manually inspect HTTP traffic between the browser and the web application for signs of vulnerabilities.
- To exploit vulnerabilities in a web application: Burp Suite's intruder tool can be used to perform brute-force attacks against web applications to test password strength or to find hidden functionality. Burp Suite's repeater tool can also be used to replay individual requests and responses to exploit vulnerabilities.
- To debug problems with a web application: Burp Suite's proxy tool can be used to intercept and inspect HTTP traffic between the browser and the web application. This can be useful for debugging problems with a web application, such as identifying errors in HTTP requests or responses.
- To learn about web application security: Burp Suite's documentation and tutorials provide a wealth of information about web application security. Burp Suite can also be used to test the security of your own web applications, which can help you to learn about web application security and to identify areas where your web applications may be vulnerable.

➢ **Test the vulnerabilities of testfire.net:**

1. Set Up Burp Suite:

- Launch Burp Suite and create a new project.
- Ensure the Proxy Listener is running on port 8080.

2. Configure Browser and Install Certificate:
   - Configure the browser to use Burp Suite as a proxy (IP: 127.0.0.1, Port: 8080).
   - Download and install the Burp Suite CA certificate to avoid SSL errors.

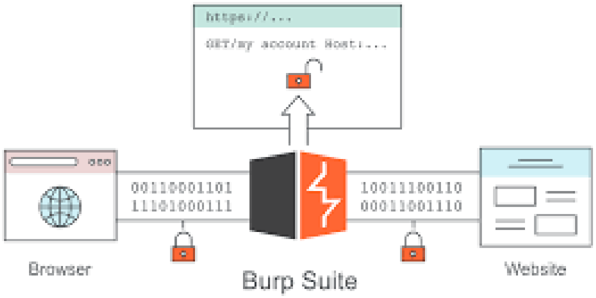
3. Define Target Scope:
   - Add the target URL (https://testfire.net) to the scope.
   - Include all URLs in the target scope for testing.

4. Explore Target Application:
   - Use Burp Suite's Spider tool to discover content and functionality.
   - View results in the Site map sub-tab.

5. Intercept and Modify Traffic:
   - Turn on intercept mode in the Proxy tab to intercept and modify requests and responses.
   - Use Raw or Params tabs to edit requests or responses.

6. Launch Attacks:
   - Use Intruder tool to launch attacks on specific requests.
   - Define attack type and payload positions.
   - Configure payload options, such as type, encoding, and processing.
   - Configure other attack settings and options in the Options sub-tab.

7. Start Attack and Analyze Results:
   - Click Start attack to launch the attack.
   - View and analyze results in the Results sub-tab.


https://...
GET/my account Host:...
00110001101
11101000111
10011100110
00011001110
Browser
Burp Suite
Website