Assignment 4

BURPSUITE

Rohan Idiculla Abraham
21BEC1080

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger. It is the most popular tool among professional web app security researchers and bug bounty hunters. Burp Suite is a platform and graphical tool that work together to do security testing on online applications. It supports the whole testing process, from the initial mapping and analysis of an application's attack surface through the discovery and exploitation of security flaws.

Why is Burp Suite Used in Cybersecurity

Burp Suite is a comprehensive framework that may be used to carry out several activities, including:

- Web crawling.
- Web application testing, both manually and automatically.
- Analysis of web applications.
- Vulnerability detection

Burpsuite also has the advantage of being built into the Chrome browser.

Features of BurpSuite

1. Spider

A web crawler or spider is employed to map the target web application. The mapping's goal is to compile a list of endpoints so that their capabilities may be examined and possible vulnerabilities can be discovered. Spidering is carried out for the straightforward reason that more attack surfaces are available during real testing if you collect more endpoints during recon.

2. Proxy

The intercepting proxy in BurpSuite enables the user to view and change the contents of requests and answers while they are being sent. Additionally, it eliminates the need for copy-and-paste by allowing the user to pass the request or answer that is being monitored to another pertinent BurpSuite tool. The proxy server can be configured to run on a specific loop-back IP address and port. Additionally, the proxy may be set up to block particular kinds of request-response pairings.

3. **Intruder**

It is a fuzzer that runs a collection of values across an input point. The results are examined for success/failure and content length after the values have been executed. Usually employed for:

- Brute-force assaults against password forms, pin forms, and other forms of this nature.
- Dictionary attacks on password fields on forms are thought to make them susceptible to XSS or SQL injection.
- Rate limitation on the web app is being tested and attacked.

4. **Repeater**

A user can submit requests repeatedly with manual adjustments using a repeater. It's employed for:

- Examining if the user-provided values are being examined.
- How successfully is the verification of user-supplied values being carried out?
- What values are expected by the server for an input parameter or request header?
- What happens when the server receives unexpected values?
- Is the server using input sanitization?
- How thoroughly the user-supplied inputs are sanitized by the server?
- What kind of cleanliness practices does the server employ?
- Which cookie is the real session cookie out of the ones that are already there?
- If there is a means to get around CSRF protection and how is it put into practice?

5. **Sequencer**

Burp Suite users apply the Sequencer tool to test the unpredictability of session tokens or other values that web applications produce. It checks the randomness of these values and how hard it would be for attackers to guess them. The Sequencer tool captures the target web app's generated values, including session tokens or other tokens used to maintain state, and examines them to identify any exploitable patterns or biases or to check if they are genuinely random.

6. **Decoder**

In Burp Suite, people use the Decoder tool to decode and encode data in different formats. It provides a simple and efficient way to convert encoded data into a human-readable format, making it an essential tool for testing and debugging web applications. The Decoder tool supports a wide range of encoding formats, including URL encoding, HTML encoding, base64 encoding, and many others. It also supports multiple data formats, such as strings, files, and binary data.