Name : Veekshitha Naragani
Reg no: 21BCE8943

TASK - 15/9/23

In Burp Suite, the "Sniper" and "Cluster Bomb" are two different payload types used for performing automated web application security testing, specifically for finding vulnerabilities like SQL Injection, Cross-Site Scripting (XSS), and more.

Why we use them ?

Sniper :

The Sniper payload type in Burp Suite is used for fine-tuning and targeting specific vulnerabilities by injecting payloads one by one into a single parameter. It is ideal for situations where you have identified a potential injection point, and you want to test it thoroughly.

Use Cases:

SQL Injection: When testing for SQL injection, you can use Sniper to inject different payloads systematically and analyze the application's responses for any signs of SQL injection vulnerabilities.

XSS Testing: Similarly, for Cross-Site Scripting (XSS) vulnerabilities, you can use Sniper to inject various payloads into input fields and see if the application reflects them back in the response.

Advantages:

Precise Testing: Sniper allows for precise, targeted testing of a single parameter, making it easier to identify vulnerabilities.

Controlled Testing: It helps you control the payload injection process, making it easier to identify where the vulnerability occurs.

Cluster Bomb :

The Cluster Bomb payload type is used for testing multiple parameters simultaneously by sending different payloads to multiple parameters in the same request. It's ideal for cases where an application might be vulnerable when multiple parameters are injected with payloads simultaneously.

Use Cases:

Blind SQL Injection: When testing for blind SQL injection, where the application does not display SQL errors, Cluster Bomb can help by injecting payloads into different parameters and observing the application's behavior.

Parameter Interaction Testing: It's useful for finding vulnerabilities that arise from interactions between multiple parameters.

Advantages:

Comprehensive Testing: Cluster Bomb allows you to test combinations of payloads in various parameters, increasing the chances of discovering complex vulnerabilities.

Time Efficiency: It can save time compared to manually crafting and sending multiple requests.
