Assignment 4

What is burp suite?

Ans:Burp Suite is an integrated platform developed by PortSwigger for performing security testing of web applications. It is commonly used by ethical hackers, security professionals, and developers to identify and address security vulnerabilities in web applications.

Why burp suite?

Ans:

Burp Suite is widely used for several reasons:

Comprehensive Testing: It offers a wide range of tools and features for assessing the security of web applications, making it suitable for various testing scenarios.

Ease of Use: Burp Suite has an intuitive interface that allows users to perform various security tests, even if they are not experts in cybersecurity.

Extensibility: It supports the use of extensions, allowing users to customize and extend its functionality to meet their specific needs.

Regular Updates: The tool is actively maintained and updated to keep up with the evolving web application security landscape.

What are the features of burp suite?

Ans:

Burp Suite includes a rich set of features for web application security testing, including but not limited to:

Proxy: Intercept and modify HTTP/S requests and responses between your browser and the web server for analysis and manipulation.

Scanner: Automated scanner for identifying common web application vulnerabilities like SQL injection, XSS, and more.

Spider: Crawls web applications to discover and map out their content and functionality.

Repeater: Allows you to manipulate and resend individual requests to the web application for testing.

Intruder: Automates various types of attacks (e.g., brute force, fuzzing) to identify vulnerabilities.

Sequencer: Analyzes the randomness of tokens or session identifiers.

Decoder: Helps in decoding and encoding data in various formats.
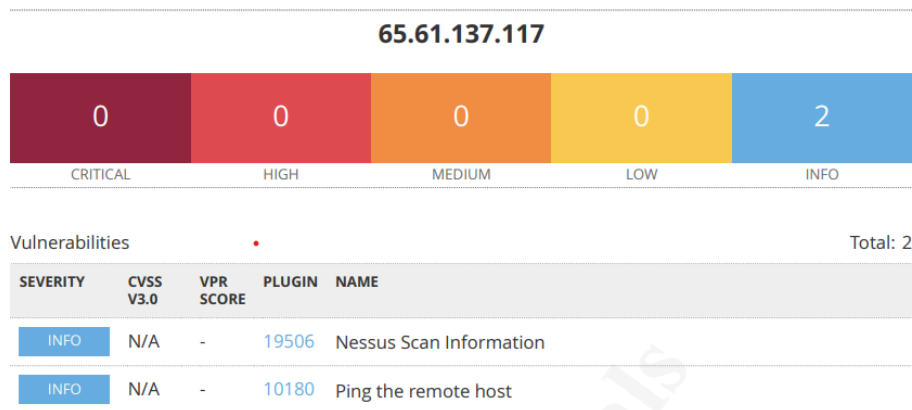
Extensibility: Supports the development and integration of custom extensions to enhance functionality.

Collaborator: Assists in identifying external service interactions and potential security issues.

Test the vulnerabilities of testfire.net

http://testfire.net

Ans:

65.61.137.117

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities   •   Total: 2

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

* indicates the v3.0 score
was not available; the v2.0
score is shown