Name = Aadish Rakesh Chougala

Reg number = 21BCE5296

College = Vellore institute of Technology, Chennai

Email = aadishrakesh.chougala2021@vitstudent.ac.in

Assignment 4 :

What is burpsuite :

A well-known and often used web application security testing tool is Burp Suite. It was created by PortSwigger, and penetration testers, security experts, and developers frequently use it to find and fix security flaws in online applications. For online application security evaluation and penetration testing, Burp Suite offers a full range of tools, including:

You may intercept and examine HTTP and HTTPS communication between your web browser and the web application by using Burp Suite, which functions as a proxy server. The security of online requests and answers may be tested and vulnerabilities found with the help of this capability.

Burp Scanner is an automated vulnerability scanner that can find common cross-site scripting (XSS) and SQL injection problems in online applications.

Why burpsuite

There are several compelling reasons why one should use Burp Suite for web application security testing and assessment:

Comprehensive Toolset

Proxy Capabilities

Automated Scanning: The Burp Scanner is an automated vulnerability scanner that can quickly identify common security issues like SQL injection, cross-site scripting (XSS), and more. It significantly speeds up the vulnerability discovery process.

Manual Testing

Customization and Extensibility

Community and Support

Regular Updates

Ethical Hacking and Compliance

Training and Skill Development

Features of burpsuite

Burp Suite is a feature-rich web application security testing tool that offers a comprehensive set of capabilities for identifying and addressing security vulnerabilities in web applications. Here are some of the key features of Burp Suite

Proxy: Burp Suite acts as a proxy server, allowing users to intercept and inspect HTTP and HTTPS traffic between their web browsers and web applications. This feature is essential for understanding and testing how web applications handle requests and responses.

Scanner: Burp Scanner is an automated vulnerability scanner that can identify common security issues, including SQL injection, cross-site scripting (XSS), and more. It accelerates the process of discovering vulnerabilities in web applications.

Spider: The Spider tool crawls a website to map its structure and identify its pages and functionality. This is useful for creating a comprehensive testing scope and ensuring that all parts of the application are assessed

Repeater: The Repeater tool allows users to manually manipulate and resend HTTP requests to a web application. This is valuable for testing how different inputs and variations affect the application's behavior.

Intruder: Burp Intruder is used for automated and customizable attacks on web applications. It enables tasks like brute force attacks, fuzzing, and parameter manipulation to identify vulnerabilities.

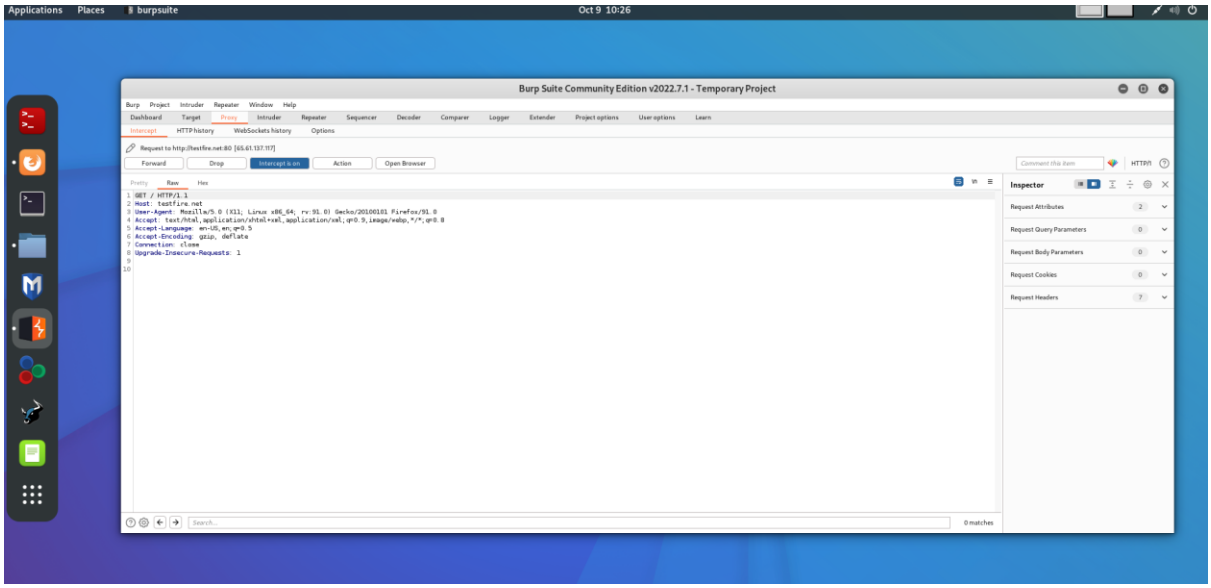
Decoder: The Decoder tool assists in encoding and decoding data in various formats, such as Base64, URL encoding, and more. It helps test applications for security issues related to data encoding and decoding.

Comparer: This tool helps users identify differences between two HTTP responses, making it easier to assess how different inputs affect an application's behavior.

Reporting: Burp Suite generates detailed and customizable reports, making it easier to communicate assessment results to stakeholders and development teams. These reports can help prioritize and track the resolution of identified vulnerabilities.

These are some of the features that would be beneficial for the people using burpsuite….

Testing


Applications
Places
burpsuite
Oct 9 10:26
Burp Suite Community Edition v2022.7.1 - Temporary Project
Inspector