Project Report

Web Application Vulnerability Assessment: Burp Suite

By- Abhinav Lather

->What is Burp Suite

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.

Types of Attacks

- Cross-site scripting(XSS)
- SQL injection
- MITM
- CSRF
- Brute Force

Burp Suite contains different functions such as:-

- Repeater-Repeater lets a user send requests repeatedly with manual modifications. It is used for verifying whether the user-supplied values are being verified.
  - Intruder-It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length.
  - Decoder-Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes.
  - Spider-It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found.

- **Proxy-** BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit.

Screenshots