ASSIGNMENT-4

Name : C Devaki Nandan Reddy

Getting started with Burp Suite

Launch Burp Suite by clicking the installed application shortcut. On Linux, the shortcut is located in the installation path that was displayed/selected during installation.

You can also launch Burp Suite from the command line to specify additional options and command line arguments.

Startup wizard

When Burp launches, the startup wizard is displayed. This lets you choose what Burp project to open, and what project configuration to use.

Selecting a project

You can choose from the following options to create or open a project:

- **Temporary project -** This option is useful for quick tasks where your work doesn't need to be saved. All data is held in memory, and is lost when Burp exits.
- **New project on disk -** This creates a new project that will store its data in a Burp project file. This file will hold all of the data and configuration for the project, and data is saved incrementally as you work. You can also specify a name for the project.
- **Open existing project -** This reopens an existing project from a Burp project file. A list of recently opened projects is shown for quick selection. When this option is selected, the Spider and Scanner tools will be automatically paused when the project reopens, to avoid sending any unintentional requests to existing configured targets. You can deselect this option if preferred.

Scanning web sites

Launching scans

Scans can be launched in a variety of ways:

- **Scan from specific URLs**. This performs a scan by crawling the content within one or more provided URLs, and optionally auditing the crawled content. To do this, go to the Burp Dashboard, and click the "New scan" button. This will open the scan launcher which lets you configure details of the scan.
- **Scan selected items**. This lets you perform an audit-only scan (no crawling) of specific HTTP requests. To do this, select one or more requests anywhere within Burp, and select "Scan" from the context menu. This will open the scan launcher which lets you configure details of the scan.
- **Live scanning**. You can use live scans to automatically scan requests that are processed by other Burp tools, such as the Proxy or Repeater tools. You can configure precisely which requests are processed, and whether they should be scanned to identify content or audit for vulnerabilities. To do this, go to the Burp Dashboard, and click the "New live task" button. This will open the live scan launcher which lets you configure details of the task.

Configuring scans

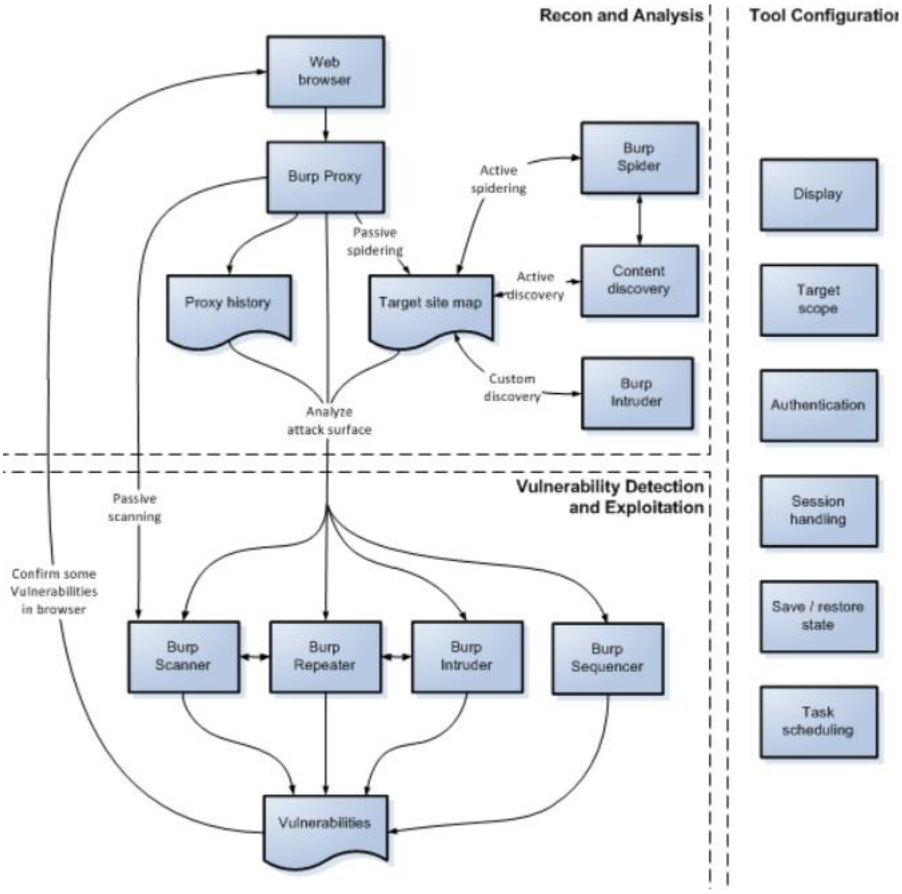
Monitoring scan activity

You can monitor the progress and results of a scan in various ways:

- The Burp Dashboard shows metrics about the progress of each task, and the issue activity log shows the issues that are reported by all scanning tasks.
- You can open the task details window for an individual scan, to view the issue activity log for only that scan, and a detailed view of the audit items for applicable tasks.
- The Target site map shows all of the content and issues that have been identified, organized by domain and URL.

Reporting

You can generate reports of issues found via Burp Scanner in HTML format. You can also export issues in XML format suitable for importing into other tools.



Configuration

You can use Burp's configuration library to manage different Burp configurations for particular tasks. For example, you might create different configurations for different types of scans. Or you might need to load a particular configuration when working on a particular client engagement. You can also save and load configurations in the form of configuration files.

Troubleshooting

If you are new to Burp and are having problems, please first read the help on Getting Started with Burp Suite, and follow the instructions there. Otherwise, the problems and solutions below might help you.

Burp doesn't run