St. Francis Institute of Technology

(An Autonomous Institution)

AICTE Approved | Affiliated to University of Mumbai
A+ Grade by NAAC: CMPN, EXTC, INFT NBA Accredited: ISO 9001:2015 Certified

Department of Information Technology

A.Y. 2025-2026
Class: BE-IT A/B, Semester: VII

Subject: Secure Application Development Lab

Student Name: Student Roll No:

Experiment – 5: Configure Burp Suite as a proxy to intercept and analyze web traffic for security testing

Aim: To configure Burp Suite as a proxy to intercept and analyze web traffic for security testing

Objectives: After study of this experiment, the student will be able to

- To understand and use Burp proxy and successful installation steps.
- To understand list of different web application
- Understand pentesting Tools

Lab objective mapped: ITL703.1 To **apply** secure programming of application code.

Prerequisite: NIL

Requirements: Personal Computer, Windows operating system browser, Internet Connection, Burp Suite software

Pre-Experiment Theory:

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. BurpSuite aims to be an all-in-one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps. It is the most popular tool among professional web app security researchers and bug bounty hunters. Its ease of use makes it a more suitable choice over free alternatives like OWASP ZAP.
The tools offered by BurpSuite are:

1. 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. Spidering is done for a simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.

2. Proxy:

BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The

proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.

3. 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. Usually, an anomaly results in a change in response code or content length of the response. BurpSuite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.

4. Repeater:

Burp Repeater is a tool that enables you to modify and send an interesting HTTP or WebSocket message over and over.

You can use Repeater for all kinds of purposes, for example to:

- Send a request with varying parameter values to test for input-based vulnerabilities.
- Send a series of HTTP requests in a specific sequence to test for vulnerabilities in multi-step processes, or vulnerabilities that rely on manipulating the connection state.
- Manually verify issues reported by Burp Scanner.

Repeater enables you to work on multiple messages simultaneously, each in its own tab. Any modifications you make to a message are saved in the tab's history. You can easily manage large numbers of open tabs with the grouping function. For HTTP requests, you can also add notes to each tab.

5. Sequencer:

The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication in sensitive operations: cookies and anti-CSRF tokens are examples of such tokens. Ideally, these tokens must be generated in a fully random manner so that the probability of appearance of each possible character at a position is distributed uniformly. This should be achieved both bitwise and character-wise. An entropy analyzer tests this hypothesis for being true. It works like this: initially, it is assumed that the tokens are random. Then the tokens are tested on certain parameters for certain characteristics. A term significance level is defined as a minimum value of probability that the token will exhibit for a characteristic, such that if the token has a characteristics probability below significance level, the hypothesis that the token is random will be rejected. This tool can be used to find out the weak tokens and enumerate their construction.

6. 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. It is used to uncover primary cases of IDOR and session hijacking.

7. Extender:

BurpSuite supports external components to be integrated into the tools suite to enhance its capabilities. These external components are called BApps. These work just like browser extensions. These can be viewed, modified, installed, uninstalled in the Extender window. Some of them are supported on the community version, but some require the paid professional version.

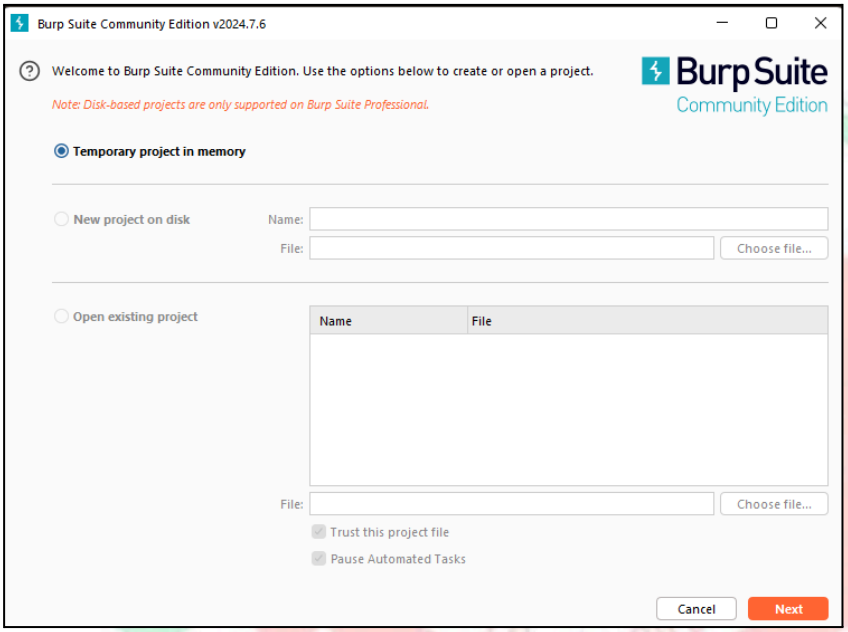
8. Scanner:

The scanner is not available in the community edition. It scans the website automatically for many common vulnerabilities and lists them with information on confidence over each finding and their complexity of exploitation. It is updated regularly to include new and less known vulnerabilities.

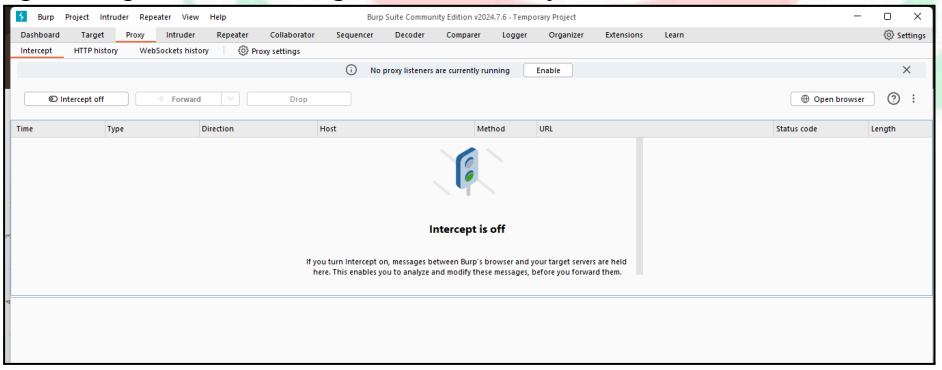
Procedure:

1. Download and install Burp Suite

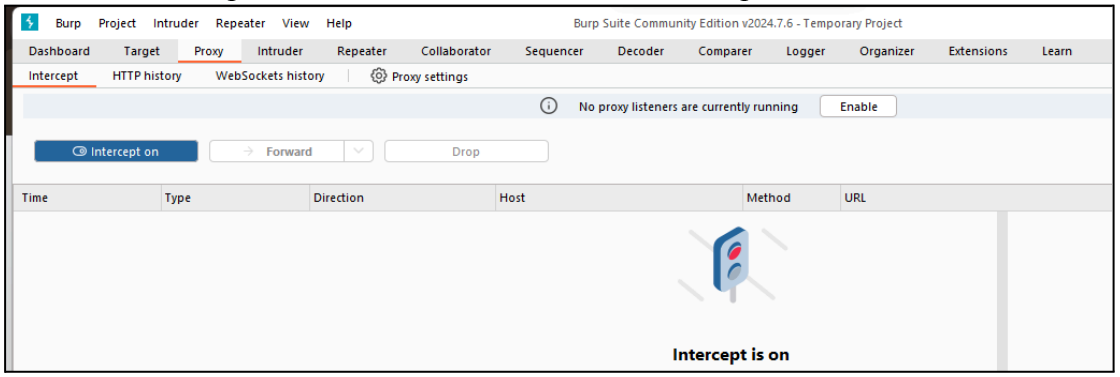
2. Launch Burp Suite after installation.



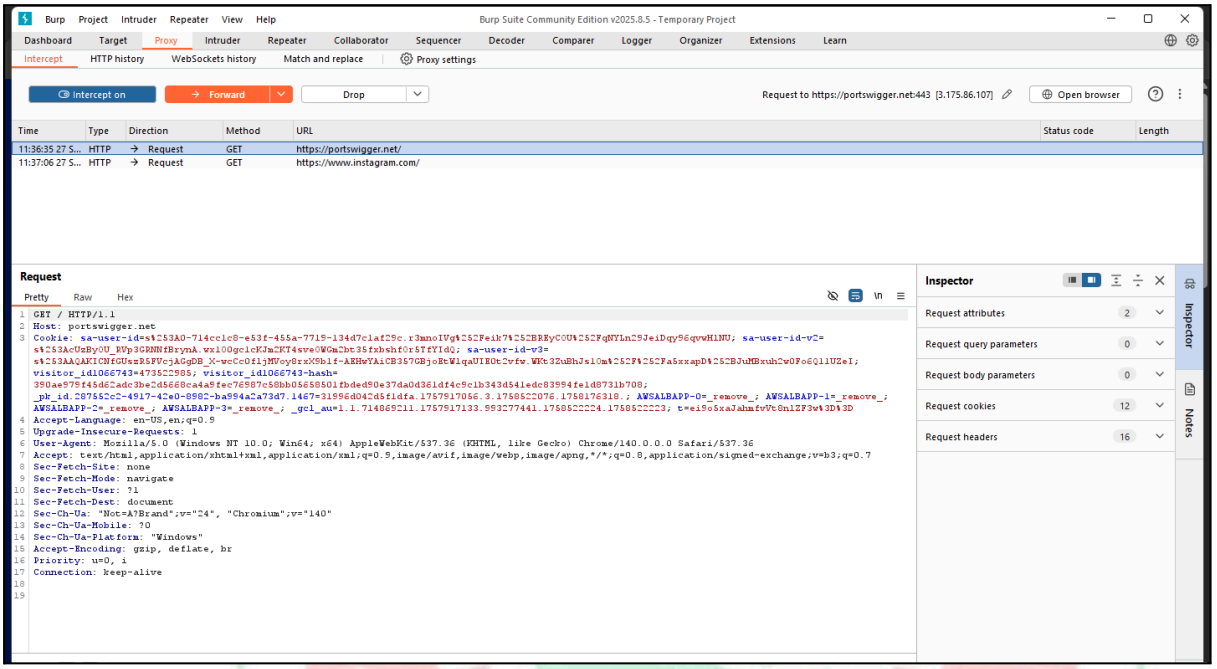
3. Open Burp Suite and navigate to the "Proxy" tab.



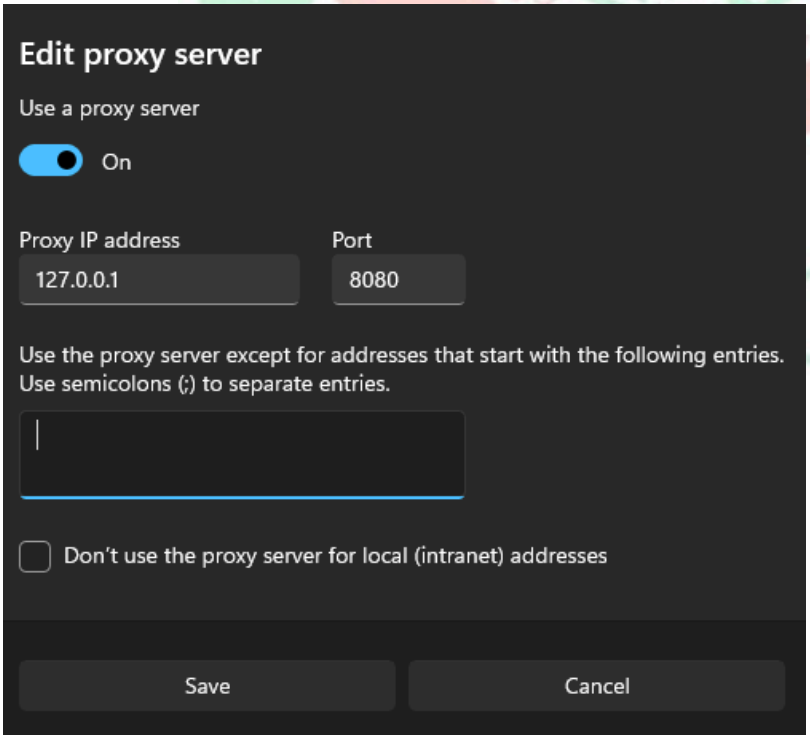
4. Go to the "Intercept" sub-tab and ensure it is set to intercept traffic.



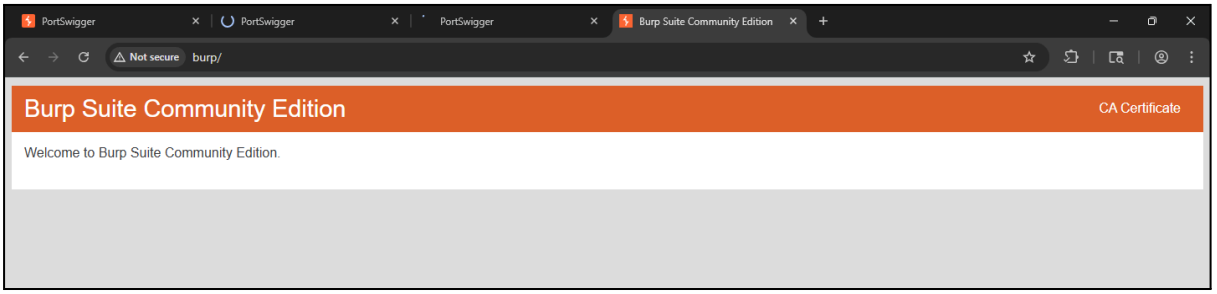
5. Click on the "Options" sub-tab under "Proxy".
6. Click on Proxy Listeners. By default, Burp Suite listens on 127.0.0.1:8080 (localhost at port 8080). Ensure it is active. Configure Your Browser to Use Burp as a Proxy.



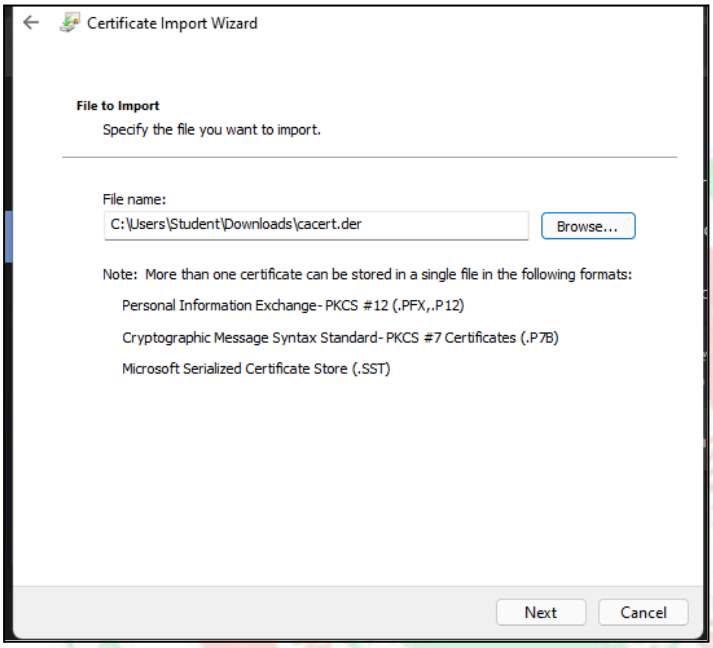
7. Go to Settings > Advanced > System > Click Open your computer's proxy settings. In the proxy settings, set the manual proxy configuration: HTTP proxy: 127.0.0.1 Port: 8080



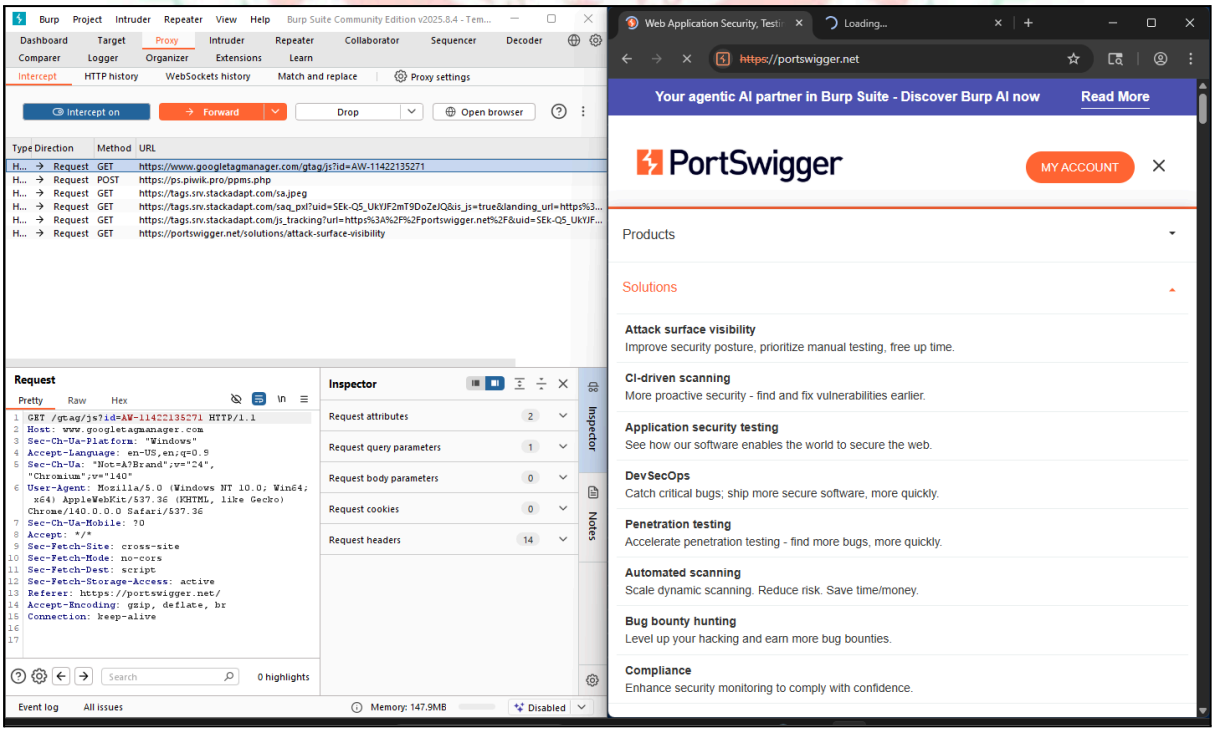
8. Apply and save the settings. Install Burp's CA Certificate (For HTTPS Traffic) In Burp Suite, go to the "Proxy" tab, and click the "Intercept is on" button to turn interception off temporarily. In your browser, visit http://burp. You'll see a page with options to download the CA certificate. Download the Burp CA certificate.



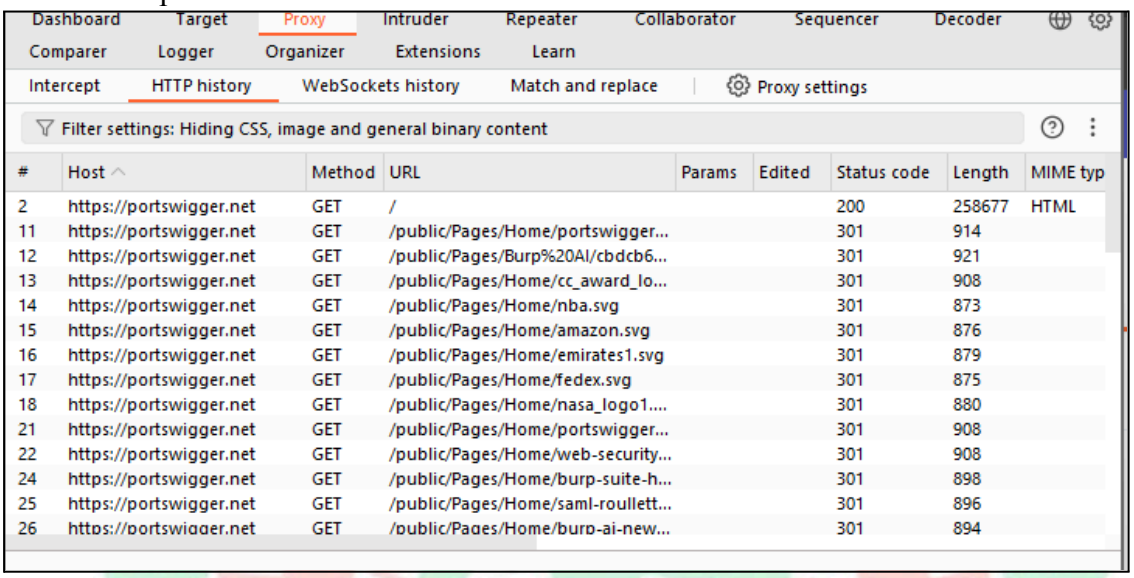
9. Install the certificate into your browser Open Settings > Security > Manage Certificates > Import the Burp CA certificate.

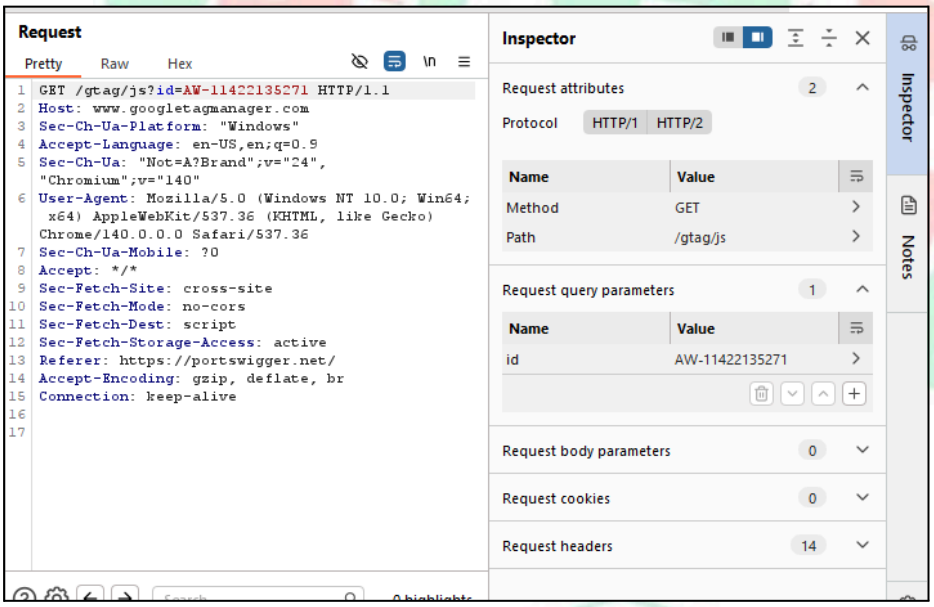


10. Restart your browser for the changes to take effect.
11. Go back to Burp Suite and ensure "Intercept is on" under the "Proxy" tab. Open any website on your browser.



12. Burp Suite will capture the traffic, and you can analyze it in the "HTTP history" and "Intercept" tabs.





Extended Theory: Nil

Post Experimental Exercise:
Questions:

- What happens when the intercept is off in the Burp Suite?
- List and discuss different pentesting tools

Conclusion:

- Write what was performed in the experiment.
- Write the significance of the topic studied in the experiment.

References:

- https://portswigger.net/burp/documentation/desktop/getting-started
- https://portswigger.net/burp
- https://www.youtube.com/watch?v=Nr2fYpStshA
- https://www.youtube.com/watch?v=TNcUrFyZrKs&t=77s