7BUISO22W Cyber Security Applications

Burp Suite Guide

University Of Westminster

Learning Objective

The objective of this lab is to give students practical, hands-on experience with Burp Suite to understand its tools and capabilities.

- If you are working on your own machine:
  - You must use Burp Suite Community Edition.
  - You must have DVWA, WebGoat, and OWASP Juice Shop running on your Kali Linux machine.
- If you are working on a CLG.43/45 machine:
  - You should use the pre-installed Burp Suite Professional Edition and docker software.

For your assignment, you need to set up the assignment scenario on Kali Linux.

Topics Covered

- Getting Started with BurpSuite
- Academy account on BurpSuite
- Understand the basics of BurpSuite
- Intercepting HTTP traffic
- Understand DREAD Threat modelling

Safety and Ethics Note

- This lab uses intentionally vulnerable systems solely for educational purposes.
- All activities must be conducted within the local lab virtual machine (VM) environment. Testing against external or production systems is strictly prohibited.

Lab Tasks

1. Obtain BurpSuite

Your ability to use Burp Suite depends on your location and setup. Burp Suite is available in different editions, each with varying features and availability.

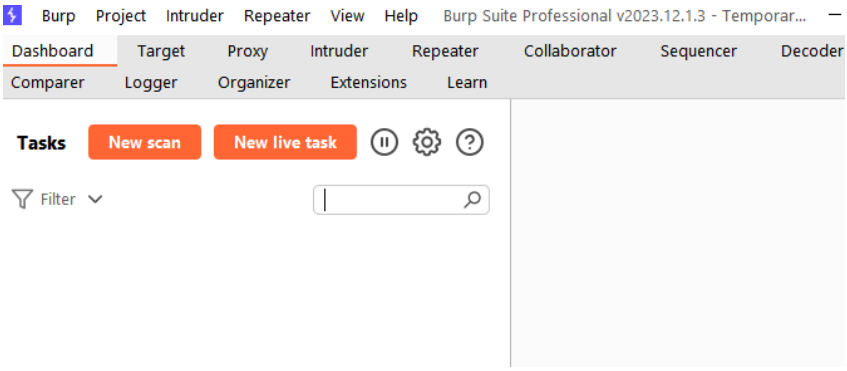

Fig.1. BurpSuite Professional Edition

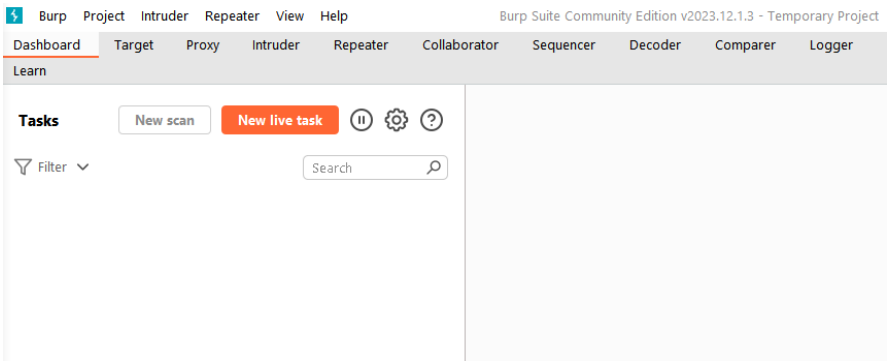

Fig.2. BurpSuite Community Edition

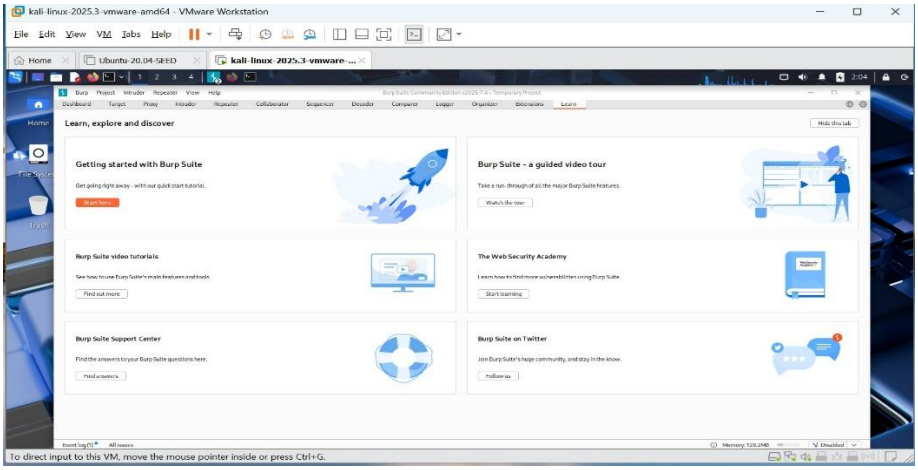

Fig 3. BurpSuite Community Edition on Kali

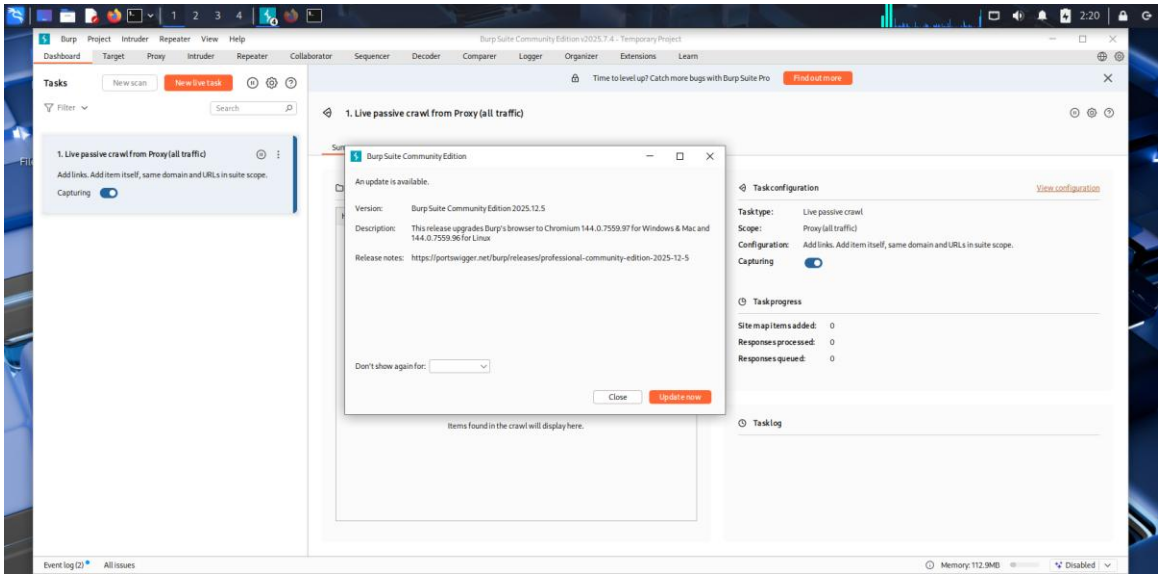

Fig 4. BurpSuite Community Edition install or update

Burp Suite Professional Edition

- Installed on university machines in Labs CLG.43 and CLG.45 on both Windows and Linux images.
- Offers more features than the Community Edition.
- Available for use at any time on lab machines. Your ability to use Burp Suite depends on your location and setup. Burp Suite is available in different editions, each with varying features and availability.

Burp Suite Community Edition

On Kali Virtual Machines:

- Pre-installed.
- To start it, open a terminal and type:
- burpsuite

On your host machine:

- You can install Burp Suite Community Edition directly on your own machine.
- To download it, use the Burp Suite download link.
- Make sure to select the installer for your correct platform (Windows, Linux, or macOS).

Burp Suite Community Edition does not auto-update. To install or update, visit: https://portswigger.net/burp/releases

For Windows:

- Download the installer, for example: burpsuite_pro_windows-x64_v2026_1_2.exe or burpsuite_community_windows-x64_v2026_1_2.exe

For Kali Linux:

- Download the latest .sh installer from the official PortSwigger website.
- Optionally, uninstall the old version or overwrite it during installation.
- To install or update using your downloaded file (e.g., burpsuite_community_linux_v2025_12_5.sh), follow the standard Linux installation steps.

1. Make the .sh file executable

Open a terminal, navigate to the folder containing the file, and run:

e.g. chmod +x burpsuite_community_linux_v2025_12_5.sh

2. Run the installer
./burpsuite_community_linux_v2025_12_5.sh

Follow the prompts to install Burp Suite. By default, it usually installs to opt/BurpSuiteCommunity or asks you for a location.

3. Launch Burp Suite

After installation, you can launch it with:

/opt/BurpSuiteCommunity/BurpSuiteCommunity

or if a desktop shortcut is created, use that.

4. Updating Burp Suite

Burp Suite Community Edition does not auto-update. To update: Download the latest .sh installer from the official PortSwigger website. Optionally, uninstall the old version (or overwrite it during installation). Run the new installer following the same steps above.

Tip: If you want a command-line shortcut to launch it anytime, you can create a symlink:

sudo ln -s /opt/BurpSuiteCommunity/BurpSuiteCommunity /usr/local/bin/burpsuite

Then you can just type:

burpsuite

2. Academy account on BurpSuite

In this module, we will work through the Burp Suite Academy tutorials and labs and apply what we learn on the OWASP VM machine and in the Assessment scenario.

- Create an account: First, please create an account on the Web Security Academy page.
- Learning paths: On the Web Security Academy, the learning paths are divided into three main categories:
    1. Server-Side Vulnerabilities
    2. Client-Side Vulnerabilities
    3. Advanced Topics

  Due to limited time in this module, we will not cover all labs in every topic. However, you are encouraged to explore the remaining labs on your own to further enhance your learning.

- Topics overview: You can view all available topics on the All Topics page of the Web Security Academy site.

- Lab exercises: Each topic includes an explanation of the vulnerability and several labs for hands-on practice, helping you to reinforce and apply your learning.

In your own time, complete this activity as part of your assignment work and explore what additional information you can discover.

3. Getting Started with Burp Suite.

You'll need an account on portswigger.net. If you don't have one already, registration is free and it grants you full access to the Web Security Academy.

Assuming you have Burp Suite ready and a Web Security Academy account, we will start by understanding the interface and the basics of the software. One way to familiarize yourself with Burp Suite and its interface is to explore the Learn tab within the software (see Figure 5).

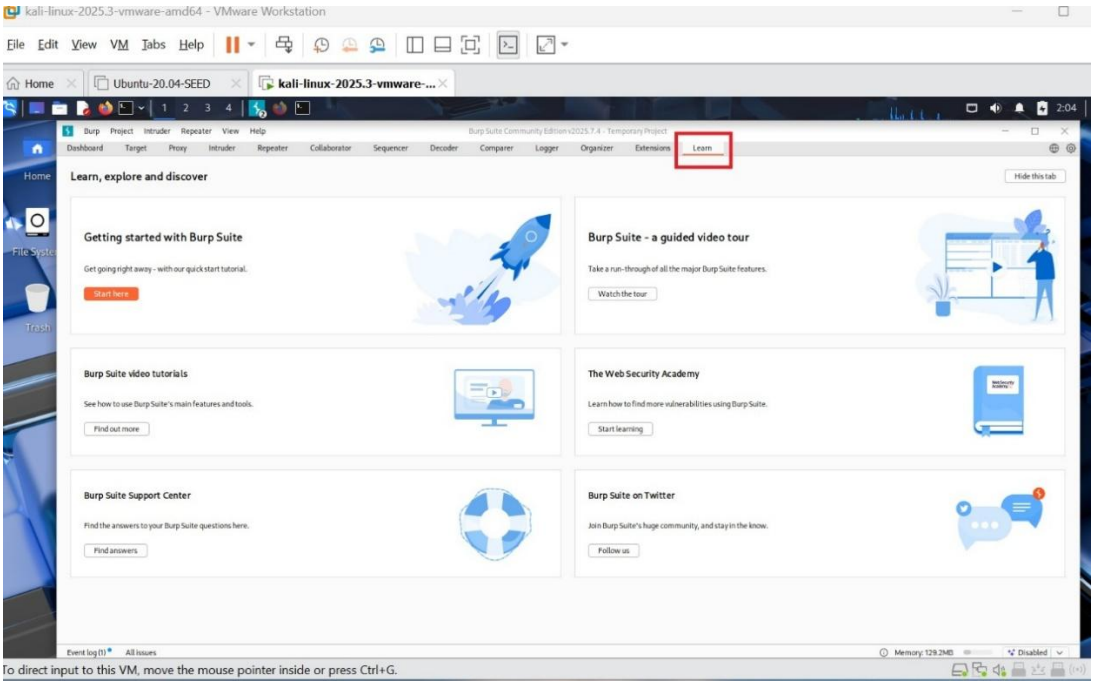

Figure 5: Learn tab on Burp Suite

Start by watching the Burp Suite User Interface guide video.

In summary, the interface tabs provide access to different tools. The following is a brief overview based on the Burp Suite documentation:

Burp Suite Tools Overview

- Dashboard – Central location for monitoring and controlling automated tasks such as vulnerability scans or live tasks.

- Target – Provides detailed information about your target applications and helps drive the testing process.

- Burp's Browser – A preconfigured browser that works with the full functionality of Burp

Suite out of the box.

- Proxy – An intercepting web proxy acting as a man-in-the-middle between your browser and the target application. Allows interception, inspection, and modification of traffic.
- Scanner (Professional only) – Advanced web vulnerability scanner that automatically crawls content and audits for various vulnerabilities.
- Intruder – Tool for automated, customized attacks against web applications; highly configurable for faster and more effective testing.
- Repeater – Allows manual manipulation and resending of individual messages, with analysis of application responses.
- Sequencer – Analyses the randomness of session tokens or other critical data intended to be unpredictable.
- Decoder – For manual or automated encoding and decoding of application data.
- Comparer – Visual tool for comparing two items of data, such as HTTP messages.
- Logger – Records and analyses HTTP traffic generated by Burp Suite.
- Inspector – Provides features for analysing and editing HTTP and WebSocket messages.
- Collaborator (Professional only) – Manual tool for identifying out-of-band vulnerabilities.
- DOM Invader – Tool for detecting DOM-based XSS vulnerabilities.
- Clickbandit – Tool for generating Clickjacking attacks.
- Message Editor – View and edit HTTP requests and responses throughout Burp Suite.
- Engagement Tools (Professional only) – Configure engagement-related tasks.
- Search – Search functionality within Burp Suite.
- Infltrator – Detects whether Burp inputs are passed to potentially unsafe APIs.
- Organizer – Store and annotate HTTP messages for further investigation.

A summary of the learning objectives and understanding will be provided after exploring these tools.

3.1 Intercepting HTTP Traffic (Requests and Responses)

First, watch the video on how to intercept HTTP traffic using the Burp Suite proxy before attempting this activity on OWASP.

Note: In the video, the Burp Suite proxy is used. This means there is no need to configure a separate proxy, as the Burp Suite proxy is already preconfigured in the Chromium browser. You can confirm this in the Proxy tab in Burp Suite when you click Open Browser.

- Visit the Burp Suite Academy website for this activity and complete the associated exercise.
- You can also perform this activity on the OWASP VM. Ensure that the OWASP VM is running before you begin.
- Take note of what you are able to capture simply by browsing the OWASP VM.
- Consider whether you find anything interesting or anything that could provide useful clues.

3.2 Modifying HTTP Traffic

In Burp Suite, you can not only intercept traffic before it reaches the server but also modify requests before they are sent.
Before attempting this on OWASP, watch the video on how to modify HTTP requests using the Burp Suite proxy. Before proceeding, ensure that you have already created a Burp Suite Academy account (as described in Section 2).

Visit the Burp Suite Academy site and complete the Modifying HTTP Requests activity.
Once you have completed the Academy activity, start the OWASP VM and practice modifying HTTP traffic. This example demonstrates one approach, but you are encouraged to explore further by browsing the OWASP application. Modifying HTTP Traffic on the OWASP VM
While the OWASP VM is running at 192.168.56.101, which is the IP address of the OWASP vulnerable machine, follow these steps:

1. Open Burp Suite (Community or Professional—either is suitable for this activity).
2. Click on the Proxy tab and ensure Intercept is OFF.
3. Open Chromium and navigate to http://192.168.56.101.
4. Select Damn Vulnerable Web Application (DVWA).
5. You will be presented with a login page. Before proceeding:
6. Turn Intercept ON by clicking *Intercept is OFF* to toggle it to *ON*.
7. Attempt to log in using the username test and password test.
8. Click Login.
9. Return to Burp Suite and locate the username and password parameters.
10. Modify them to username: **admin** and password: **admin.**
11. Click Forward in Burp Suite. You should now be logged in with administrator privileges.
12. Browse the OWASP VM and see if you can identify and modify other HTTP requests.

3.3 Setting the Target scope

- In Burp Suite, the messages you intercept may come from many different sources and websites. However, in a penetration test, the scope is usually limited to a specific target application. You can define a target scope so that Burp Suite ignores HTTP traffic from other sites.
- Visit the Burp Suite Academy website and follow the Setting the Target Scope activity.

  Note: You are not required to complete all the steps in this lab. The purpose of this activity is to learn how to define the target scope, not to solve the "Information disclosure in error messages" lab itself.

- Try to define the target scope in Burp Suite for the OWASP VM.

3.4 Reissue requests with Burp Repeater

An important tool in Burp Suite is the Repeater tool. Let's explore how it works.

- Visit the Burp Suite Academy website and follow the Reissue Requests with Burp Repeater activity.
- Next, explore the OWASP VM to see if you can identify anything interesting and practice manipulating HTTP requests by changing different parameters.
- Using Chromium (the proxy browser in Burp Suite), visit the BodgeIt Store and explore the available products.
    - Use the Repeater tool to determine how many products are available.
    - Note: The server responses may differ from those shown in the Burp Suite Academy example. Carefully examine the responses.
- Using Chromium, visit the Joomla Shop and explore the available products.
    - Use the Repeater tool to determine how many products are available.
    - Visit the Gallery page and see if you can identify how many images are present.
    - **Note:** Again, the server responses may differ from the Burp Suite Academy example. Review the responses closely.

Run Your First Scan

- An important tool in Burp Suite is the Burp Scanner.
- **Burp Scanner is only available in Burp Suite Professional** and Burp Suite Enterprise Edition. If you are using Burp Suite Community Edition, you will not be able to follow this tutorial.
- Before starting, make sure you clear any filters and remove any defined target scope.
- Visit the Burp Suite Academy website and follow the Run Your First Scan activity.
- After completing the activity, try scanning the OWASP VM. Experiment with different scan configuration settings and observe what each option provides.
    - Note: Scans may take some time to complete.

Generate a Report

- Review the Generate Reports activity on the Burp Suite Academy website to learn how to create reports from your findings.
- For your assignment, you will be required to generate a report for the scenario in which you conduct the penetration test.

4. Understand DREAD Threat modelling

DREAD: A Vulnerability Assessment Model - DREAD is an acronym that represents the components used to assess a vulnerability. The model quantifies threats by assigning a numerical value (typically 1–10) to five specific categories, then averaging them to determine a risk score:

D – Damage: How significant would the damage be if the attack succeeded? (e.g., data loss, financial impact).
R – Reproducibility: How easy is it to reproduce the attack?
E – Exploitability: How much time, effort, and expertise are required to exploit the threat?
A – Affected Users: If the threat were exploited, what percentage of users would be impacted?
D – Discoverability: How easy is it for an attacker to discover this vulnerability?

Calculating the DREAD Score

1. Assign a value to each of the five components, ranging from **low severity (0)** to **high severity (10)**.
2. Calculate the overall DREAD score as the **average of the five component values**:

$$\text{Overall DREAD} = \frac{D + R + E + A + D}{5}$$

The **DREAD** model continues to serve as a high-level quantitative framework for risk assessment, particularly useful for communicating security risks to non-technical stakeholders.

Additional Notes

- You can read more about this model here: DREAD Threat Modelling Technique and OWASP Threat Modelling Process.
- History: DREAD was first used by Microsoft as part of their **Security Development Lifecycle (SDL).**
- Current Use: While DREAD is less commonly used today, it remains a useful method for prioritizing vulnerabilities. Some consider it subjective, as security analysts must quantify each component based on their assessment of severity.

- Assignment Application: For each vulnerability you identify in your assignment, provide an **overall DREAD score** along with a brief justification for each component. See the example below:

Vulnerability	Damage (D) (0–10)	Reproducibility (R) (0–10)	Exploitability (E) (0–10)	Affected Users (A) (0–10)	Discoverability (D) (0–10)	Overall DREAD Score	Justification / Notes
Example: SQL Injection	9	8	7	8	9	8.2	High damage, easily reproducible, affects many users, attacker can discover easily

DREAD Calculator (simple web app)

A straightforward online calculator where you enter scores for each DREAD category and it computes your risk score. DREAD Calculator (simple online tool).