**Document Report**

**On**

# INSTALLATION OF BURPSUITE DAST AND ACTIVATION OF LICENSE

**Name: AJOY A G**

**Submission Date: 17.06.2025**

# Table of Contents

## Introduction

This document explains the installation and License of **Burp Suite DAST** application.

## Goal

This document serves the purpose of explaining the step-by-step process of installation of the application and activation of the license of Burp Suite DAST.

## What is Burp Suite?

Burp Suite is tool used for **web application security** testing and developed by **PortSwigger**.

## What is DAST?

**DAST (Dynamic Application Security Testing)** is a type of testing tool that scans a running application such as a web application to find vulnerabilities without access to the source code, by interacting with the application just like a real user or attacker would.

## What is Burp Suite DAST?

Burp Suite DAST refers to the **Dynamic Application Security Testing**.

## Architecture Overview (Standard)

The below diagram shows the core components of BurpSuite DAST and the connections between them.

## DAST Server

It’s the main application server.

Coordinates between other components.

DAST server is always installed on the same machine as web server.

## Web Server

Provides interface to user via **web UI** or one of the **API**.

**Web server** is always installed on the same machine as **DAST server**.

## Database

Buite Suite uses **SQL database** to store all application data, including **scan data**.

We can use two options:

1. **Embedded Database:**
    a. Can be installed on the same machine as the **Web** and **DAST server**.
    b. Used only for **trails** and **evaluation** of Burp Suite DAST, can’t be used for production use.
2. **External Database:**
    a. This option enables the use of existing **infrastructure database** even **database backup**.
    b. Used for **production use**.

## Service

Burp Suite DAST installs the following services the your machine:

- **burpsuiteenterpriseedition_agent.service**
- **burpsuiteenterpriseedition_enterpriseserver.service**
- **burpsuiteenterpriseedition_webserver.service**
- **burpsuiteenterpriseedition_db.service ***

*** burpsuiteenterpriseedition_db.service** is only installed if you're using an embedded database rather than your own external one.

## Scans and Scanning Machines

For a standard instances, scans run on a scanning machine.

There are two ways to setup a scanning machine:

1. **Single-Machine Setup**

a. Use **one computer** for everything.
b. Its runs both **DAST server** and the **scans**.
c. Up to 5 concurrent scans at a time.

2. **Multi-Machine Setup**
    a. Use **multiple computers**.
    b. One computer runs **DAST server**, and other servers runs **scans**.
    c. More then 5 concurrent scans at a time.

After deployment, you can group scanning machines into scanning pools, which gives you greater control over scanning resources.

## Single vs Multi-Machine Architecture

### Single Machine Architecture

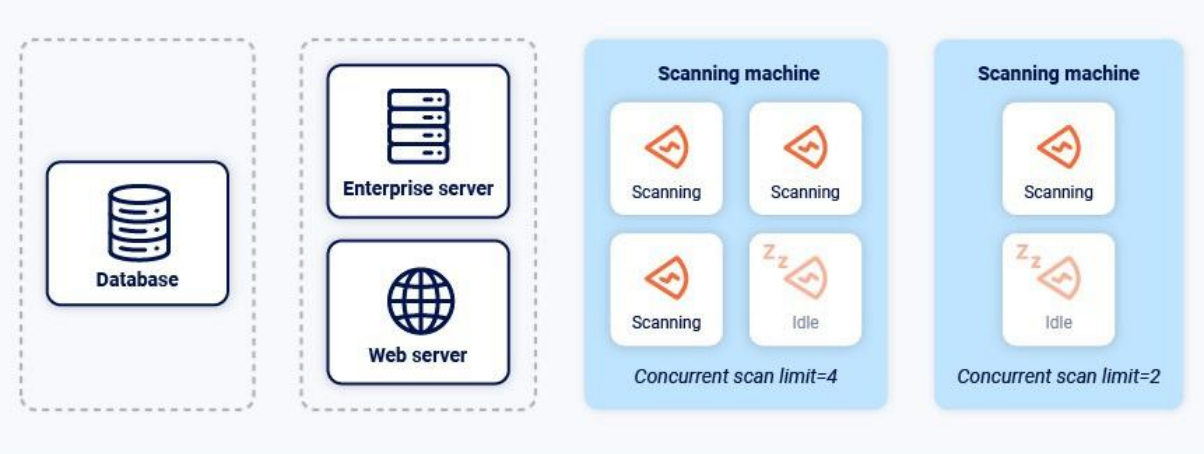
1. Can run all component on a single machine, including embedded database.
2. It's used for only trail and evaluations of Burp Suite DAST not for production use.

Diagram below shown a single-machine architecture:

## Multi-Machine Architecture

1. Can run all component on a various machine, including external database for storage.
2. It's used for production use of Burp Suite DAST.

The diagram below shows a multiple-machine architecture, with an external database and separate scanning machines:



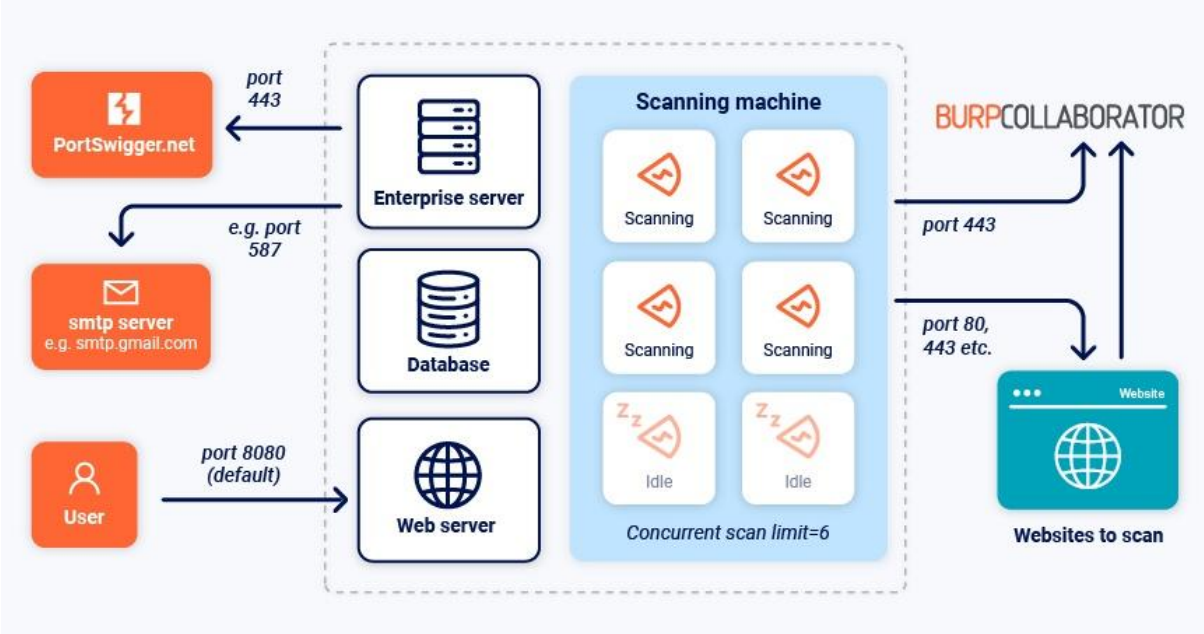

## Configuring your Network and Firewall Settings (Standard)

To make the Burp Suite DAST work properly, we must configure the firewall to allow components to communicate with each other and the public web.

**Warning**

For security reasons, make sure that your scanning machines can only reach systems that you intend to scan. Failure to do so may result in unintended user access to internal functionality.

1. Allow the **users** and **API clients** to access the **web server**, they should use port **8080**, **8443** or **another port** during installation process.
2. To activate license and enable automatic software update, allow the DAST server to access **portswigger.net** on port 443.
3. To allow email notification, give the DAST server access to the SMTP server.
4. Allow the machine to access websites that you want to scan on the relevant ports, via a proxy server if necessary.
5. To gain the full benefit of Burp Collaborator's out-of-band vulnerability detection technology, allow the machine to access ***.burpcollaborator.net** and ***.oastify.com** on ports **80** and **443**. Also ensure the target application can access these domains on the same ports.




## Prerequisite for a standard installation

We need to provide some technical details when installing Burp Suite DAST to make the installation process smooth. We have to check below mentioned topics beforehand starting the installation process.

### Port

Burp Suite DAST uses port **8080 (HTTP)** or **8443 (HTTPS)**, or any port of choice.

### TLS Certificate

Configuration of TLS certificate is optional and needed only in production use.

### Installation Location

Need to specify separate directories for Burp Suite DAST application itself, like:

1. DAST application.
2. Logs.
3. Data when installation.

### System User

For windows, no manual user setup is required. DAST applications is installed as a windows service, that runs under the default

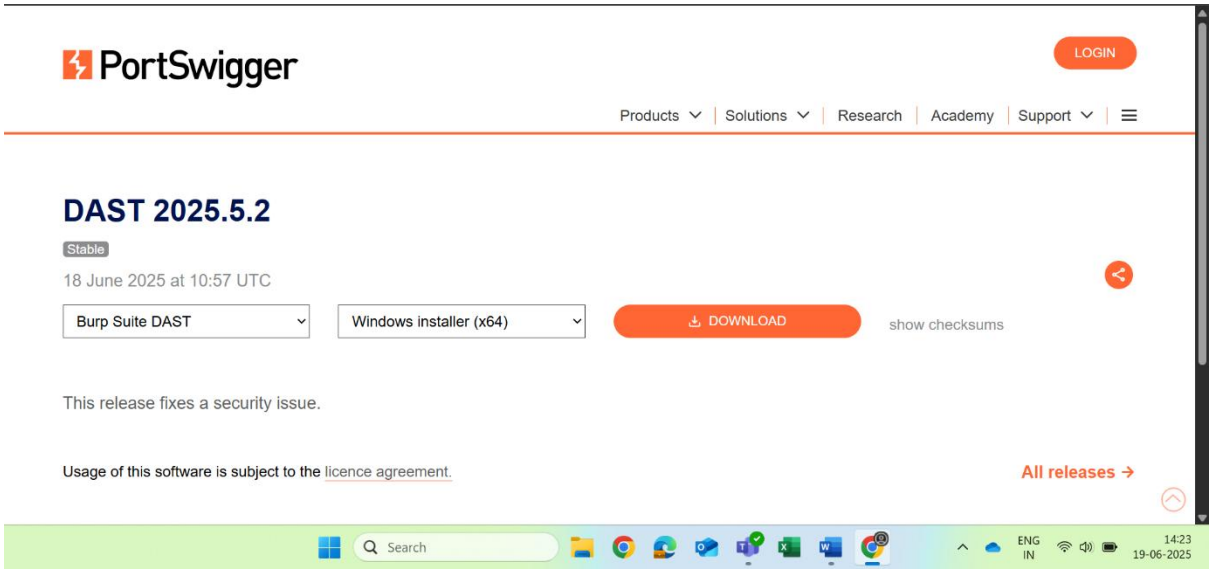
## Installing Burp Suite DAST (Standard)

Before starting the installation make sure to read the prerequisites for standard installation

## Step 1: Download the installer

Download the Burp Suite DAST installer using the link below-
https://portswigger.net/burp/releases/enterprise/latest

Clicking the above link will redirect to the select destination directory page.

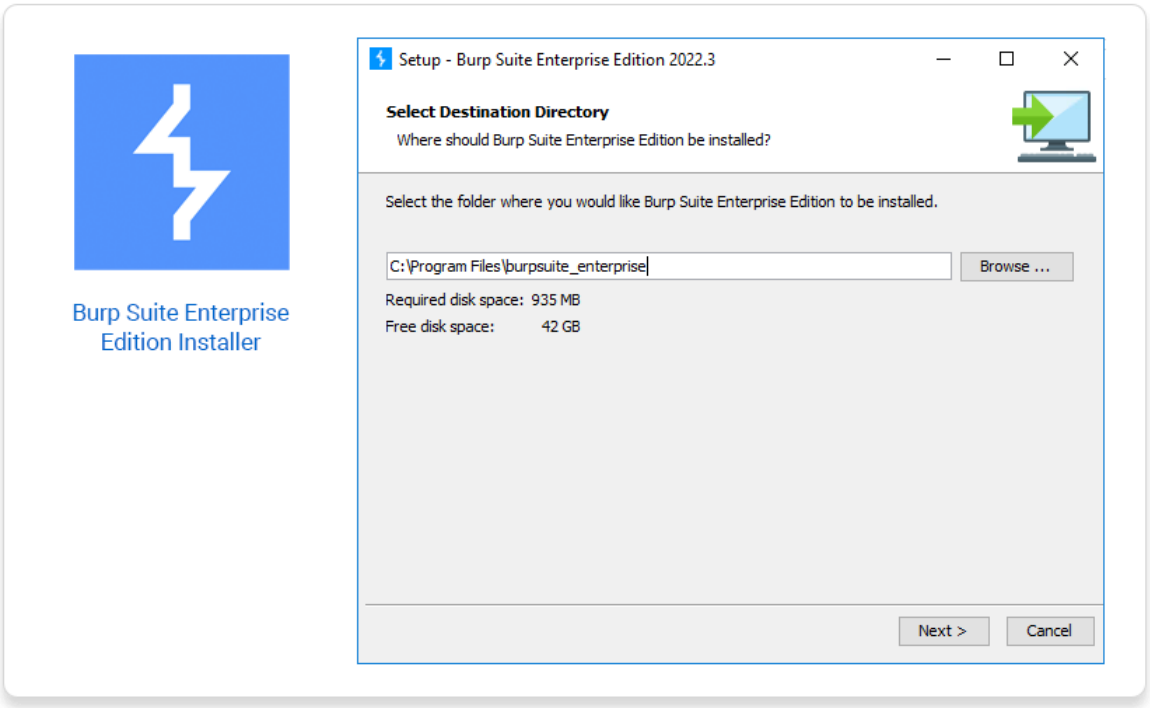



## Step 2: Extract and run the installer

**Windows:**

1. Extract the installer burpsuite_enterprise_windows-x64_vYYYY_MM.exe from the installer zip file.
2. Right-click the installer file and select **Run as administrator**.

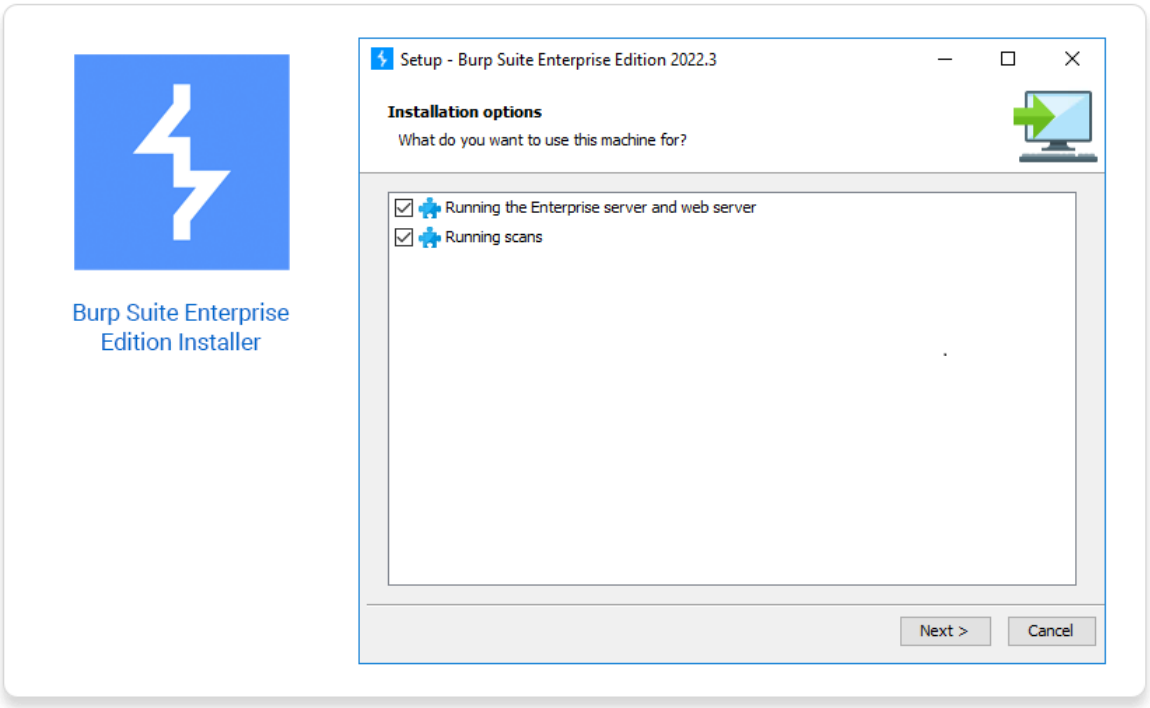
## Step 3: Choose an install location




The destination directory is the directory in which the DAST server itself will be installed.

Enter or select a directory and then click **Next** to display the **Installation options** screen.

## Step 4: Select the components to install

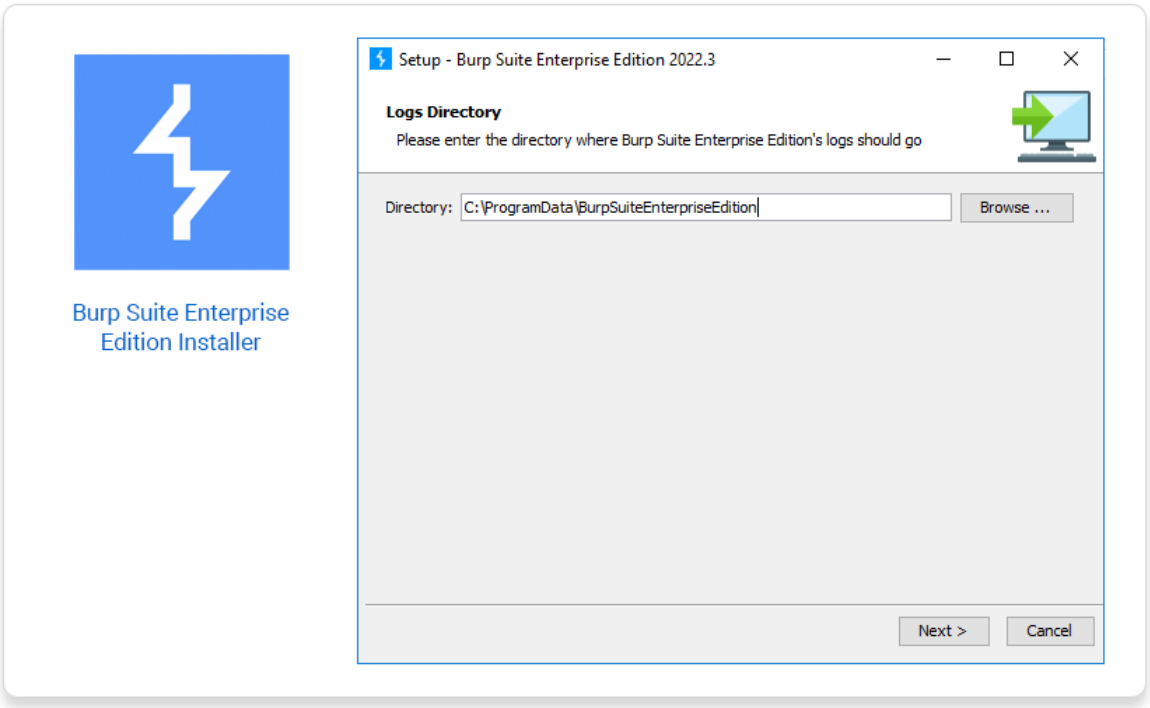



The **Installation options** screen enables you to choose which components of Burp Suite DAST you want to install on your machine.

For a single-machine architecture - with the DAST server and scanning components all on the same machine - make sure that both the **Running the DAST server and web server** and **Running scans** boxes are selected.

Click **Next** to display the **Logs Directory** screen.

## Step 5: Specify a logs directory

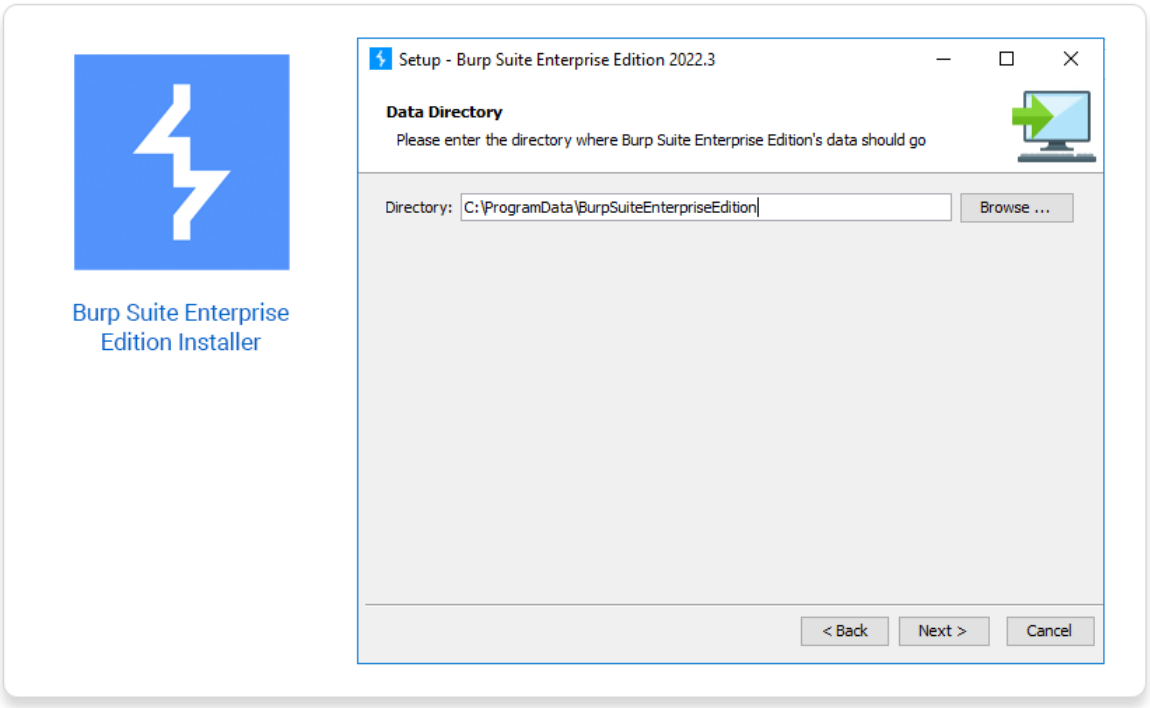



---

The logs directory is the folder that Burp Suite DAST saves all generated logs to.

Enter or select a directory and then click **Next** to display the **Data Directory** page.

## Step 6: Specify a data directory




The data directory is the folder that Burp Suite DAST saves application data to.

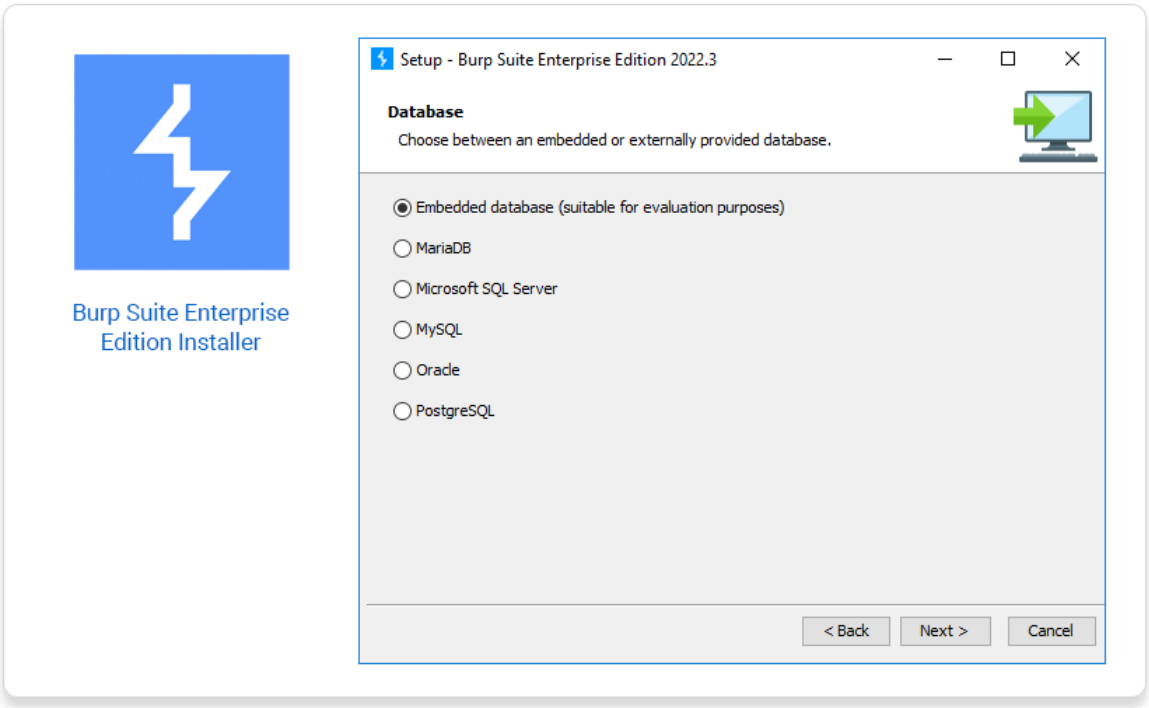
Enter or select a directory and then click **Next**.

## Step 7: Select a user to run processes

Enter the **Username** of the system user (that is, the user on your machine as opposed to a Burp Suite DAST user) that you want to run Burp Suite DAST processes under. If this user does not already exist on your system then the installer creates a user at the end of the process with the default name burpsuite.

Click **Next** to display the **Database** screen.

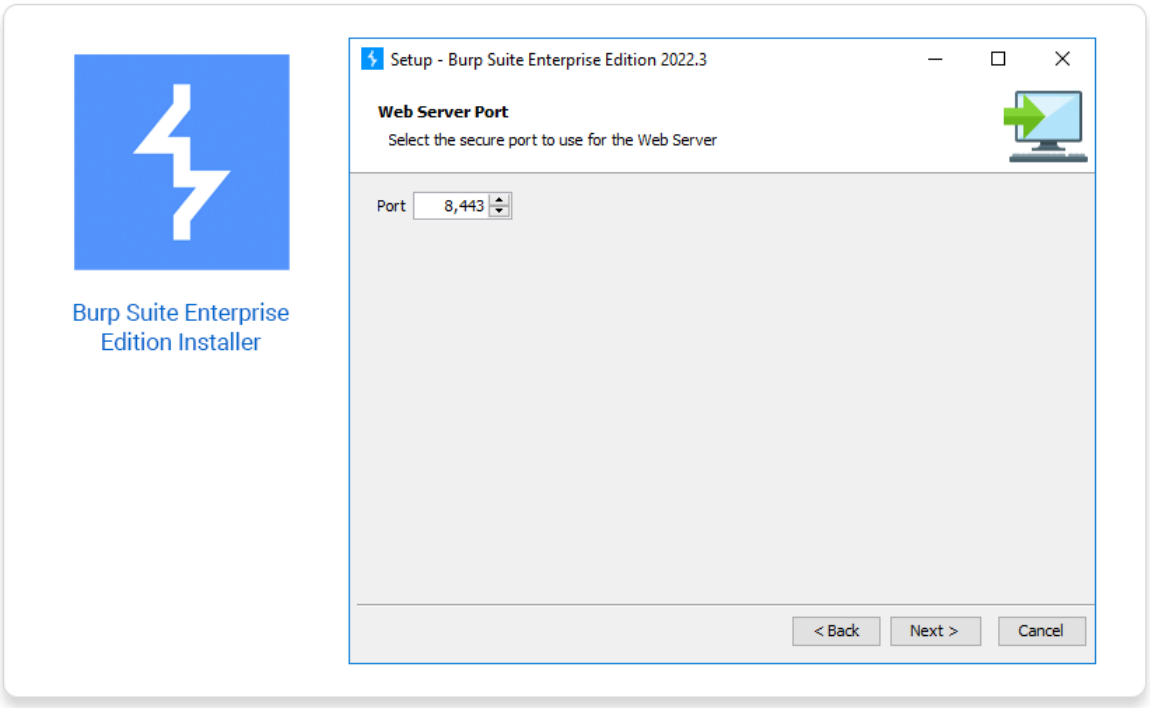
## Step 8: Select database options




Select whether you want to use the **Embedded database** or your own external database. Only use the embedded database to evaluate Burp Suite DAST. It is not intended for production use.

Click **Next** to display the **Web Server Port** screen.

## Step 9: Specify a web server port

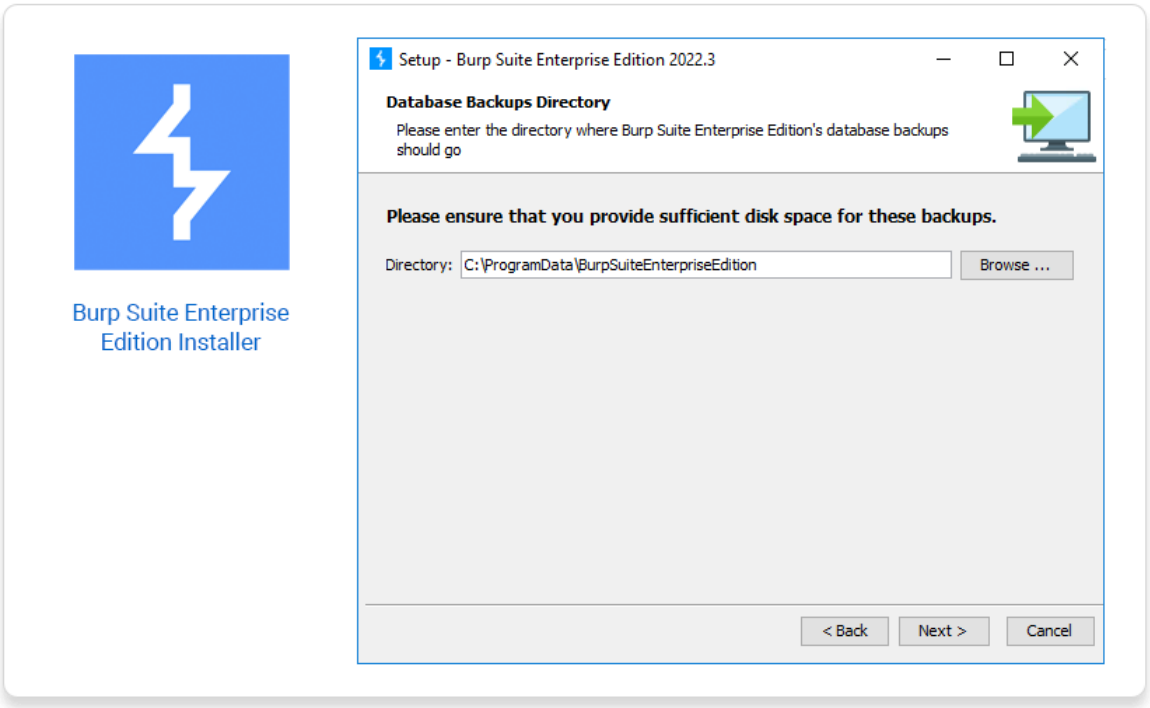



The web server port is the port through which you can access the Burp Suite DAST application in your browser.

We are selecting **port 8080** for out server.

Click **Next**.

### Step 10: Specify a database backups directory




The database backups directory is the folder that Burp Suite DAST backs up the embedded database to.

Enter or select a directory and then click **Next**.

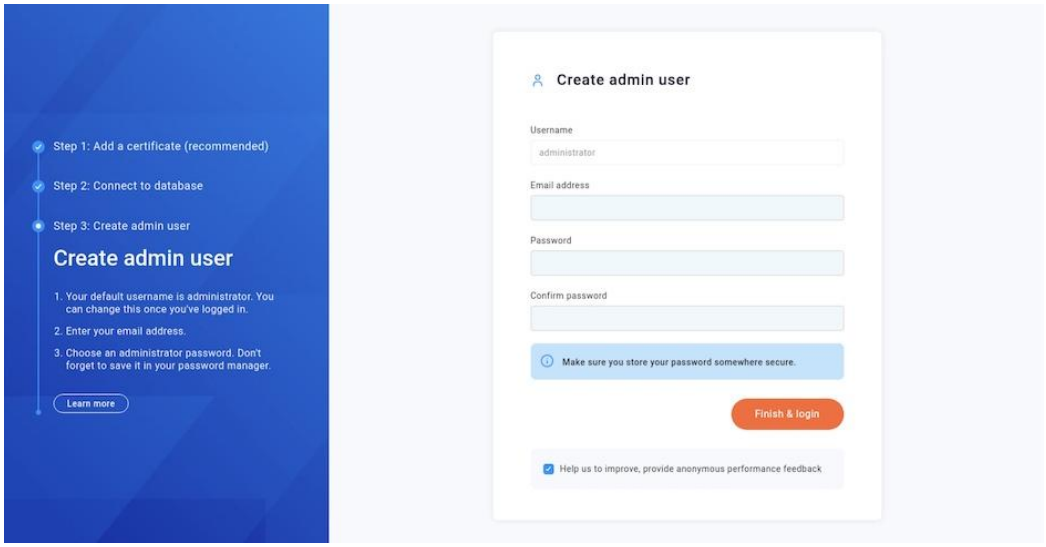
### After installation

Now that you have installed Burp Suite DAST, you need to complete the final part of the configuration in the app itself. Access the app in your browser. By default, this should be **http://localhost:8080**

## Configuring Burp Suite DAST (Standard)

The first time you access Burp Suite DAST after installation, the application prompts you to create an administrator user.

## Configuring admin user details

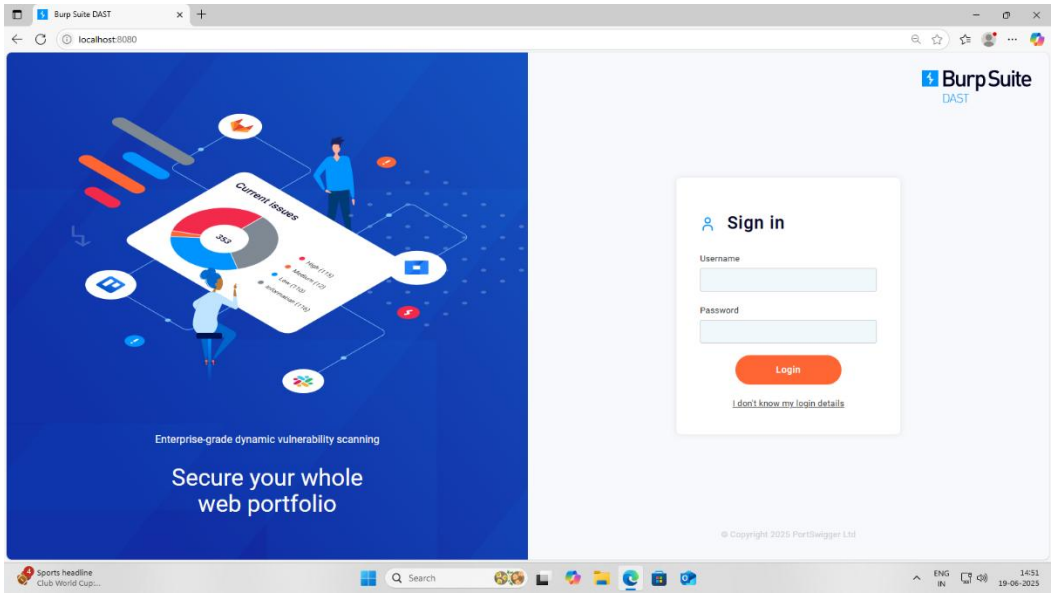



The final step in the configuration process is to set up your Burp Suite DAST admin user. This step is necessary for all Burp Suite DAST instances.

To do so, enter the **Email address** and **Password** for the admin user on the **Create admin user** page, then confirm your password and click **Finish & login** to complete the configuration process. The application displays the **Sign in** page.

### Warning

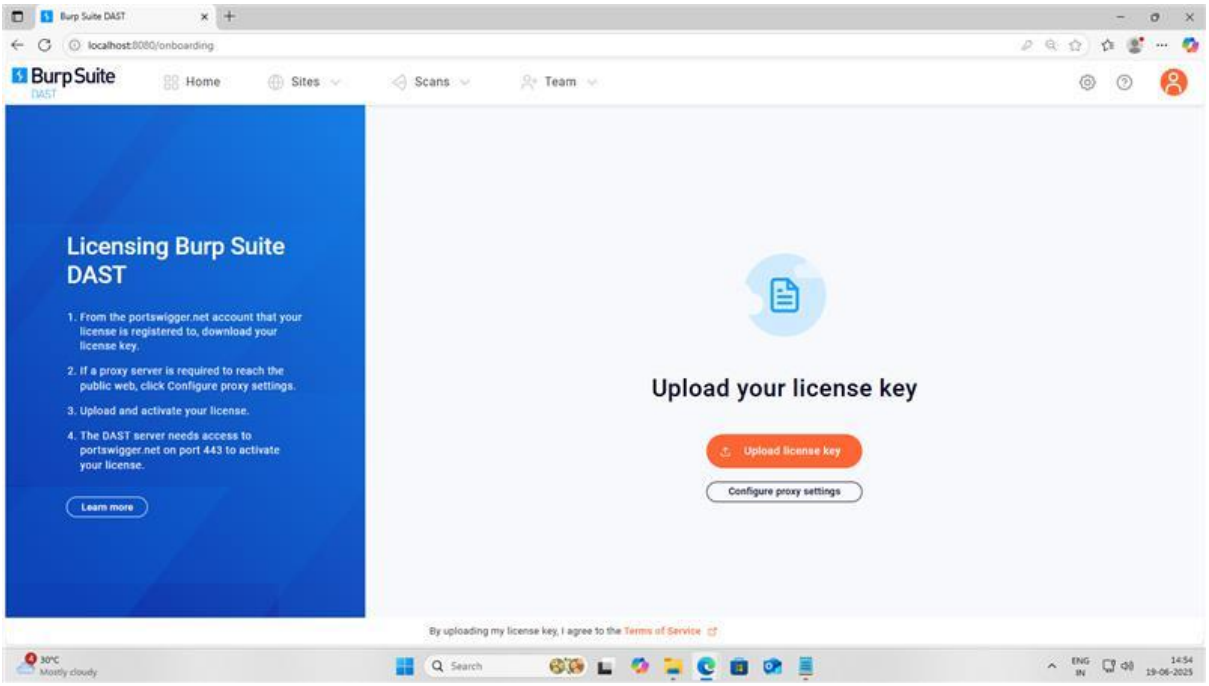
Make sure you save your password somewhere secure. You will need it to log in to Burp Suite DAST.



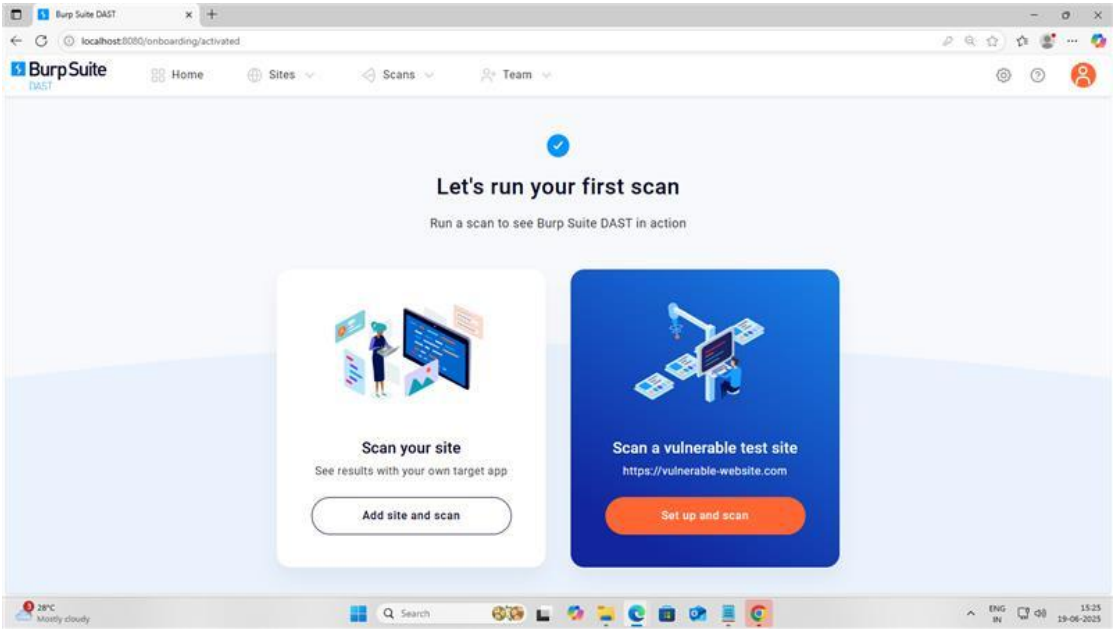

Once you have configured your admin username, you can sign in and begin using Burp Suite DAST. When you log in to Burp Suite DAST for the first time, you are prompted to activate your license.

## Activating your license (Standard)

When you log in to Burp Suite DAST for the first time, you are prompted to activate your license before you can begin using the product.



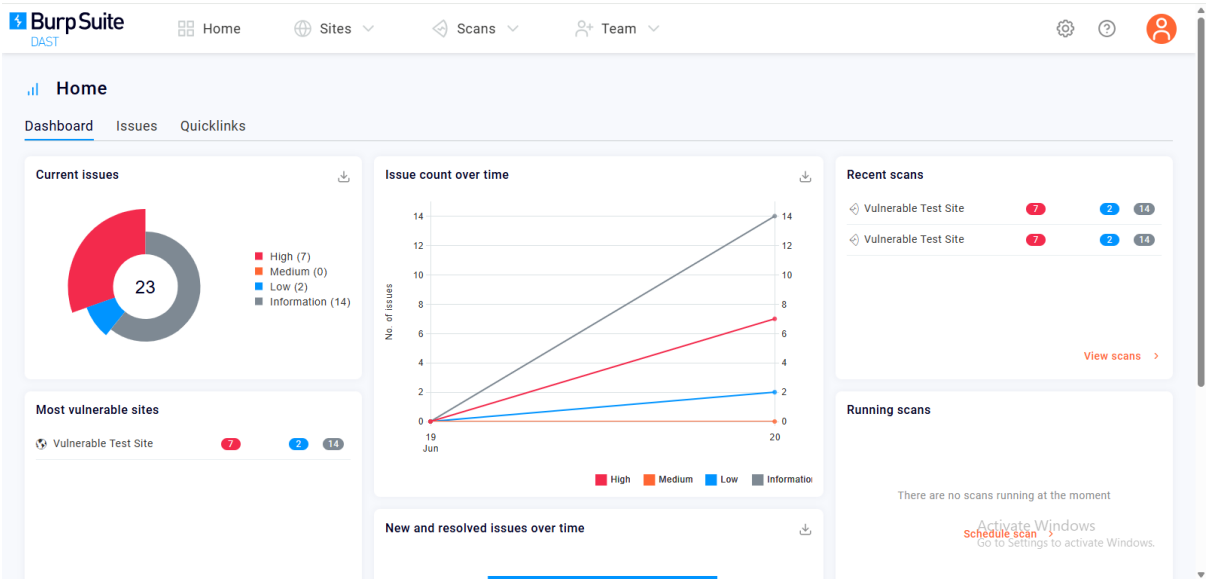

1. When prompted, click **Upload license key** and select the license key that you downloaded earlier. If you can't find your key, you can download it again from your account page on portswigger.net.




2. If your license was activated successfully, the system displays a confirmation message. If a connection could not be established to portswigger.net, you are prompted to configure an HTTP proxy before continuing.

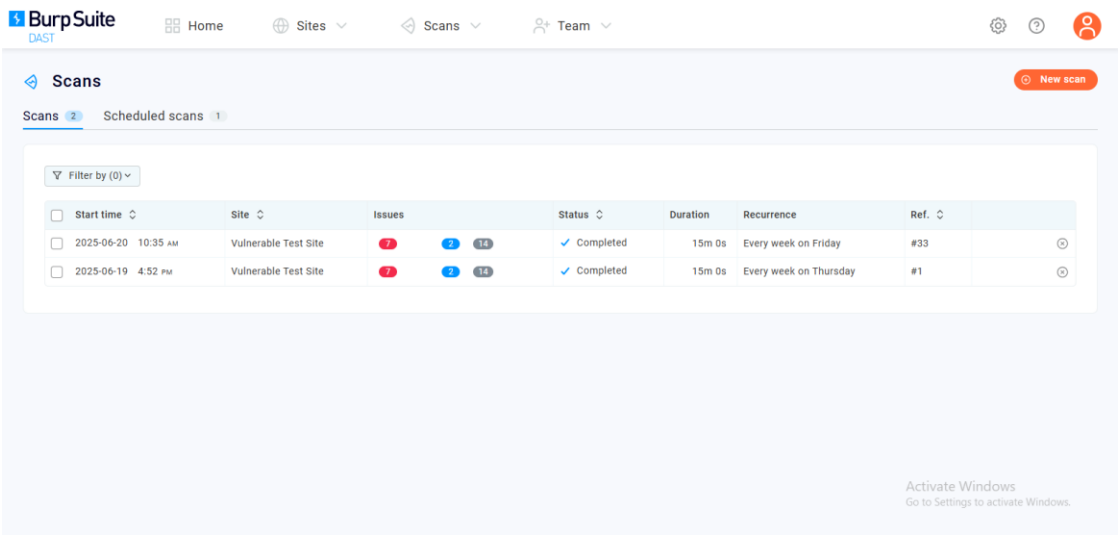
# Overview Of Burp Suite DAST

Dashboard of Burp Suite DAST




# Site & Scan Setup

List of Sites and Schedule/Manual Scan.




### Target Site Configuration

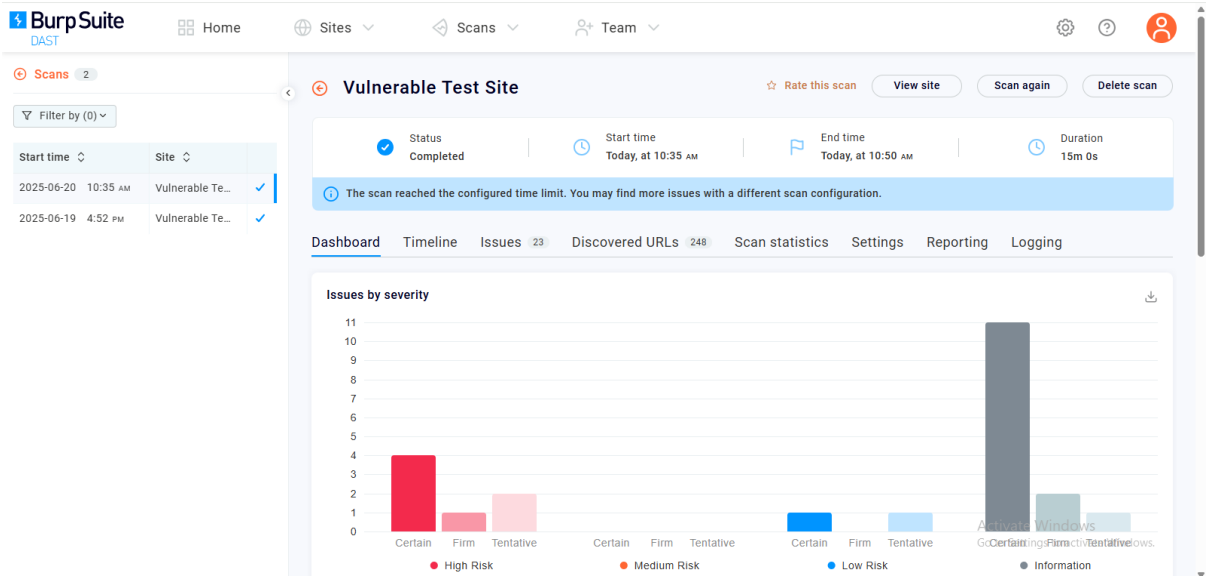
- **Target URL:** https://portswigger-labs.net
- **Authentication: Username –** Carlos; **Password –** Hunter!
- **Tags Applied:** internship, basic scan

### Scan Configuration

- **Scan Type:** Simple scan using default settings

- **Profile Settings:**
    - Crawl depth: Medium
    - Audit speed: Balanced
    - Issue types: Enabled by default (XSS, SQLi, CSRF, etc.)

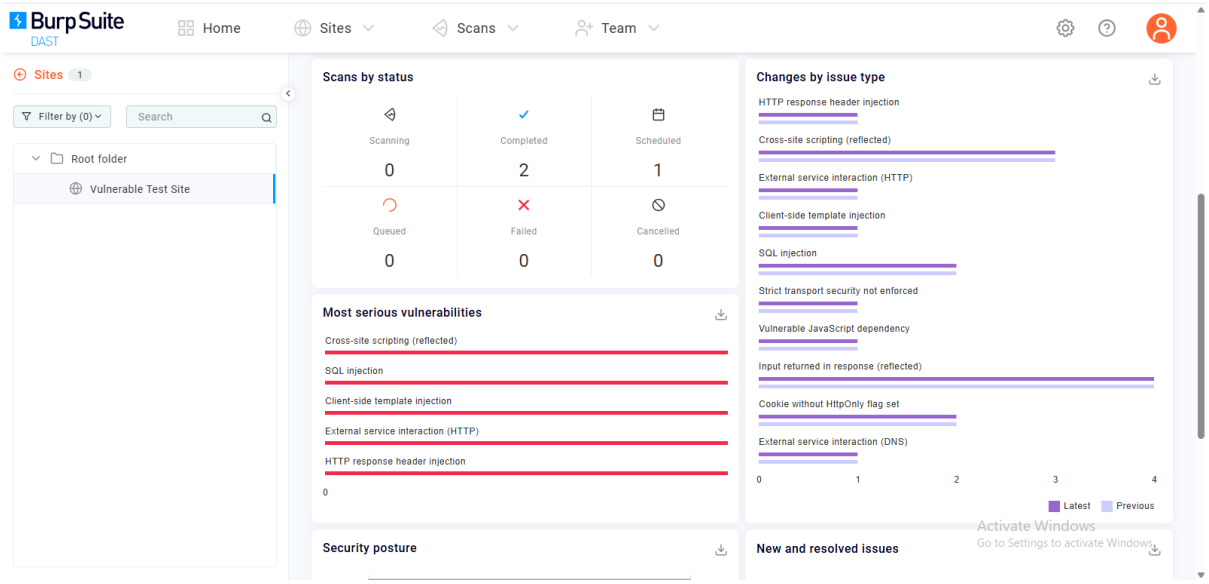
## Scanning & Monitoring




### Initial Scan Execution

- Scan was manually initiated from the Burp Suite DAST dashboard.
- The scan completed successfully in approximately 15–20 minutes.
- No errors or interruptions were observed during the scan.

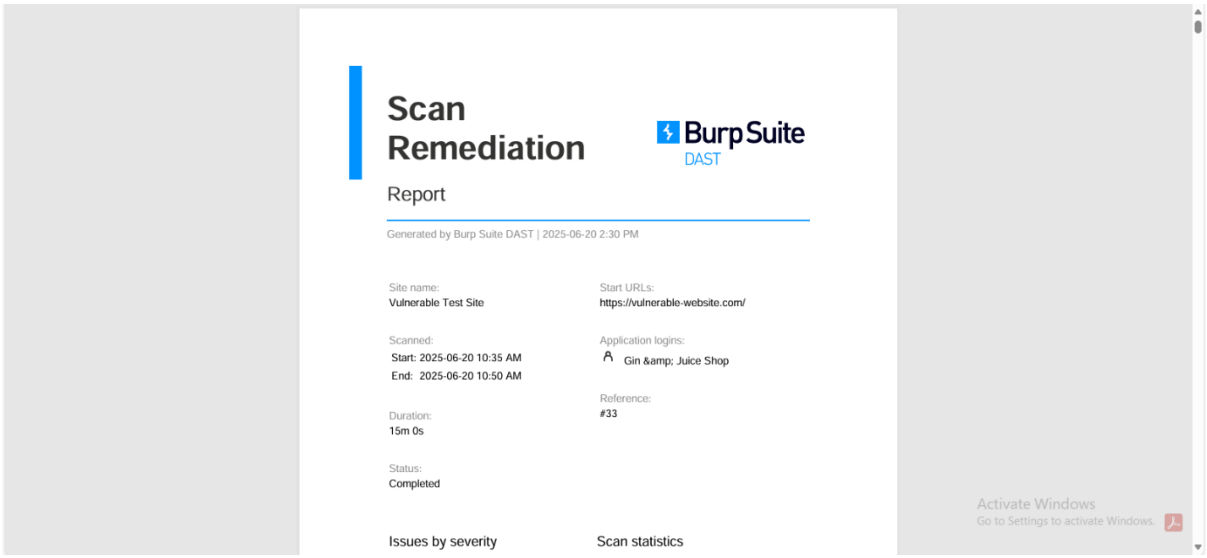
## Results Analysis




### Vulnerabilities Detected

1. **Reflected XSS**
    - **Location:** /vulnerabilities/xss_r/
    - **Severity:** Medium
    - **Impact:** JavaScript execution in browser
    - **Reproduction:** <script>alert('XSS')</script>
    - **Remediation:** Encode output, apply Content Security Policy (CSP)
2. **Information Disclosure**
    - **Location:** /vulnerabilities/info_disclosure/
    - **Severity:** Low
    - **Impact:** Sensitive data visible in response
    - **Remediation:** Remove or mask sensitive data

## Reporting & Collaboration




**Report Generation**

- **Format:** HTML
- **Contents:**
    - Summary of scan
    - List of detected issues
    - Severity ratings
    - Basic remediation suggestions
- **Distribution:** Shared with mentor for review

## Conclusion

This simple scan validated the installation and operational readiness of Burp Suite DAST. It demonstrated the tool's ability to detect basic vulnerabilities and generate actionable reports. The next steps may include configuring more advanced scan profiles and integrating Burp Suite DAST into CI/CD pipelines for continuous security testing.