



# VIT<sup>®</sup>

## Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

### **INFORMATION SECURITY MANAGEMENT LAB**

#### **EXPERIMENT-2**

<b>GROUP NO. :</b>	<b>11</b>
<b>TEAM MEMBER 1 :</b>	<b>Namit Mehrotra</b>
<b>REG. NO. :</b>	<b>21BCE0763</b>
<b>TEAM MEMBER 2 :</b>	<b>Purva Sharma</b>
<b>REG.NO :</b>	<b>21BCE0169</b>
<b>SUBJECT CODE :</b>	<b>BCSE354E</b>
<b>SUBJECT TITLE :</b>	<b>Information Security Management</b>
<b>LAB SLOT :</b>	<b>L29+L30</b>
<b>SEMESTER :</b>	<b>Winter Semester 2023-2024</b>
<b>GUIDED BY :</b>	<b>NIHA K</b>

# INSTALLATION Procedure

Burp Suite, a widely employed cybersecurity tool for web application security testing, can be installed on Windows by following these steps. Ensure your system meets the specified minimum requirements:

## Minimum Requirements for Kali Linux Installation:

**Operating System:** Kali Linux (version compatible with Burp Suite).

**Memory (RAM):** At least 2 GB RAM.

**Disk Space:** Ensure a minimum of 500 MB free disk space.

For Kali Linux, additional considerations include compatibility with the specific version of the operating system.

Now, let's consider the installation procedure for windows

## Minimum Requirements for Windows Installation:

**Operating System:** Windows 7 or later.

**Memory (RAM):** At least 2 GB RAM.

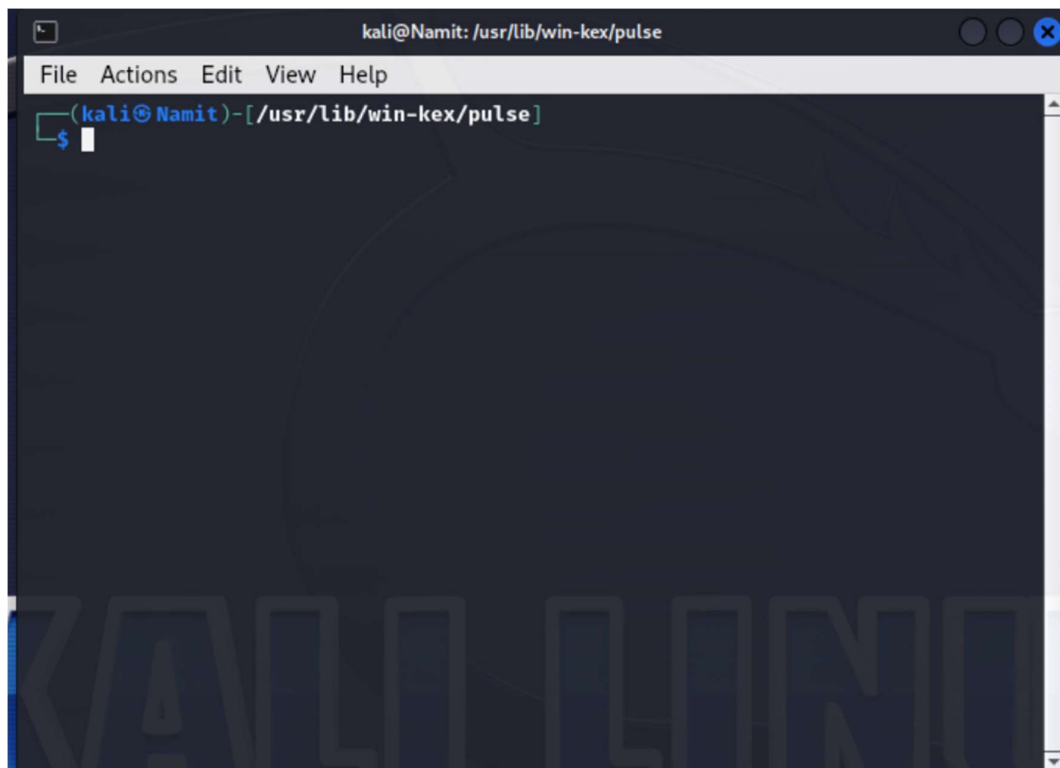
**Disk Space:** A minimum of 500 MB free disk space.

## Installation Procedure in Kali Linux:

### 1. Using sudo apt install:

#### 1. Open a Terminal:

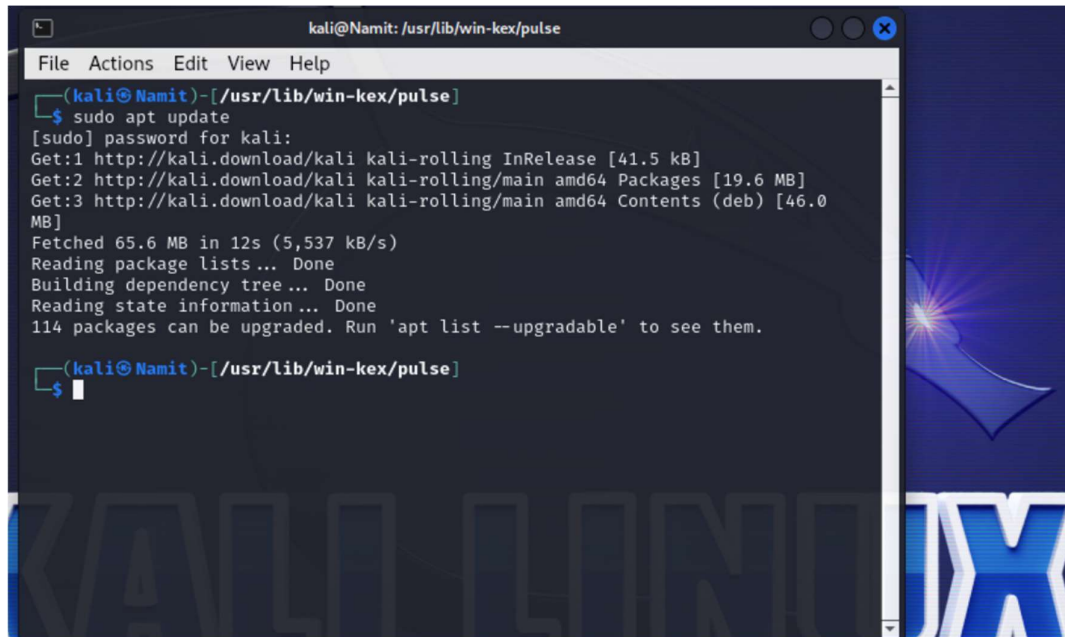
- Open a terminal on your Kali Linux system.



## 2. Update Package List:

- Update the package list to make sure you have the latest information about available packages.

**sudo apt update**

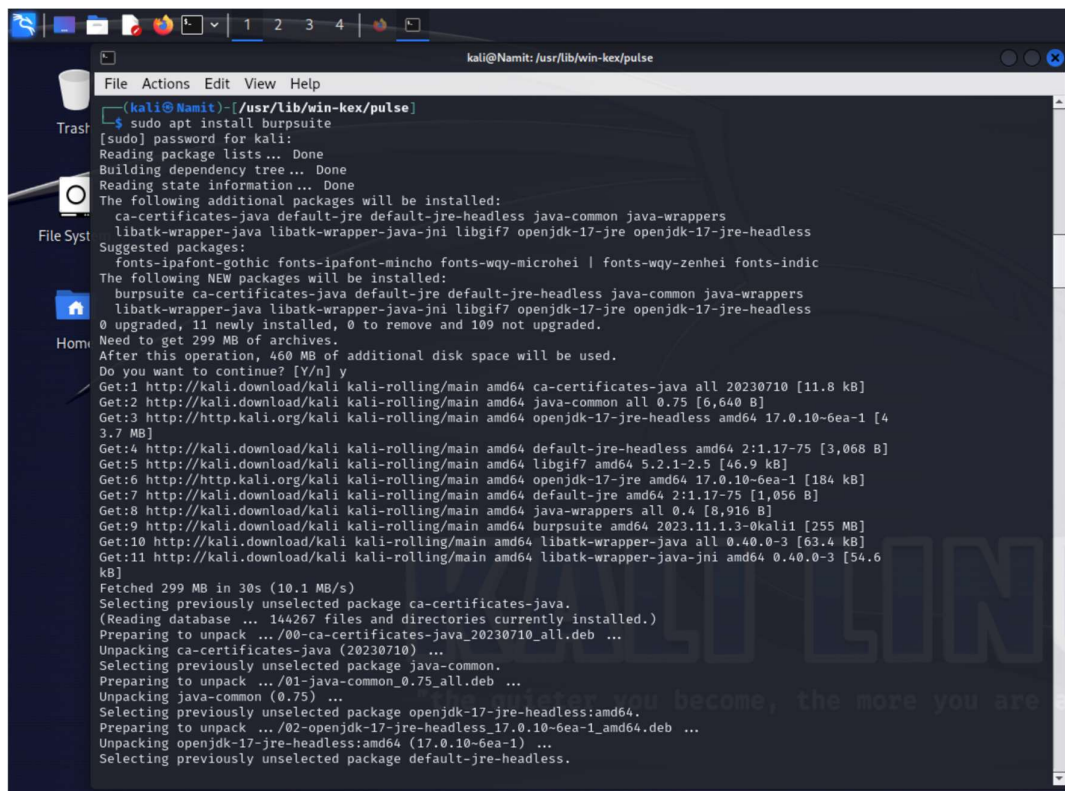


```
kali@Namit: /usr/lib/win-kex/pulse
File Actions Edit View Help
(kali@Namit)-[/usr/lib/win-kex/pulse]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.6 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [46.0 MB]
Fetched 65.6 MB in 12s (5,537 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
114 packages can be upgraded. Run 'apt list --upgradable' to see them.
(kali@Namit)-[/usr/lib/win-kex/pulse]
$
```

## 3. Install Burp Suite:

- Use the **sudo apt install burpsuite** command to install Burp Suite.

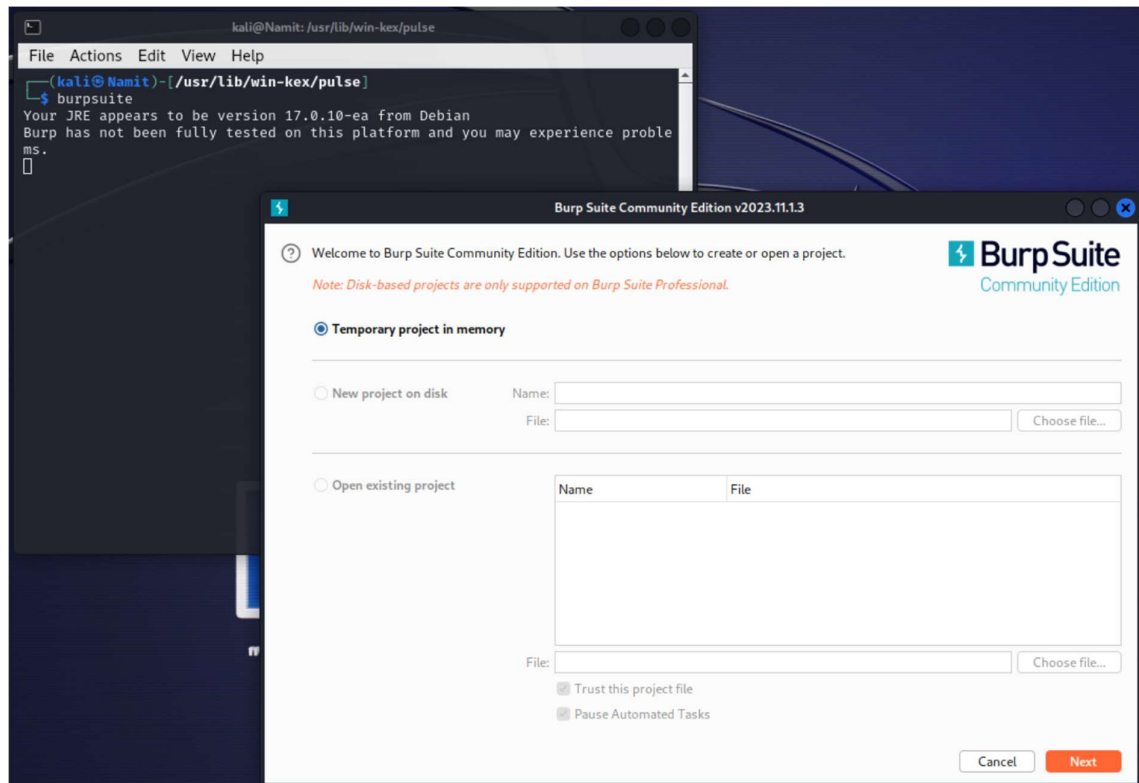
**sudo apt install burpsuite**



```
kali@Namit: /usr/lib/win-kex/pulse
File Actions Edit View Help
(kali@Namit)-[/usr/lib/win-kex/pulse]
$ sudo apt install burpsuite
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ca-certificates-java default-jre default-jre-headless java-common java-wrappers
  libatk-wrapper-java libatk-wrapper-java-jni libgif7 openjdk-17-jre openjdk-17-jre-headless
Suggested packages:
  fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei | fonts-wqy-zenhei fonts-indic
The following NEW packages will be installed:
  burpsuite ca-certificates-java default-jre default-jre-headless java-common java-wrappers
  libatk-wrapper-java libatk-wrapper-java-jni libgif7 openjdk-17-jre openjdk-17-jre-headless
0 upgraded, 11 newly installed, 0 to remove and 109 not upgraded.
Need to get 299 MB of archives.
After this operation, 460 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 ca-certificates-java all 20230710 [11.8 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 java-common all 0.75 [6,640 B]
Get:3 http://kali.org/kali kali-rolling/main amd64 openjdk-17-jre-headless amd64 17.0.10-6ea-1 [4
3.7 MB]
Get:4 http://kali.download/kali kali-rolling/main amd64 default-jre-headless amd64 2:1.17-75 [3,068 B]
Get:5 http://kali.download/kali kali-rolling/main amd64 libgif7 amd64 5.2.1-2.5 [46.9 kB]
Get:6 http://kali.org/kali kali-rolling/main amd64 openjdk-17-jre amd64 17.0.10-6ea-1 [184 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 default-jre amd64 2:1.17-75 [1,056 B]
Get:8 http://kali.download/kali kali-rolling/main amd64 java-wrappers all 0.4 [8,916 B]
Get:9 http://kali.download/kali kali-rolling/main amd64 burpsuite amd64 2023.11.13-0kali1 [255 MB]
Get:10 http://kali.download/kali kali-rolling/main amd64 libatk-wrapper-java all 0.40.0-3 [63.4 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 libatk-wrapper-java-jni amd64 0.40.0-3 [54.6
kB]
Fetched 299 MB in 30s (10.1 MB/s)
Selecting previously unselected package ca-certificates-java.
(Reading database ... 144267 files and directories currently installed.)
Preparing to unpack .../00-ca-certificates-java_20230710_all.deb ...
Unpacking ca-certificates-java (20230710) ...
Selecting previously unselected package java-common.
Preparing to unpack .../01-java-common_0.75_all.deb ...
Unpacking java-common (0.75) ...
Selecting previously unselected package openjdk-17-jre-headless:amd64.
Preparing to unpack .../02-openjdk-17-jre-headless_17.0.10-6ea-1_amd64.deb ...
Unpacking openjdk-17-jre-headless:amd64 (17.0.10-6ea-1) ...
Selecting previously unselected package default-jre-headless.
Preparing to unpack .../03-default-jre-headless_2:1.17-75_amd64.deb ...
Unpacking default-jre-headless (2:1.17-75) ...
Selecting previously unselected package libgif7:amd64.
Preparing to unpack .../04-libgif7_5.2.1-2.5_amd64.deb ...
Unpacking libgif7:amd64 (5.2.1-2.5) ...
Selecting previously unselected package openjdk-17-jre:amd64.
Preparing to unpack .../05-openjdk-17-jre_17.0.10-6ea-1_amd64.deb ...
Unpacking openjdk-17-jre:amd64 (17.0.10-6ea-1) ...
Selecting previously unselected package libatk-wrapper-java-jni:amd64.
Preparing to unpack .../06-libatk-wrapper-java-jni_0.40.0-3_amd64.deb ...
Unpacking libatk-wrapper-java-jni:amd64 (0.40.0-3) ...
Selecting previously unselected package libatk-wrapper-java:amd64.
Preparing to unpack .../07-libatk-wrapper-java_0.40.0-3_amd64.deb ...
Unpacking libatk-wrapper-java:amd64 (0.40.0-3) ...
Selecting previously unselected package java-wrappers.
Preparing to unpack .../08-java-wrappers_0.4_all.deb ...
Unpacking java-wrappers (0.4) ...
Selecting previously unselected package burpsuite.
Preparing to unpack .../09-burpsuite_2023.11.13-0kali1_amd64.deb ...
Unpacking burpsuite (2023.11.13-0kali1) ...
Setting up ca-certificates-java (20230710) ...
Setting up java-common (0.75) ...
Setting up openjdk-17-jre-headless:amd64 (17.0.10-6ea-1) ...
Setting up default-jre-headless (2:1.17-75) ...
Setting up libgif7:amd64 (5.2.1-2.5) ...
Setting up openjdk-17-jre:amd64 (17.0.10-6ea-1) ...
Setting up libatk-wrapper-java-jni:amd64 (0.40.0-3) ...
Setting up libatk-wrapper-java:amd64 (0.40.0-3) ...
Setting up java-wrappers (0.4) ...
Setting up burpsuite (2023.11.13-0kali1) ...
Processing triggers for libc-bin (2.34-1) ...
```

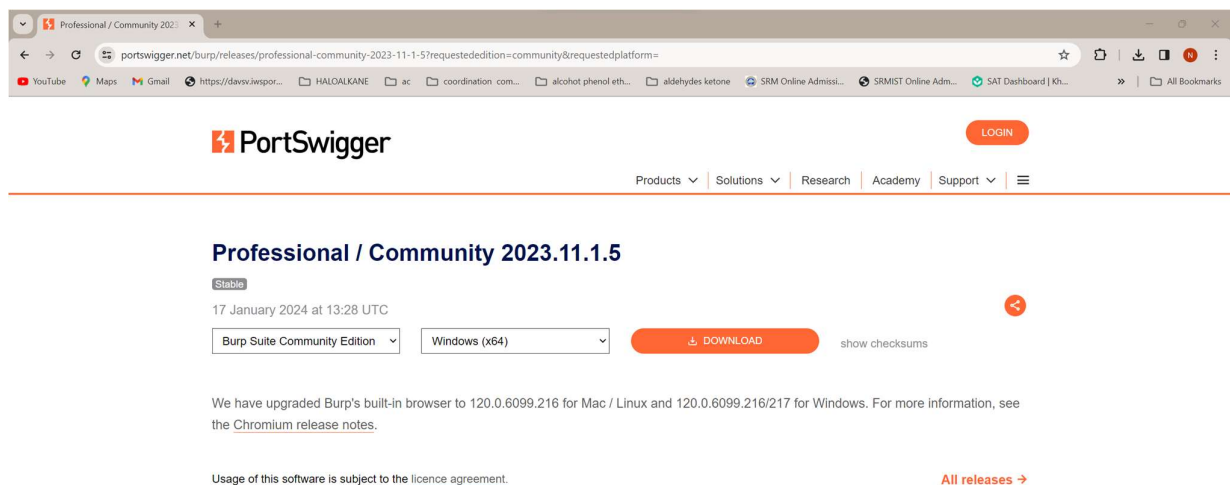
#### 4. Launch Burp Suite:

- Once the installation is complete, you can launch Burp Suite from the applications menu or by typing **burpsuite** in the terminal.



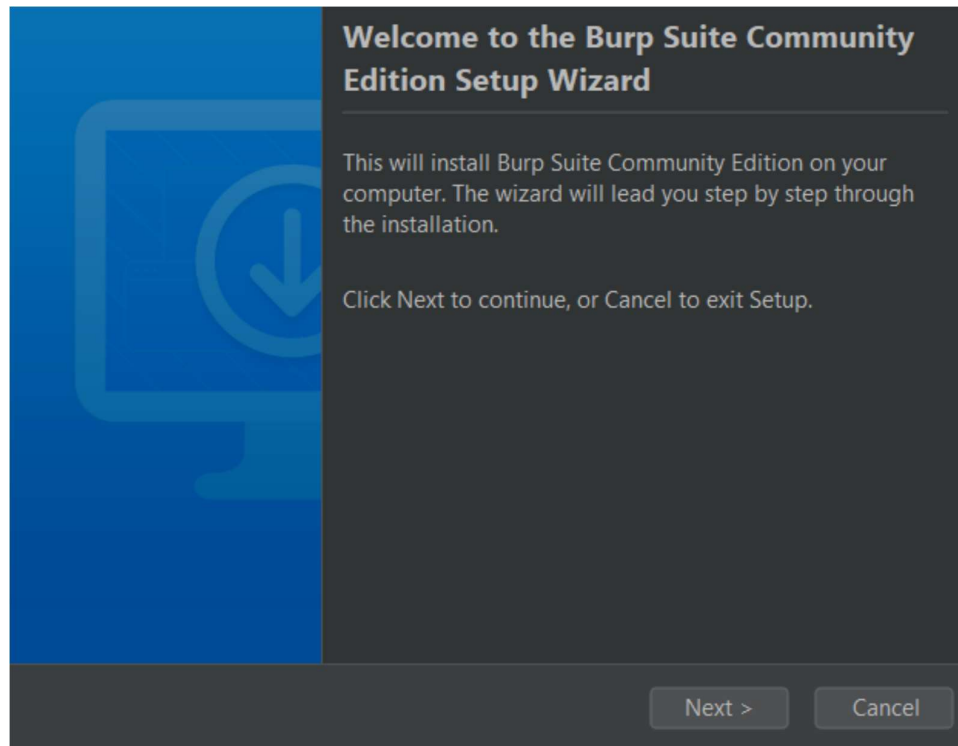
#### 2. Download from the Official Website for windows:

- Visit the Burp Suite Website:** Go to the official Burp Suite website at <https://portswigger.net/burp>.
- Download Burp Suite:**
  - Navigate to the "Download" section.
  - Choose the appropriate edition (Community or Professional) and click on the download link.
  - Save the installer file to your computer.



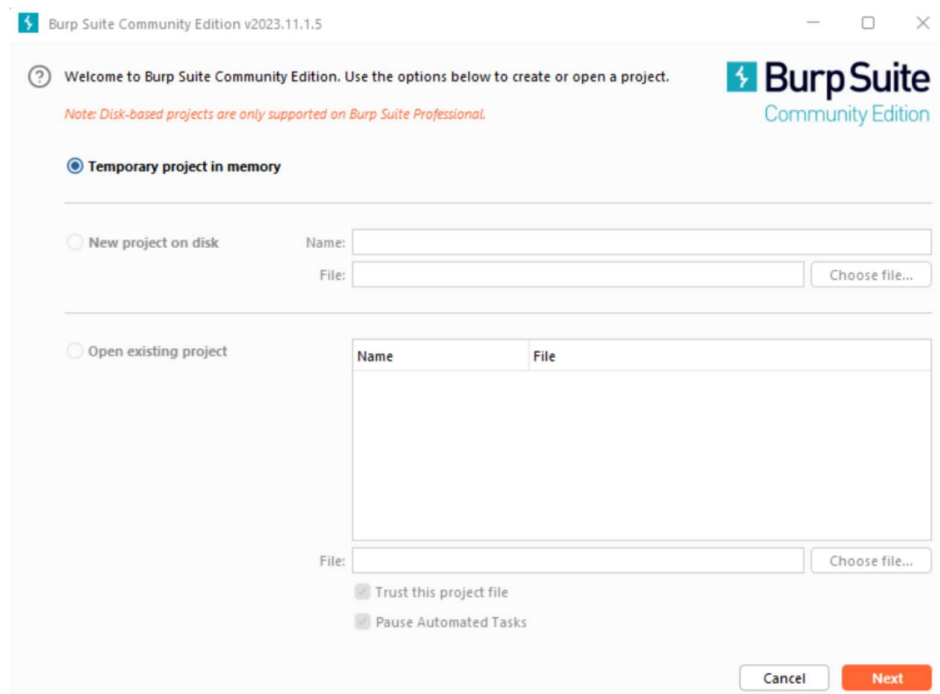
### 3. Run installer file

- Once the download is complete, run the
- Follow the instructions to complete the installation



### 4. Run Burpsuite

After installation, you can launch Burp Suite



## **5. Verify Burp Suite's Operational Status:**

1. Navigate to the "Proxy" tab within Burp Suite.
2. Confirm that the Intercept feature is disabled by default, and ensure the Proxy listener is actively running on 127.0.0.1:8080.
3. By default, Burp Suite initiates a proxy listener on localhost:8080. This represents the host and port through which our browser connects to proxy traffic via Burp Suite. We will maintain these default settings. The Intercept tool is initially activated in Burp Suite's default configuration. To verify this setting, go to User Options > Miscellaneous > Proxy Interception. While Intercept may be enabled at startup, some users prefer to deactivate it, which can be achieved by selecting "Always disable." Regardless, users can manually toggle Intercept on and off through Proxy > Intercept > Toggle Intercept.

## **2. Perform a study on Information Security Management (ISM) Tool which you have choose and explain**

Burp Suite, developed by PortSwigger, is widely employed in ethical hacking and penetration testing. It offers a suite of tools that empower users to manually modify requests, features an automated scanner to detect vulnerabilities, and provides an intercepting proxy for in-depth traffic analysis. Security professionals leverage its robust capabilities, including Burp Spider for comprehensive application crawling and mapping, as well as Burp Intruder for automating customized attacks. With its user-friendly interface, regular updates, and seamless integration options, Burp Suite stands out as the preferred tool in the dynamic field of cybersecurity, enabling experts to identify and address issues effectively.

## **Q. Which OSI Network layer it is used?**

### **OSI Network Layer:**

- Burp Suite primarily operates at Layer 7, the Application Layer, in the OSI model. Tailored specifically for the evaluation and security of online applications, Burp Suite proves indispensable in the realm of web application security testing.

**Q. List the protocol it handles and explain each.**

**Protocols Supported:**

**A. HTTPS (Hypertext Transfer Protocol Secure):**

Burp Suite can intercept and decode HTTPS traffic for encrypted communication, offering a crucial means to assess the security of applications utilizing secure connections.

**B. HTTP (Hypertext Transfer Protocol):**

Burp Suite intercepts and scrutinizes HTTP requests and responses, allowing security experts to inspect and modify the exchanged content between clients and servers.

**C. FTP (File Transfer Protocol):**

For fundamental FTP exchanges, Burp Suite enables security specialists to examine and control file transfers.

**D. WebSocket:**

Burp Suite's ability to intercept and analyze WebSocket traffic is crucial for testing contemporary web applications relying on real-time data transmission.

**E. DNS (Domain Name System):**

While not its primary focus, Burp Suite can assist in security evaluations related to DNS.

**Q. Which kind of attack it handles and explain the diagnosing method or technique.**

**Types of Attacks and Diagnosing Methods:**

Burp Suite, a versatile tool, is adept at identifying and addressing various security vulnerabilities. It handles common attacks such as:

**A. Cross-Site Scripting (XSS):** Intercepting and analyzing client-server traffic to locate and exploit XSS vulnerabilities.

**B. Cross-Site Request Forgery (CSRF):** Identifying and mitigating CSRF problems by examining requests and associated tokens.

**C. SQL Injection:** Testing for SQL injection vulnerabilities by modifying HTTP requests to detect and prevent unauthorized database access.

**D. Session Hijacking:** Assisting in identifying session management flaws and the associated risks of session hijacking.

**E. Security Misconfigurations:** Utilizing scanning features to discover web application misconfigurations, including exposed sensitive data or default credentials.

**Q. Identify in which stage of Information Security Management System Lifecycle the tool will be used.**

**Information Security Management System Lifecycle Stage:**

Burp Suite is most commonly utilized during the Testing and Evaluation stage of the Information Security Management System (ISMS) lifecycle. Security experts use it to examine online applications for vulnerabilities, conduct security audits, and perform penetration tests. This contributes to the detection and remediation of vulnerabilities before application deployment, ensuring a more secure environment for users.

In summary, Burp Suite, operating at the OSI model's Application Layer, is a valuable tool for web application security, supporting multiple protocols, addressing various types of attacks, and playing a prominent role in the testing and assessment stage of the Information Security Management System lifecycle.