

## EXPERIMENT 6

### Aim -

Use burp proxy to test web applications and burp suites.

### Theory -

#### **Burp proxy:**

Burp Proxy operates as a web proxy server between the browser and target applications. It enables you to intercept, inspect, and modify traffic that passes in both directions. You can even use this to test using HTTPS.

Burp Proxy is an essential component of Burp Suite's user-driven workflow. You can use it to send requests to Burp's other tools.

#### What is Burp Suite?

Burp Suite software is the best toolbox for web security testing. In web security testing, the incursion also protects engineer grace. Used to find and exploit search flaws. Burp Suite is therefore designed to be used by point-and-click. Understanding how systems are attacked is essential for everyone working in security, whether they are developers or security professionals. Burp Suite is a platform and graphical tool that work together to do security testing on online applications. It supports the whole testing process, from the initial mapping and analysis of an application's attack surface through the discovery and exploitation of security flaws.

Burp Suite is a proxy program that enables us to track, examine, and alter requests made by our browsers before they are forwarded to a distant server.

Burp Suite is a prominent web application security solution. It gives us the ability to manually test for vulnerabilities, intercepts HTTP messages, and change a message's body and header.

It was created by a business with the alias Portswigger, whose creator Dafydd Stuttard also works there. BurpSuite is designed to be an all-in-one toolkit, and BApps are add-ons that may be installed to expand its functionality.

It is the most widely used tool among experts in online app security and bug bounty hunters. It is a better option than free substitutes like OWASP ZAP because of how

simple it is to use. The community edition of Burp Suite is accessible for free, whereas the professional edition and the enterprise edition need payment.

### Why is Burp Suite Used in Cybersecurity

Burp Suite is a comprehensive framework that may be used to carry out several activities, including:

- Web crawling.
- Web application testing, both manually and automatically.
- Analysis of web applications.
- Vulnerability detection

Burp Suite also has the advantage of being built into the Chrome browser.

### Tools:

#### **BurpSuite provides the following tools:**

##### 1. Spider

A web crawler or spider is employed to map the target web application. The mapping's goal is to compile a list of endpoints so that their capabilities may be examined and possible vulnerabilities can be discovered. Spidering is carried out for the straightforward reason that more attack surfaces are available during real testing if you collect more endpoints during recon.

##### 2. Proxy

The intercepting proxy in BurpSuite enables the user to view and change the contents of requests and answers while they are being sent. Additionally, it eliminates the need for copy-and-paste by allowing the user to pass the request or answer that is being monitored to another pertinent BurpSuite tool. The proxy server can be configured to run on a specific loop-back IP address and port. Additionally, the proxy may be set up to block particular kinds of request-response pairings.

##### 3. Intruder

It is a fuzzer that runs a collection of values across an input point. The results are examined for success/failure and content length after the values have been executed. The response code or response content length changes as a result of an anomaly most

frequently. For its payload slot, BurpSuite supports dictionary files, brute-force attacks, and single values. The invader is employed for:

- Brute-force assaults against password forms, pin forms, and other forms of this nature.
- Dictionary attacks on password fields on forms are thought to make them susceptible to XSS or SQL injection.
- Rate limitation on the web app is being tested and attacked.

#### 4. Repeater

The Repeater module enables you to manually modify and replay individual requests. This feature is useful for testing specific scenarios and observing how the application responds to different inputs.

#### 5. Sequencer

The sequencer, an entropy checker, verifies the unpredictability of tokens produced by the webserver. These tokens, like cookies and anti-CSRF tokens, are typically used for authentication in sensitive processes. The ideal way to produce these tokens is completely random, which will distribute the likelihood of each potential character appearing at each location equally. Bitwise and character wise approaches should be used to accomplish this. This hypothesis' validity is examined with an entropy analyzer.

#### 6. Decoder

The decoder provides a list of common encoding techniques such as URL, HTML, Base64, Hex, and so on. When searching for specific data chunks inside the values of parameters or headers, this tool is quite helpful. Additionally, it is employed in the development of payloads for several vulnerability classes. Primary instances of IDOR and session hijacking are also uncovered using it.

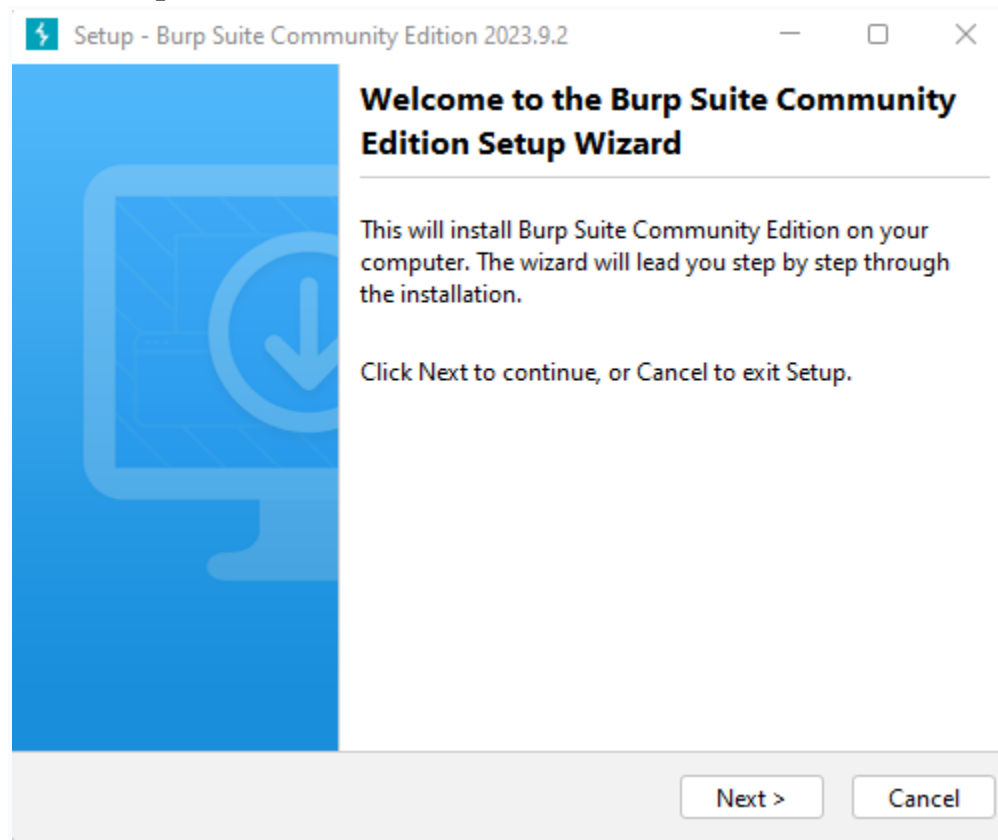
#### 7. Extender

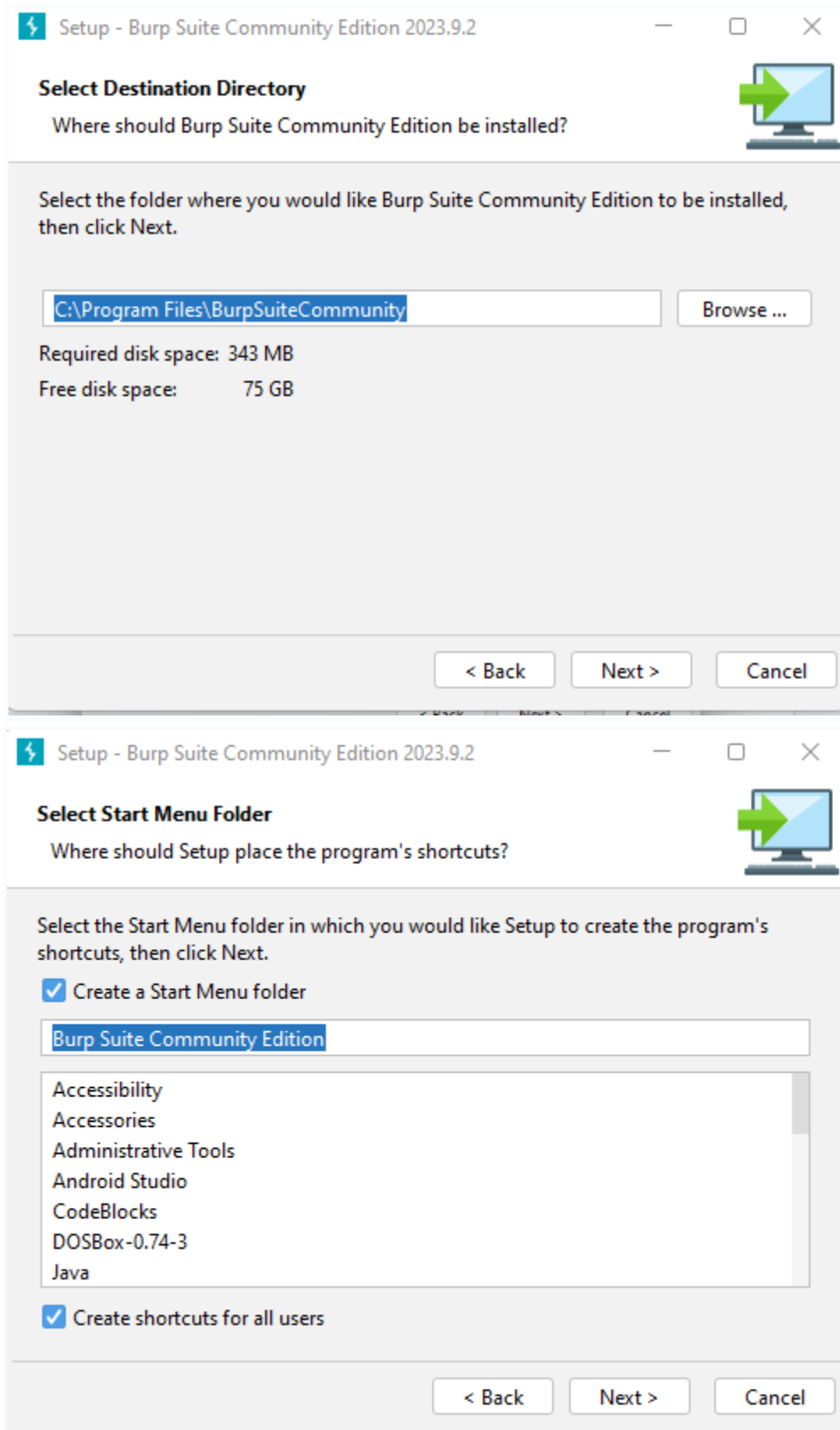
BurpSuite enables the integration of extra components into the toolkit to expand its functionality. These external components are referred to as BApps. These perform the same tasks as browser extensions... The Extender window allows you to examine, modify, install, and remove them. Some of them are supported by the free community version, while others need the professional version, which is a paid upgrade.

#### 8. Scanner

The community edition does not have a scanner. It automatically analyses the website for a variety of common vulnerabilities and provides them together with details on the reliability of each discovery and the difficulty of exploiting them. It is routinely updated to add brand-new, and lesser-known vulnerabilities.

### Installation of burp suite:





⚡ Burp Suite Community Edition v2023.9.2

?

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

⚡ Burp Suite

Community Edition

☒ Temporary project

☐ New project on disk

Name:

File:  [Choose file...](#)

☐ Open existing project

Name	File
------	------

File:  [Choose file...](#)

☒ Trust this project file

☒ Pause Automated Tasks

Cancel

Next

⚡ Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.9.2 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions **Learn** Settings


Learn, explore and discover

Hide this tab

Getting started with Burp Suite

Get going right away - with our quick start tutorial.

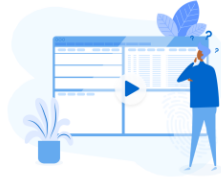
[Start here](#)



Burp Suite - a guided video tour

Take a run-through of all the major Burp Suite features.


[Watch the tour](#)



Burp Suite video tutorials

See how to use Burp Suite's main features and tools.


[Find out more](#)



The Web Security Academy

Learn how to find more vulnerabilities using Burp Suite.


[Start learning](#)



Burp Suite Support Center

Find the answers to your Burp Suite questions here.


[Find answers](#)



Burp Suite on Twitter

Join Burp Suite's huge community, and stay in the know.

[Follow us](#)



Try searching any website through the portswigger browser you will get the details of all the requests sent to the server.

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
1	https://notion-kanban.ne...	GET	/									✓	34.124.186.36	
2	https://notion-kanban.ne...	GET	/									✓	34.124.186.36	

**Request**

Pretty **Raw** Hex

```

1 GET / HTTP/1.1
2 Host: notion-kanban.netlify.app
3 Sec-Ch-Ua:
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: ""
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17

```

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookie
1	https://notion-kanban.ne...	GET	/									✓	34.124.186.36	
2	https://notion-kanban.ne...	GET	/									✓	34.124.186.36	
3	https://chatspheredient.n...	GET	/									✓	34.143.223.220	
4	https://chatspheredient.n...	GET	/									✓	34.143.223.220	
5	https://chatspheredient.n...	GET	/									✓	34.143.223.220	
6	https://chatspheredient.n...	GET	/									✓	34.143.223.220	

```

1 GET / HTTP/1.1
2 Host: chatspheredient.netlify.app
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
10 Sec-Ch-Ua:
11 Sec-Ch-Ua-Mobile: ?0
12 Sec-Ch-Ua-Platform: ""
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17

```

## Conclusion-

Used burp suite to monitor requests to different websites.