Experiment No. 2

Aim: Crawling and scanning a web application using Burp Spider and Scanner .

Learning Objective: To learn how to use Burp Spider and Scanner tools to map a web application's structure and automatically identify potential security vulnerabilities.

Theory:

What Is a Burp Suite?

Burp Suite is a web application security testing platform. It provides manual and automated tools to help cybersecurity professionals and developers identify vulnerabilities in web applications.

Developed by PortSwigger, Burp Suite integrates into the testing process, offering a suite of modular tools for tasks such as scanning, crawling, and analysis. This platform is useful for both manual and automated testing, offering flexibility and integration capabilities. It supports numerous extensions, which allow users to tailor the suite to meet project needs.

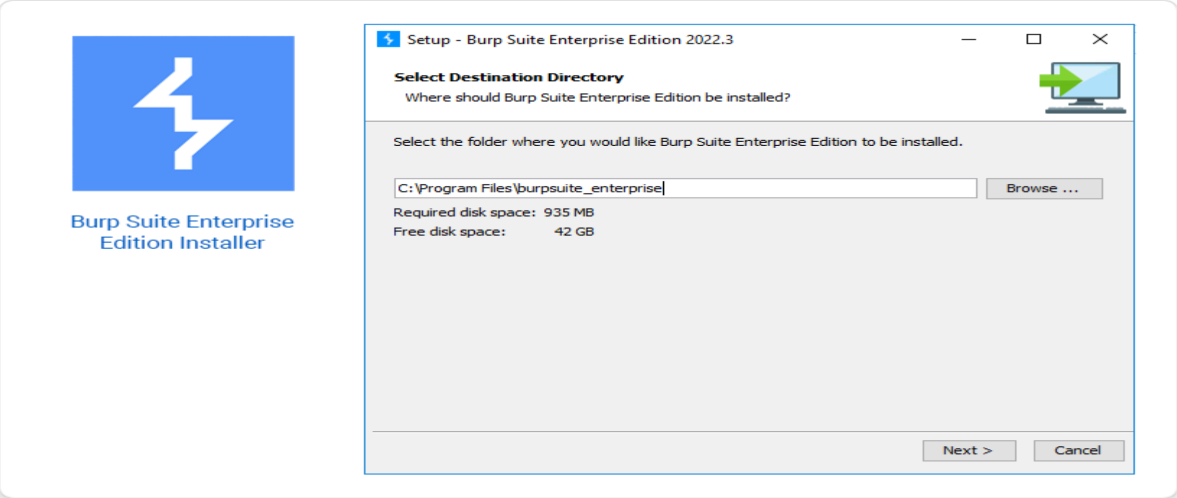
How to set up and start using Burp Suite

Step 1: Downloading and Installing Burp Suite

To begin, you'll need to have the latest version of Burp Suite:

1. **Download Burp Suite:** You can choose between the Professional Edition and the Community Edition, depending on your needs. Visit the official PortSwigger website to access the download links.
2. **Install Burp Suite:** After downloading the installer, run it to install Burp Suite on your system. Follow the on-screen instructions to complete the installation. If you're using the Professional Edition, you'll be prompted to enter your license key. For first-time users,

you can skip any project file or configuration setup by clicking **Next**, followed by **Start**



Burp Suite Enterprise Edition Installer
Setup - Burp Suite Enterprise Edition 2022.3
Browse ...
Next >
Cancel

Select Destination Directory

Where should Burp Suite Enterprise Edition be installed?

Select the folder where you would like Burp Suite Enterprise Edition to be installed.

C:\Program Files\burpsuite_enterprise

Required disk space: 935 MB
Free disk space: 42 GB

Step 2: Intercepting HTTP Traffic

To start using Burp Proxy to intercept traffic:

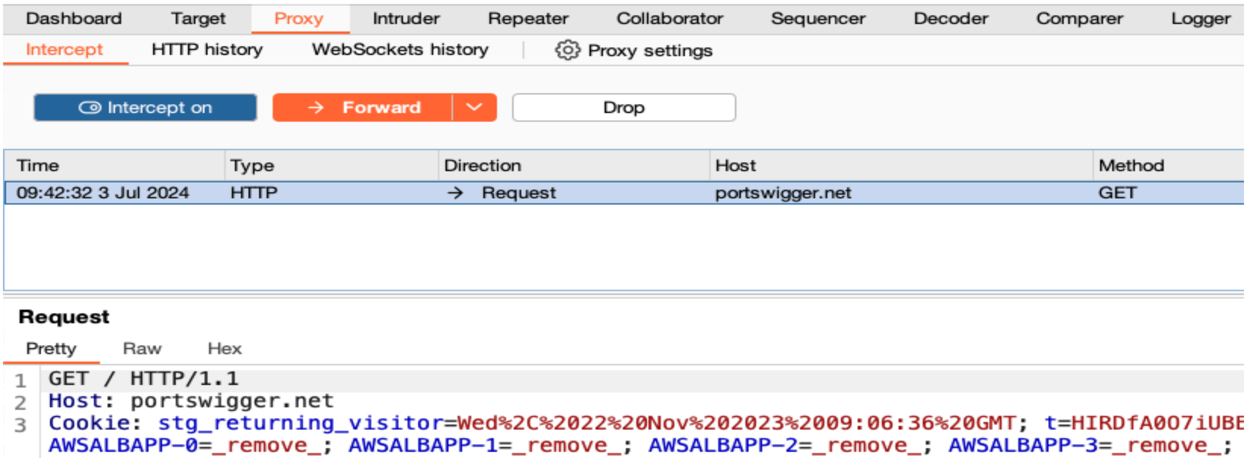
1. **Launch the Burp browser:** Navigate to the **Proxy** tab in Burp Suite, then click on **Intercept** and set the intercept toggle to **Intercept on**. Then, click **Open Browser** to launch Burp's preconfigured browser. Arrange your windows so that both Burp Suite and the browser are visible.

2. **Intercept a request:** In the Burp browser, try opening a website. You'll notice that the page doesn't load immediately because Burp Proxy has intercepted the HTTP request. This intercepted request is displayed under the **Intercept** tab under **Proxy**, allowing you to check it before forwarding it to the server.

3. **Forward the request:** Click on **Forward** to send the intercepted request to the server. You may need to forward multiple requests before the page fully loads in Burp's browser.

4. **Switch off interception:** After examining the necessary requests, you can switch off interception by toggling **Intercept off** in the **Proxy** tab. This allows subsequent traffic to pass through Burp Proxy without interruption.
5. **Access the HTTP history:** To review all HTTP traffic, navigate to the **HTTP history** tab under **Proxy**. Here, you can see a detailed log of all HTTP requests and responses that have passed through Burp Proxy. Clicking on any entry will display the raw HTTP data, which is useful for understanding how the web application interacts

with the server.



Time	Type	Direction	Host	Method
09:42:32 3 Jul 2024	HTTP	→ Request	portswigger.net	GET

Request

Pretty Raw Hex

```
GET / HTTP/1.1
Host: portswigger.net
Cookie: stg_returning_visitor=Wed%2C%2022%20Nov%202023%2009:06:36%20GMT; t=HIRDfA007iUBE
AWSALBAPP-0=_remove_; AWSALBAPP-1=_remove_; AWSALBAPP-2=_remove_; AWSALBAPP-3=_remove_;
```

Step 3: Modifying and Setting Target Scope for HTTP Requests

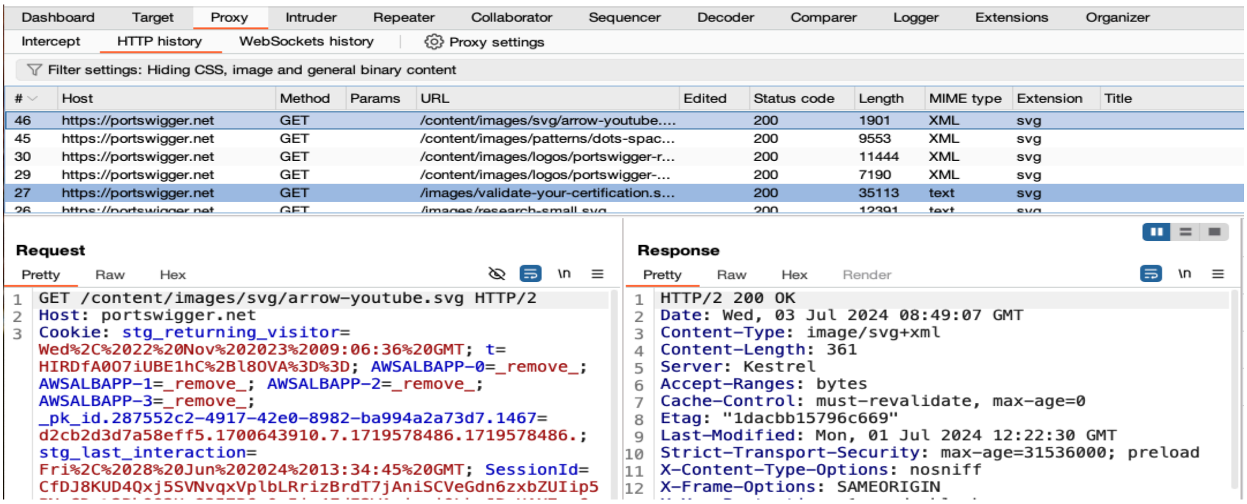
To modify the intercepted HTTP requests:

1. **Visit the vulnerable website:** Before modifying requests, make sure interception is switched off in Burp. Then, use Burp's browser to visit a deliberately vulnerable website provided by PortSwigger.

2. **Intercept a request:** Switch interception back on, and interact with the website (e.g., adding an item to a shopping cart). Burp Proxy will intercept the request, allowing you to study the parameters involved.

3. **Modify the request:** Examine the intercepted request and locate a parameter of interest (e.g., the price of an item). Manually change the value of this parameter to test how the server responds to unexpected inputs. Once modified, click **Forward** to send the altered request to the server. To send multiple requests, click **Forward all**.

4. **Exploit the identified vulnerability:** After forwarding the modified request, check the website in the Burp browser to see if the modification was successful.



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	Params	URL	Edited	Status code	Length	MIME type	Extension	Title
46	https://portswigger.net	GET		/content/images/svg/arrow-youtube....		200	1901	XML	svg	
45	https://portswigger.net	GET		/content/images/patterns/dots-spac...		200	9553	XML	svg	
30	https://portswigger.net	GET		/content/images/logos/portswigger-r...		200	11444	XML	svg	
29	https://portswigger.net	GET		/content/images/logos/portswigger-...		200	7190	XML	svg	
27	https://portswigger.net	GET		/images/validate-your-certification.s...		200	35113	text	svg	
26	https://portswigger.net	GET		/images/research-small.svg		200	12391	text	svg	

Request

Pretty Raw Hex

```
GET /content/images/svg/arrow-youtube.svg HTTP/2
Host: portswigger.net
Cookie: stg_returning_visitor=
Wed%2C%2022%20Nov%202023%2009:06:36%20GMT; t=
HIRDfA007iUBE1hC%2Bl8OVA%3D%3D; AWSALBAPP-0=_remove_;
AWSALBAPP-1=_remove_; AWSALBAPP-2=_remove_;
AWSALBAPP-3=_remove_;
_pk_id.287552c2-4917-42e0-8982-ba994a2a73d7.1467=
d2cb2d3d7a58eff5.1700643910.7.1719578486.1719578486.;
stg_last_interaction=
Fri%2C%2028%20Jun%202024%2013:34:45%20GMT; SessionId=
CfDJ8KUD4Qxj5SVNvqxVplbLRrizBrdT7jAniSCVeGdn6zxbZUIip5
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Date: Wed, 03 Jul 2024 08:49:07 GMT
Content-Type: image/svg+xml
Content-Length: 361
Server: Kestrel
Accept-Ranges: bytes
Cache-Control: must-revalidate, max-age=0
Etag: "1dacbb15796c669"
Last-Modified: Mon, 01 Jul 2024 12:22:30 GMT
Strict-Transport-Security: max-age=31536000; preload
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

Learning Outcome: Learned to effectively crawl and scan a web application using Burp Spider and Scanner.

Conclusion:

……………………………………………………………………………………………………

……………………………………………………………………………………………………

……………………………………………………………………………………

Name:

Class: BE-CSE

Roll No.:

For Faculty Use

Correction Parameters	**Formative Assessment [40%]**	**Timely completion of Practical [40%]**	**Attendance / Learning Attitude [20%]**	
Marks Obtained				