SAD LAB EXPERIMENT NO.: 06

Aim: To use BURP Proxy to test Web Applications.

To do:

1. What is BURP Suite?
2. Features
3. Tools offered by BURP Suite
4. Download and perform.

Theory:

BURP Suite:

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. BurpSuite aims to be an all in one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps.

It is the most popular tool among professional web app security researchers and bug bounty hunters. Its ease of use makes it a more suitable choice over free alternatives like OWASP ZAP. Burp Suite is available as a community edition which is free

Features:

1. **Web Application Scanning:** BURP Suite can automatically scan web applications to identify vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and more.
2. **Automated and Manual Testing:** It allows both automated scanning and manual testing, giving users flexibility to identify and exploit vulnerabilities.
3. **Web Crawling:** BURP Suite can crawl a website to discover different pages and endpoints, aiding in comprehensive testing.
4. **Intruder Functionality:** The Intruder tool lets you test various attack vectors by modifying parameters, payloads, and performing brute-force attacks.
5. **Repeater:** This tool lets you modify and resend HTTP requests to observe their impact on the application's behaviour.
6. **Proxy:** BURP Suite acts as a proxy between the user and the application, allowing traffic interception, analysis, and modification.
7. **Session Management:** It helps manage user sessions and cookies, ensuring effective testing of authenticated areas of a web application.
8. **Reporting:** BURP Suite generates detailed reports of identified vulnerabilities, aiding in clear communication and documentation.

Tools offered by BURP Suite:

1. **Spider:**

   It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found. Spidering is done for the simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.

2. **Proxy:**

   BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.

3. **Intruder:**

   It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. BurpSuite allows brute-force, dictionary file and single values for its payload position.

4. **Repeater:**

   Repeater lets a user send requests repeatedly with manual modifications. It is used for:

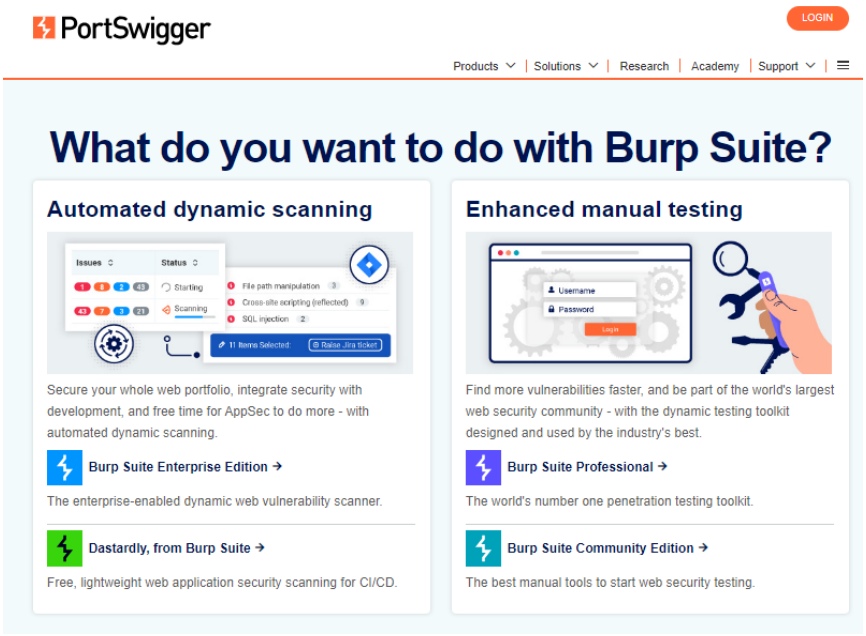
   - Verifying whether the user-supplied values are being verified.
   - If user-supplied values are being verified, how well is it being done?
   - What values is the server expecting in an input parameter/request header?
   - How does the server handle unexpected values?
   - Is input sanitation being applied by the server?

5. **Sequencer:**

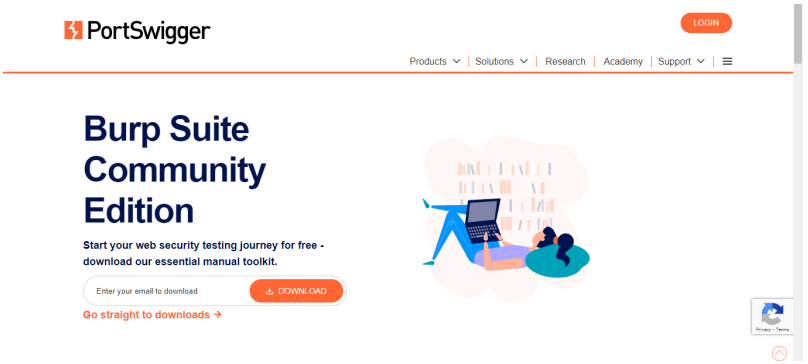
   The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication in sensitive operations: cookies and anti-CSRF tokens are examples of such tokens. Ideally, these tokens must be generated in a fully random manner so that the probability of appearance of each possible character at a position is distributed uniformly. This should be achieved both bit-wise and character-wise. An entropy analyzer tests this hypothesis for being true.

Downloading Steps:

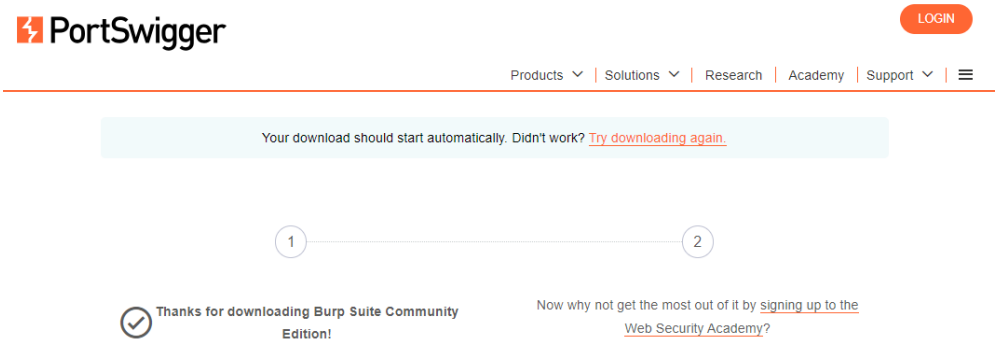
1. Go to Link:



2. Click on Burp Suite Community Edition:

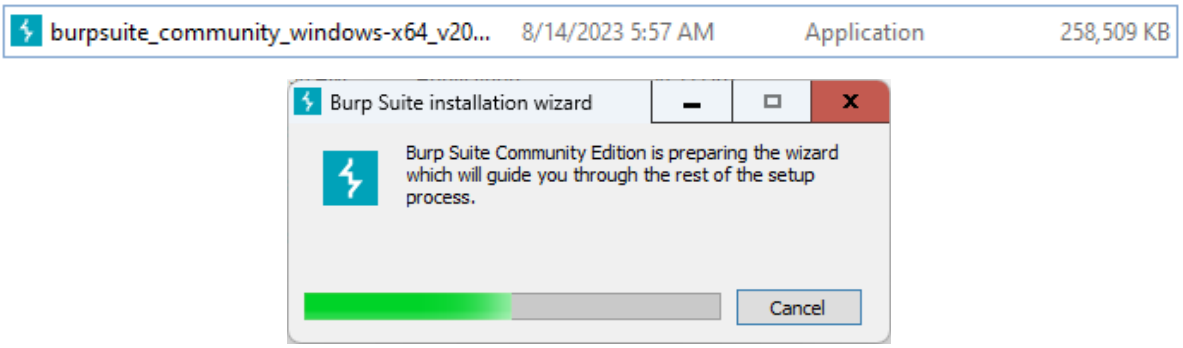


3. Put your Email ID and the downloading will start

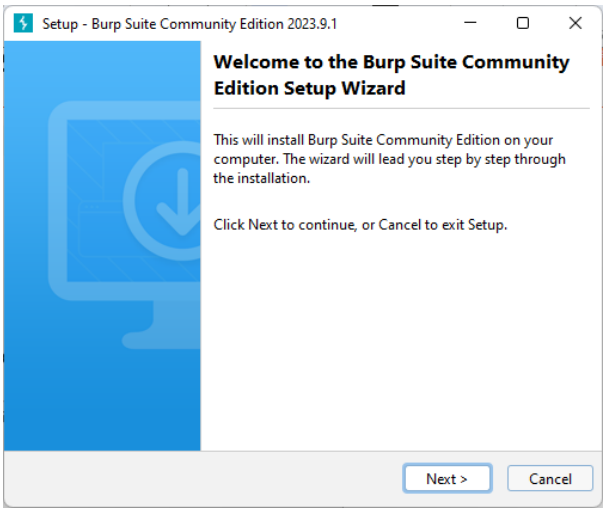


Installation Steps:

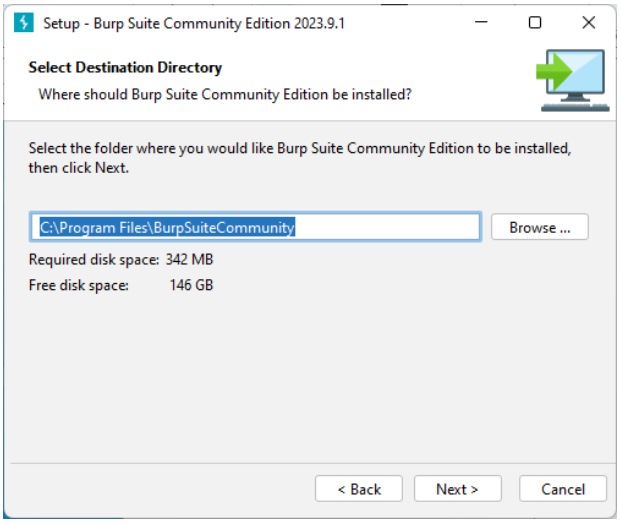
1. Double click on the Burp Suite exe file.



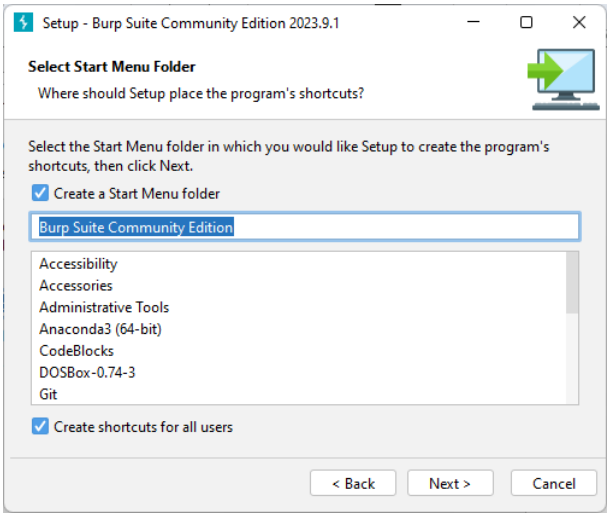
2. Click on Next.

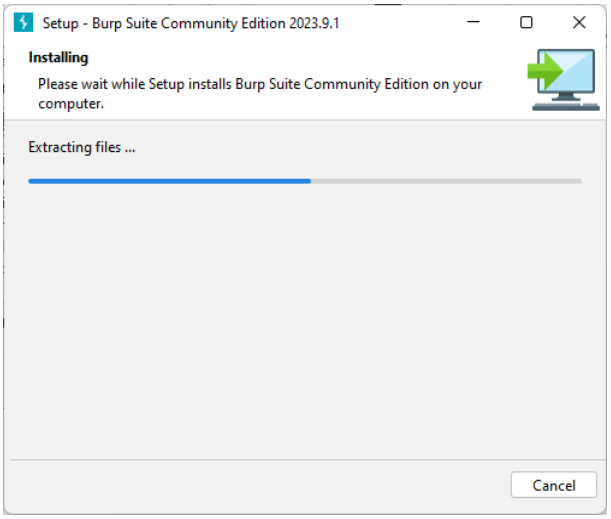


3. Select the location for the installation of your application and then click on Next.

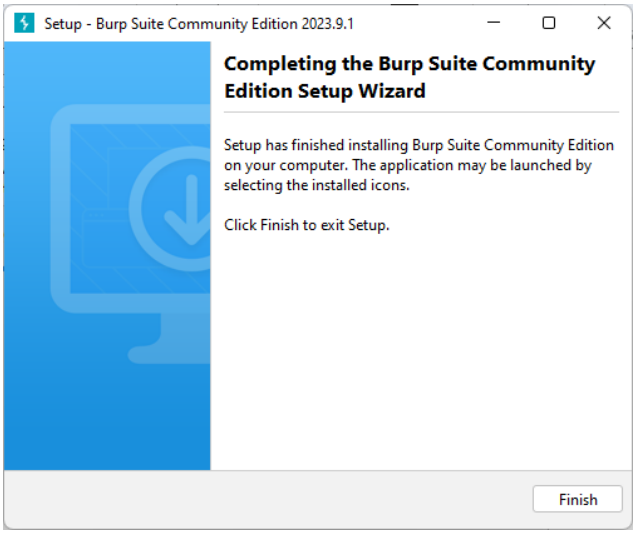


4. Select Start Menu Folder and click Next:



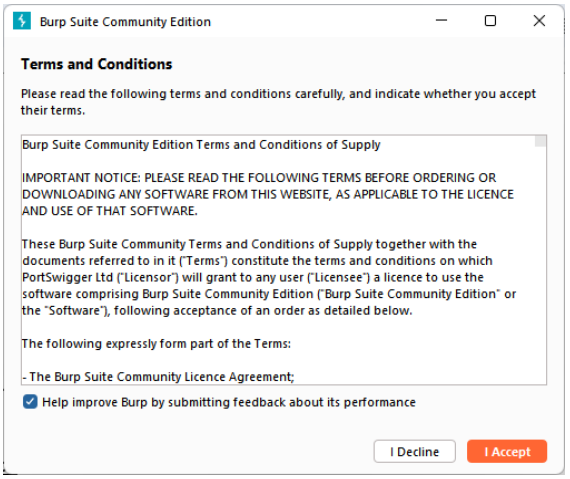


5. Click on Finish:

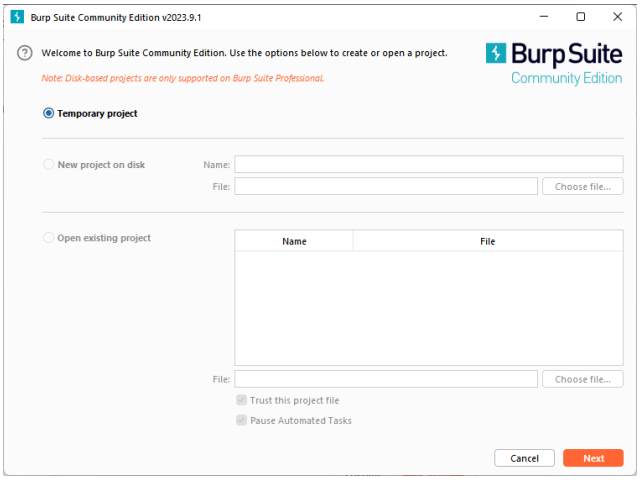


Implementation:

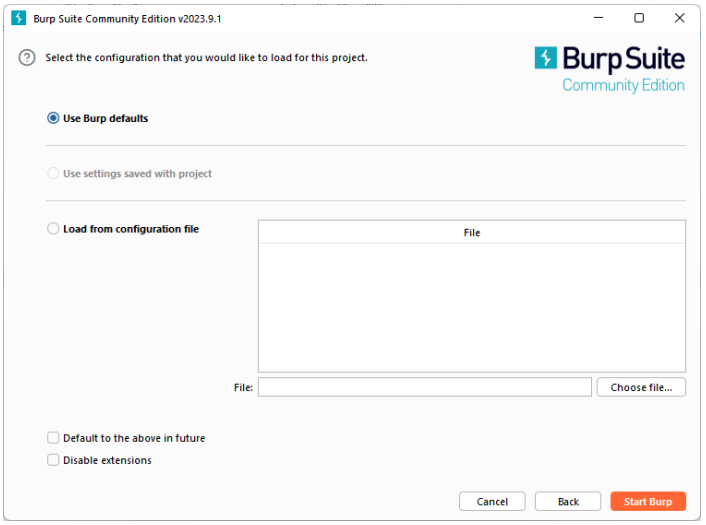
1. Open Burp Suite application and click on Accept:



2. Now, run the installer and open the Burp Suite software.

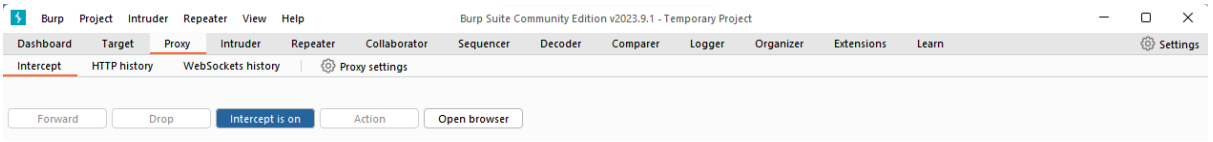


3. Intercepting HTTP traffic with Burp Proxy.
    a. 1. Go to the Proxy -> Intercept tab.

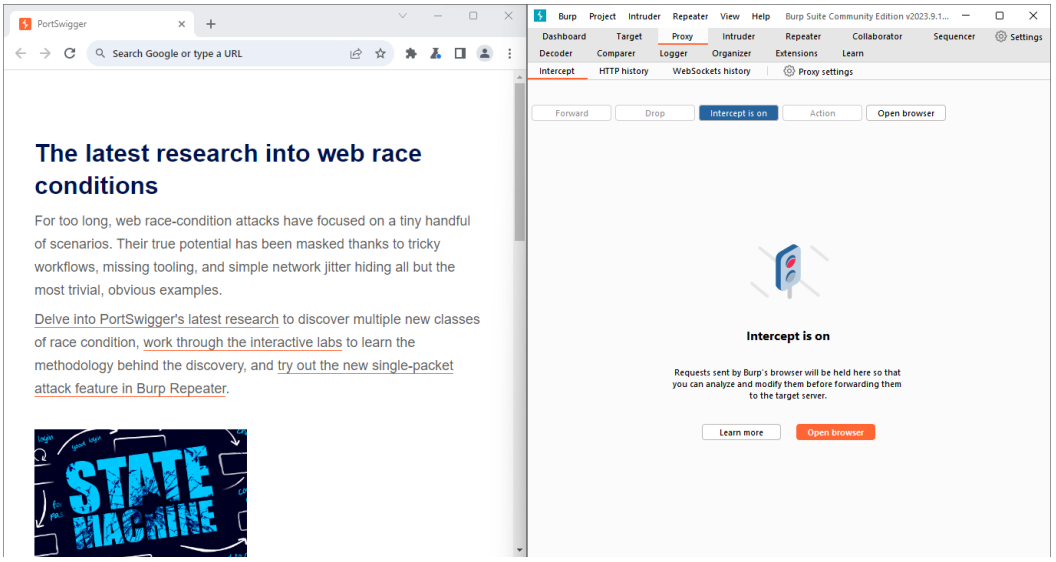


b. Click the Intercept is off button, so it toggles to Intercept is on.

c. Click Open Browser. This launches Burp's browser, which is preconfigured to work with Burp right out of the box. Position the windows so that you can see both Burp and Burp's browser.

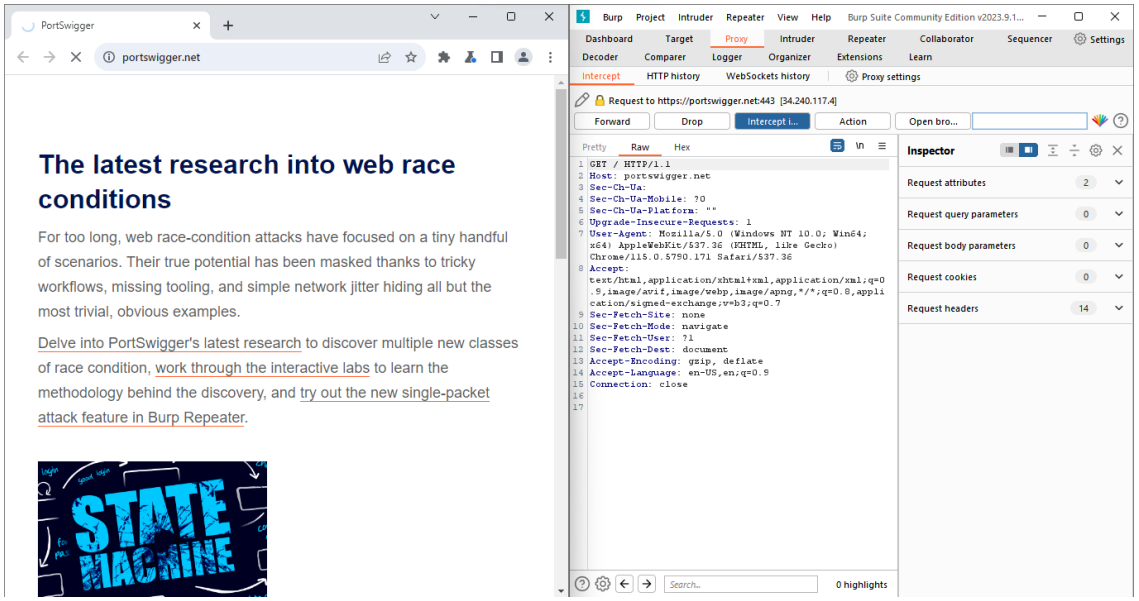


d. Using Burp's browser, try to visit https://portswigger.net and observe that the site doesn't load. Burp Proxy has intercepted the HTTP request that was issued by the browser before it could reach the server. You can see this intercepted request on the Proxy -> Intercept tab.

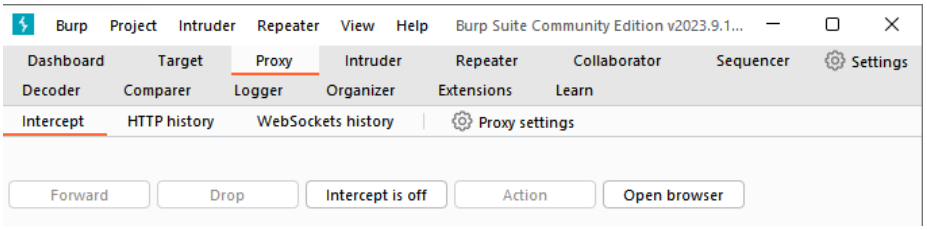


The request is held here so that you can study it, and even modify it, before forwarding it to the target server.

e. Click the Forward button several times to send the intercepted request, and any subsequent ones, until the page loads in Burp's browser.

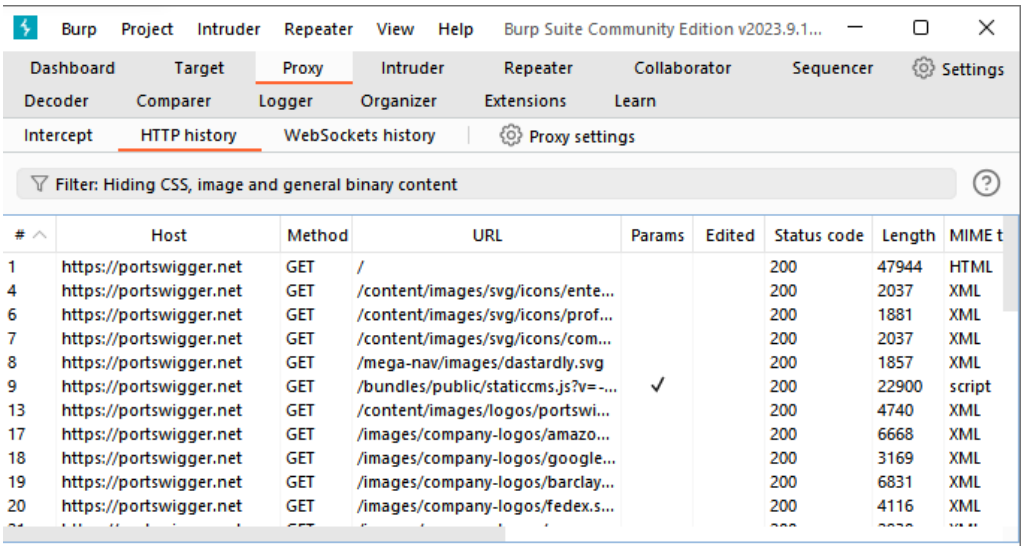


f. Due to the number of requests browsers typically send, you often won't want to intercept every single one of them. Click the Intercept is on button so that it now says Intercept is off.



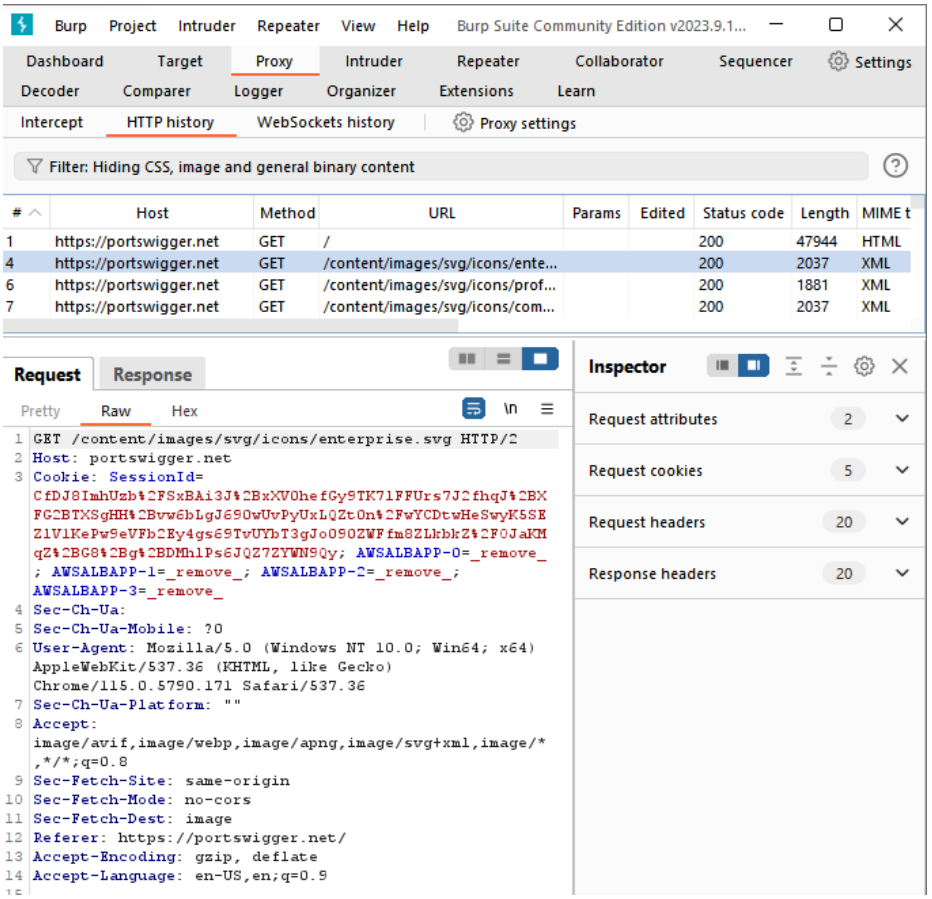
Go back to the browser and confirm that you can now interact with the site as normal.

g. In Burp, go to the Proxy > HTTP history tab. Here, you can see the history of all HTTP traffic that has passed through Burp Proxy, even while interception was switched off.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME t
1	https://portswigger.net	GET	/			200	47944	HTML
4	https://portswigger.net	GET	/content/images/svg/icons/ente...			200	2037	XML
6	https://portswigger.net	GET	/content/images/svg/icons/prof...			200	1881	XML
7	https://portswigger.net	GET	/content/images/svg/icons/com...			200	2037	XML
8	https://portswigger.net	GET	/mega-nav/images/dastardly.svg			200	1857	XML
9	https://portswigger.net	GET	/bundles/public/staticcms.js?v=-...	✓		200	22900	script
13	https://portswigger.net	GET	/content/images/logos/portswi...			200	4740	XML
17	https://portswigger.net	GET	/images/company-logos/amazo...			200	6668	XML
18	https://portswigger.net	GET	/images/company-logos/google...			200	3169	XML
19	https://portswigger.net	GET	/images/company-logos/barclay...			200	6831	XML
20	https://portswigger.net	GET	/images/company-logos/fedex.s...			200	4116	XML

h. Click on any entry in the history to view the raw HTTP request, along with the corresponding response from the server.



Conclusion:

In this experiment we learned how to use BURP Proxy to test Web Applications.