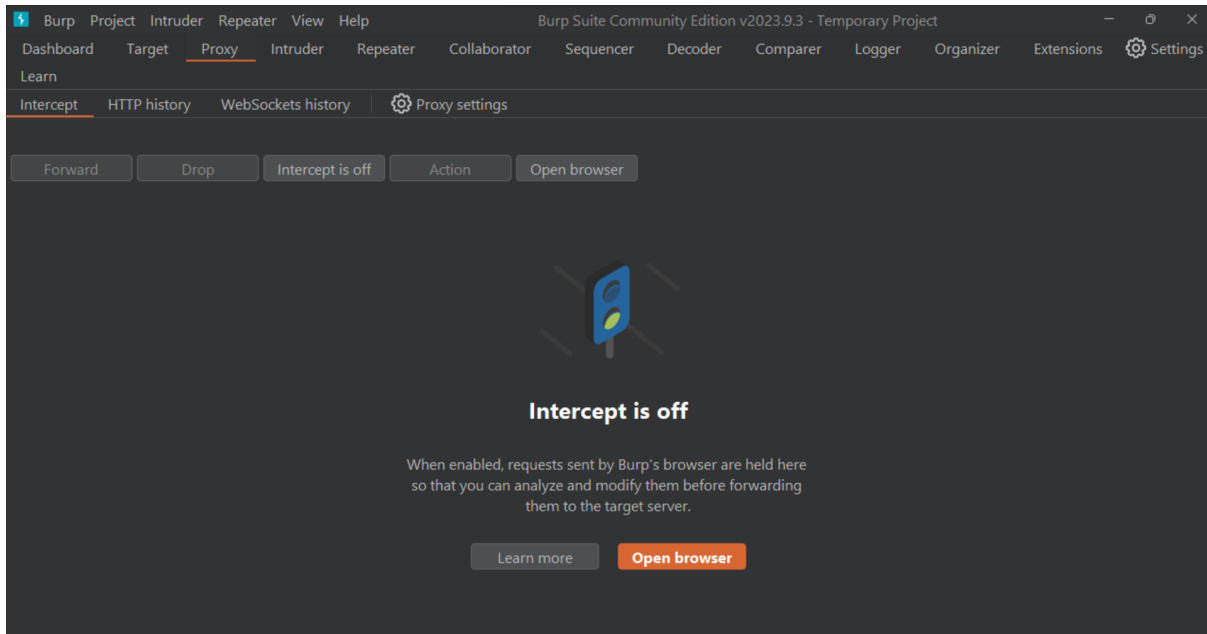


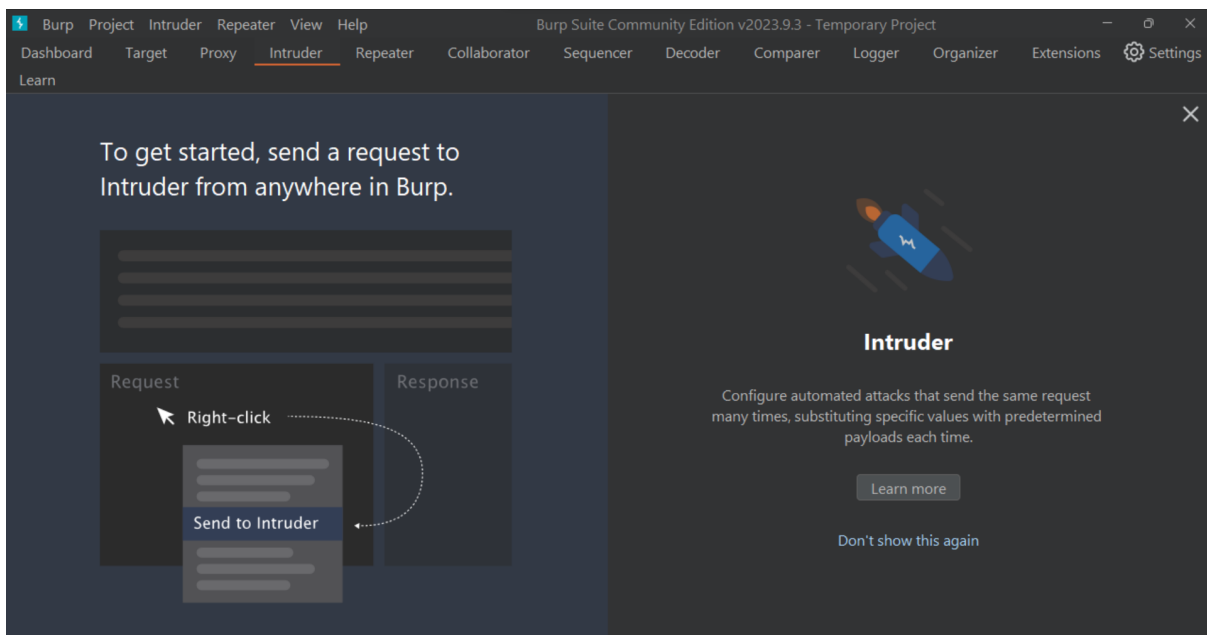
Actividad 5

Cómo usar Burp Suite.

Proxy: Capturar las peticiones al interferir las peticiones que se realizan entre el cliente y el servidor.



Intruder: Esta pestaña es de ataques programados, pues permite configurar múltiples ataques al mismo tiempo.que incluyen fuerza bruta, inyecciones sql, etc.



Repeater: Simula la respuesta, lo que nos permite controlar de forma manual las peticiones HTTP interceptadas por el proxy, cambiar parámetros, cabeceras y enviarlas nuevamente.

The screenshot shows the Burp Suite Repeater tab. The target is `https://0a42002c04ccb840809a3a0600cf000d.web-security-academy.net`. The request is a GET to `/filter?category=Corporate+gifts'+OR+1=1--`. The response is an HTTP 200 OK with content type `text/html; charset=utf-8` and a content length of 11553. The response body shows the beginning of an HTML document with a head section containing two link tags for CSS files.

Request	Response
1 GET /filter?category=Corporate+gifts'+OR+1=1-- HTTP/2	1 HTTP/2 200 OK
2 Host: 0a42002c04ccb840809a3a0600cf000d.web-security-academy.net	2 Content-Type: text/html; charset=utf-8
3 Cookie: session=V9TmbVbd1PDQ31dYkAJgcPh4MRM3CMHi	3 X-Frame-Options: SAMEORIGIN
4 Sec-Ch-Ua: "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"	4 Content-Length: 11553
5 Sec-Ch-Ua-Mobile: ?0	5
6 Sec-Ch-Ua-Platform: "Windows"	6 <!DOCTYPE html>
7 Upgrade-Insecure-Requests: 1	7 <html>
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)	8 <head>
	9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
	10 <link href=/resources/css/labsEcommerce.c

Target: Hace un mapeo de la aplicación. Aunque no se capturen peticiones todo se irá a Target y ahí estará toda la estructura de la página web.

The screenshot shows the Burp Suite Target tab. The site map on the left lists various domains. The main panel shows a list of requests with columns for Host, Method, URL, Params, Status code, Length, and MIME type. The request list includes a GET to `/academyLabHeader` (status 101), a GET to `/login` (status 200), a GET to `/my-account?id=admin...` (status 200), a POST to `/login` (status 302), and several other GET requests to `/logout`, `/my-account`, `/my-account/change-e...`, and `/resources/css/labs.css`.

Host	Method	URL	Params	Status code	Length	MIME type
https://0a620046047de...	GET	/academyLabHeader		101	147	
https://0a620046047de...	GET	/login		200	5229	HTML
https://0a620046047de...	GET	/my-account?id=admin...		200	5338	HTML
https://0a620046047de...	POST	/login		302	195	
https://0a620046047de...	GET	/				
https://0a620046047de...	GET	/logout				
https://0a620046047de...	GET	/my-account				
https://0a620046047de...	GET	/my-account/change-e...				
https://0a620046047de...	GET	/resources/css/labs.css				