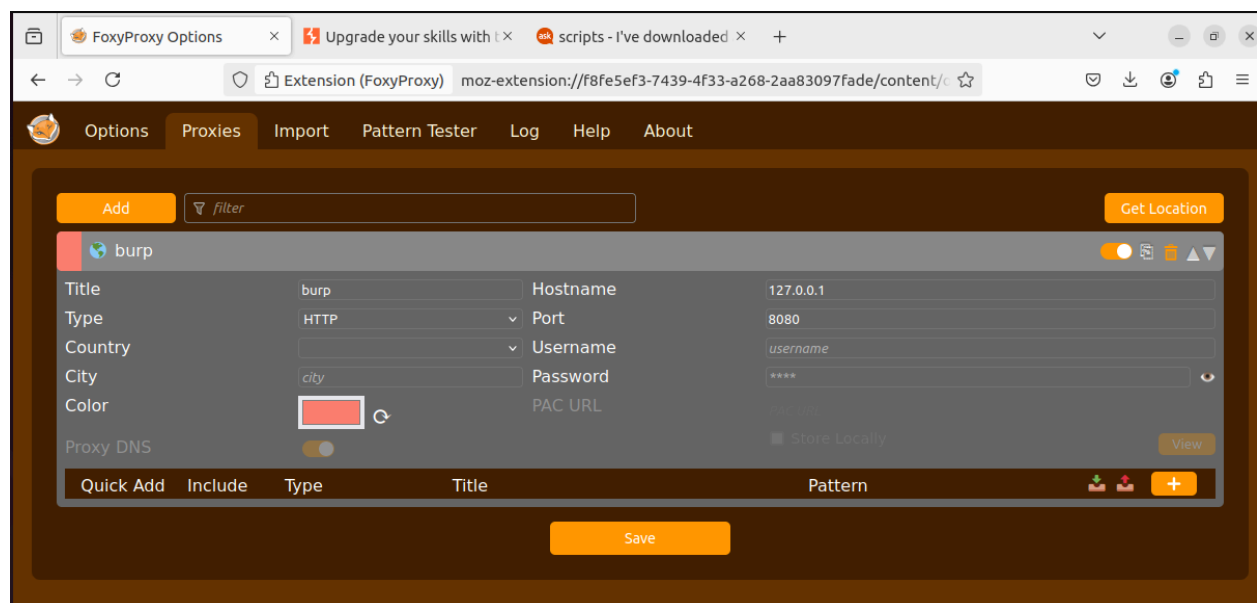
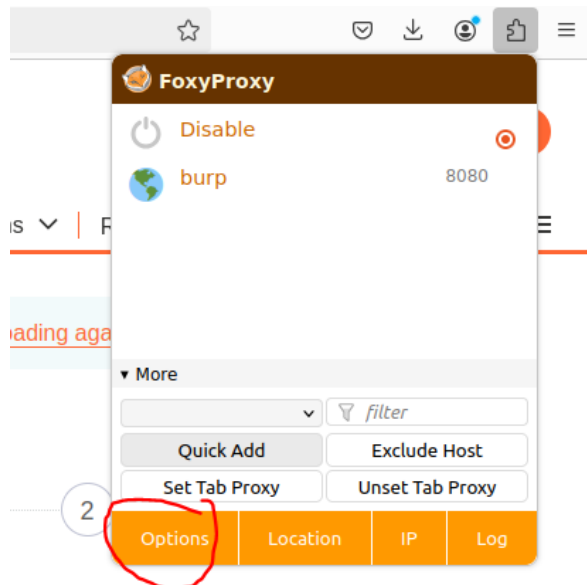


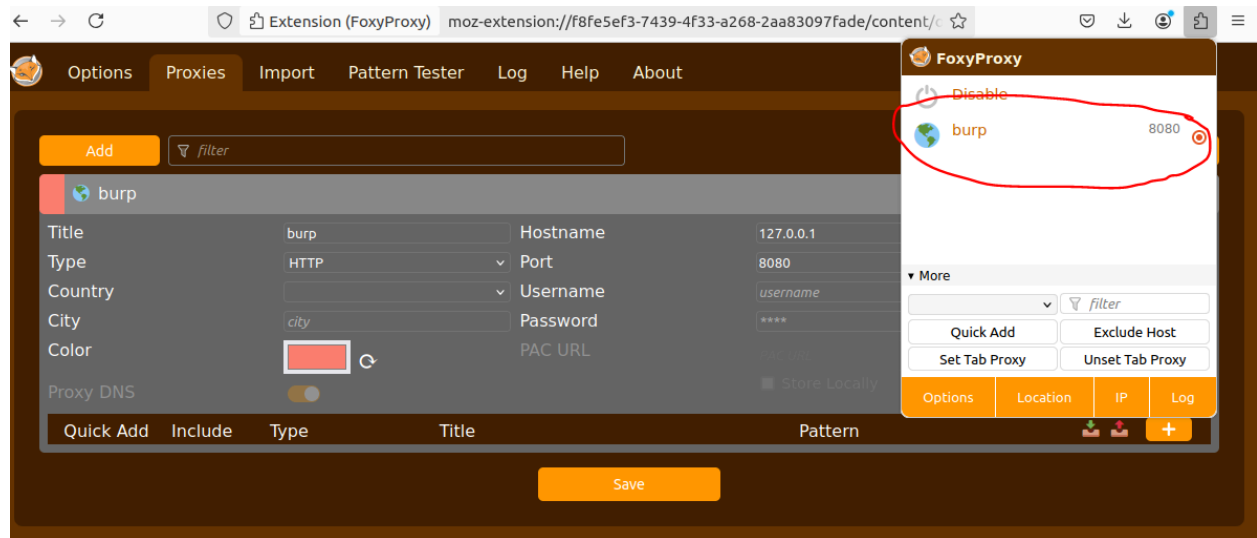
Para realizar una intercepción proxy vamos a necesitar Burpsuite (programa) y una extensión en nuestro navegador (FoxyProxy).

Foxy Proxy:

Primero descargamos y instalamos la extensión en nuestro navegador de confianza. Una vez instalado vamos a ir dentro de la configuración de la misma y vamos a configurar esta proxy:

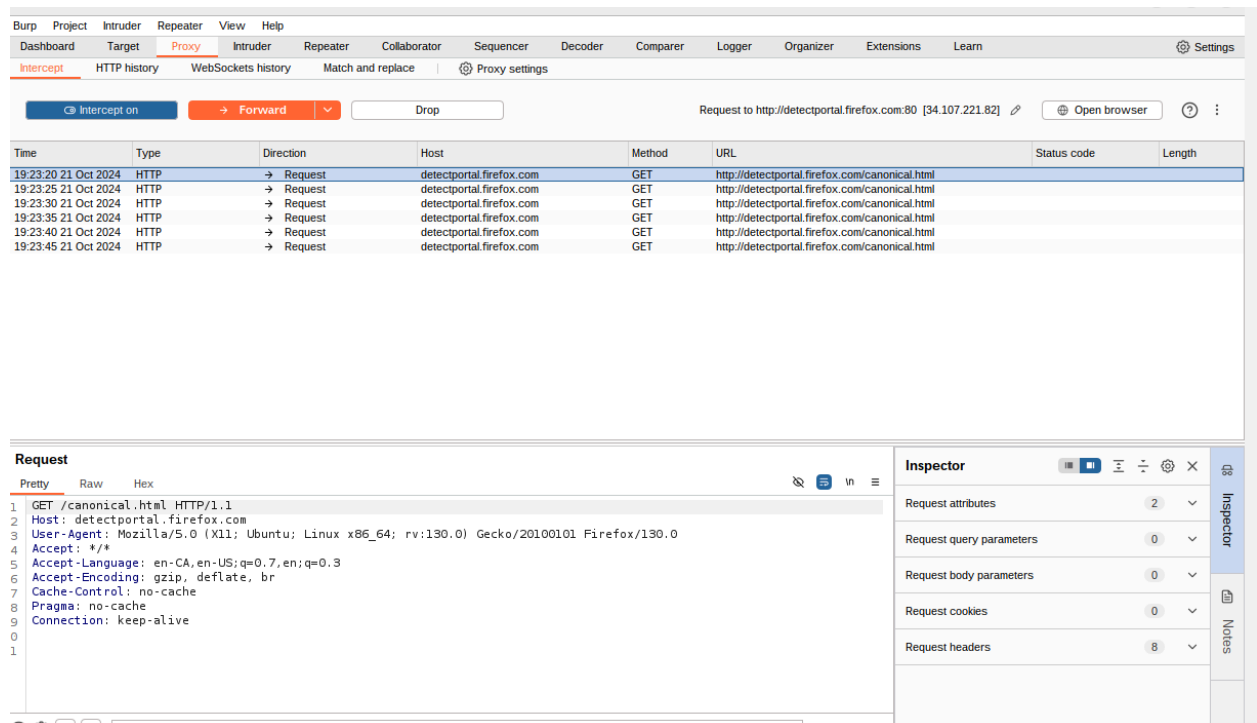


Una vez configurado solo nos haría falta encender nuestro proxy para comenzar a interceptar datos:



Burpsuite:

Dentro de burpsuite si ahora vamos a la sección Proxy > Intercept y activamos el botón donde pone Intercept off poniendolo en on empezaremos a interceptar conexiones como vemos en la imagen posterior:



Si a una de estas peticiones le damos click derecho y Send to intruder si nos vamos a la pestaña de intruder veremos que se nos ha abierto la query. Por ejemplo en este caso estamos enviando un usuario y una contraseña a un login:

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	POST /login HTTP/1.1				1	HTTP/1.1 404 Not Found			
2	Host: 10.0.1.51:3000				2	X-Powered-By: Express			
3	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0				3	Content-Type: application/json; charset=utf-8			
4	Accept: */*				4	Content-Length: 28			
5	Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3				5	ETag: W/"1c-ZEVVcvtFhxKX/QUvVKqKxwGbbNA"			
6	Accept-Encoding: gzip, deflate, br				6	Date: Mon, 30 Sep 2024 15:42:07 GMT			
7	Referer: http://10.0.1.51:3000/login.html				7	Connection: keep-alive			
8	Content-Type: application/json				8	Keep-Alive: timeout=5			
9	Content-Length: 47				9				
10	Origin: http://10.0.1.51:3000				10	{			
11	Connection: keep-alive					"message": "User not found"			
12	Priority: u=0					}			
13									
14	{								
	"username": "usuario",								
	"password": "contraseña"								
	}								

A la izquierda de la pantalla hay un boton para añadir variables con el que podremos cambiar los datos de usuario y contraseña al realizar la query.

Extensions Learn Settings

Start attack

Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

0 highlights Clear

Length: 317

Memory: 101.4MB

También tendremos que elegir que tipo de ataque vamos a utilizar en la sección de arriba:

Choose an attack type

Attack type: **Sniper**

Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

Pitchfork
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on.

Cluster bomb
This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.

Buttons: Add §, Clear §, Auto §, Refresh

Start attack

Tenemos 4 tipos de ataque distintos:

-Sniper y battery ram iteran sobre 1 dato

-Pitchfork y clusterbomb iteran sobre varios datos (Clusterbomb interesa más ya que la otra compara las listas solo en orden y no todos los datos).

Una vez seleccionado esto en la sección de payloads introduciremos la lista o listas sobre las que se va a iterar:

Positions **Payloads** Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: **1** Payload count: 111

Payload type: **Simple list** Request count: 111

Start attack

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Buttons: Paste, Load ..., Remove, Clear, Deduplicate, Add

Enter a new item

Add from list ... [Pro version only]

Una vez hecho todo esto lanzamos el ataque y esperamos el resultado.