



HACKING ÉTICO

Unidad 2. Actividad 2



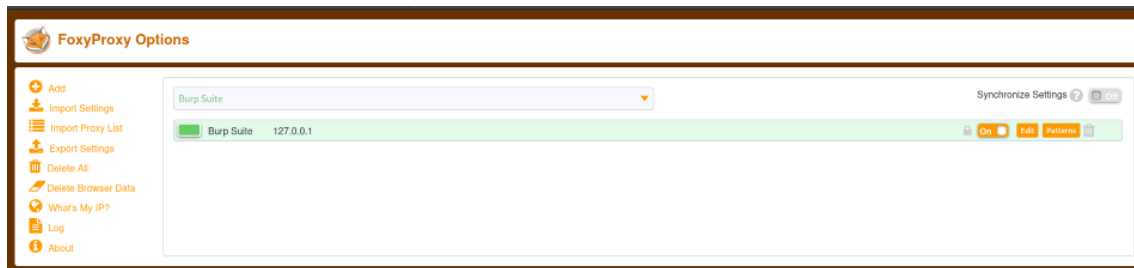
23 DE OCTUBRE DE 2023
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

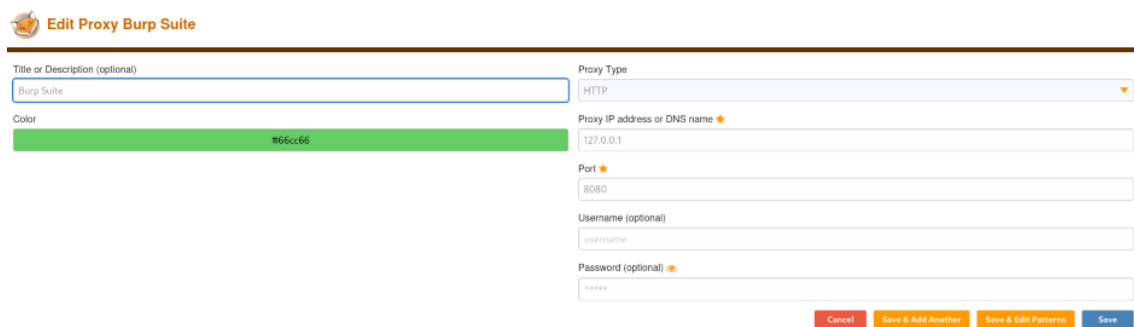
Ejercicio 1	2
Ejercicio 2	2
Ejercicio 3	4
Ejercicio 4	5

Ejercicio 1. Configura Firefox para usar Burpsuite.

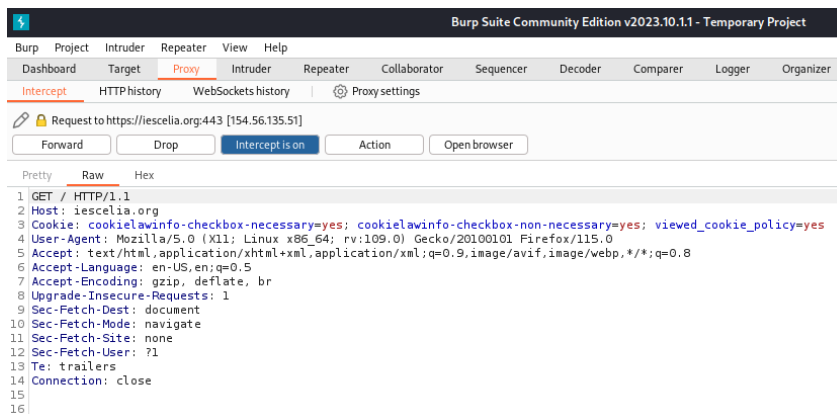
Lo primero que vamos a hacer es instalarlo(esto lo hicimos en clase por eso ya esta configurado):



Ahora lo configuramos y lo activamos:



Por ultimo, añadimos el certificado en Firefox y usamos Burpsuite en iescelia.org:



Ejercicio 2. Navegas desde un televisor...

La siguiente web muestra qué navegador estás usando gracias a cierta cabecera HTTP... ¿Qué cabecera es?

La cabecera de User-agent.

Primero busco en la página que nos ha proporcionado Pablo el tipo de televisor que nos pide:

Dalvik/2.1.0 (Linux; U; Android 5.1.1; BRAVIA 4K 2015 Build/LMY48E.S265)

This user agent string belongs to Dalvik browser running on Android OS. The browser is developed by Google Inc and renders web pages using the WebKit engine.

Browser	
Name	Dalvik
Version	2.1
Architecture	32-bit
Developer	Google Inc
Rendering Engine	WebKit
Type	Application

Platform	
Name	Android
Version	5.1
Architecture	32-bit
Developer	Google Inc

Device	
Name	Bravia 4K 2015
Type	TV
Pointer	mouse
Vendor	Sony
Brand	Sony

Ahora simplemente cambio el user agent que tengo por el que me sale en la página:

```
Request to https://whatmyuseragent.com:443 [168.235.86.235]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /maps?lat=40.9018&lon=-4.0069 HTTP/2
2 Host: whatmyuseragent.com
3 Cookie: PHPSESSID=c95db8351ff6c6d3da9581b4fe1f0681; _ga_Z9VC120307=GS1.1.1698137465.1.1.1698139380.0.0.0; _ga=GA1.1.1985775599.1698137466;
   _gads=ID=119932c3357fcc0a-2299a2256ee000ae:T=1698137469:RT=1698139324:S=ALNI_MbP4qzVRFcuroDZ-BCDLRfdiskWlQ; __gpi=
   UID=00000cc04ca9c559:T=1698137469:RT=1698139324:S=ALNI_MZQG3YQP6YVTt2moXp62N0nLF0E1A
4 User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; BRAVIA 4K 2015 Build/LMY48E.S265)
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://whatmyuseragent.com/
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

Ahora como vemos hemos puesto otro user agent:

Your User Agent

Dalvik/2.1.0 (Linux; U; Android 5.1.1; BRAVIA 4K 2015 Build/LMY48E.S265)

Copy

Your IP Address

77.225.197.13

Location

Country Name: Spain

City Name: San Ildefonso

Latitude: 40.9018

Longitude: -4.0069

Y por tanto nos saldrá el televisor que nos pide el ejercicio:

Opera System Information	
Name:	Android TV
Version:	5
Platform:	unknown

Device Information	
Name:	Bravia 4K 2015
Brand:	Sony
Type:	Tv

Ejercicio 3

Primero usamos investigamos y se puede cambiar en accept-lenguaje, despues vamos a www.google.es y cambiamos el accept-lenguaje en burp por el idioma chino:

The screenshot shows the Burp Suite interface. At the top, the 'Intercept' tab is active, showing a request to `https://www.google.es:443 [142.250.200.131]`. The 'Intercept is on' button is highlighted. Below the request details, the 'Raw' tab is selected, displaying the raw HTTP request. The request headers are as follows:

```
1 GET / HTTP/2
2 Host: www.google.es
3 Cookie: AEC=Ackid1R3XKBb5AR620GAMu2ikCF6w0qV02A2ppt7hRhRi2sEY9SuvLcFiEY; __Secure-ENID=
  15_SE=SKxiui4ghwCXN0sNw17rpLF7rdCqf4mmuqY7t6b2FAfsU_eEb1Yazb6jhd3Mbu_XLeaRowF4GABn4LneN8pGqgRHet rWv8B2XU0Bru_VaOdGRRl2rQweOHREHzk14TpiL3029
  j8r6X0iikRZx50kYLiJvM5IKJbYG0i9fgrnSIA; CONSENT=PING+354; SOCS=CAESHA8BehJnd3NfmjAyMzEwMTItMF95QzQaAmVzIAEaBgiAwLypBg
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: zh-Hant,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14
15
```

Below the request details, the Google homepage is visible in Chinese. The search bar is at the top, and the Google logo is in the center. The text 'Google 搜尋' and '好手幫' are visible. At the bottom, there are links for 'Google 提供: Español català galego eslovak'.

Ejercicio 4. Cabecera Host (NO FUNCIONA)

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: 16.45.226.165
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Request to http://16.45.226.165:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: www.bmw.es
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Ahora editamos el Host por www.bmw.es

Burp Suite Community Edition v2023.10.11 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

14 x 15 x 16 x 17 x +

Send Cancel < >

Target: http://16.45.226.165

Request

Pretty Raw Hex

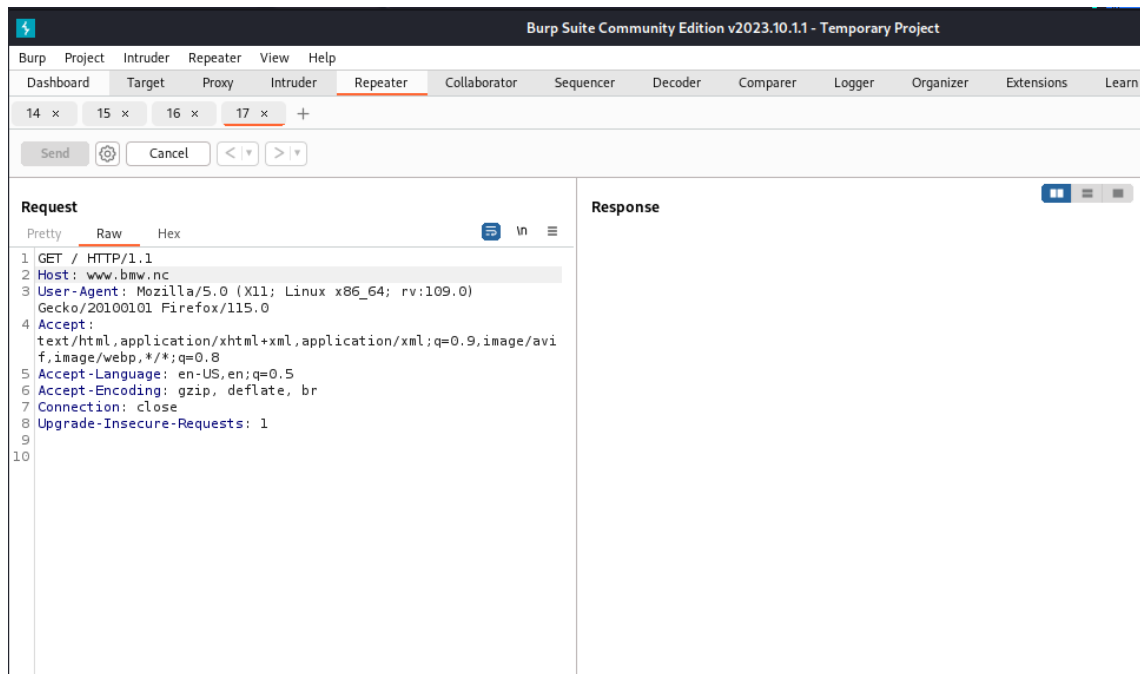
```
1 GET / HTTP/1.1
2 Host: www.bmw.es
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Response

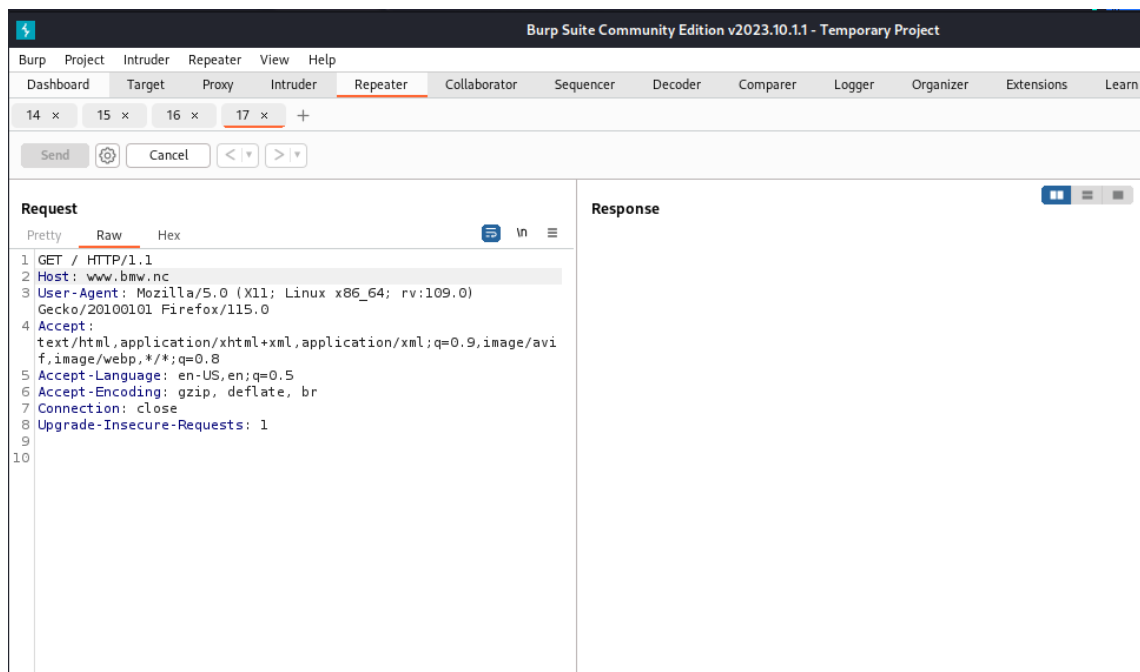
Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers

Ahora por www.bmw.nc



Ahora por www.bmw.sk



PREGUNTAR NO ENTIENDO

NO FUNCIONA