HACKING ÉTICO

Unidad 2. Actividad 2

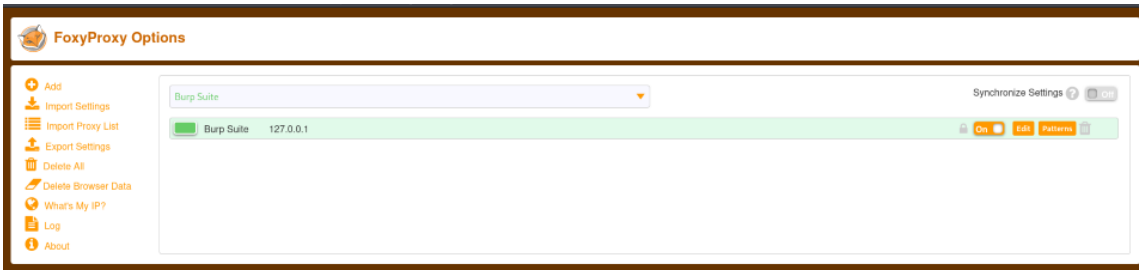
23 DE OCTUBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

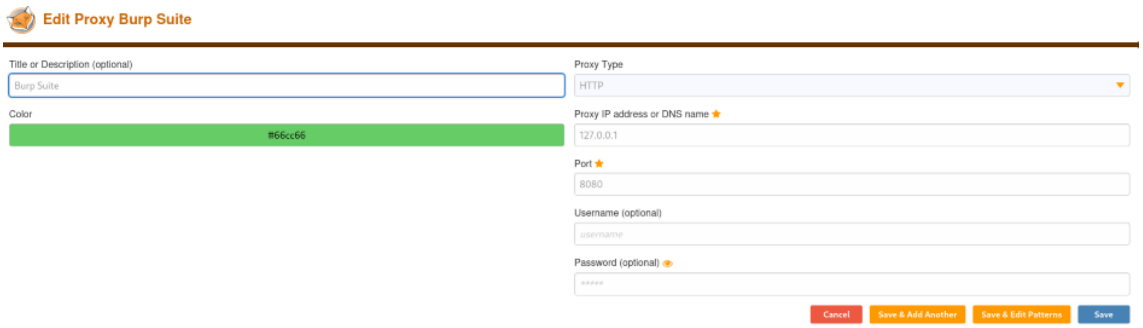
Índice

Ejercicio 1. Configura Firefox para usar Burpsuite.

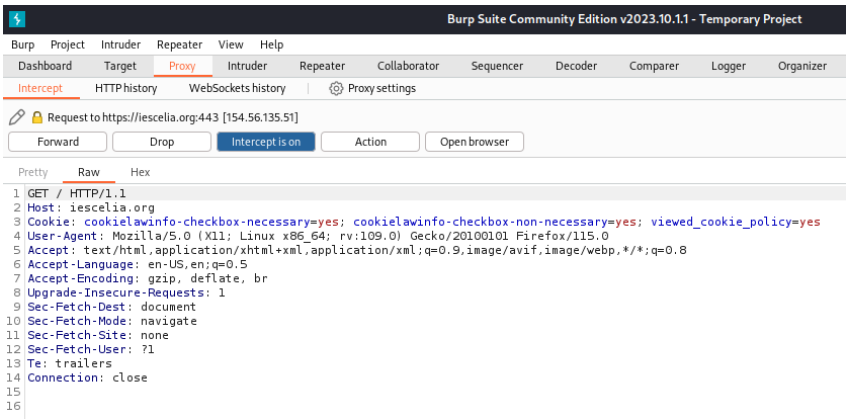
Lo primero que vamos a hacer es instalarlo(esto lo hicimos en clase por eso ya esta configurado):



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)

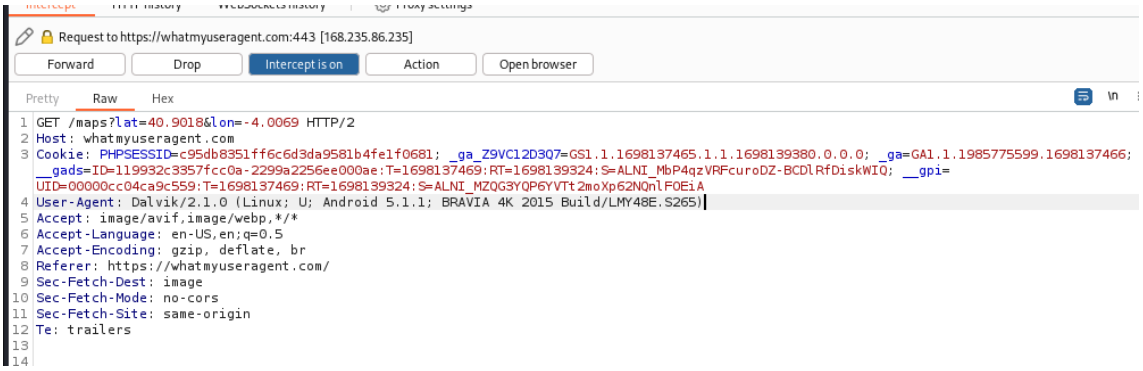
This user agent string belongs to Dalvik browser running on Android OS. The browser is developed by Google Inc and renders web pages using the WebKit engine.

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

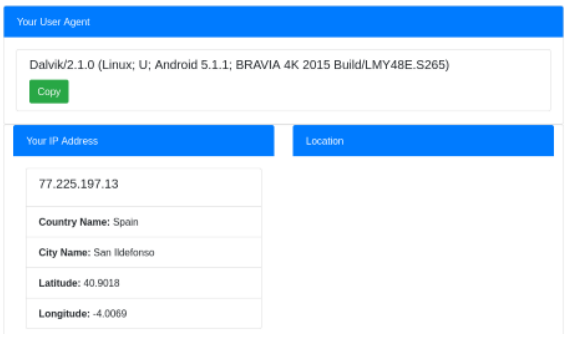
Platform	
Name	Android
Version	5.1
Architecture	32-bit
Developer	Google Inc

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:



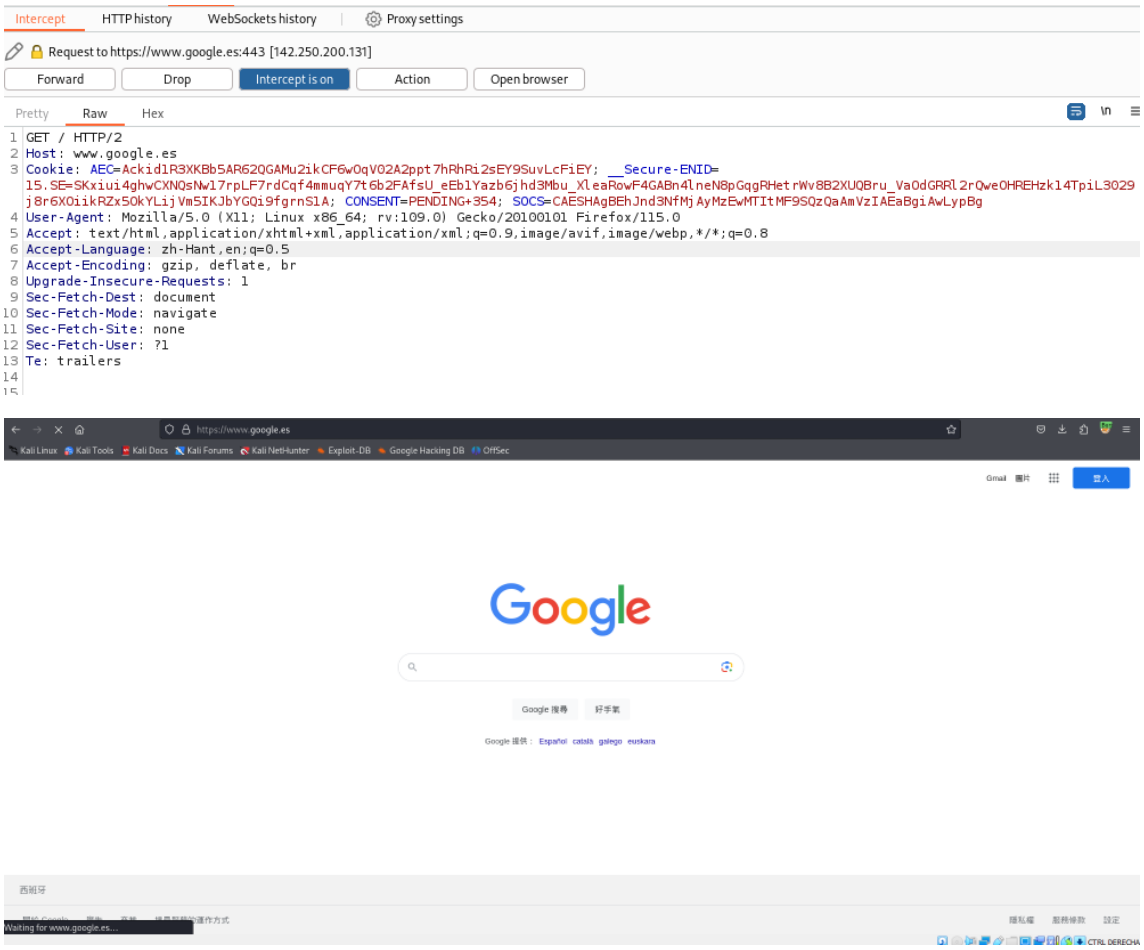
Ahora como vemos hemos puesto otro user agent:



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

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:

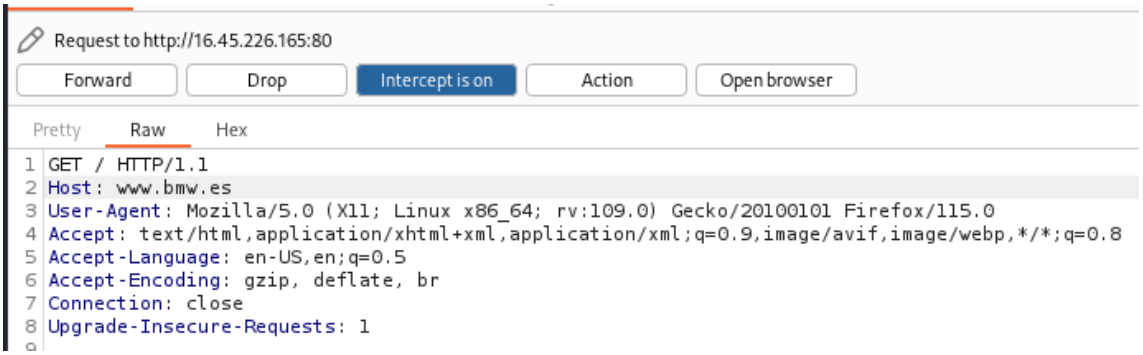


Ejercicio 4. Cabecera Host (NO FUNCIONA)

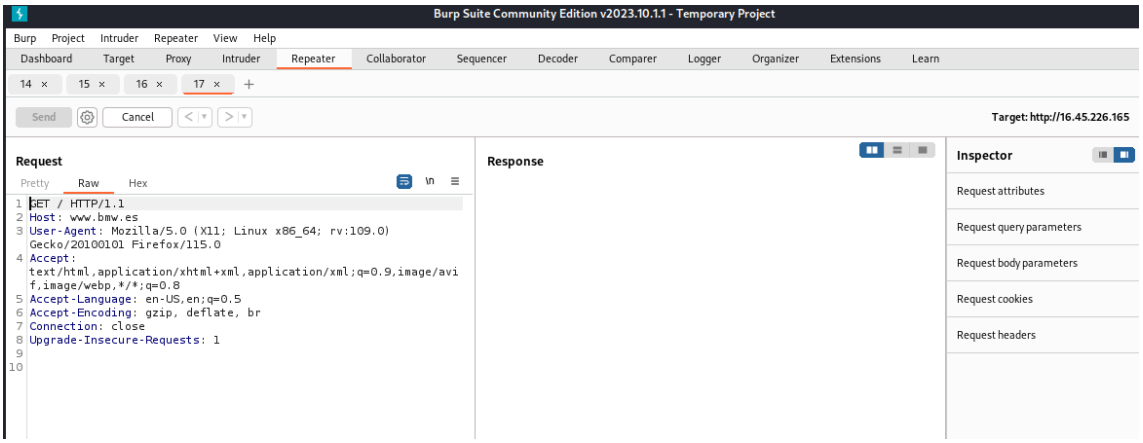
Request

Pretty Raw Hex

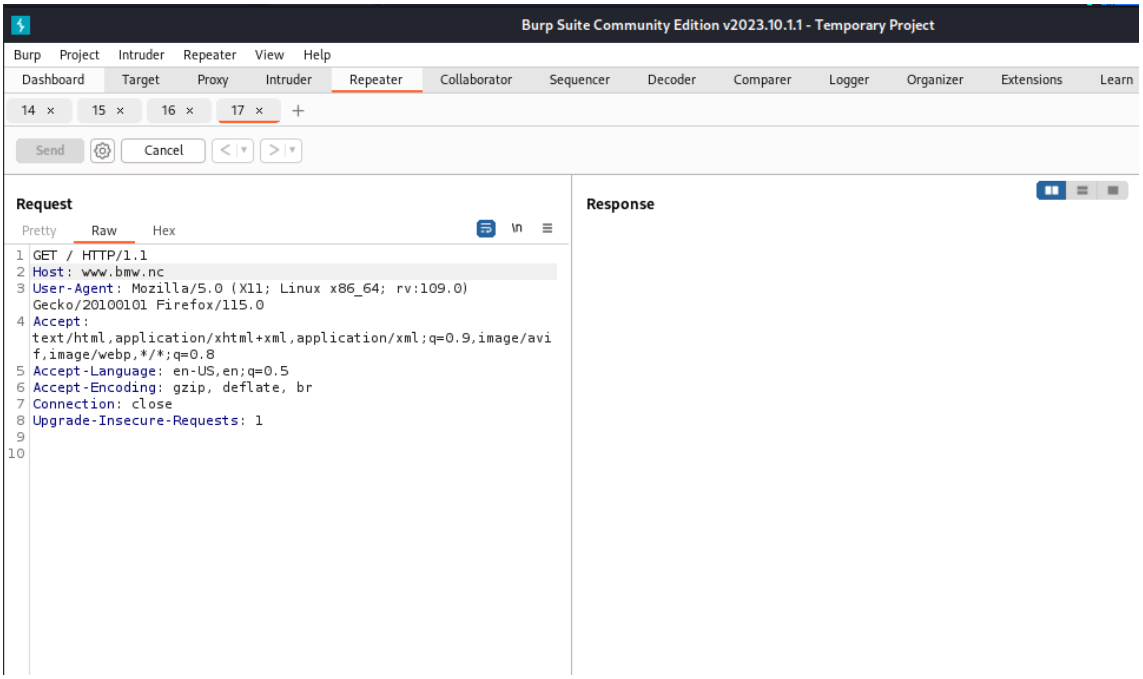
```
1 GET / HTTP/1.1
2 Host: 16.45.226.165
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br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



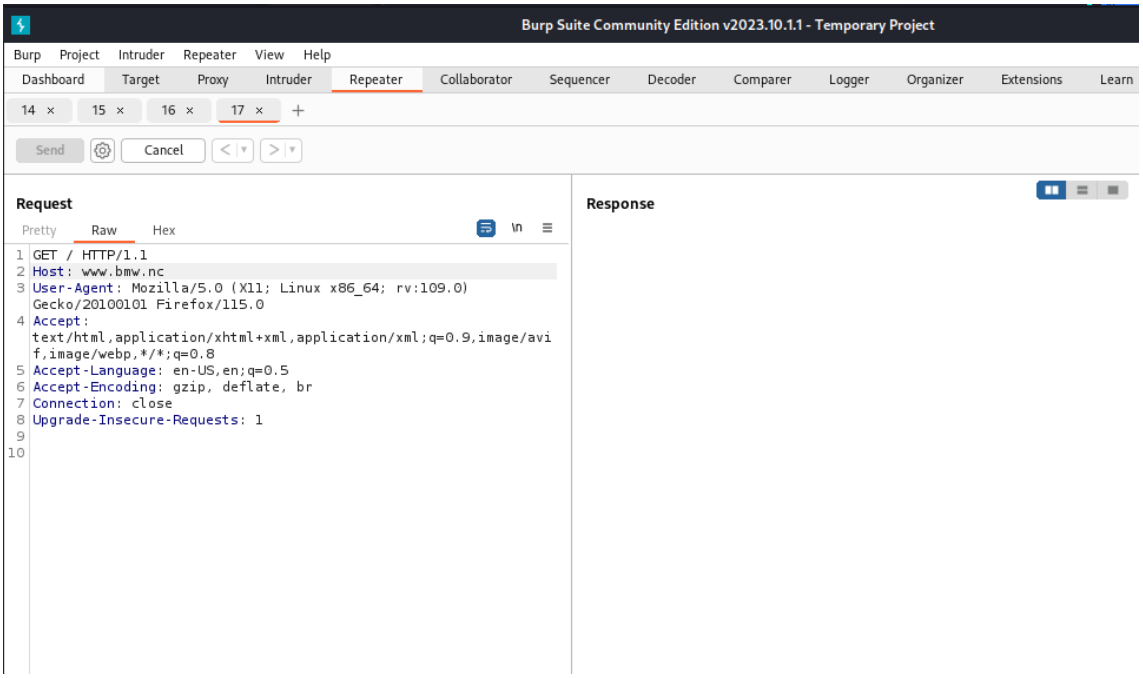
Ahora editamos el Host por www.bmw.es



Ahora por www.bmw.nc



Ahora por www.bmw.sk



PREGUNTAR NO ENTIENDO

NO FUNCIONA