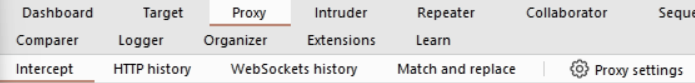
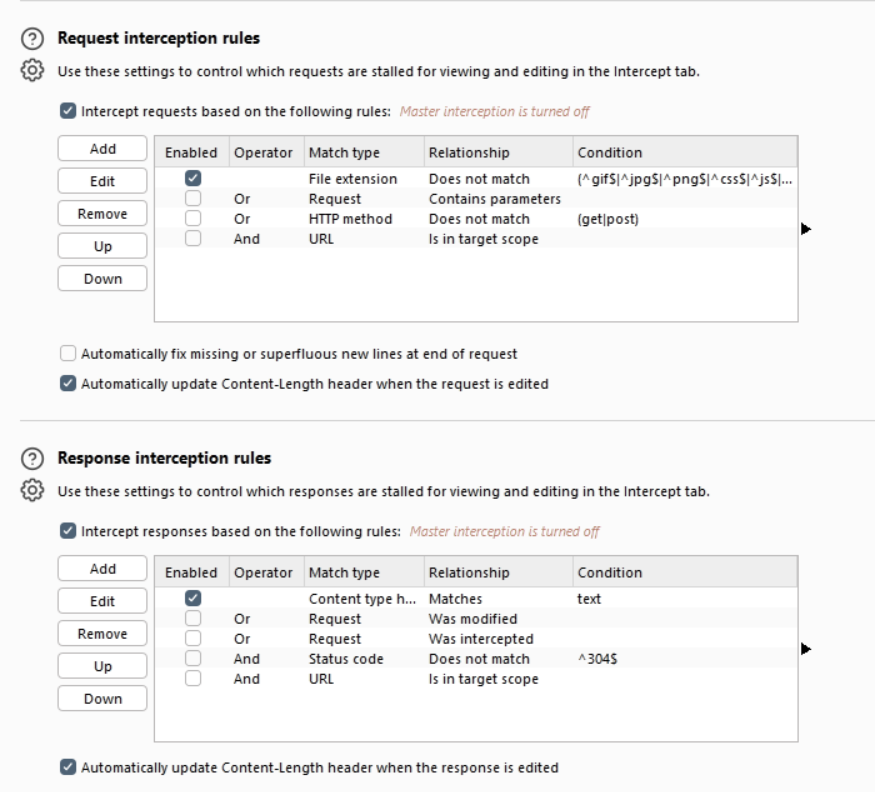
1. Acceder a Mutillidae II

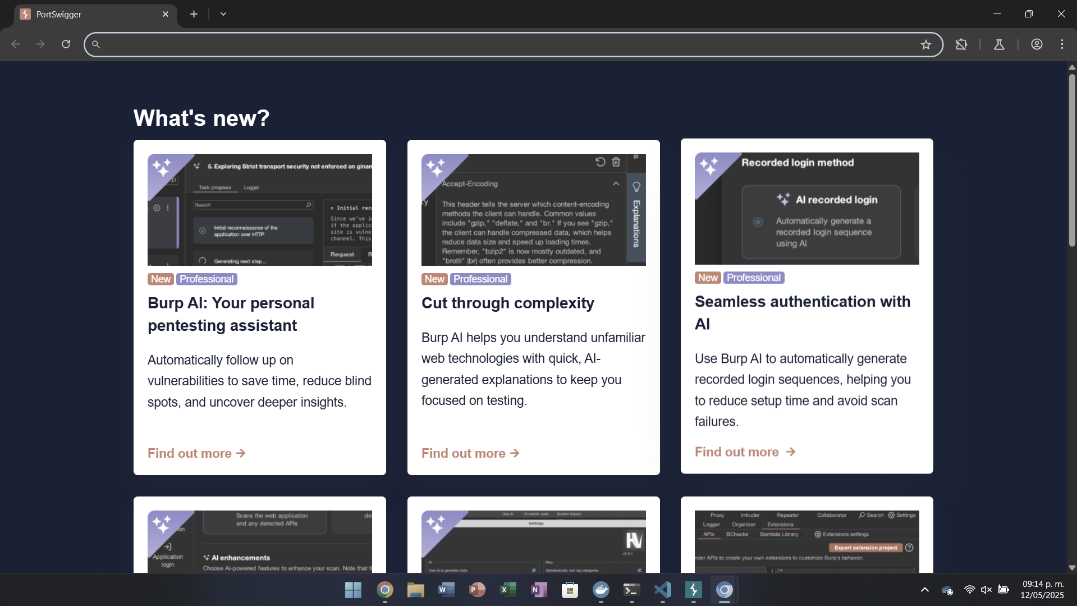
En la aplicación de Burpsuit nos dirigimos a Proxy > Configuración de Proxy.

[](https://github.com/Jsoto0404/Hacking_etico/blob/main/Pruebas%20de%20Aplicaciones%20Web/Burp%20Suite/Actividad%201/image-1.png)

Habilitamos las opciones de “Interceptar respuestas basadas en las siguientes reglas”.

[](https://github.com/Jsoto0404/Hacking_etico/blob/main/Pruebas%20de%20Aplicaciones%20Web/Burp%20Suite/Actividad%201/image.png)

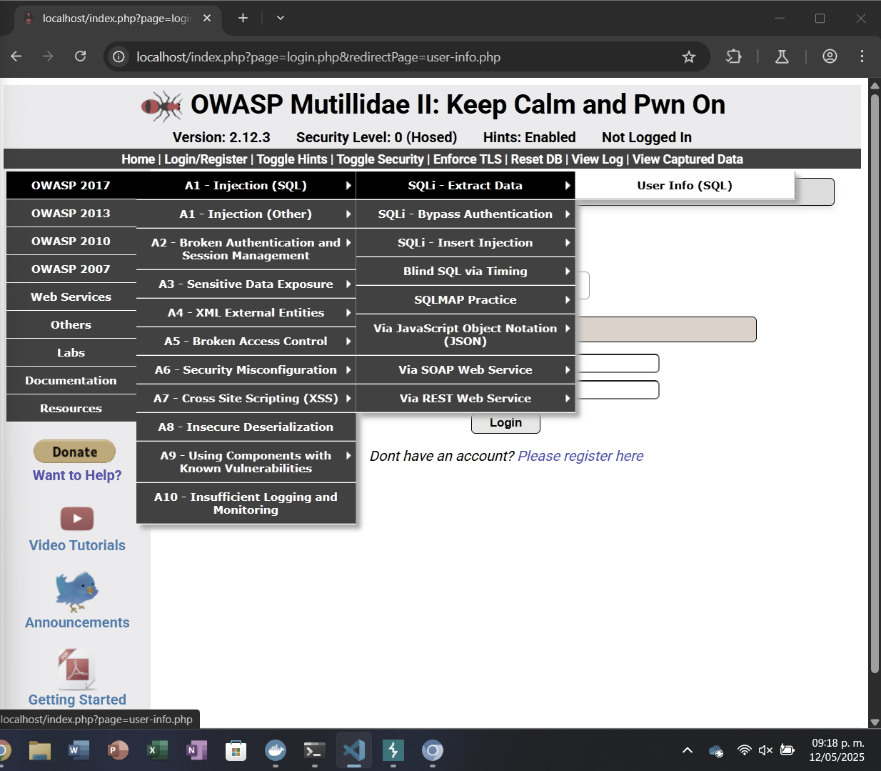
Se cierra la configuración del proxy y abrimos el open browser

[](https://github.com/Jsoto0404/Hacking_etico/blob/main/Pruebas%20de%20Aplicaciones%20Web/Burp%20Suite/Actividad%201/image-2.png)

1. Registro del usuario

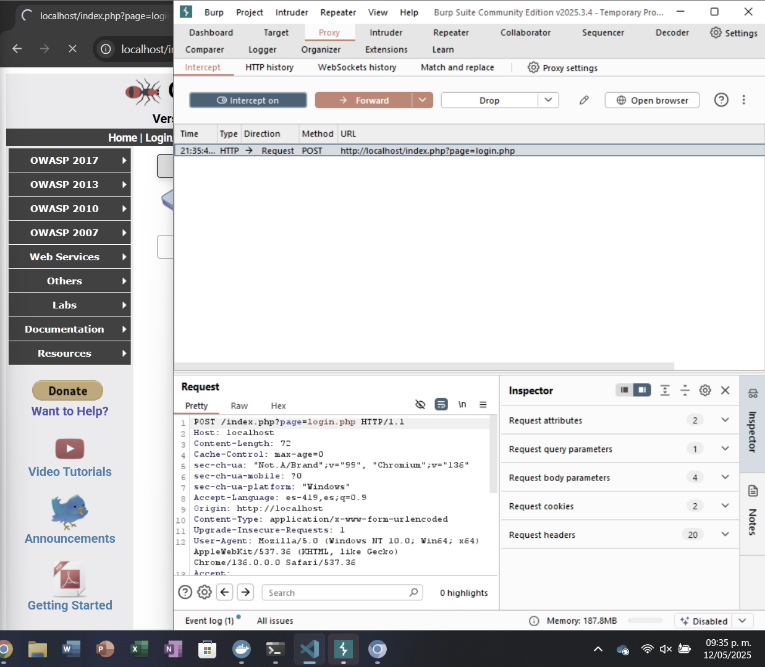
Se ingresa a localhost, accesamos a Owasp 2017> AI - Inyección (SQL) > SQLi Extract Data > User Info (SQL) > Regístrese aquí. 2.2.- Creamos un usuario con contraseña.

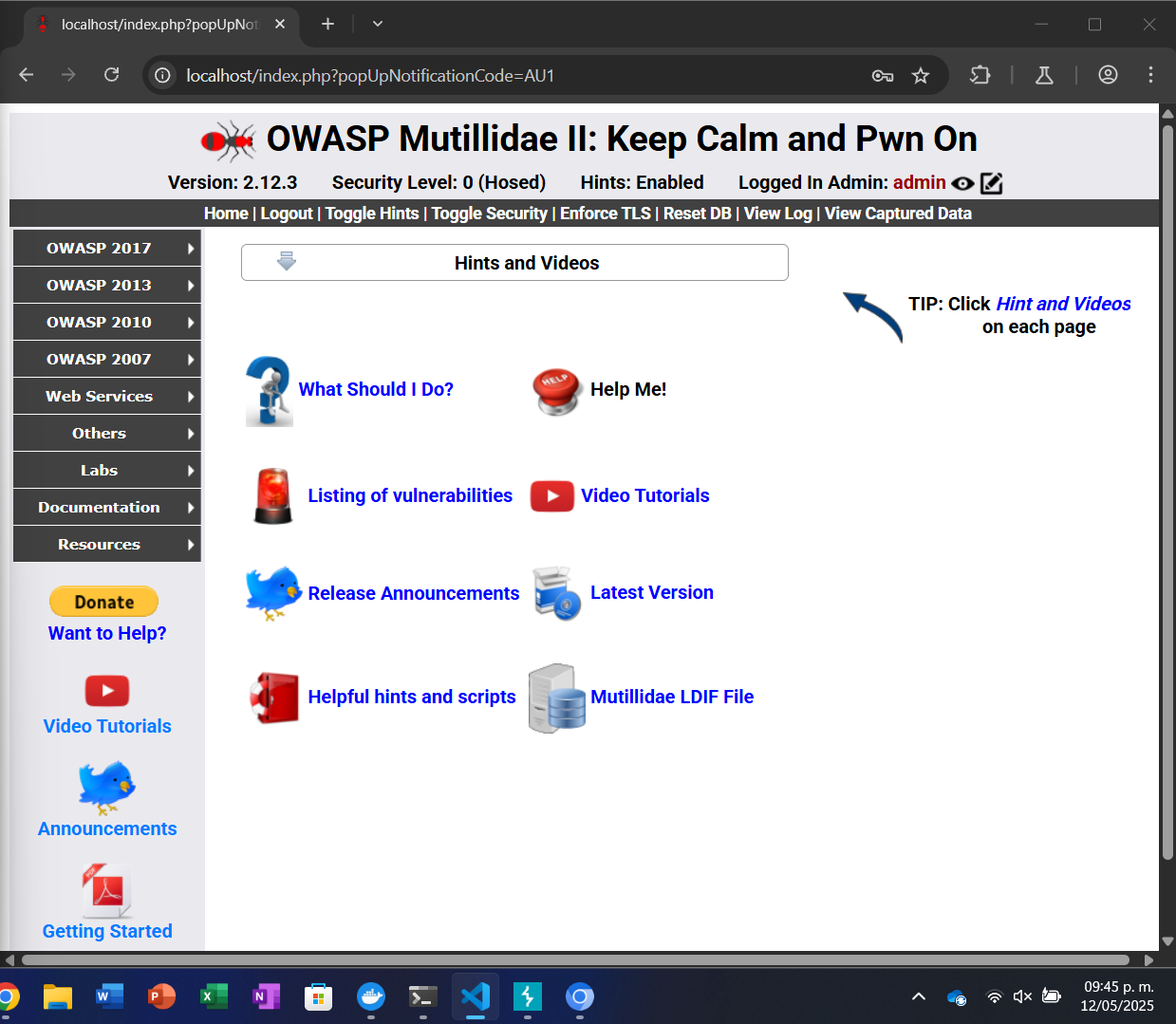
Después de seleccionar Create Account, regresamos a User Lookup (SQP) ingresamos los datos de la nueva cuenta y damos clic en View Account Details.

[](https://github.com/Jsoto0404/Hacking_etico/blob/main/Pruebas%20de%20Aplicaciones%20Web/Burp%20Suite/Actividad%201/image-3.png)

Leila

En BurpSuit activamos la intercepción en la cual, cada vez que se envie una consulta, el sistema lo interceptará y nos mostrarán los datos que se están enviando al servidor.

[](https://github.com/Jsoto0404/Hacking_etico/blob/main/Pruebas%20de%20Aplicaciones%20Web/Burp%20Suite/Actividad%201/image-7.png) 3.2

 3.5.- Cambiamos el UID que en este caso de 42 pasa a 1, aplicamos cambios y damos forward. [](https://github.com/Jsoto0404/Hacking_etico/blob/main/Pruebas%20de%20Aplicaciones%20Web/Burp%20Suite/Actividad%201/image-10.png)