**OWASP ZAP**

Curso: Automatizacion de Pruebas

huRTADO PONCE, DILIAN ANABEL

MAMANI CAYO, MARIO

Rojas Salinas, ZARELA

Repositorio: https://github.com/zareliux/jb\_vulnerability\_tarea

2020

Contenido

[**1.** **Abrir OWASP ZAP** 1](#_Toc57126412)

[**2.** **Configurar el proxy** 3](#_Toc57126413)

[**3.** **Navegar sobre https://todoist.com** 5](#_Toc57126414)

[**4.** **Administrar plugins de prueba** 9](#_Toc57126415)

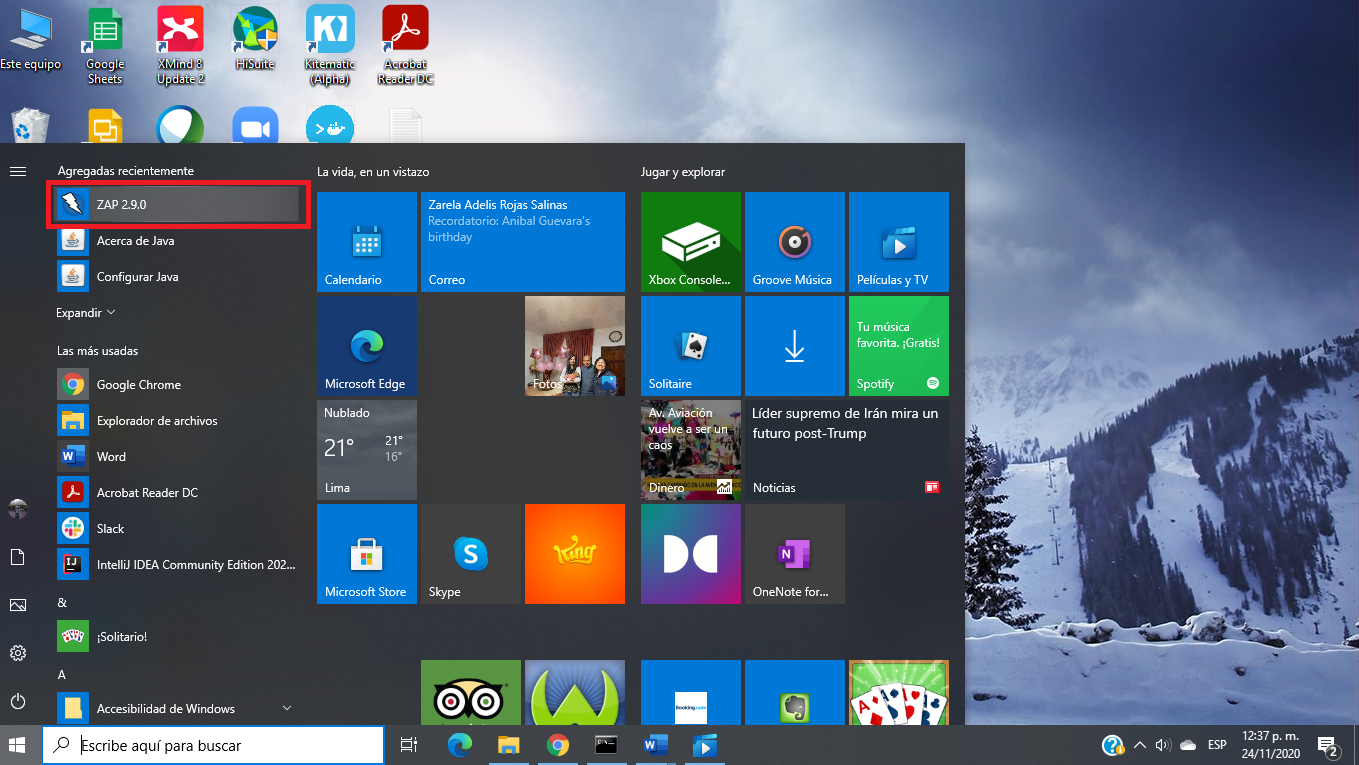
[**5.** **Filtrar según tecnologías** 10](#_Toc57126416)

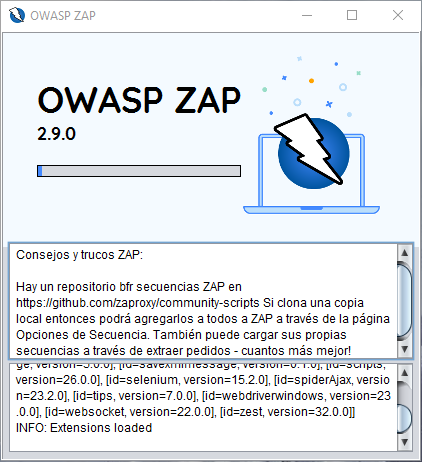
[**6.** **Ejecutar el Escaneo de vulnerabilidades** 11](#_Toc57126417)

[**7.** **Genera Reporte** 13](#_Toc57126418)

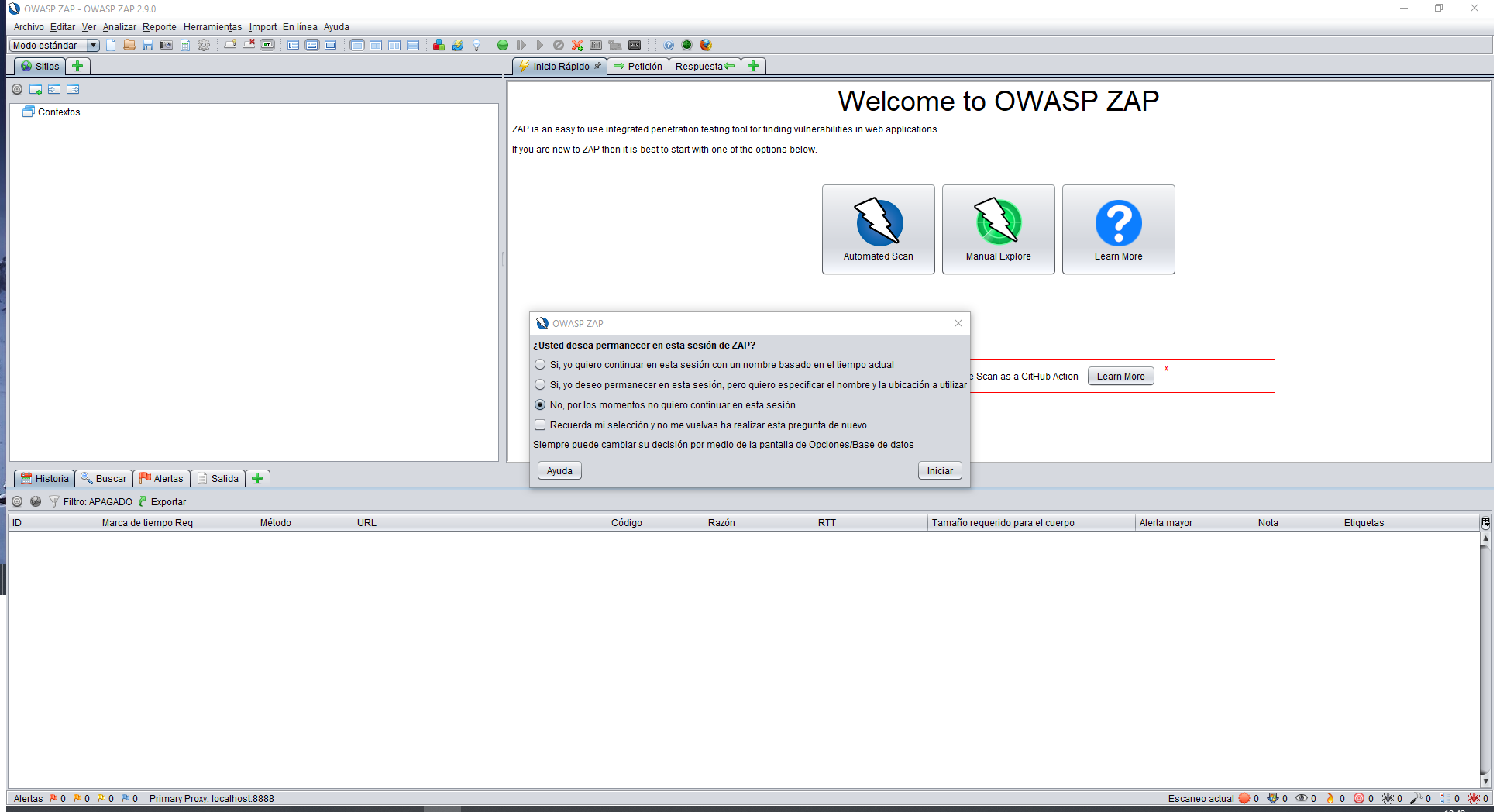
# **Abrir OWASP ZAP**

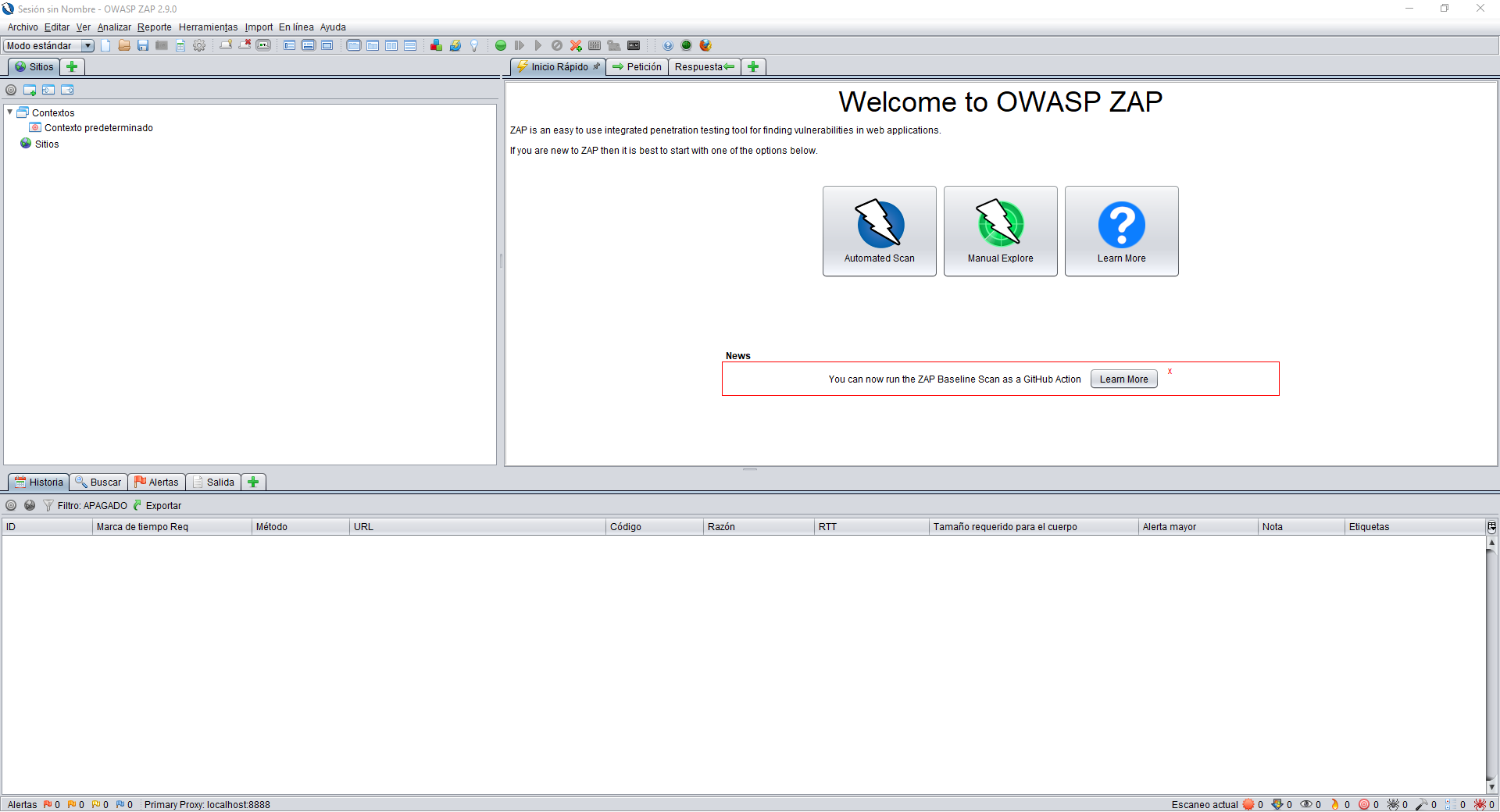
* 1. Hay muchas formas de abrir el OWASP ZAP en esta ocasión estamos ingresando por el ícono del menú de Inicio





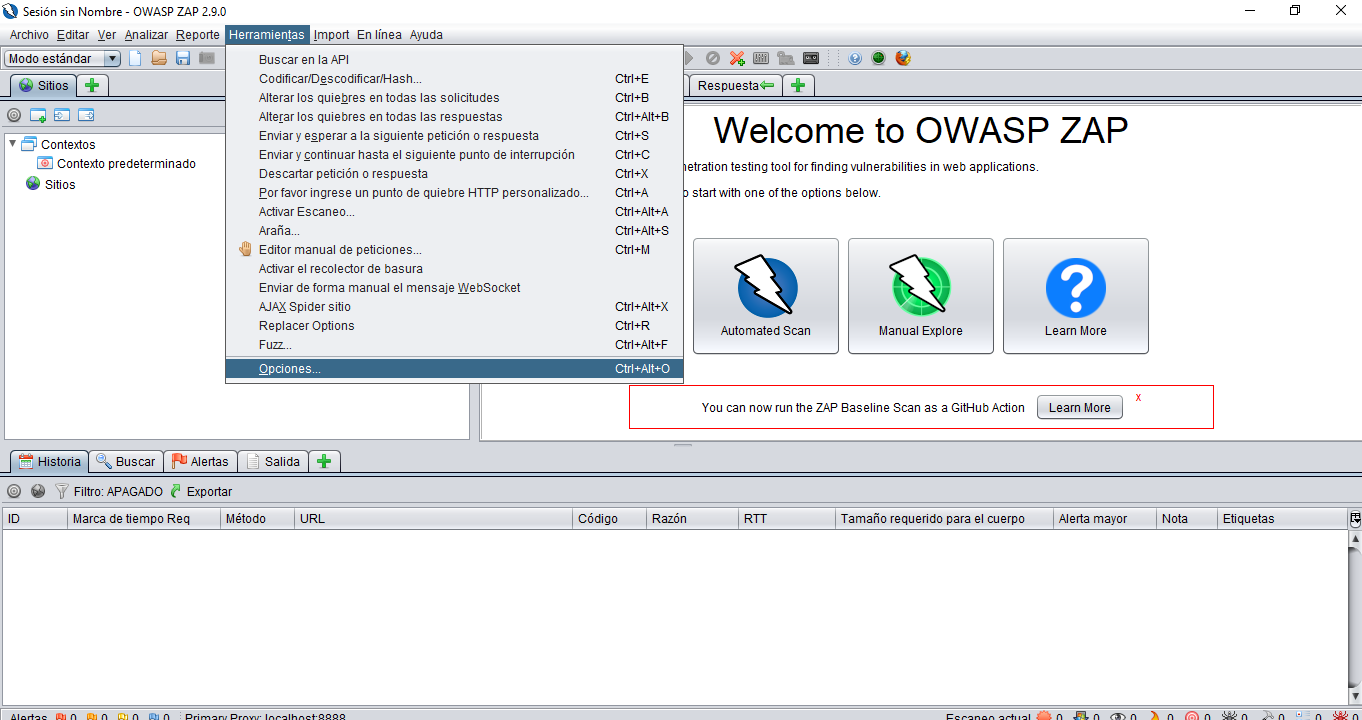
* 1. Una vez que abre el aplicativo. Cerrar el dialogo que se muestra con la “X”



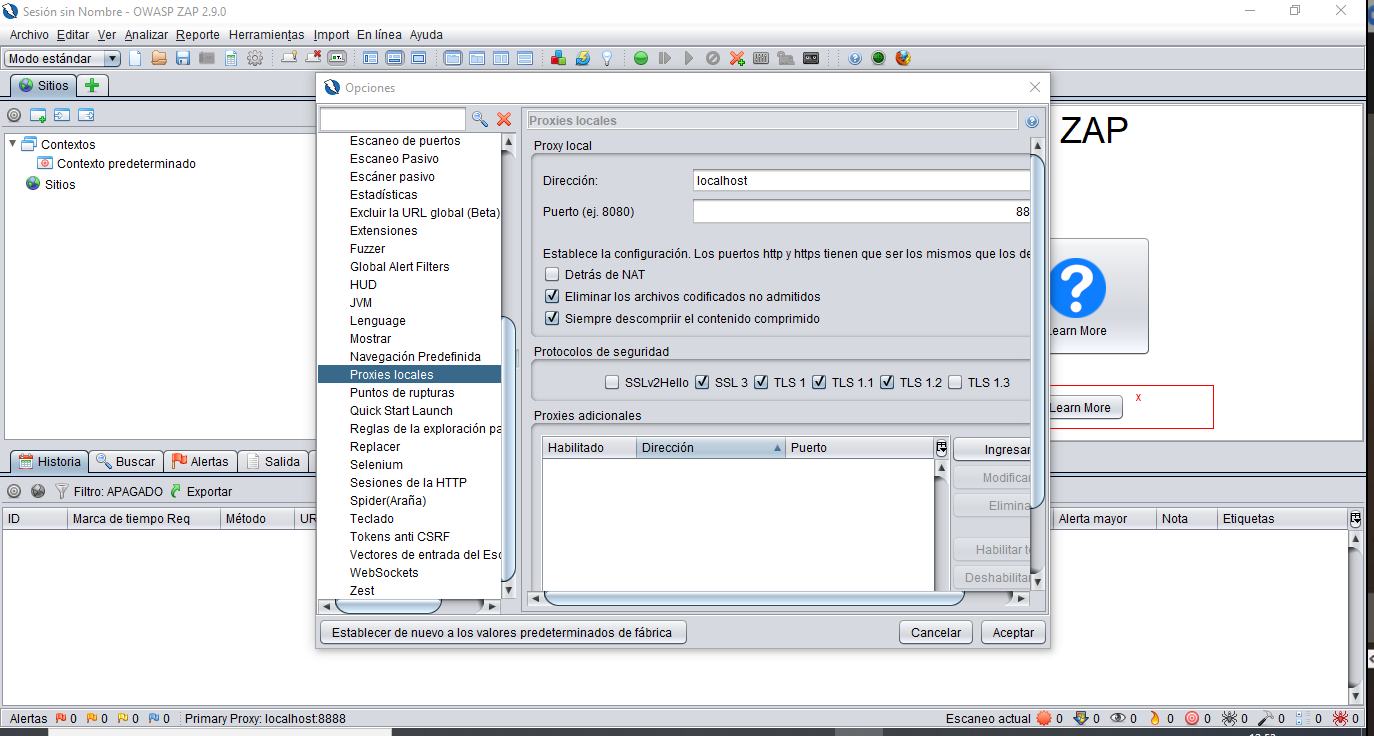


# **Configurar el proxy**

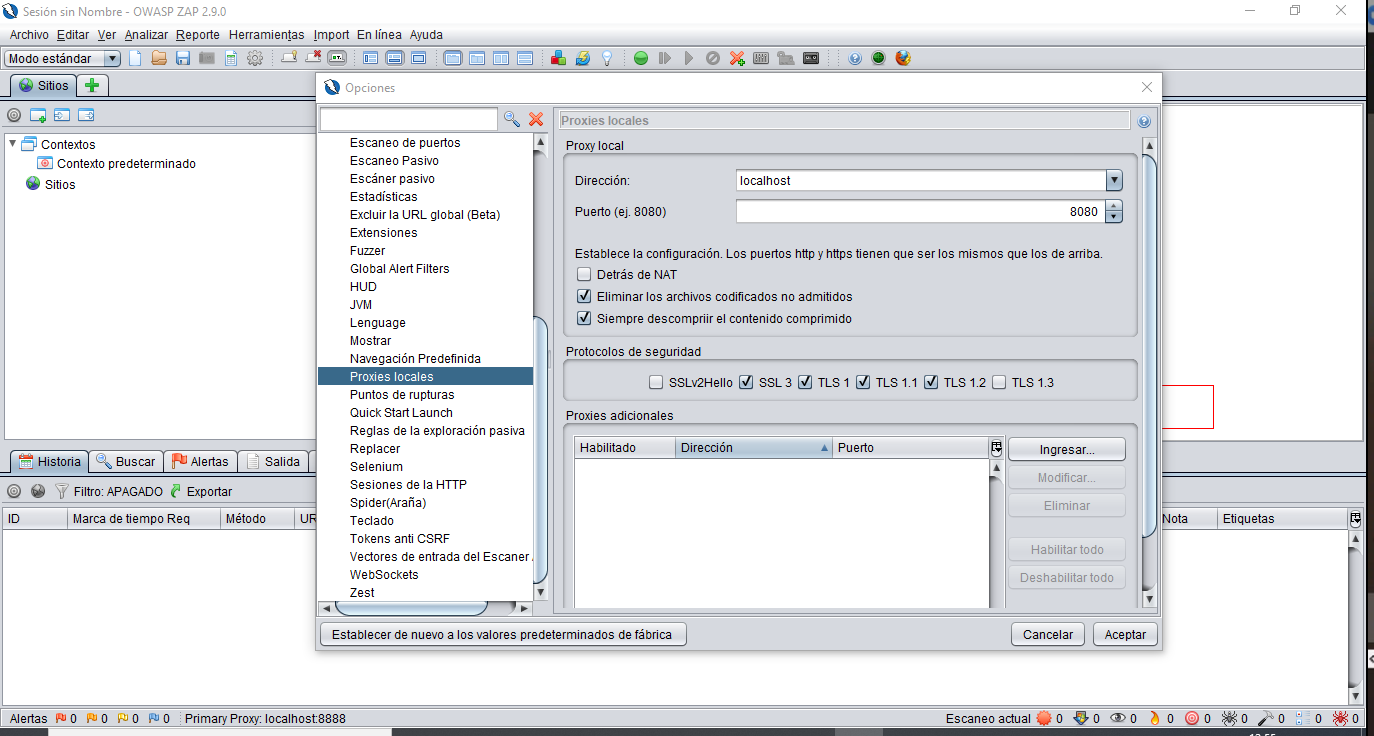
* 1. Seleccionar en menú la opción de Herramientas y ahí seleccionar opciones.



* 1. En la venta de opciones buscar la opción Proxies locales.

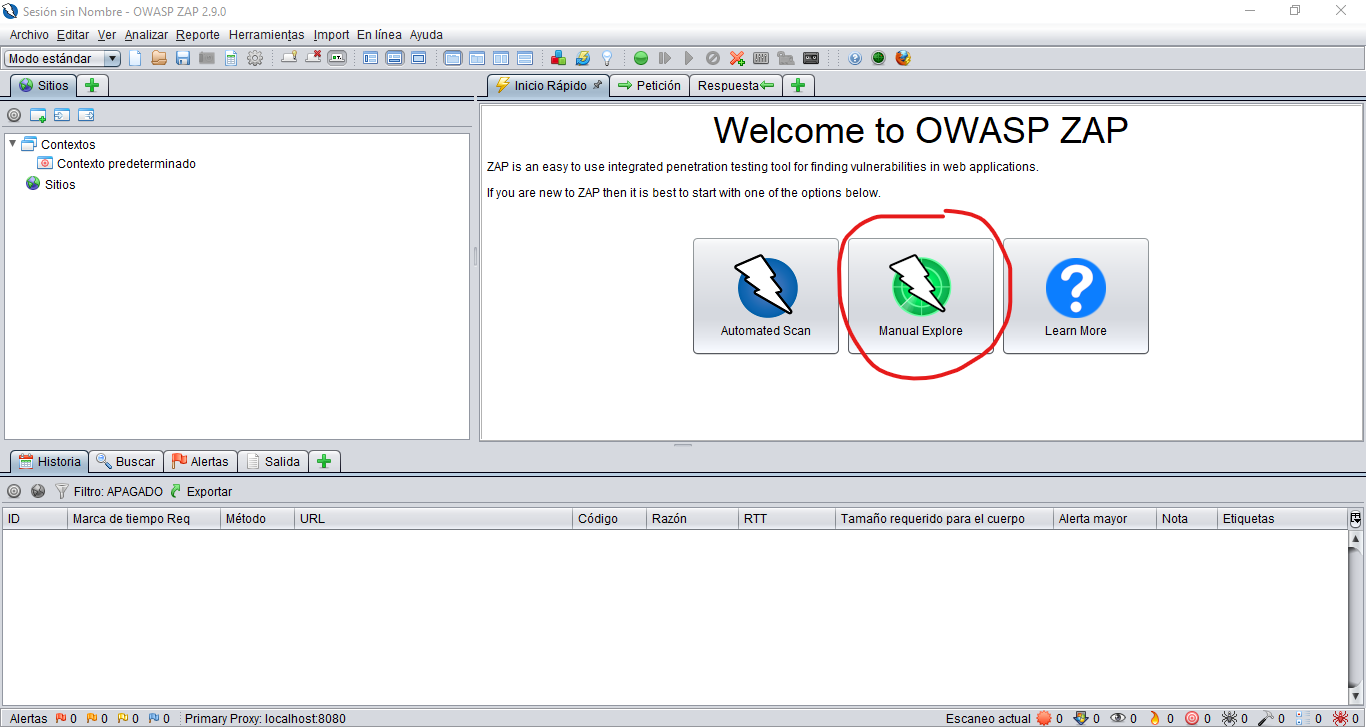


* 1. En el puerto configurar el puerto 8080 y seleccionar Aceptar.

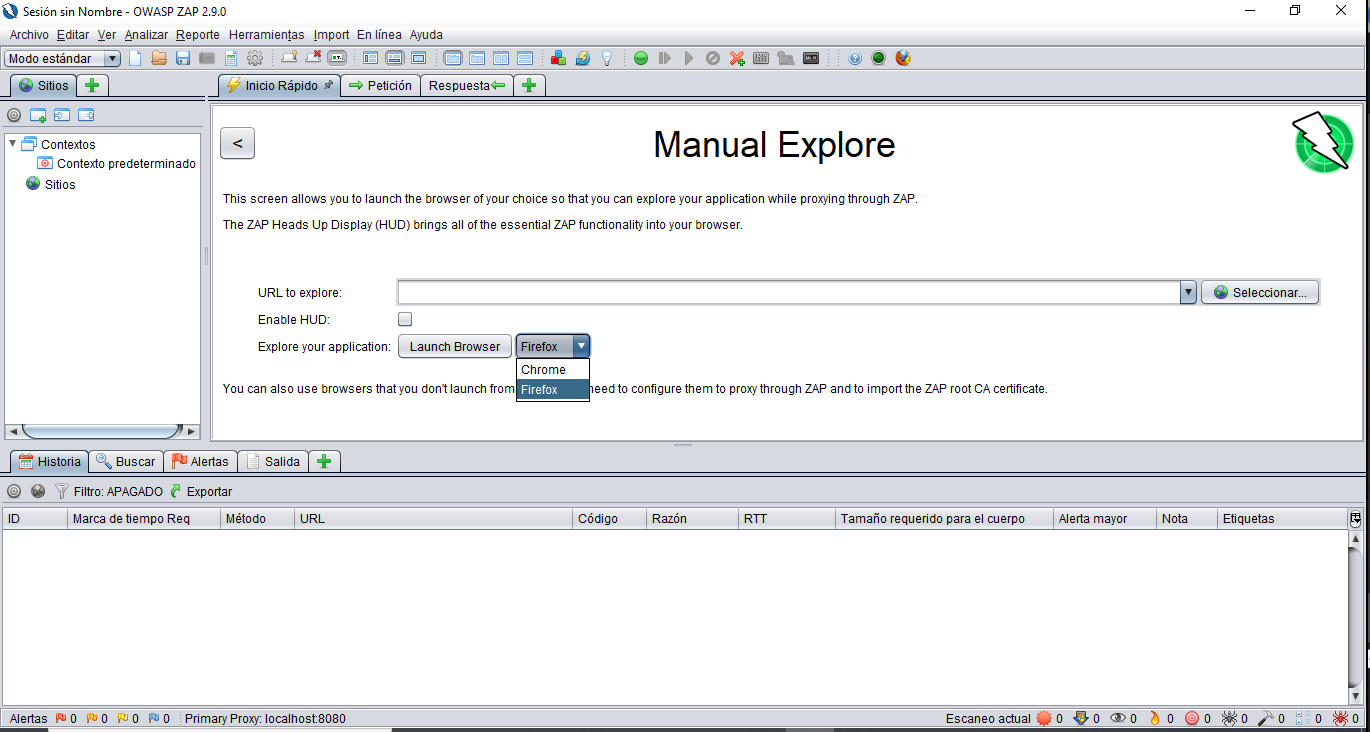


# **Navegar sobre** **https://todoist.com**

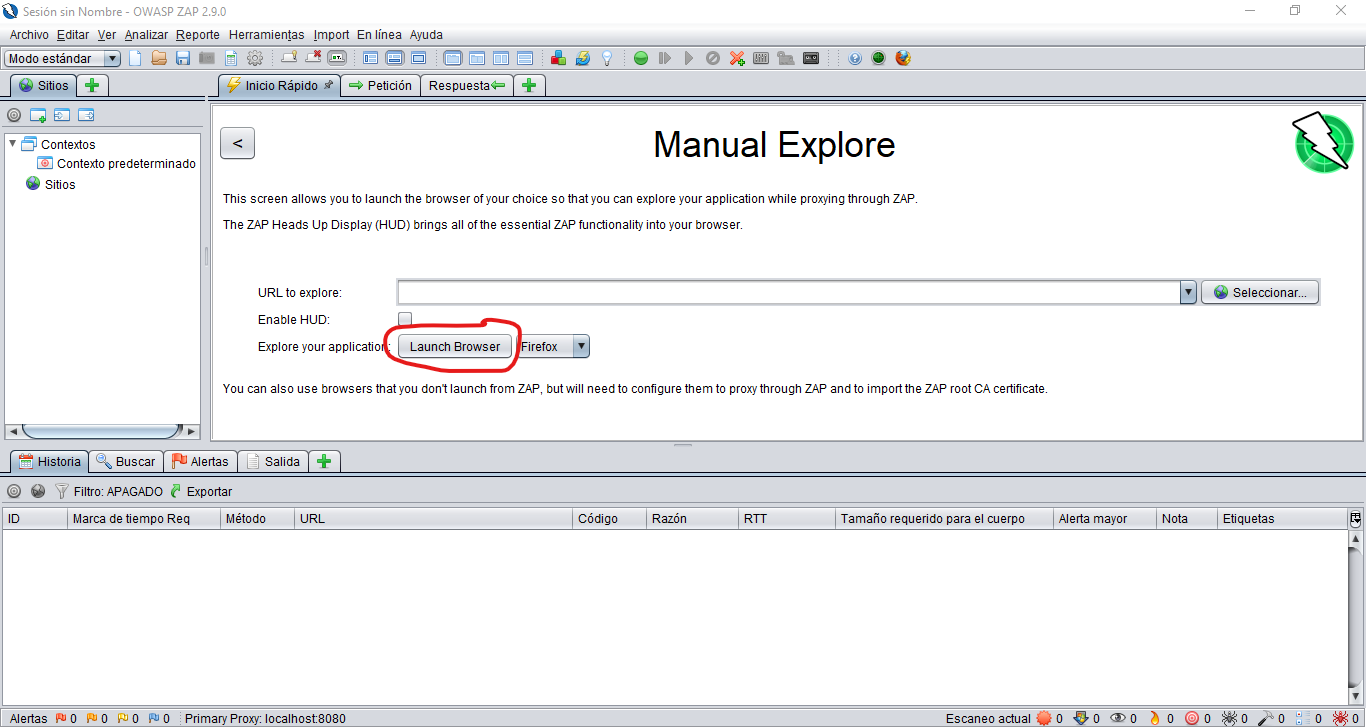
* 1. En El inicio rápido seleccionar Manual Explore

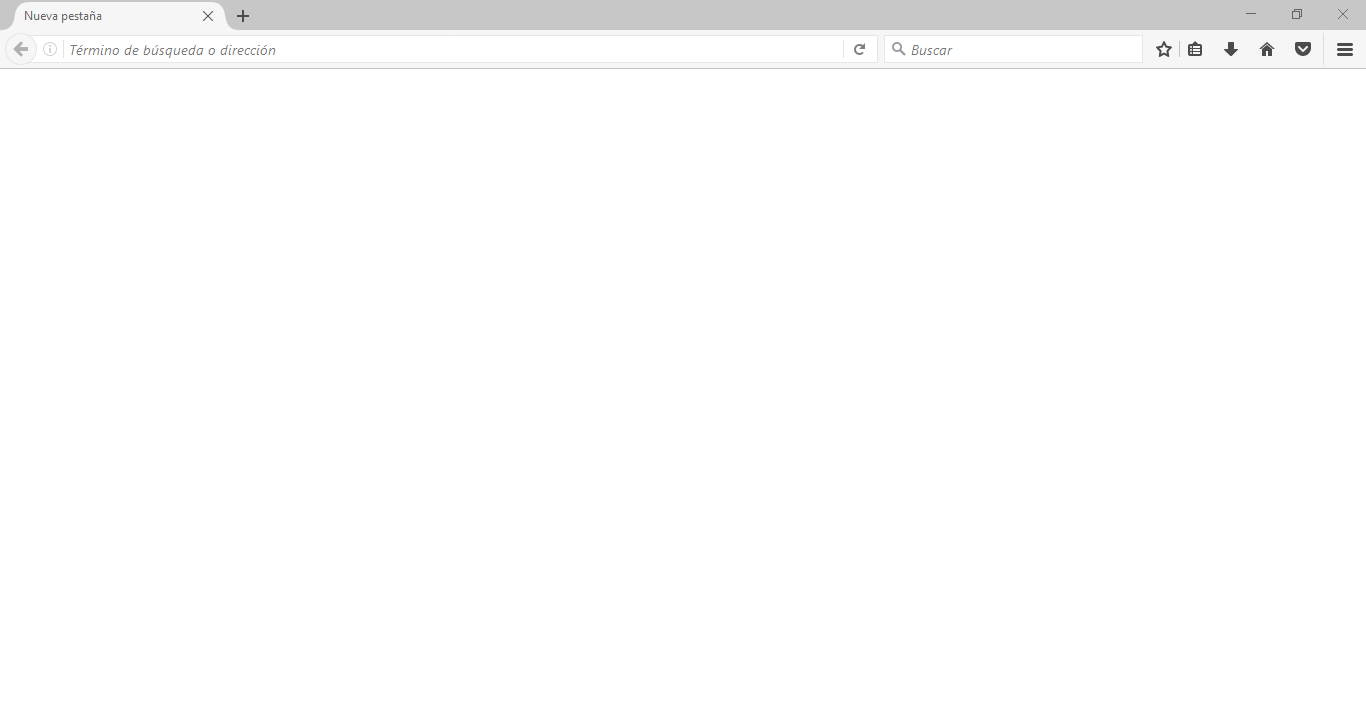


* 1. En explore your aplication seleccionar Firefox



* 1. Seleccionar Launch Browser y se abrirá un navegador.

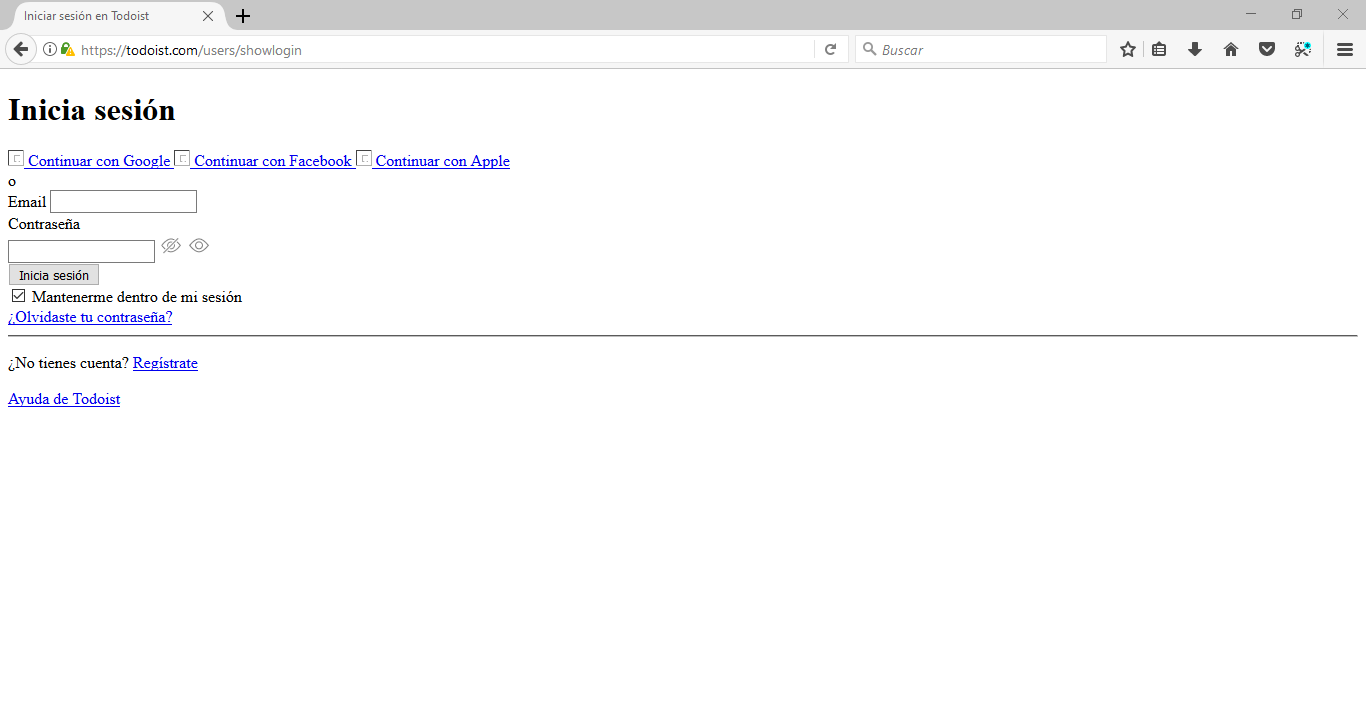
**

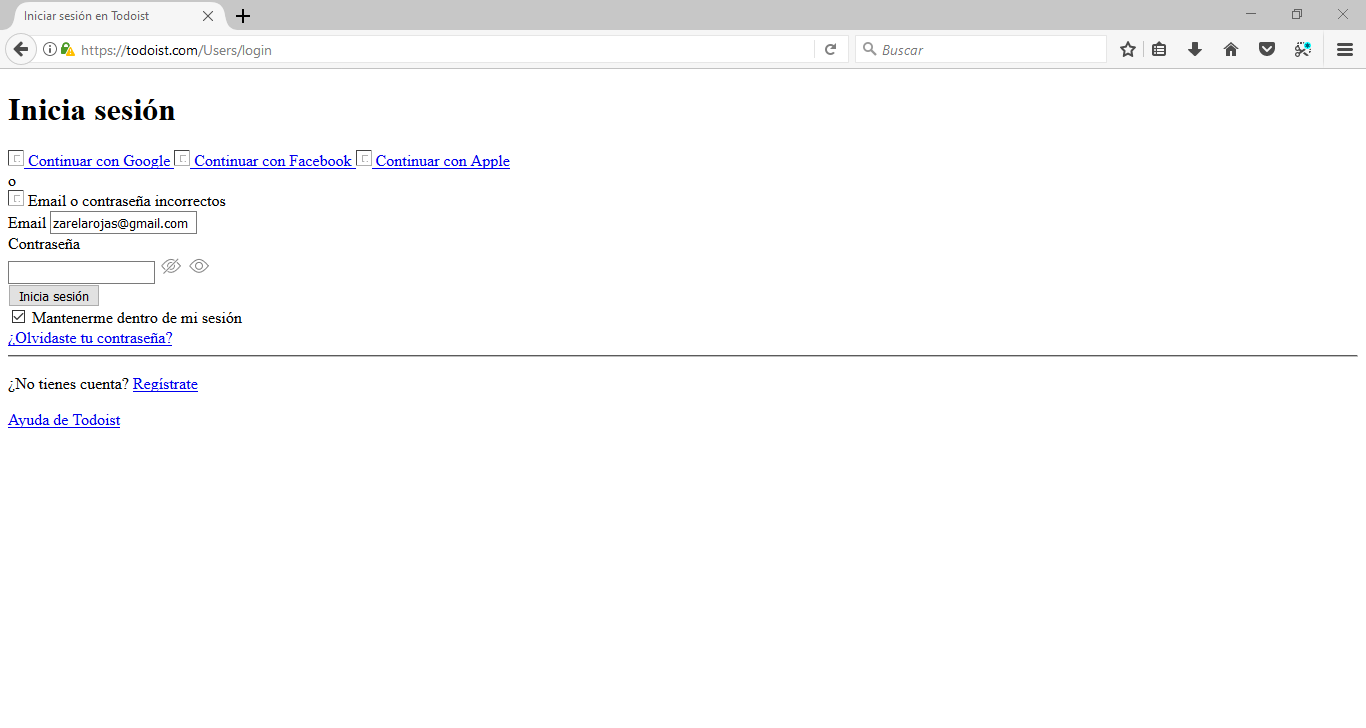
**

* 1. *En el Browser colocar la dirección web:* [*https://todoist.com*](https://todoist.com)

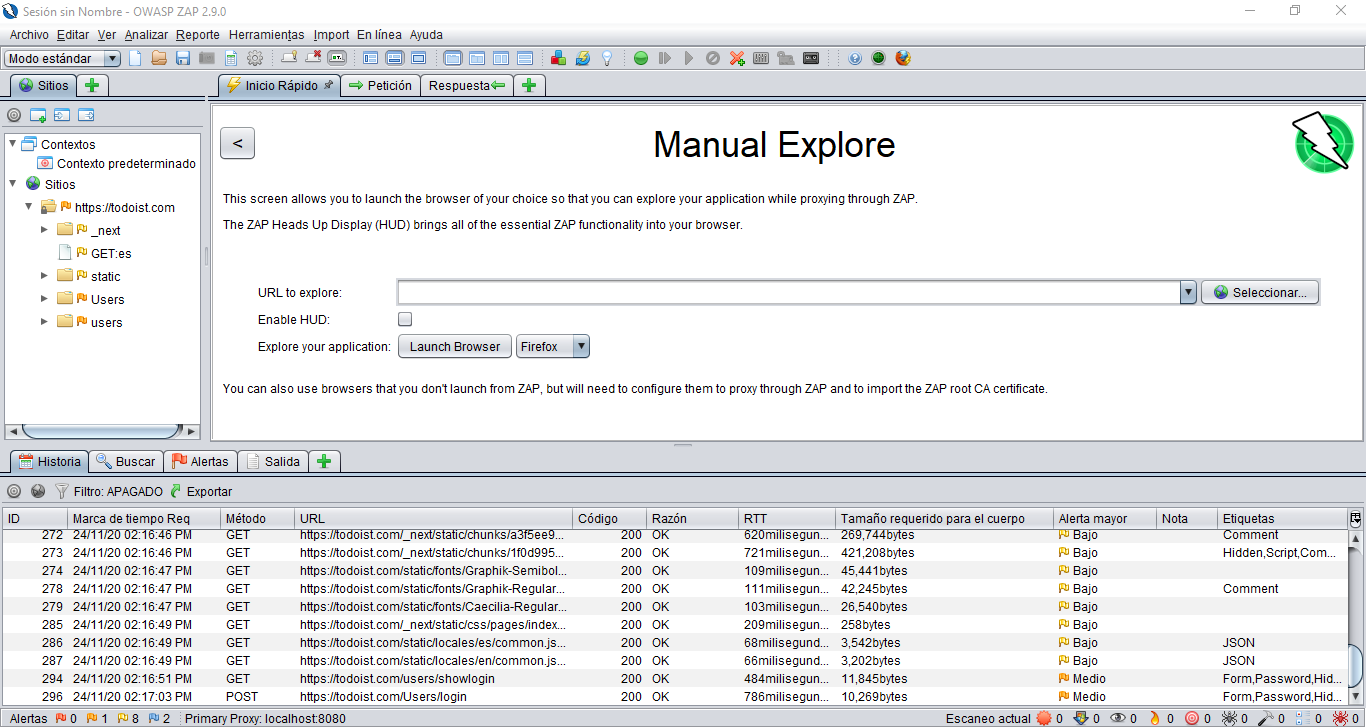
**

* 1. *Tratar de hacer un inicio de sesión.*

**

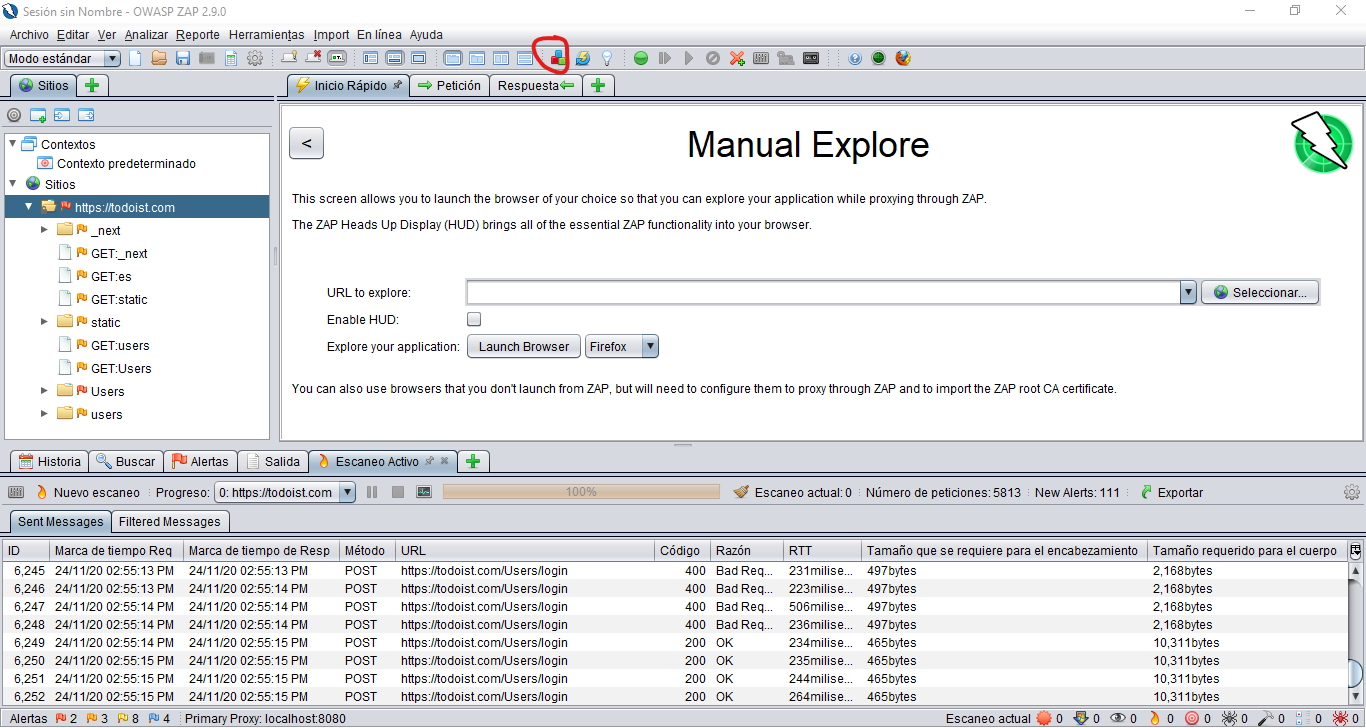
**

* 1. *Al regresar al OWASP ZAP se podrá ver el script grabado*

**

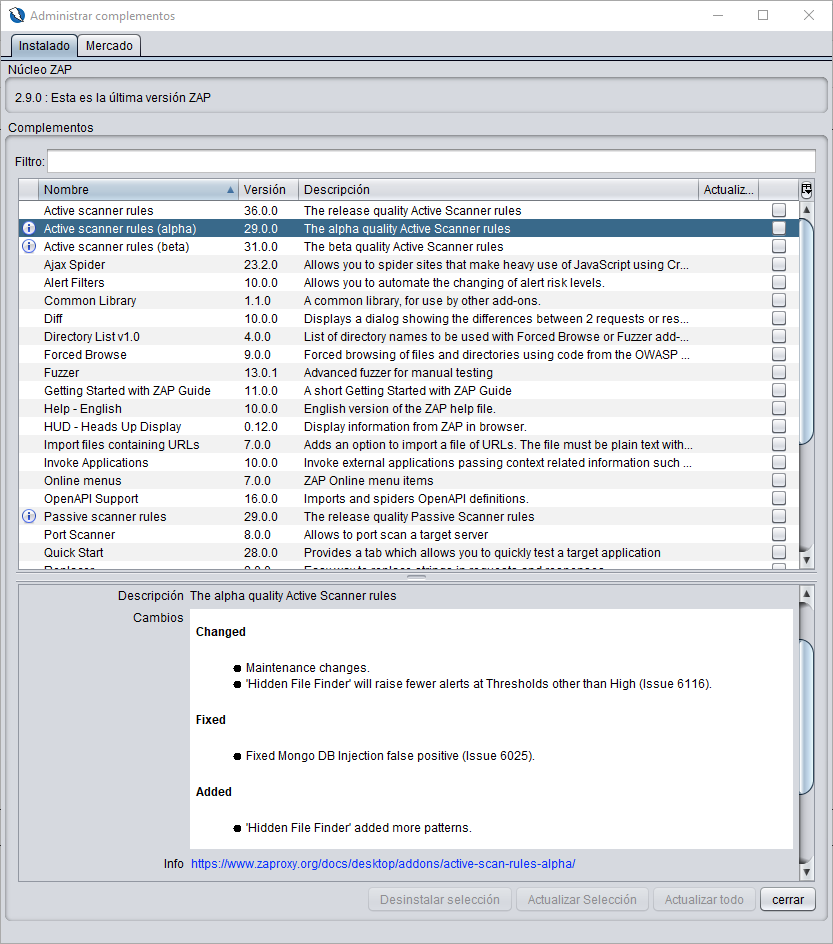
# **Administrar plugins de prueba**

* 1. Seleccionar Administrar complementos



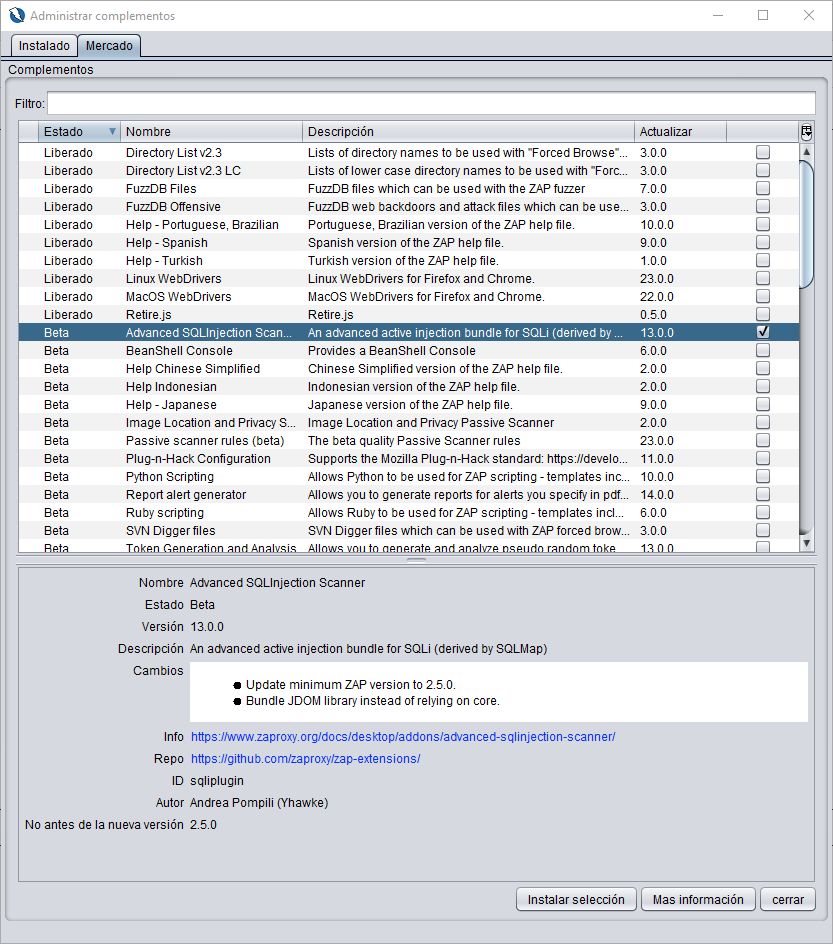
* 1. En la ventana Administrar Complementos hay dos pestañas

1. Instalado -> Se muestra todos los plugins instaldos. Si hubiera nuevas versiones en esta pestaña se indica y se puede actualizar.



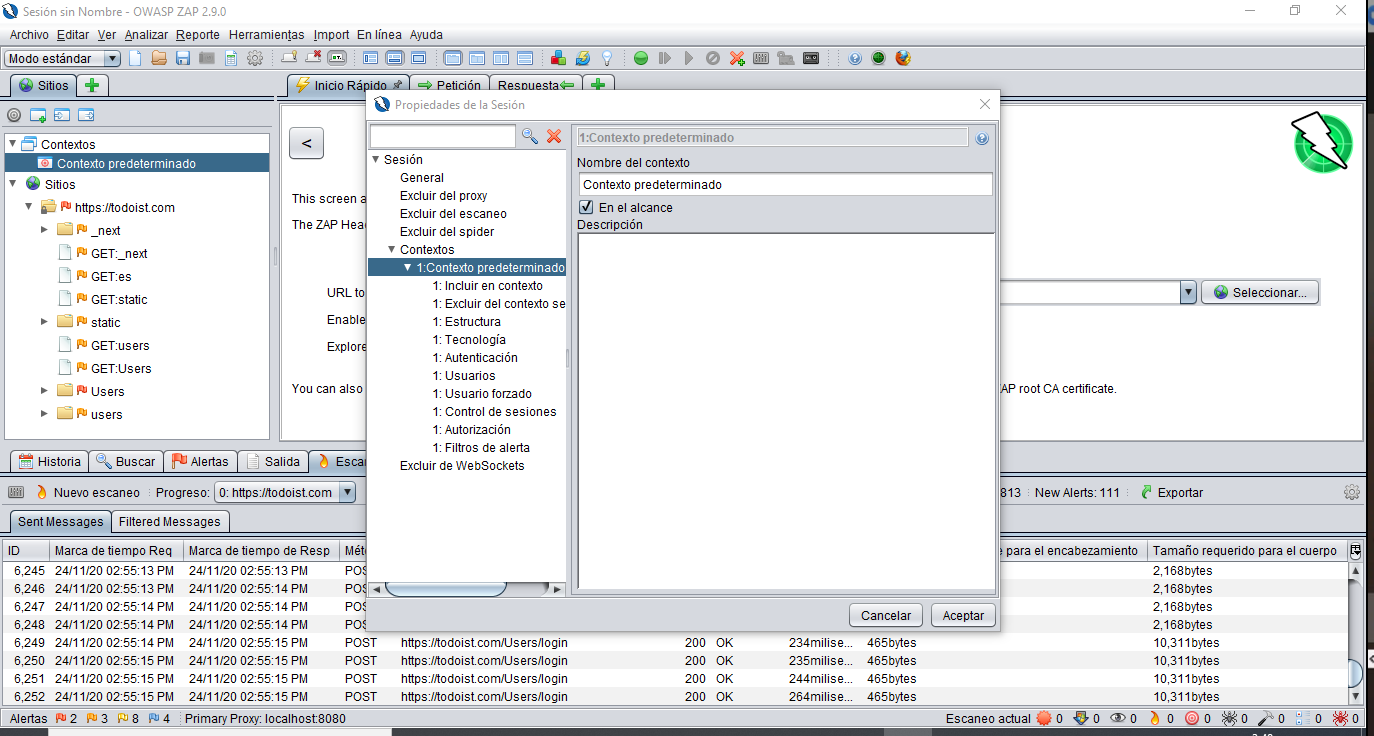
1. Mercado -> Se muestran todos los plugins disponibles. Si quieres aumenta rseleccionas uno y lo

instalas.

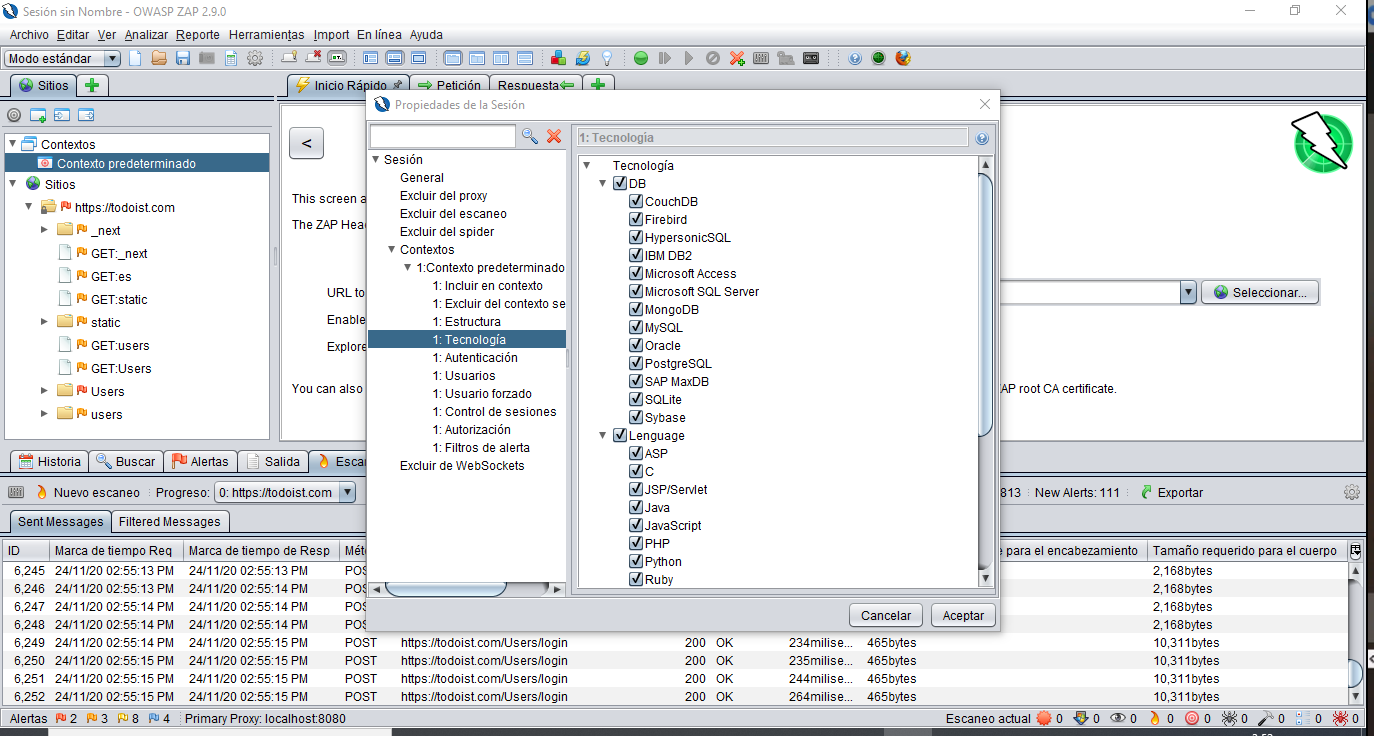


# **Filtrar según tecnologías**

* 1. En la ventana de Contextos, en la opción Contexto predeterminado dar doble click. Se abrirá la ventana Propiedades de la sesión.

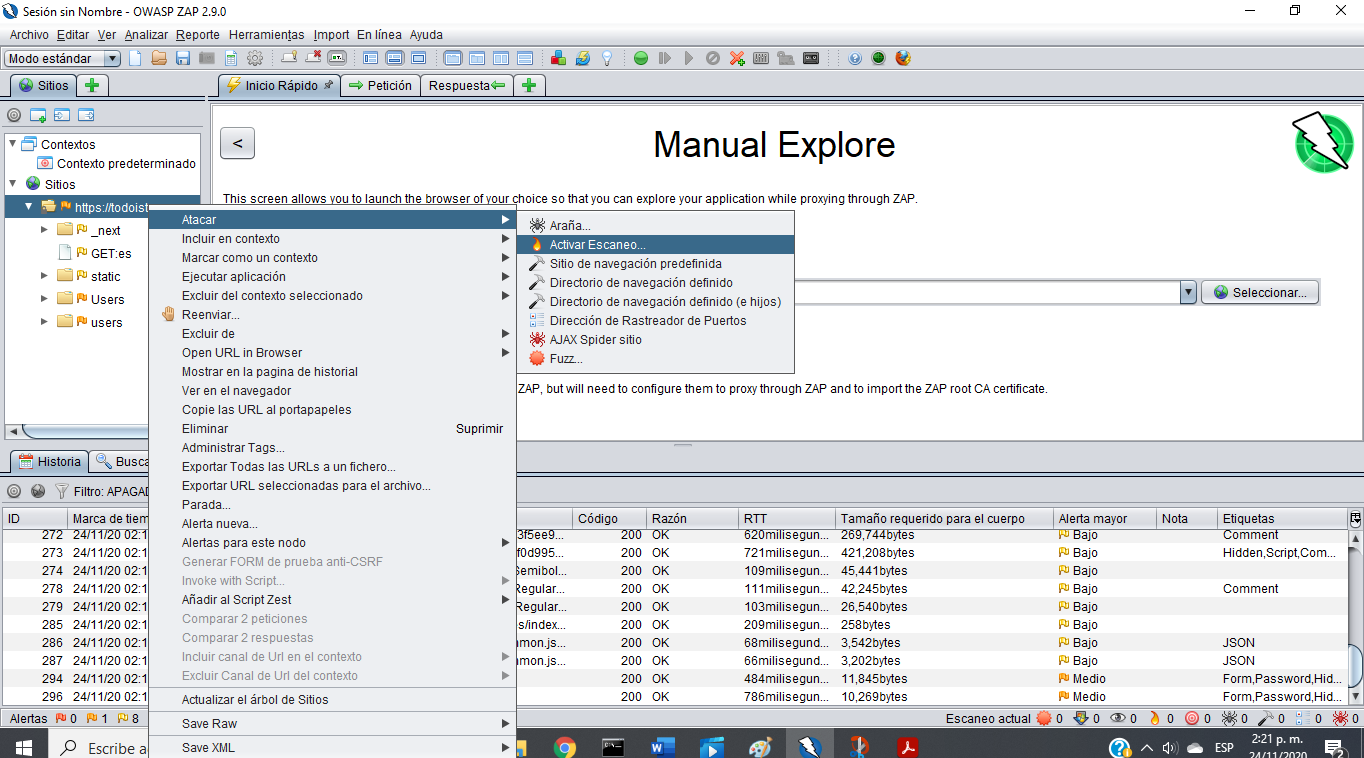


* 1. Seleccionar en Contextos la opción tecnología. Se mostrarán todas las tecnologías disponibles. Selecciona con un check todas las que deseas ejecutar. Y selecciona aceptar para guardar los cambios.

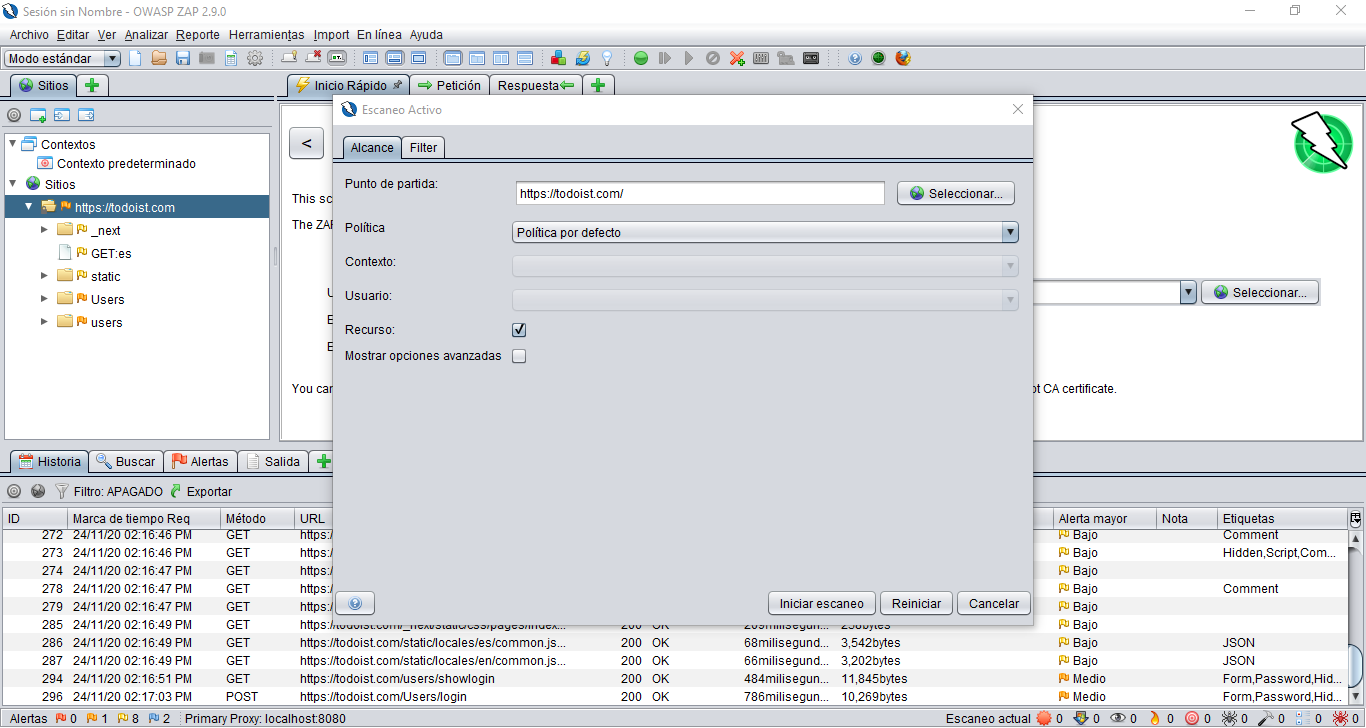


# **Ejecutar el Escaneo de vulnerabilidades**

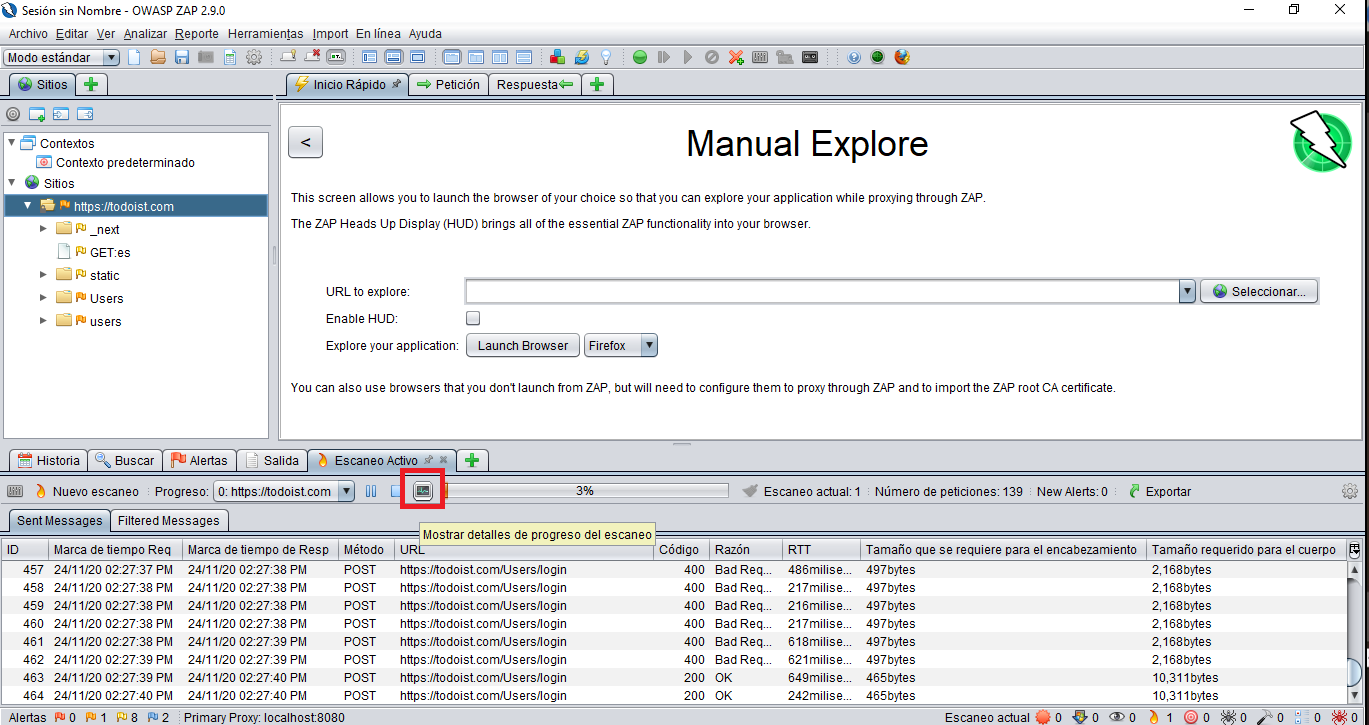
* 1. En la carperta de la URL ingresada hace click derecho y seleccionar ataca y luego activar escaneo

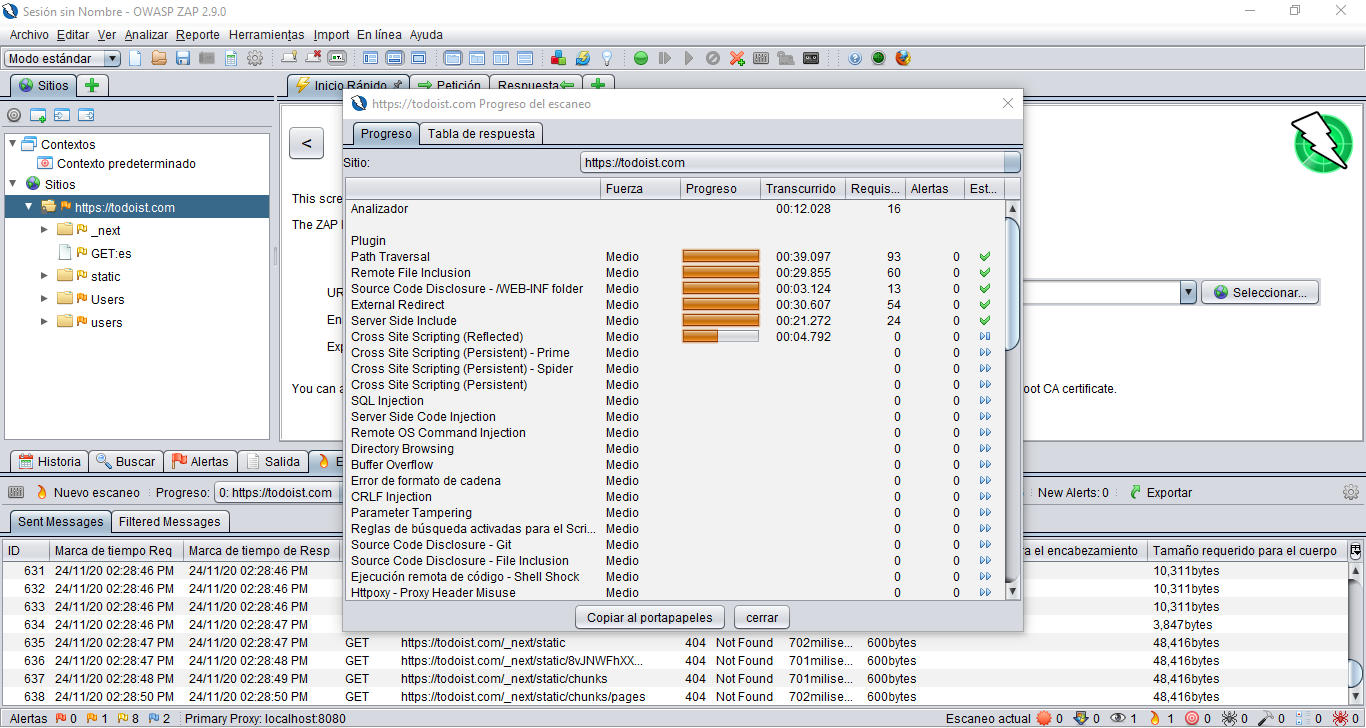


* 1. En la ventana Escaneo Activo validar que en el punto de partida se muestre la URL ingresada y luego seleccionar Iniciar escaneo.



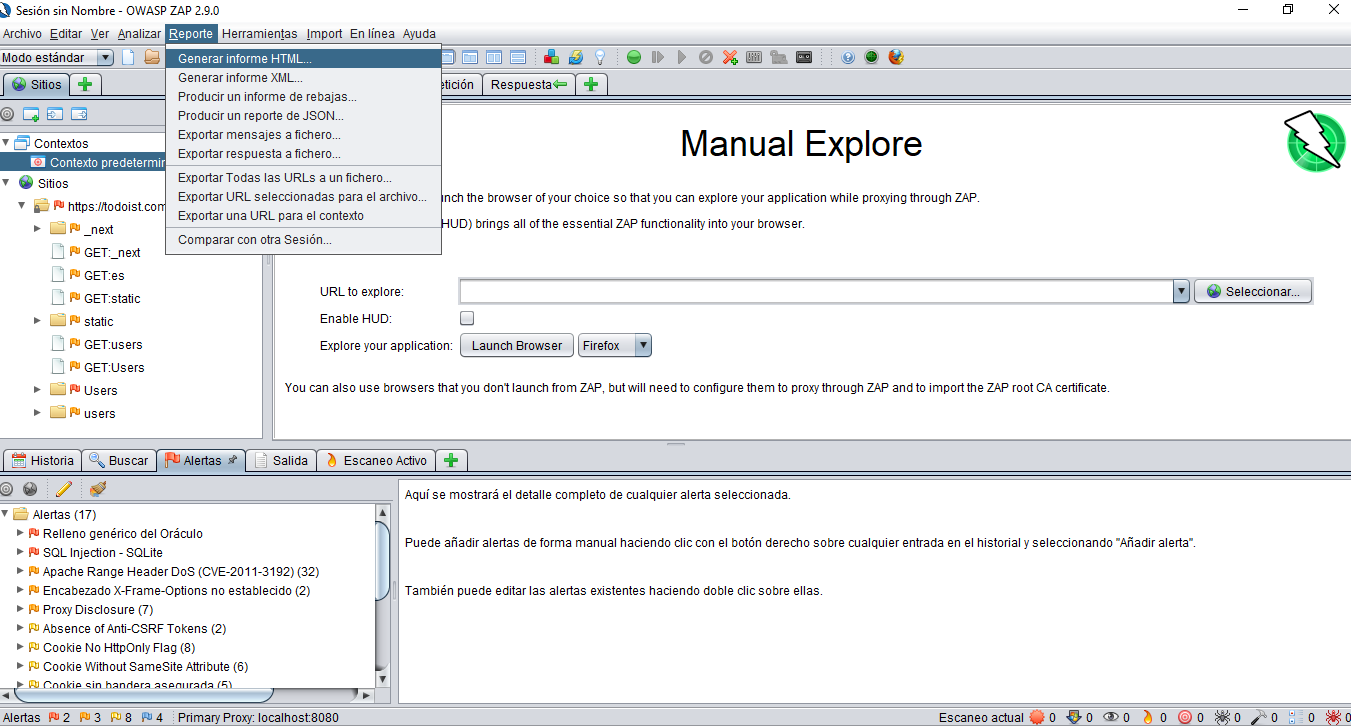
* 1. Para ver el progreso del escaneo seleccionar



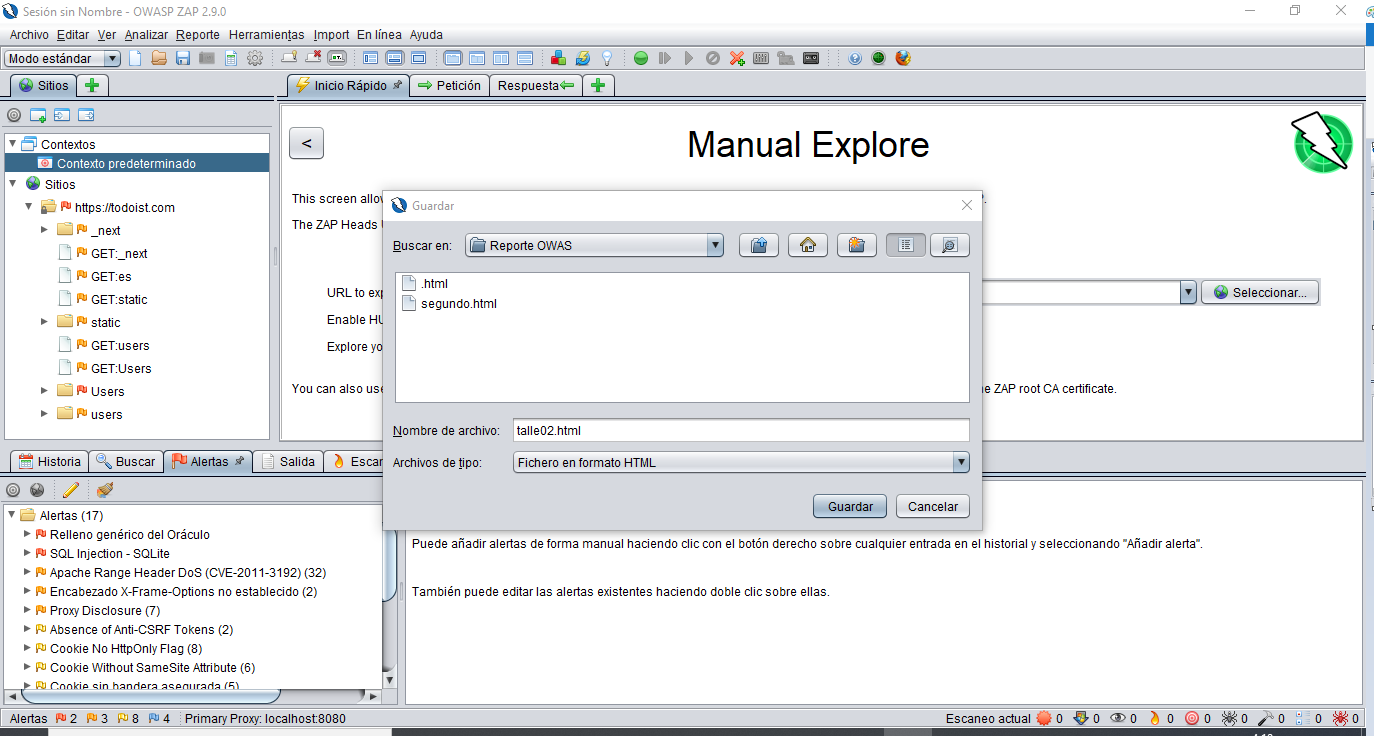


# **Genera Reporte**

* 1. En el menú seleccionar la opción reporte y luego Generar informe HTML



* 1. En la ventana seleccionar la ubicación donde se guardará el reporte y escribir el nombre del archivo. Seleccionar Grabar.



* 1. El reporte se mostrará en una ventana.

