PRÁCTICA 2 TEMA 2

14 DE ENERO DE 2025

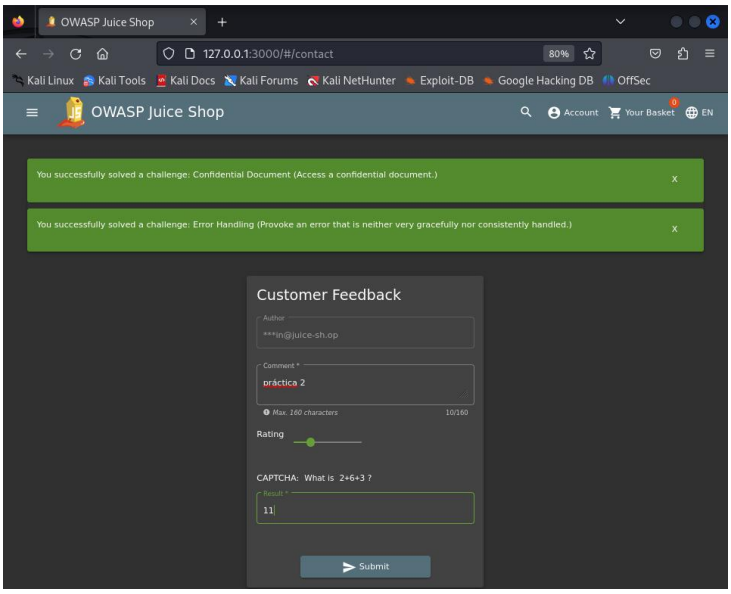
CIBERSEGURIDAD

Puesta en Producción Segura.

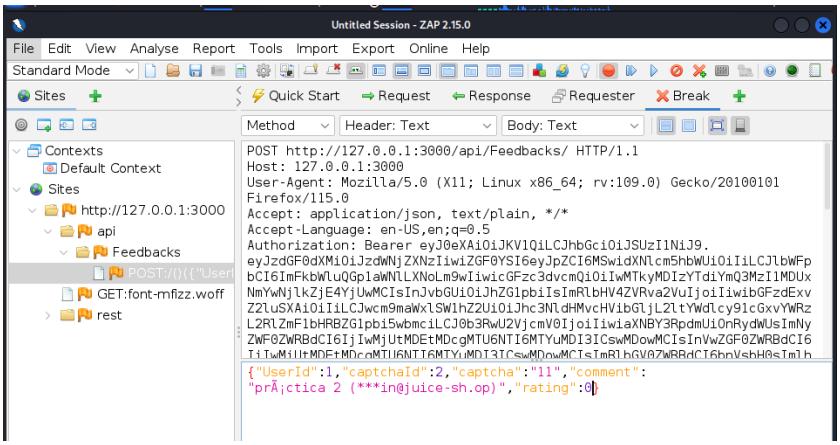
EJERCICIO 1.

En primer lugar, para completar el logro de Zero Stars de nuevo, debemos conectar el Proxy, Juice Shop y Zap al mismo tiempo.

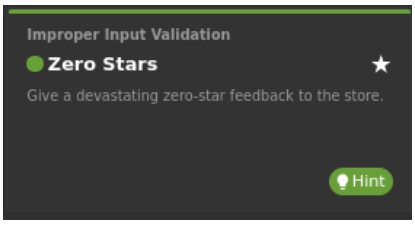
Una vez tengamos todo conectado, accedemos al localhost (127.0.0.1) para abrir Juice Shop y nos dirigimos a la página de las reseñas del cliente. Completamos los campos, en mi caso de comentario puse práctica 2, lo valoré con 2 puntos (ya que es el campo que vamos a modificar, por lo que no servirá de mucho lo que pongamos ahora y completaremos el captcha matemático. Una vez enviado, debería abrirse la ventana de ZAP automáticamente.



A continuación, en el ZAP, buscamos la petición POST (nos tendría que haber salido de forma automática ya que habíamos establecido un Breakpoint) y, en el apartado de "Rating" o puntuación, cambiaremos el 2 por el 0. Una vez hecho esto, enviamos el resultado mediante el botón "Submit and Continue to Next Breakpoint".

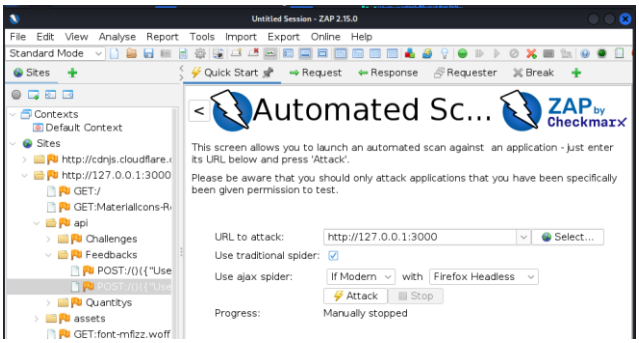


Como podemos ver, obtendríamos el logro Zero Stars.

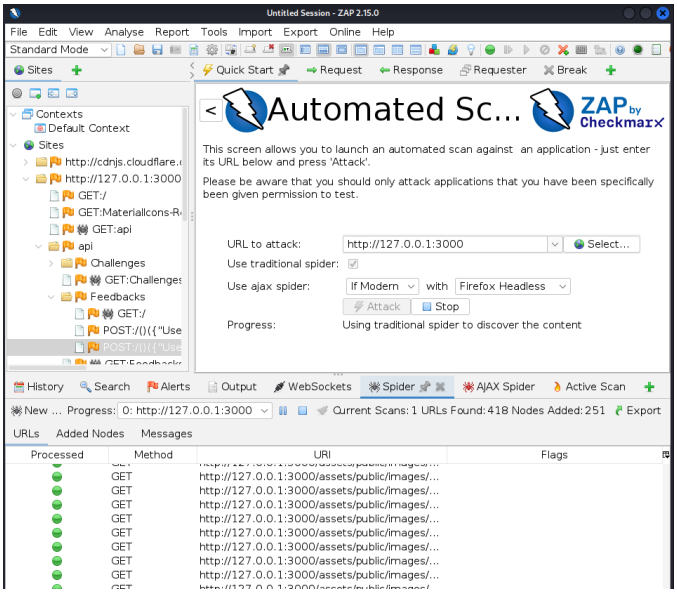


EJERCICIO 2.

En primer lugar, tendremos que pulsar en “Automated Scan” y, en la URL a atacar, pondremos la del Juice Shop, http://127.0.0.1:3000. Una vez hecho esto, pulsaremos en el botón “Attack”

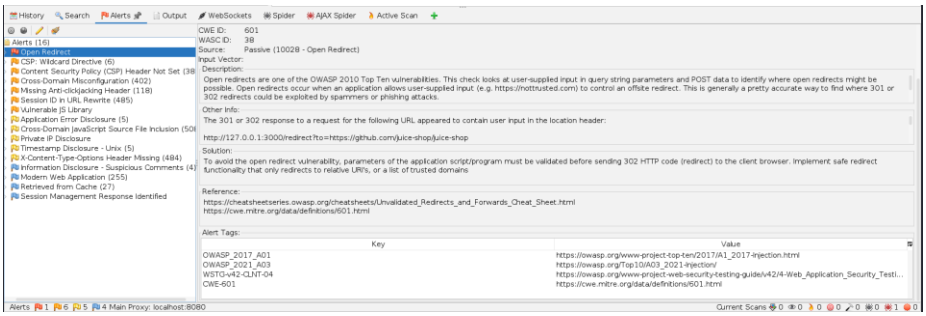


Una vez iniciado el escaneo, comenzarán a mostrarse los resultados en el menú inferior.



Si pulsamos en el apartado Alerts del menú inferior, podremos ver todas las vulnerabilidades encontradas tras el escaneo.

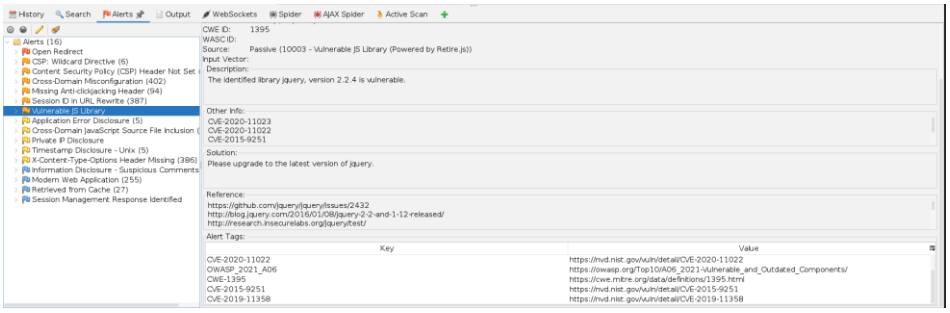
El primero que he elegido, es el más grave, como podemos ver indicado con una bandera roja. Este indica el fallo Open Redirect, en el cual, no se validan las URL a las que se van a realizar las redirecciones de los sitios que las pidan. Esto puede provocar que se puedan encontrar abiertas para cualquier tercero que quiera abusar del sistema. En muchas de las alertas, podemos ver los códigos CVE con los que podremos ver en profundidad la vulnerabilidad.



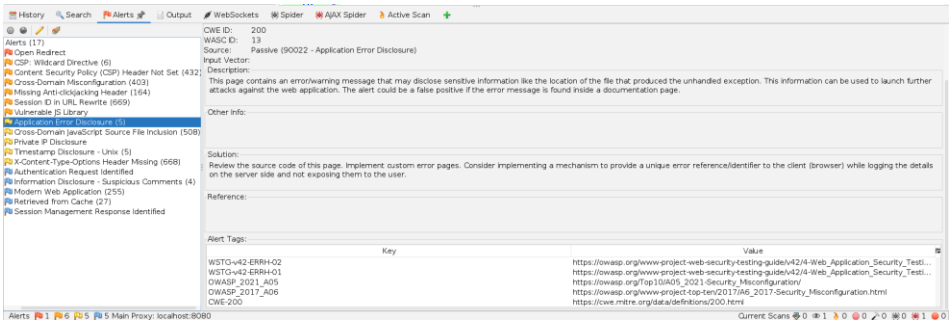
La segunda vulnerabilidad, es una de bandera naranja, es decir, de las segundas más peligrosas.

Esta indica que no existe ningún tipo de protección ante ataques de Clickjacking, un tipo de técnica maliciosa que busca obtener información mediante los clics que hacen los usuarios en páginas web aparentemente inocentes.

La tercera vulnerabilidad, otra de bandera naranja, se trata de una falta de actualizaciones de la librería jquery, lo cual lo hace vulnerable.



La cuarta, de bandera amarilla, lo que indica que es una vulnerabilidad algo peligrosa, indica que la página contiene un error o un mensaje de advertencia que podría contener información sensible.



La última, de nuevo de bandera amarilla, indica que una IP privada ha sido encontrada en el cuerpo del mensaje HTTP, lo que podría ser perjudicial debido a que pueden atacar con mayor facilidad a los sistemas gracias a este dato.