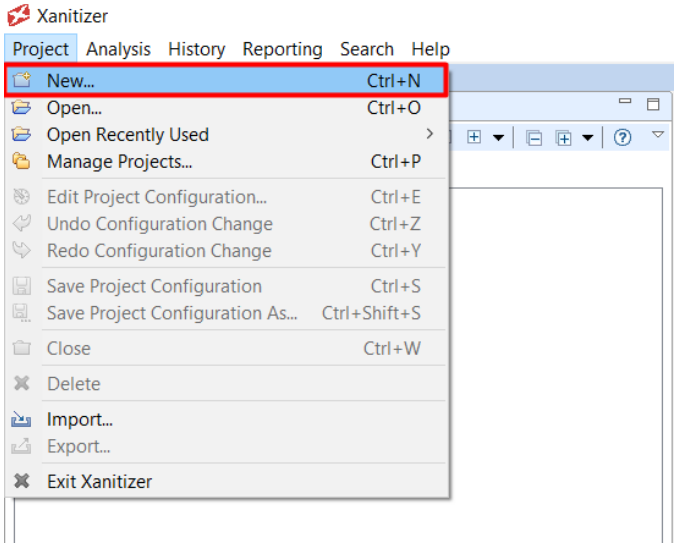
Taller de Xanitizer

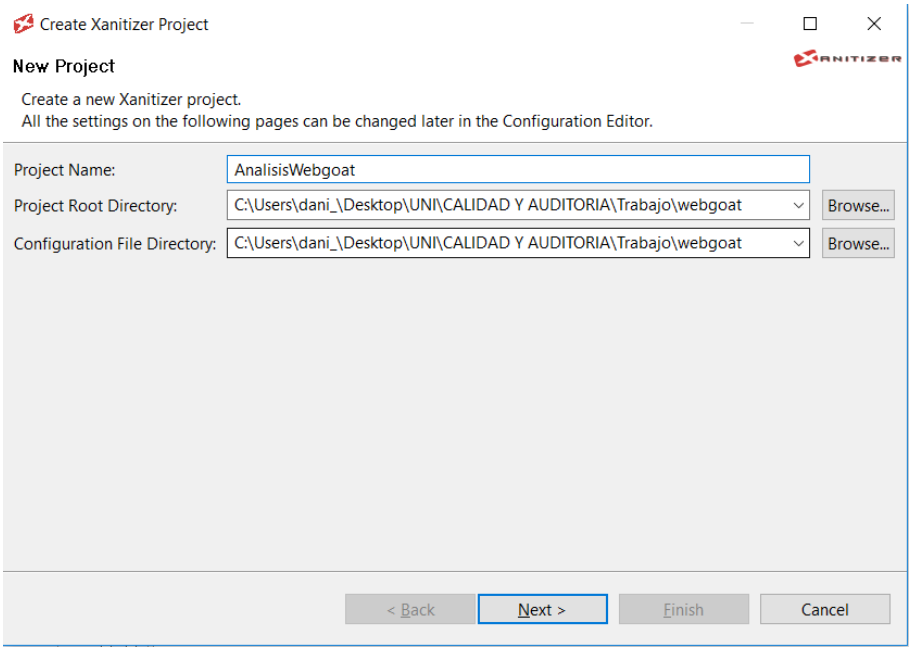
Autor: Daniel Peñil Núñez

Creación del proyecto de análisis

1. Accedemos en la barra superior al menú "***Project***" y elegimos la opción "***New…***".

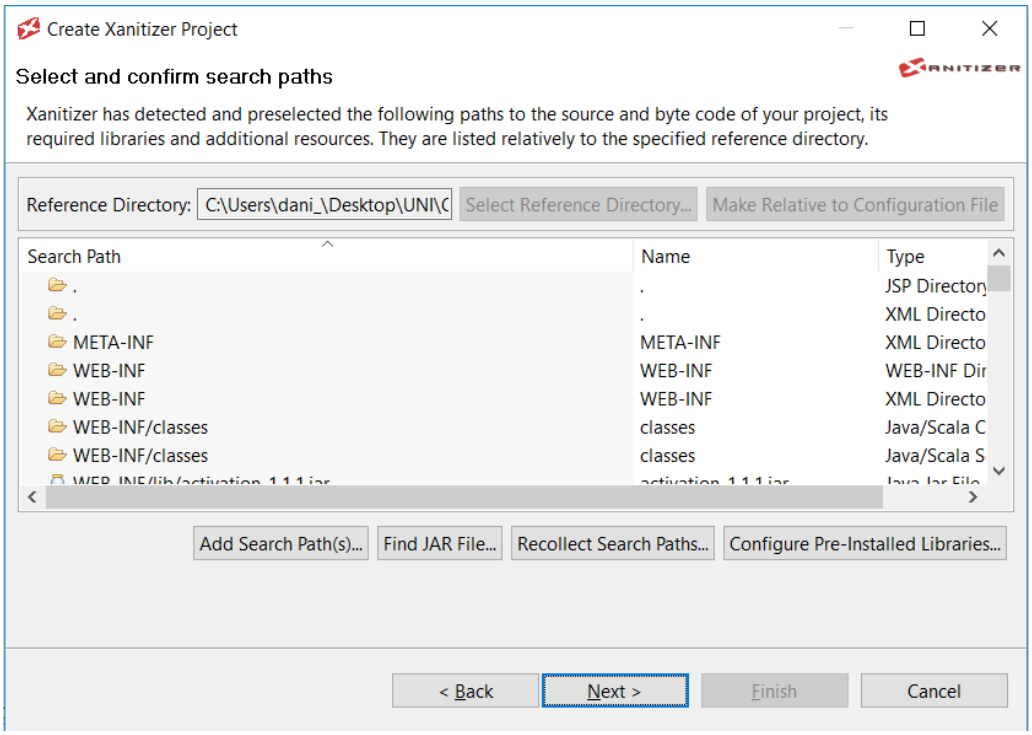


2. Se nos abrirá una ventana como la siguiente:

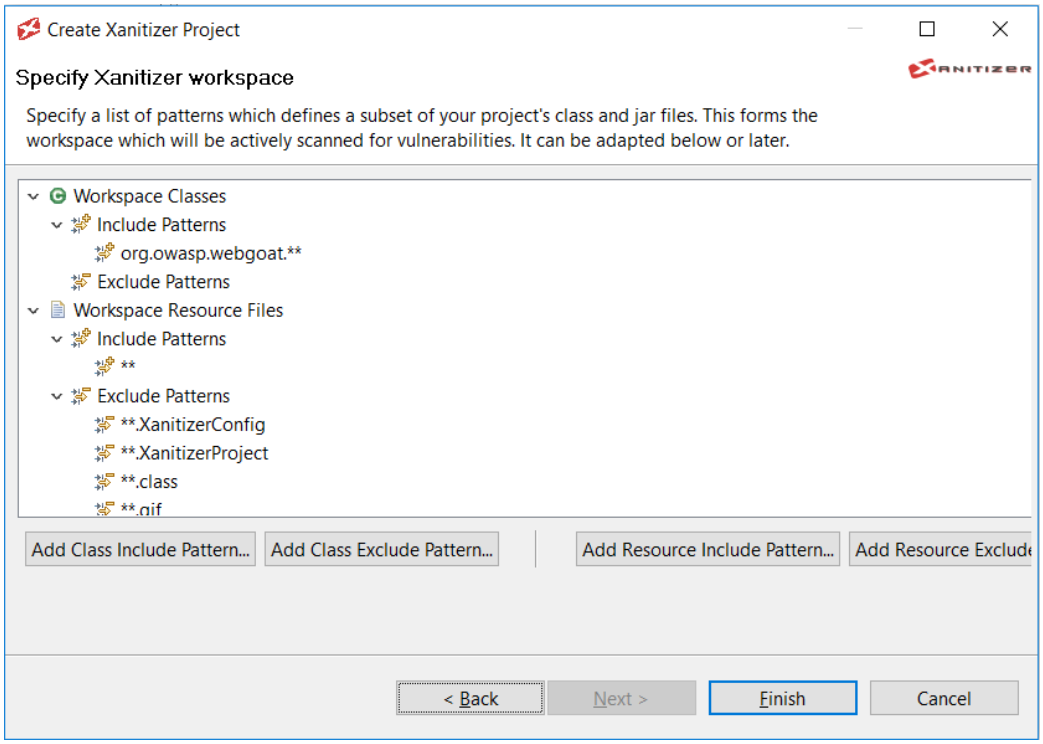


3. En "***Project Name***" introducimos el nombre que queremos dar al proyecto de Xanitizer.
4. En "***Project Root Directory***" debemos indicar la ruta del proyecto a analizar, que es la misma donde se incluirán los datos del proyecto Xanitizer.
5. La ubicación del archivo de configuración se autorrellenará con la ubicación del proyecto, la dejamos así, aunque podríamos elegir otra ubicación.

6. Hacemos click en “**Next >**” para continuar.



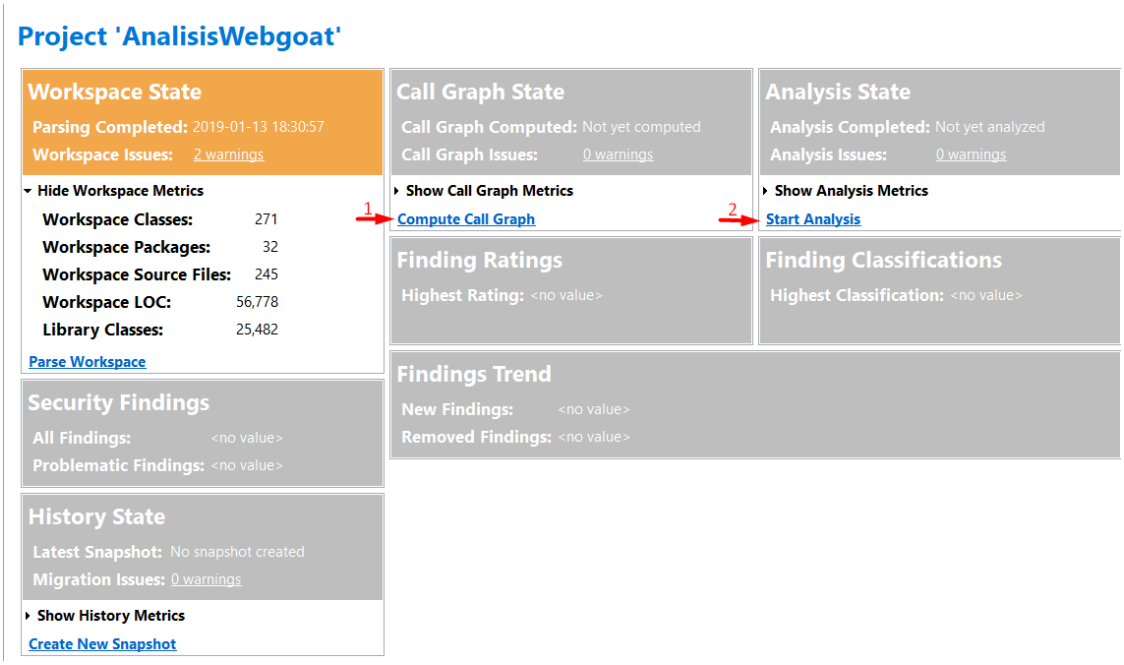
5. En este paso nos indica los directorios y los archivos que han sido reconocidos en la carpeta del proyecto y que van a ser incluidos en el análisis. No añadimos nada y continuamos.



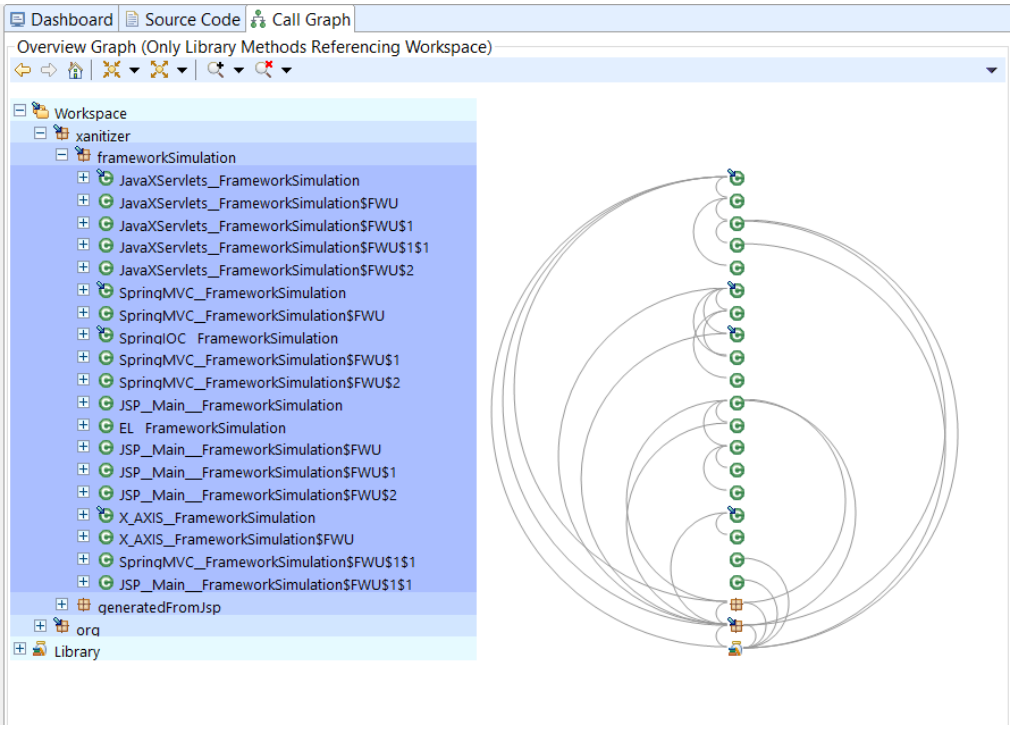
6. Por último, se nos muestran los archivos que no van a ser analizados, podríamos añadir más reglas, pero lo vamos a dejar como está.

Análisis del proyecto base

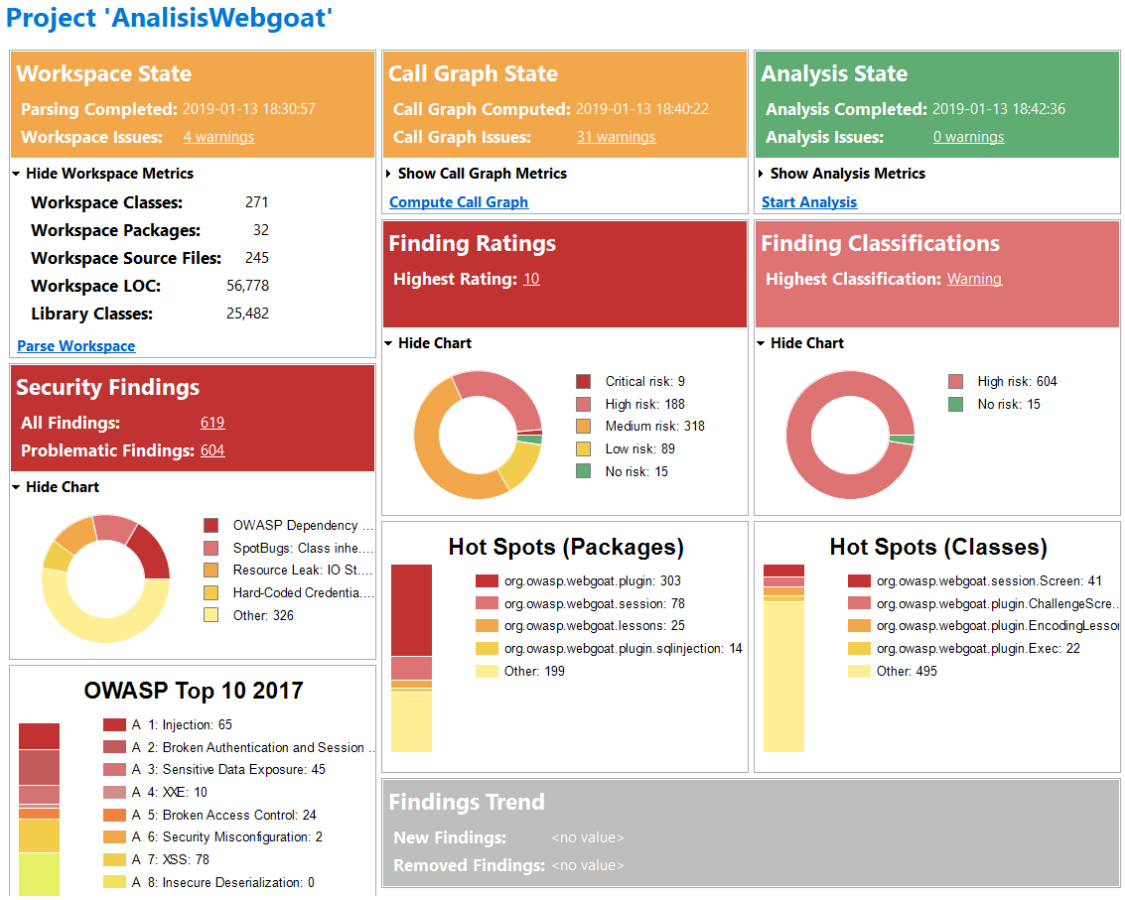
1. Tras haber definido el proyecto se habrá llevado a cabo un análisis inicial sobre la estructuración del proyecto (nos aparecerá a la izquierda) y sus dependencias. Ya podemos ver en los resultados que aparecen 2 warnings aunque ahora no nos detendremos en ello.



2. A continuación, para realizar el análisis de seguridad del proyecto tendremos que, en primer lugar, generar el "***Call graph***" del proyecto y a continuación seleccionar la opción de "***Start análisis***", como se muestra en la imagen superior.



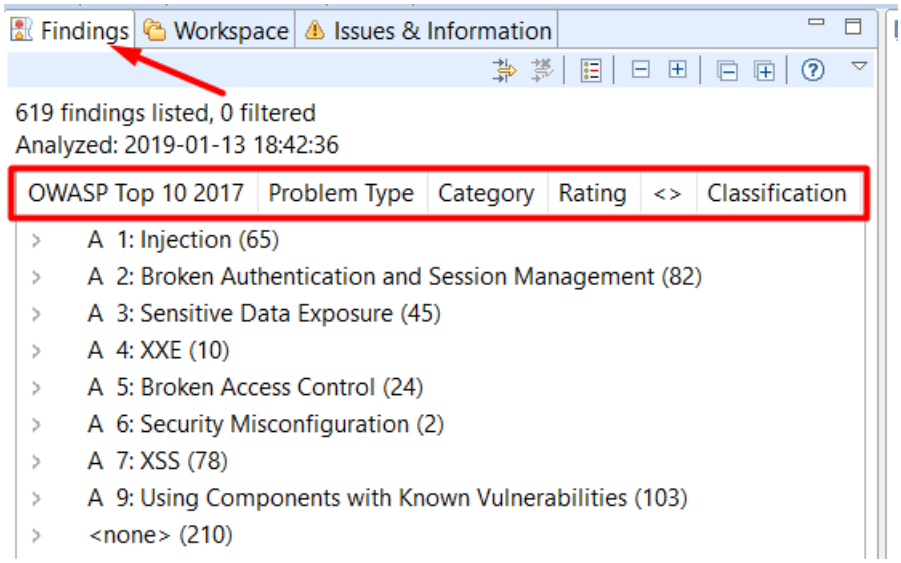
3. Tras generar el "***Call graph***" se nos habrá abierto esta pestaña donde podemos ver el esquema de llamadas entre clases del proyecto completo, habría que ir navegando entre paquetes y clases para verlo en detalle.



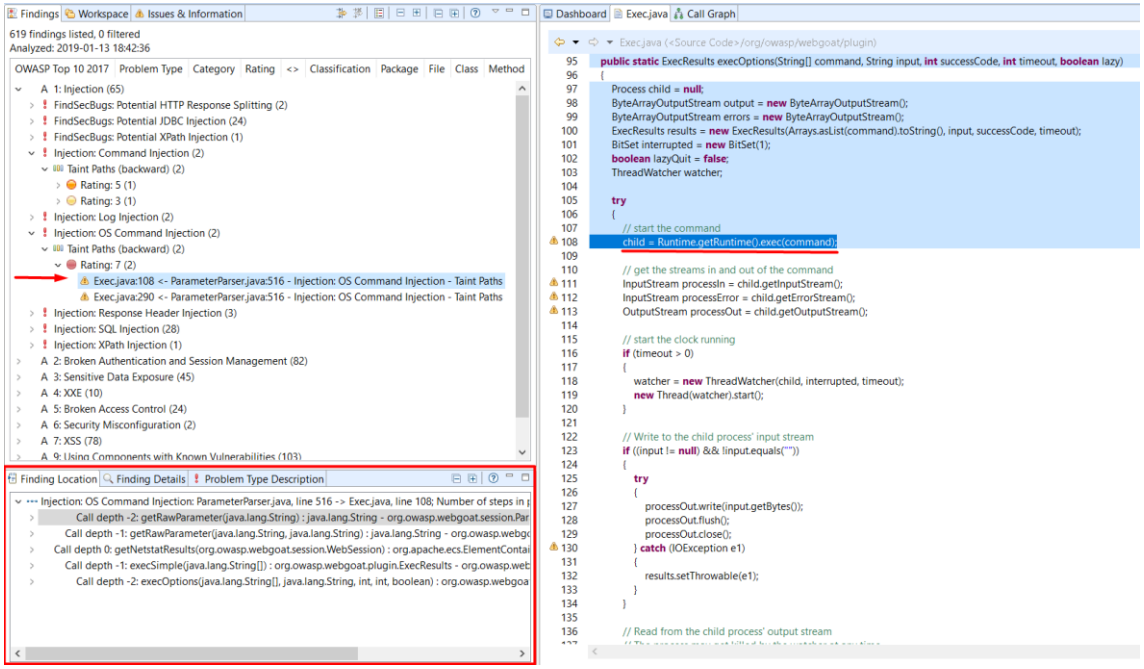
4. Finalmente, tras ejecutar el análisis completo el panel de control se habrá rellenado con una serie de gráficas donde podemos observar la cantidad y la magnitud de las vulnerabilidades del proyecto.

Análisis de una vulnerabilidad

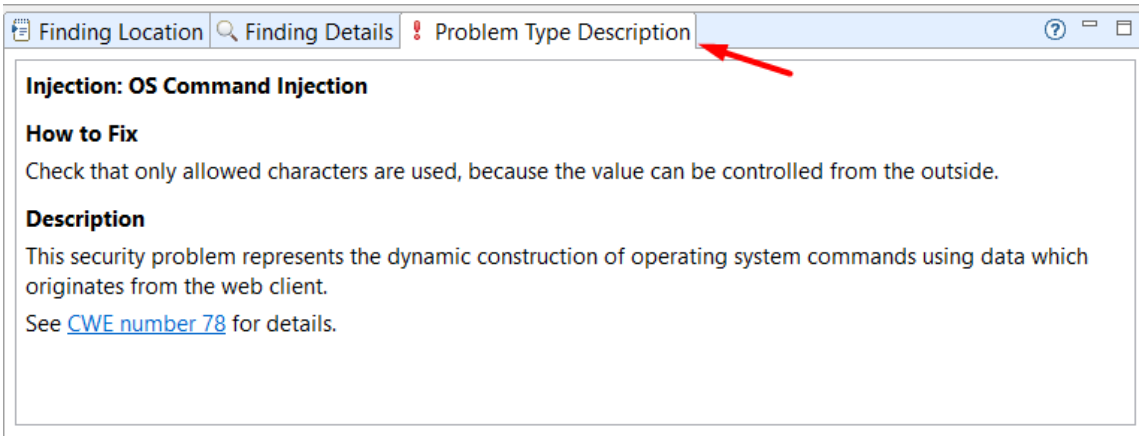
1. Accedemos en la vista lateral izquierda a la pestaña "***Findings***".



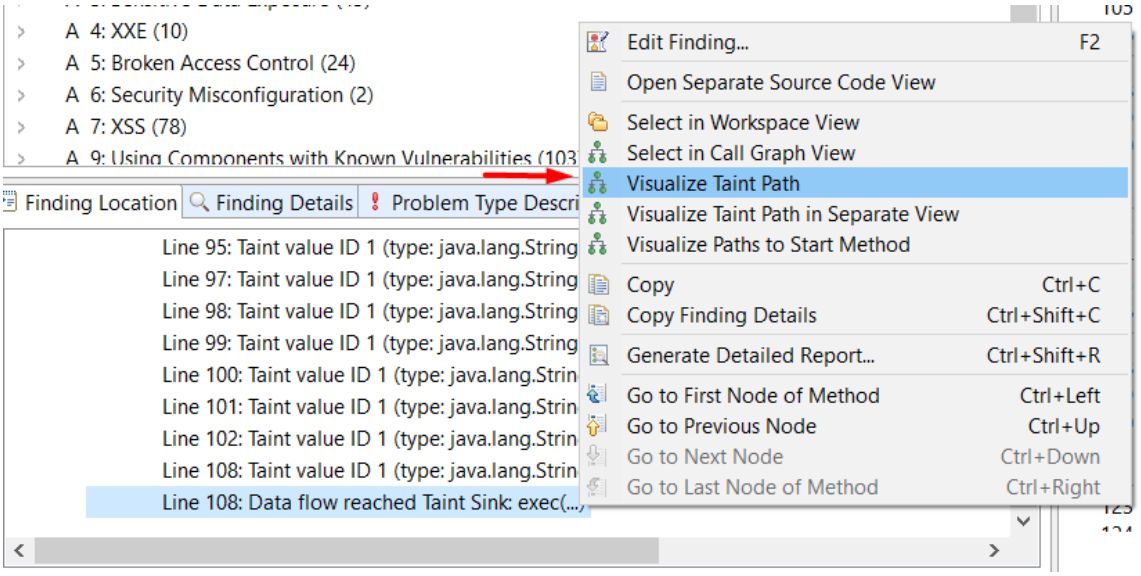
2. En la barra marcada en rojo podemos seleccionar el orden en el que se categorizan los errores, en el siguiente paso veremos un desglose. Para continuar con el taller lo dejamos como está.



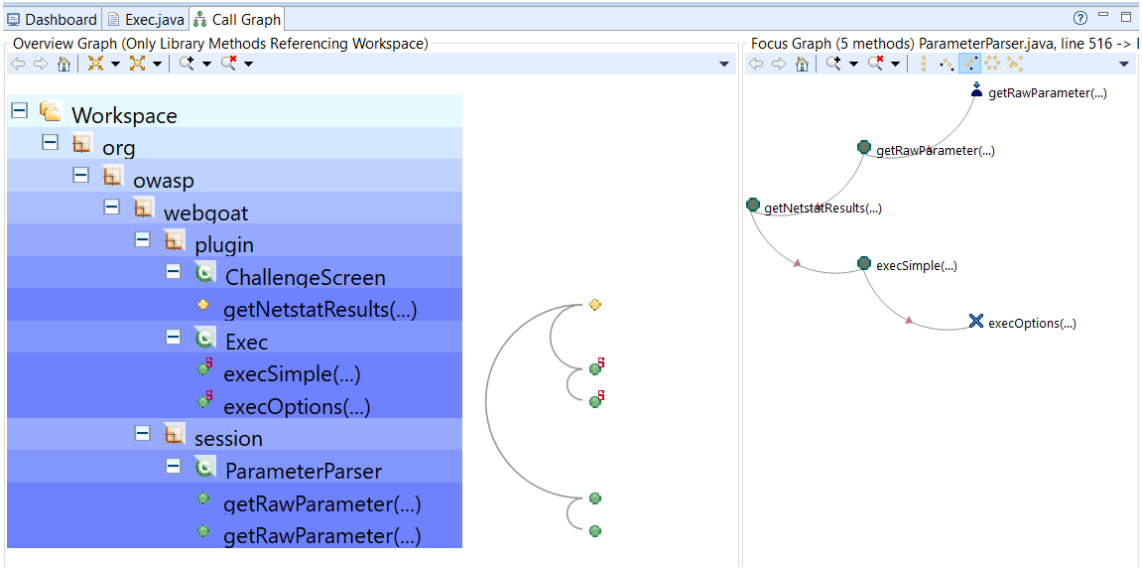
3. Nos vamos a centrar en una vulnerabilidad que permite inyección de comandos al sistema operativo que actúa como servidor. Desglosamos categorizaciones hasta que llegamos al error que queremos analizar y lo seleccionamos.
4. En la vista inferior izquierda, podemos observar que ahora nos aparece la pila de llamadas que se siguen desde el origen hasta llegar a la vulnerabilidad.
5. En la vista principal, se nos abrirá el editor con la clase donde se encuentra la última llamada que produce la vulnerabilidad, es decir el lugar donde reside y, posiblemente, deba corregirse el fallo.



6. Para obtener más información del tipo de problema detectado podemos acceder en la vista inferior izquierda a la pestaña "***Problem Type Description***".



7. Por último, algo que nos permite Xanitizer y es bastante útil es proceder a mostrar la pila de llamadas que habíamos visto previamente, pero de forma gráfica en el "***Call graph***" generado durante el análisis inicial.



El flujo mostrado anteriormente se puede aplicar a cualquier tipo de fallo. Como hemos podido ver, Xanitizer nos permite realizar un análisis profundo de las vulnerabilidades del sistema así como sus posibles orígenes de explotación y, aunque no lo hayamos mencionado, también nos detecta deficiencias en la calidad del código dado que la calidad y la seguridad de un producto software siempre van unidas de la mano.