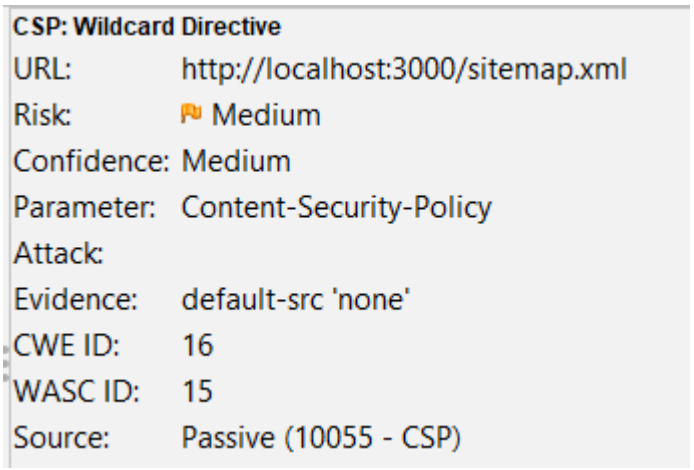
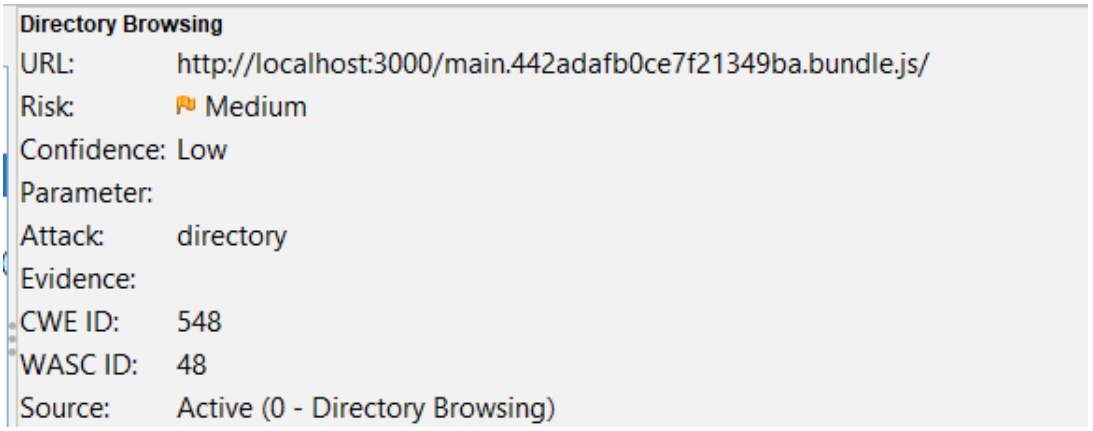
PRUEBAS OWASP

- CSP: Wildcard Directive (Riesgo Medio)



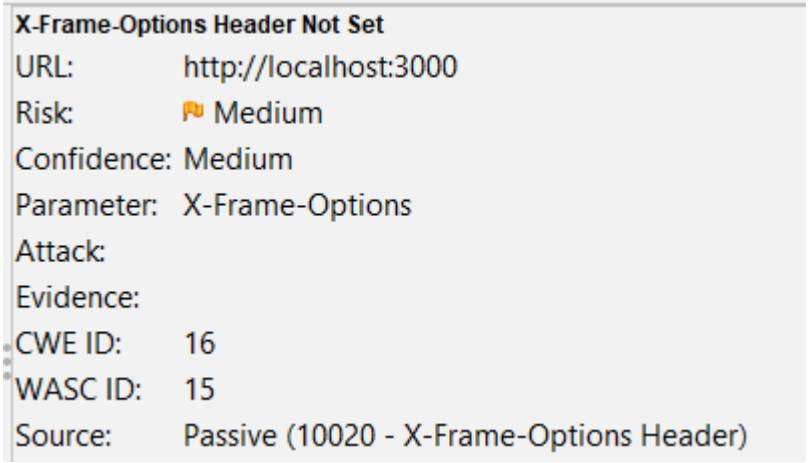
Problema :
Las siguientes directivas permiten fuentes comodín (o ancestros), no están definidas o tienen una definición demasiado amplia:
marco-ancestros, forma-acción
Solución :
Asegúrese de que su servidor web, servidor de aplicaciones, equilibrador de carga, etc.esté configurado correctamente para establecer el encabezado Content-Security-Policy.

- Directory Browsing (Riesgo Medio)



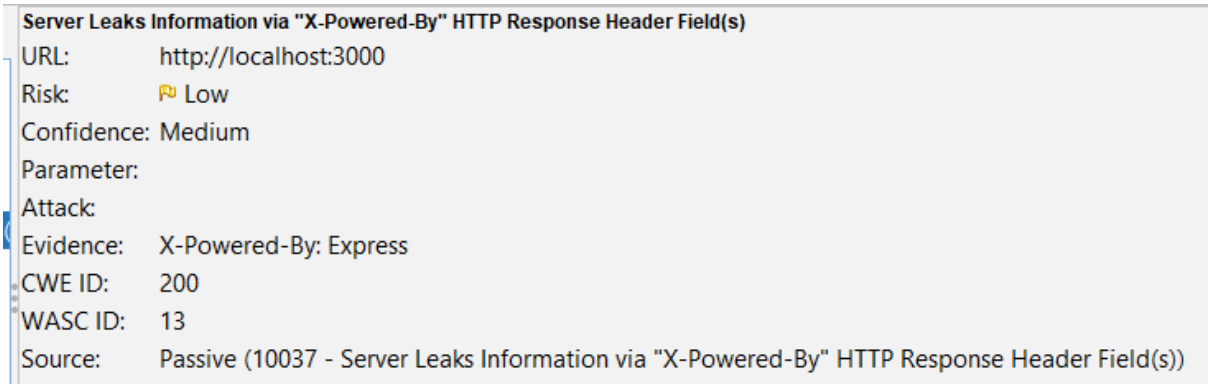
Problema :
Es posible ver la lista del directorio. La lista de directorios puede revelar scripts ocultos, incluir archivos, archivos de origen de respaldo, etc., a los que se puede acceder para leer información confidencial.
Solución :
Desactive la exploración de directorios. Si es necesario, asegúrese de que los archivos enumerados no presenten riesgos.

- X-Frame-Options Header Not Set (Riesgo Medio)



Problema :
El encabezado X-Frame-Options no se incluye en la respuesta HTTP para proteger contra ataques 'ClickJacking'.
Solución :
La mayoría de los navegadores web modernos admiten el encabezado HTTP X-Frame-Options. Asegúrese de que esté configurado en todas las páginas web devueltas por su sitio (si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET), entonces querrá usar SAMEORIGIN; de lo contrario, si nunca espera la página para enmarcar, debe usar DENY. ALLOW-FROM permite que sitios web específicos enmarquen la página web en navegadores web compatibles).

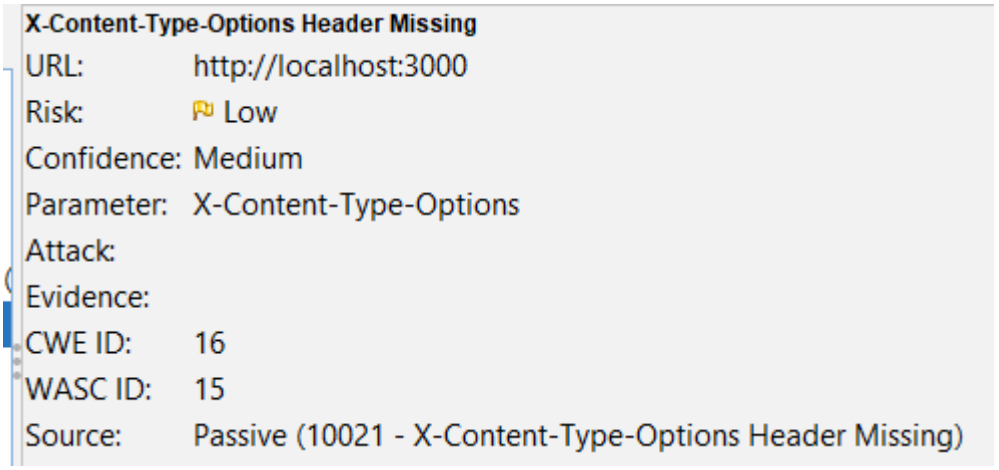
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (Riesgo Bajo)



Problema :
El servidor web / de aplicaciones está filtrando información a través de uno o más encabezados de respuesta HTTP "X-Powered-By". El acceso a dicha información puede facilitar que los atacantes identifiquen otros marcos / componentes de los que depende su aplicación web y las vulnerabilidades a las que dichos componentes pueden estar sujetos.
Solución :

Asegúrese de que su servidor web, servidor de aplicaciones, equilibrador de carga, etc. esté configurado para suprimir los encabezados "X-Powered-By".

- X-Content-Type-Options Header Missing (Riesgo Bajo)



Problema :
El encabezado Anti-MIME-Sniffing X-Content-Type-Options no se estableció en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de la respuesta, lo que podría hacer que el cuerpo de la respuesta se interprete y muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox usarán el tipo de contenido declarado (si se establece uno), en lugar de realizar un rastreo de MIME
Solución :
Asegúrese de que la aplicación / servidor web establezca el encabezado Content-Type de manera adecuada y que establezca el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.
Si es posible, asegúrese de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realice ningún rastreo de MIME, o que la aplicación web / servidor web pueda indicarle que no realice el rastreo de MIME.