Preguntas:

a) ¿Para qué sirve “Content-Security-Policy”?

Es una capa de seguridad adicional que ayuda a prevenir y mitigar algunos tipos de ataque, incluyendo Cross Site Scripting (XSS) y ataques de inyección de datos. Como en nuestro caso el script llama a durante los métodos AJAX a servidores de terceros (https://ssaatt.com) hemos de permitir esas peticiones.

b) Documéntate y explica el significado de la anterior línea (que debe aparecer en la cabecera del documento index.html).

content="default-src 'self' *; stylesrc 'self' * 'unsafe-inline'; script-src * 'unsafe-inline' ; img-src * data: "

El atributo *http-equiv* da información sobre el contenido del atributo *content*, en este caso: *"Content-Security-Policy"*.

content incluye una serie de directivas de políticas, cada una de las cuales describe la política para un determinado tipo de recurso o área de política. Una política debe incluir una directiva de políticas *default-src*, que es una alternativa para otros tipos de recursos cuando no tienen políticas propias, *script-src* para evitar la ejecución de scripts en línea, así como bloquear el uso de *eval()*. Una política debe incluir una directiva *default-src* o *style-src* para restringir la aplicación de estilos en línea desde un elemento <*style*> o un atributo *style*.

'self' incluye al origen actual, pero no a sus subdominios.

'unsafe-inline' permite JavaScript y CSS integrados.

data: permite todas las imágenes siempre que comiencen por *data:*