Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Monterrey

TE3003B.503

Integración de robótica y sistemas inteligentes (Gpo 503)

Socio Formador
Manchester Robotics Ltd

PhD. Arturo Eduardo Cerón López

MidTerm Act - Extra points

Alumno

Fernando Cuéllar Martínez A00827540

Campus Monterrey **Tecnológico de Monterrey**

Domingo 28 may 2023 Monterrey, N. L.

Se investiga qué es CORS y cómo afecta a una aplicación Web: 10%

Los navegadores online utilizan el protocolo Cross-Origin Resource Sharing (CORS) para evitar el acceso no autorizado mediante código JavaScript a los recursos que se originan en un dominio diferente. Esta política se aplica para proteger los datos y la información privada cuando se alojan en otros sitios web utilizando la autorización explícita del propietario del recurso.

El método CORS permite que un sitio web solicite permiso para acceder a los recursos de otro sitio web. Cualquier elemento al que se pueda acceder a través de la URL, como un recurso API, un archivo JavaScript o una imagen, se conoce como recurso.

El navegador del usuario puede impedir que una aplicación online solicite el acceso a un recurso que se encuentra en un dominio diferente al de la aplicación. Sin embargo, el servidor que aloja el recurso tiene la capacidad de establecer una política CORS que permita el acceso desde el dominio de la aplicación.

La política CORS puede tener un impacto en una aplicación online que necesita acceso a recursos en varios dominios. Si la política no está configurada correctamente, el navegador puede rechazar las solicitudes de acceso a estos recursos, algo que puede provocar errores y mal funcionamiento de la aplicación. Como resultado, es esencial que los desarrolladores web comprendan y configuren correctamente la política de CORS para asegurarse de que las aplicaciones web funcionen correctamente.

Datos curiosos de CORS:

- Una especificación común para la web es CORS: Fue creado por el consorcio World Wide online (W3C) para abordar los problemas de seguridad que surgen cuando las personas solicitan recursos de origen cruzado en los navegadores online.

- CORS se basa en el uso de encabezados HTTP: el intercambio de encabezados HTTP especiales que indican restricciones y permisos de acceso permite la comunicación entre el cliente (navegador) y el servidor.

- Fue desarrollado como una solución para los ataques de scripting entre sitios (XSS): Antes de CORS, los navegadores utilizaban técnicas como JSONP (JSON con relleno) para permitir solicitudes de origen cruzado, pero estas técnicas tenían limitaciones y presentaban riesgos de seguridad.

- CORS usa dos categorías distintas de solicitudes: Las solicitudes CORS pueden ser simples o previamente revisadas. Las solicitudes simples no requieren una solicitud adicional al servidor antes de enviar la solicitud real; sin embargo, las solicitudes preflighted envían una solicitud OPTIONS antes de la solicitud real para verificar los permisos.

- Los navegadores implementan las políticas CORS de varias maneras: Aunque CORS is un estándar, cada navegador puede usar su propia política de seguridad CORS, que puede cambiar el comportamiento y las restricciones.

Referencias y bibliografía

Control de acceso HTTP (CORS) - HTTP | MDN. (n.d.). Developer.mozilla.org. https://developer.mozilla.org/es/docs/Web/HTTP/CORS

Cross-Origin Resource Sharing. (2014). W3.org. https://www.w3.org/TR/cors/

IBM. (n.d.). *IBM Documentation*. Www.ibm.com. Retrieved May 8, 2023, from https://www.ibm.com/docs/en/app-connect/11.0.0?topic=about-understanding-cross-origin-resource-sharing-cors

MS-Tdykstra (n.d.). *Enable Cross-Origin Requests (CORS) in ASP.NET Core*. Learn.microsoft.com. Retrieved May 8, 2023, from https://docs.microsoft.com/en-us/aspnet/core/security/cors?view=aspnetcore-6.0