Hola,

Al desarrollar la web y evitar posibles casos de inyección de código mediante el API, es recomendable que uses ciertas medidas de seguridad:

En los campos que sean claves (como la zona, ciudad, tipo u operación), valida que sean numéricos.
Por ejemplo, si recibes un parámetro por GET para filtrar por key_zona, sabiendo que key_zona es siempre numérico, valida que efectivamente sea numérico y en caso de no serlo no hacer la petición a la API.

Es recomendable crear una función propia en vez de usar las funciones nativas, por si recibe estos datos con algún formato concreto que no sea puramente numérico (por ejemplo, valores numéricos separados por comas), o cualquier otra manera en la que se pueda recibir estos parámetros y que sepas que es como debe recibirse.

Otro tipo de campo son los campos de texto, en el caso de la referencia, para buscar en la API debes de validar antes, que la cadena de texto con la referencia no contenga código malicioso. Debes de comprobar que no contiene ningún comando SQL, la extensión del texto, si contiene paréntesis anidados o comillas, etc.

Además de lo anteriormente mencionado, debes de tener en cuenta que existe un firewall a nivel de proveedor que también puede detectar estos ataques si los filtros fallaran. Si sucediera esto el firewall del servidor os bloquearía, y la gestión para levantar este bloqueo podría demorarse horas, durante este tiempo la API no daría servicio. Los bloqueos se realizan por IP de donde proviene el ataque de inyección de código.

Para cualquier duda puedes contactar con nosotros en el 966 673 149
O también podes escribir a webs@inmovilla.com