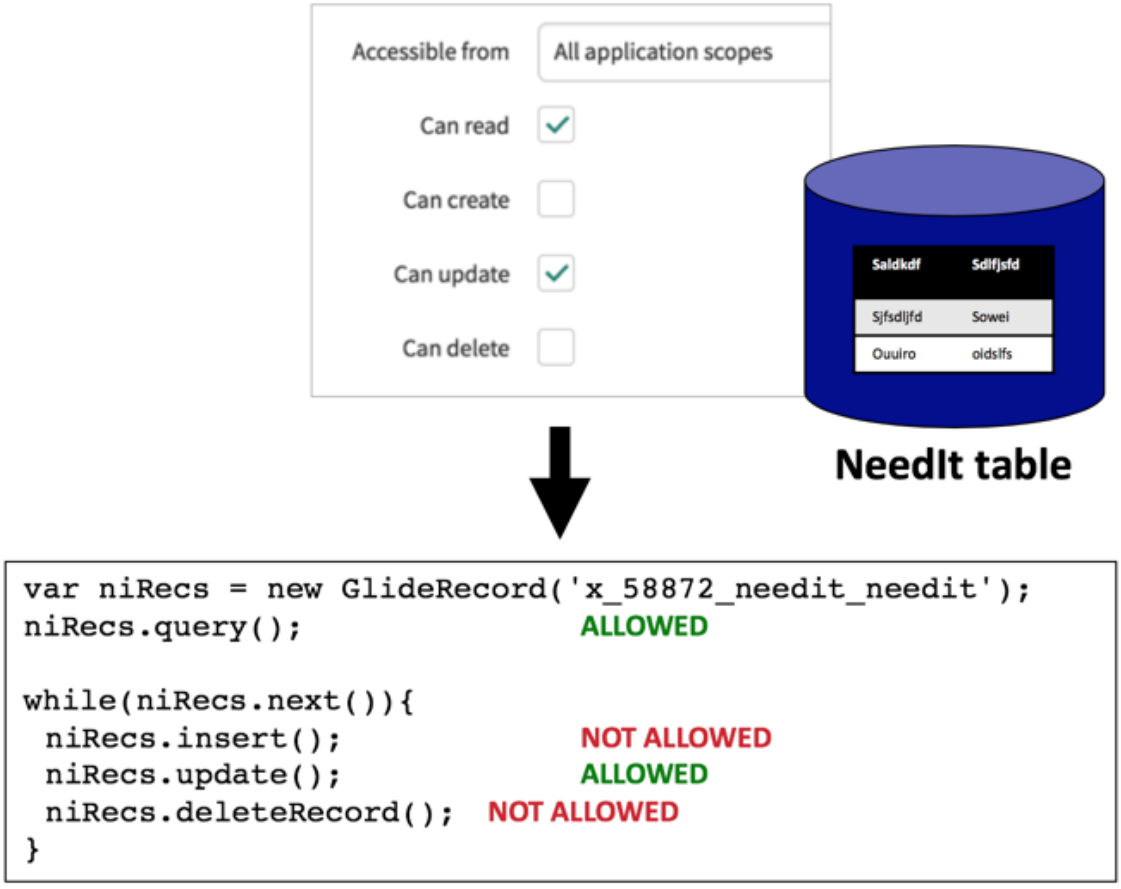
ServiceNow Application Developer

Securing Applications Against Access from Other Applications > Application Access Database Settings

The *Can read*, *Can create*, *Can update*, and *Can delete* Application Access options grant scripts from other application scopes the ability to perform database operations against the table records.

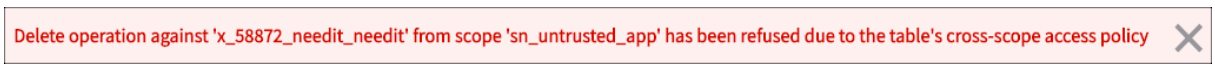
In the default case, all application scope scripts can read the table's records but cannot perform any other database operations. The *GlideRecord* API contains methods for interacting with the ServiceNow database. The permissions in the *Application Access* database settings control which *GlideRecord* methods are allowed and which are not.

In the example, all application scopes can read and update *NeedIt* table records. An out-of-scope script is trying to read, insert, update, and delete records from the *NeedIt* table. The script can read and update the *NeedIt* table records but cannot insert or delete. Note that the script is nonsensical as it does not make sense to insert, update, and delete the same record. The methods are shown to demonstrate what can and cannot be done.



Script from out of scope application

If a script attempts to perform an operation that is not allowed, admin users see a message:



In this case, the out-of-scope application attempted to delete *NeedIt* table records. Although the delete operation did not happen, the script continued to execute. Attempting to perform unauthorized database operations does not cause crashes or damage to table records.