FileMaker Server Security and plugins

On a FileMaker Server plugins can do a lot. Whether you use our MBS Plugin or a few of the others available. They all may offer functions to delete files, to upload files via FTP or to encrypt files. All functions you may use yourself to do backups to remote locations in your scripts.

For all your solutions you must make sure that:

- You do not simply pass user entered text to evaluate or SQL function in FileMaker.
- You do not allow databases on servers with user accounts who can edit scripts or layouts.
- You make sure you limit the plugin features to those you need.

For the first point, well you can let the user enter a calculation and use Evaluate to get the result. e.g. your user enters a number and you multiply it. But what if they enter a plugin call instead? Well, using GetAsNumber first may help to convert input to a number first and strip function calls. Or other cases you may need to remove brackets to remove function calls.
Same for text used in SQL statements, where user can enter SQL commands in text fields and they are executed. But you pass values as parameters and not put them in the SQL directly, right?

Second point means if an user has the chance to modify a script, they could write anything there, including calls to sabotage, steal or delete data. Not to mention creating new scripts which they can trigger anything anywhere. So please limit permissions.

Third, for the MBS Plugin, you can use Plugin.SetFunctions function to limit the list of functions to the ones you need. So maybe instead of 4900 functions, you may only need 20 of them. So you can pass a list of function names and the plugin disables all other functions and you can't call them anymore. With Plugin.LimitFunction you can limit a function to be only called by a certain function. For example you can limit Files.Delete to a script which needs deleting files, but disallow it for all other scripts.

See also an older blog post: Shared FileMaker Server Hosting and Plugin Security