Security

Overview

Security for the file upload widget is managed through an exit program. Since the file upload widget is writing files to the IFS (and can overwrite existing files, depending on configuration), it is very important to ensure that the control is used appropriately.

Since web-based applications depend on values that are sent from the browser, it's possible for a malicious user to "fake" these values in an attempt to trick the application into taking some action that should not be available to the user.

For example, the file upload widget has several validation properties, such as the number of files that can be uploaded, their maximum sizes, etc. To eliminate any chance of a clever hacker faking these values, the file upload control uses an exit program which is called for each file upload and must "approve" the file upload using the actual file details that were received at the server.

This allows the customer complete control over file upload security and ensures that only approved files are actually uploaded.

Exit Program Source Code

Source code for the exit program is supplied in file PROFOUNDUI/QRPGLESRC. The source member is PUIUPLEXIT. The program object is not provided. Customers must compile their own version of the exit program into the PROFOUNDUI library. The name of the compiled exit program object must be PROFOUNDUI/PUIUPLEXIT if your profound installation is in the PROFOUNDUI library.

Customer exit programs will not be modified or replaced during a product update installation; however, the PUIUPLEXIT source member **will** be overwritten with an update. We recommend saving your source member into a different library.

Note: Do not modify the prototype or procedure interface given in the example exit program source member. Any changes here will result in the program failing to perform normally.

Using the Exit Program

The exit program will be called once for each file that is uploaded during a transaction. The exit program must approve each file for upload, or the entire transaction will be cancelled and no files will be uploaded.

The following parameters are passed to the exit program:

- **FileInfo (input):** This data structure contains useful information that the exit program can use to decide whether or not to allow uploading the file. The parameter contains the following subfields:
    - **WidgetId:** The id (as specified in the "id" property) of the file upload widget used in this transaction.
    - **Directory:** The directory where the file will be uploaded to.
    - **Name:** The name of the file.
    - **Type:** The Internet Media Type (i.e. 'text/plain', 'image/gif', etc.) of the file, as reported by the user agent.
    - **Size:** The size (in bytes) of the file.
    - **Exists:** *On if the file already exists on the IFS, *Off otherwise.
- **Allow (output):** The exit program returns 1 in this field to allow the file upload. Any other value returned in this field results in the file upload being prevented.
- **ErrorMsg (output):** An error message to be displayed when the exit program prevents a file upload. If not populated, a generic error message will be given when a file upload is prevented. This parameter is ignored completely when the exit program allows the file upload.

If the exit program does not exist, or if some error occurs while calling it, the entire transaction will be aborted and no files will be uploaded.