Table of Contents

Foswiki::Sandbox

package Foswiki::Sandbox

This package provides an interface to the outside world. All calls to system functions, or handling of file names, should be brokered by the `sysCommand` function in this package.

API version $Date: 2009-04-21 03:53:50 +0200 (Tue, 21 Apr 2009) $ (revision $Rev: 6075 (2010-01-17) $)

Since *date* indicates where functions or parameters have been added since the baseline of the API (TWiki release 4.2.3). The *date* indicates the earliest date of a Foswiki release that will support that function or parameter.

Deprecated *date* indicates where a function or parameters has been deprecated. Deprecated functions will still work, though they should *not* be called in new plugins and should be replaced in older plugins as soon as possible. Deprecated parameters are simply ignored in Foswiki releases after *date*.

Until *date* indicates where a function or parameter has been removed. The *date* indicates the latest date at which Foswiki releases still supported the function or parameter.

StaticMethod untaintUnchecked ($string) -> $untainted

Untaints `$string` without any checks. If $string is undefined, return undef.

This function doesn't perform **any** checks on the data being untainted. Callers **must** ensure that `$string` does not contain any dangerous content, such as interpolation characters, if it is to be used in potentially unsafe operations.

StaticMethod untaint ($datum, \&method, ...) -> $untainted

Calls &$method($datum, ...) and if it returns a non-undef result, returns that result after untainting it. Otherwise returns undef.

\&method can indicate a validation problem in a couple of ways. First, it can throw an exception. Second, it can return undef, which then causes the untaint function to return undef.

StaticMethod validateWebName($name) -> $web

Check that the name is valid for use as a web name. Method used for validation with untaint(). Returns the name, or undef if it is invalid.

StaticMethod validateTopicName($name) -> $topic

Check that the name is valid for use as a topic name. Method used for validation with untaint(). Returns the name, or undef if it is invalid.

StaticMethod normalizeFileName($string) -> $filename

Throws an exception if `$string` contains filtered characters, as defined by `$Foswiki::cfg{NameFilter}`

The returned string is not tainted, but it may contain shell metacharacters and even control characters.

StaticMethod sanitizeAttachmentName($fname) -> ($fileName, $origName)

Given a file name received in a query parameter, sanitise it. Returns the sanitised name together with the basename before sanitisation.

Sanitation includes filtering illegal characters and mapping client file names to legal server names.

StaticMethod sysCommand($class, $template, %params) -> ($data, $exit)

Invokes the program described by `$template` and `%params`, and returns the output of the program and an exit code. STDOUT is returned. STDERR is THROWN AWAY. $class is also ignored, and is only present for compatibility.

The caller has to ensure that the invoked program does not react in a harmful way to the passed arguments. `sysCommand` merely ensures that the shell does not interpret any of the passed arguments.

$template is a template command-line for the program, which contains typed tokens that are replaced with parameter values passed in the `sysCommand` call. For example,

```
my ( $output, $exit ) = Foswiki::Sandbox->sysCommand(
    $command,
    FILENAME => $filename );
```

where `$command` is a template for the command - for example,

```
/usr/bin/rcs -i -t-none -kb %FILENAME|F%
```

`$template` is split at whitespace, and " strings contained in it are replaced with `$params{VAR}`. `%params` values may consist of scalars and array references. Array references are dereferenced and the array elements are inserted. " can optionally take the form '%VAR|T%', where FLAG is a single character type flag. Permitted type flags are

- `U` untaint without further checks -- dangerous,
- `F` normalize as file name,
- `N` generalized number,
- `S` simple, short string,
- `D` RCS format date

- Changes
- Notifications
- RSS Feed
- Statistics
- Preferences

- **User Reference**
- BeginnersStartHere
- TextFormattingRules
- Macros
- FormattedSearch
- QuerySearch
- DocumentGraphics
- SkinBrowser
- InstalledPlugins

- **Admin Maintenance**
- Reference Manual
- AdminToolsCategory
- InterWikis
- ManagingWebs
- SiteTools
- DefaultPreferences
- WebPreferences

- **Categories**
- Admin Documentation
- Admin Tools
- Developer Doc
- User Documentation
- User Tools

- **Webs**
- Public
- System