

Table of Contents

Var ENCODE	1
ENCODE {"string"} -- encodes a string to HTML entities.....	1

VarENCODE

You are here: Wiki >System Web>VarENCODE (09 Jan 2009, ProjectContributor)EditAttach

ENCODE{"string"} -- encodes a string to HTML entities

- Encode "special" characters to HTML numeric entities. Encoded characters are:
 - ◆ all non-printable ASCII characters below space, except newline ("`\n`") and linefeed ("`\r`")
 - ◆ HTML special characters "<", ">", "&", single quote (') and double quote (")
 - ◆ TML special characters "%", "[", "]", "@", "_", "*", "=", and "| "
- Syntax: `%ENCODE{"string"}%`
- Supported parameters:

Parameter:	Description:	Default:
"string"	String to encode	required (can be empty)
type="entity" type="safe" type="html" type="quotes" type="url"	Control how special characters are encoded entity: Encode special characters into HTML entities, like a double quote into <code>&#034;</code> . Does not encode <code>\n</code> or <code>\r</code> . safe: Encode characters ' "<>% into HTML entities. html: As type="entity" except it also encodes <code>\n</code> and <code>\r</code> quotes: Escape double quotes with backslashes (<code>\</code> "), does not change other characters url: Encode special characters for URL parameter use, like a double quote into <code>%22</code> (this is the default)	type="url"

- Example: `%ENCODE{"spaced name"}%` expands to `spaced%20name`
- Values of HTML input fields must be entity encoded.
Example: `<input type="text" name="address" value="%ENCODE{ "any text" type="entity" }%" />`
- Double quotes in strings must be escaped when passed into other macros.
Example: `%SEARCH{ "%ENCODE{ "string with "quotes" type="quotes" }%" noheader="on" }%`
- ENCODE can be used to filter user input from URL parameters and similar to protect against cross-site scripting. The safest approach is to use `type="entity"`. This can however prevent an application from fully working. You can then use `type="safe"` which encodes only the characters ' "<>% into HTML entities (same as `encode="safe"`). When ENCODE is passing a string inside another macro always use double quotes (") `type="quote"`. For maximum security against cross-site scripting you are advised to install the Foswiki:Extensions.SafeWikiPlugin.
- Related: URLPARAM

Topic revision: r1 - 09 Jan 2009 - 13:00:00 - ProjectContributor

- [.System](#)

- [Log In](#)

- **Toolbox**

- [Users](#)
- [Groups](#)
- [Index](#)
- [Search](#)
- [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](#)

•
•
 Copyright © by the contributing authors. All material on this site is the property of the contributing authors.
Ideas, requests, problems regarding Wiki? Send feedback