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 (`"`)
  - TWiki special characters `"%"`, `"["`, `"]"`, `"@"`, `"_"`, `"*"`, `"="` and `"|"`
- Syntax: `%ENCODE{"string"}%`
- Supported parameters:

Parameter:	Description:	Default:
`"string"`	String to encode	required (can be empty)
`type="url"`	Encode special characters for URL parameter use, like a double quote into `%22`	(this is the default)
`type="quotes"`	Escape double quotes with backslashes (`\"`), does not change other characters. This type does not protect against cross-site scripting.	`type="url"`
`type="moderate"`	Encode special characters into HTML entities for moderate cross-site scripting protection: `"<"`, `">"`, single quote (`'`) and double quote (`"`) are encoded. Useful to allow TWiki variables in comment boxes.	`type="url"`
`type="safe"`	Encode special characters into HTML entities for cross-site scripting protection: `"<"`, `">"`, `"%"`, single quote (`'`) and double quote (`"`) are encoded.	`type="url"`
`type="entity"`	Encode special characters into HTML entities, like a double quote into `&#034;`. Does **not** encode newline (`\n`) or linefeed (`\r`).	`type="url"`
`type="html"`	Encode special characters into HTML entities. In addition to `type="entity"`, it also encodes space, `\n` and `\r`. Useful to encode text properly in HTML input fields.	`type="url"`

- Example: `%ENCODE{"spaced name"}%` expands to `spaced%20name`
- ⚠ ***Notes:***
  - Values of HTML input fields should encoded as `"html"`.
    Example: `<input type="text" name="address" value="%ENCODE{ "any text" type="html" }%" />`
  - Double quotes in strings must be escaped when passed into other TWiki variables.
    Example: `%SEARCH{ "%ENCODE{ "string with "quotes"" type="quotes" }%" noheader="on" }%`
  - Use `type="moderate"`, `type="safe"` or `type="entity"` to protect user input from URL parameters and external sources against cross-site scripting (XSS). `type="entity"` is the safest mode, but some TWiki applications might not work. `type="safe"` provides a safe middle ground, `type="moderate"` provides only moderate cross-site scripting protection.

- Related: FORMFIELD, QUERYPARAMS, URLPARAM

This topic: TWiki > VarENCODE
Topic revision: r6 - 2011-06-14 - TWikiContributor

Ideas, requests, problems regarding TWiki? Send feedback
Note: Please contribute updates to this topic on TWiki.org at TWiki:TWiki.VarENCODE.