Escape HTML Characters

In this howto I'm gonna show you how you can escape HTML characters, nice and easy using PHP.

Also, we offer you a online Escape HTML Characters Tool on our site. Enjoy!

This is useful for example to prevent users enter malicious HTML or javascript code into your site using the public forms like guestbooks or message boards. Also this can be useful if you want to embed code into your page without being translated by browsers into HTML elements corresponding.

To do this we have two functions in PHP: htmlentities and htmlspecialchars.

I will comment these functions separately.

htmlentities() function

It is present in PHP4 and PHP5. In the simplest form, it takes as parameter the string to be converted:$str='Reconn.us'
$escaped_html=htmlentities($str);

The result will be like this:
Reconn.us

The text is converted so every element that has a corespondent in HTML will be converted to that. For example, '&' (ampersand) becomes '&'.

If you also want to convert quotes, you may want to make use of the second parameter of this function, quote_style :$str='Reconn.us'
$escaped_html=htmlentities($str,ENT_QUOTES);

This will result in this string:Reconn.us

The options for quote_style parameter are:

- ENT_COMPAT - Will convert double-quotes and leave single-quotes alone.

-ENT_QUOTES - Will convert both double and single quotes.

- ENT_NOQUOTES - Will leave both double and single quotes unconverted. (This is the default)

The third parameter for this function is charset and the default is ISO-8859-1.

To see how this function works, try our Online Escape HTML Tool !

Next, I will explain you how htmlspecialchars() function works and the differences between these functions.

htmlspecialchars() function

Is very much like htmlentities() function. Unlike this function, it does not convert all applicable characters to HTML entities, but only some of them:

- '&' (ampersand) becomes '&'

- '"' (double quote) becomes '"' when ENT_NOQUOTES is not set.

- ''' (single quote) becomes ''' only when ENT_QUOTES is set.

- '<' (less than) becomes '<'

- '>' (greater than) becomes '>'

Otherwise, functions parameters are the same: string htmlspecialchars (string $string [, int $quote_style [, string $charset]]);

To see the difference between these two functions I will show you an example:

The simple text:Confirmar contraseña

for htmlentities() function will output: Confirmar contraseña

and for htmlspecialchars() function will output: Confirmar contraseña

See the difference? For the first function, the special Spanish character ñ is translated also, while for the second is left unchanged.