Cheat sheet

Quick reference if you just need to know how to escape stuff!

Do's and Don'ts

- Use only `query_result_no_html` and `fetchByAssoc(..., -1, false)` or `fetchByAssocNoHtml`, we don't want that pesky `to_html` function to be called
- Do not generate html strings in php, use templates or `HtmlString::build`
- Do not echo html code in PHP, use Smarty
- Do not use `VStr::toJsAttr` method
- Do not try to build js code from PHP, use .js files or `<script>` tags in templates
- Do not use `html_entity_decode`, `htmlentities`, `htmlspecialchars`, `addslashes`, it's probably not needed (unless you are working on legacy code)
- Do not use `to_html`, `from_html`, `decode_html` , these were always a bad idea

How to's:

In	How do I handle... ?	... like this:
Smarty, html code	standard variable	`{$VARIABLE}`
	variable, but it's a HtmlString	`{$VARIABLE}`
	variable, but it's a string and already html	`{$VARIABLE nofilter}` or `{$VARIABLE|rawhtml}`

In	How do I handle... ?	... like this:
`{capture}` blocks		
Smarty, inside `<script>`	string variable	`var myvar = '{$VARIABLE}';`
	object or array variable	`var mylist = {$VARIABLE|json_encode};`
	string inside url	`var url = "index.php?module={$VARIABLE|escape:"url"}";`
Smarty, js in attributes	string variable	

```
{capture assign="capname"}
  <div>.... html code
{$VARIABLE} </div>
{capture}

{$capname nofilter}
```

```
{* using escape in
"javascript" mode *}
<span
onclick="myFunction('{$PARA
M|escape:"javascript"}')">L
ink</span>

{* using out VStr::toJs
method *}
<span
onclick="myFunction2('{VStr
::toJs($PARAM)}')">Link2
</span>
```

In	How do I handle... ?	... like this:
string in url	`<span onclick="location.href='index.php?mode={$MODPARAM|escape:"url"|escape:"javascript"};>Link 3</span>`	

Revision #2
Created 2026-01-23 15:29:18 UTC by m.maporti
Updated 2026-05-05 12:02:45 UTC by Daniele