XSS Prevention Cheat Sheets

Kentico Encoding Methods

CONTEXT	Class	Method	Description
HTML	HTML Helper	HTMLEncode(string inputText)	Converts special characters in a string into HTML entities.
		HTMLDecode(string inputText)	Decodes HTML entities in a string.
		EncodeForHtmlAttribute(string inputText)	Returns an HTML-encoded string to be used in an HTML attribute.
	Query Helper	GetText(string name, ...)	Returns an HTML-encoded query string parameter.
JS	Script Helper	GetString(string text)	Returns encoded text for use in JavaScript strings encapsulated with apostrophes.

Encoding Method Outputs

Class	Method	Results	
HTMLHelper	HTMLEncode(...)	In	<script>alert('XSS')</script>
		Out	<script>alert('XSS')</script>
	HTMLDecode(...)	In	<script>alert('XSS')</script>
		Out	<script>alert('XSS')</script>
	EncodeForHtmlAttribute(...)	In	"onmouseover='alert(document.cookie)'
		Out	"onmouseover='alert(document.cookie)'

Class	Method	Results	
Query Helper	GetText(...)	In	?objectname=<script>alert('XSS')</script>
		Out	?objectname=<script>alert('XSS')</script>

Class	Method	Results	
Script Helper	GetString(...)	In	</script><script>alert('XSS')</script>
		Out	'\</script\>\<script\>alert(\'XSS\')\</script\>'