

PMB - Problèmes fonctionnels #148

HTML non échappé dans l'affichage des paramètres (Administration/Outils/paramètres)

01/11/2017 10:59 AM - Jean-François FALCONNIER

Status:	Proposé	Start date:	01/11/2017
Priority:	Urgent	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:			
Description			
<p>Il est nécessaire d'échapper les caractères HTML lors de la construction de la page pour éviter leur interprétation par le navigateur. Les balises <link> <style> <images> ne doivent en aucun cas être incluses telles quelles à cet endroit là. La météo par exemple est activée par le paramètre show_meteo, mais sans échappement, l'image est appelée lorsque l'on consulte les paramètres quelque soit ce réglage.</p>			
admin/param/param_func.inc.php, ligne 124			
<pre>print "<td class='ligne_data'>\$param->valeur_param</td><td valign='top'>\$param->comment_param</td>\n</tr>";</pre>			
devrait être:			
<pre>print "<td class='ligne_data'>".htmlspecialchars(\$param->valeur_param)."</td><td valign='top'>".htmlspecialchars(\$param->comment_param)."</td>\n</tr>";</pre>			