µWeb - Bug #598

500 error should be protected against xss attacks

2012-01-26 15:48 - Jan Klopper

Status:	Closed	**Start date:**	2012-01-26
Priority:	High	**Due date:**	
Assignee:	Jan Klopper	**% Done:**	100%
Category:	PageMaker	**Estimated time:**	0.00 hour
Target version:		**Spent time:**	1.00 hour

Description

Currently the 500 error handler displays all scope vars as a list, if these scope vars contain html, this html is presented unescaped to the browser, providing an xss exploit opertunity.

This should **all** be fixed.

Associated revisions

Revision 3366:65f6e2c86f08 - 2012-01-26 17:20 - Elmer de Looff

TemplateConditional statements must now use only tag variables. These now get a local name that is stored in a dictionary for eval(expr, locals=). This resolves #598.

Revision 178:54112d4389c6 - 2012-01-26 17:20 - Elmer de Looff

TemplateConditional statements must now use only tag variables. These now get a local name that is stored in a dictionary for eval(expr, locals=). This resolves #598.

Revision 3369:f2073fc5017d - 2012-01-26 19:21 - Elmer de Looff

Updated http500 template to use proper template conditional statements, and wrap all error outputs with html-escaping. This resolves #598.

Revision 179:99a0f6bf230c - 2012-01-26 19:21 - Elmer de Looff

Updated http500 template to use proper template conditional statements, and wrap all error outputs with html-escaping. This resolves #598.

History

#1 - 2012-01-26 19:49 - Elmer de Looff

- Status changed from New to Resolved

- Assignee changed from Elmer de Looff to Jan Klopper

- % Done changed from 0 to 70

This has been fixed. All variables will be properly html-escaped before ouput. When templates are captured in local variables, this will cause their literal html source to be printed for the human eye. Double escaping might happen but then the displayed source will show the single-escaped source as desired.

Also fixed bugs with conditional statements in the http500 template, which were illegal in the current fixed version.

#2 - 2012-02-09 19:32 - Elmer de Looff

Applied in changeset commit:65f6e2c86f08.

#3 - 2012-02-09 19:32 - Elmer de Looff

Applied in changeset commit:f2073fc5017d.

#4 - 2012-02-10 10:45 - Jan Klopper

- Status changed from Resolved to Closed

- % Done changed from 70 to 100

tested, this works correctly now