It's not recommended to escape ' to &apos;

08/10/2012 08:32 AM - spastorino (Santiago Pastorino)

Status: Closed
Priority: Normal
Assignee: xibbar (Takeyuki FUJIOKA)
Target version: 2.0.0
ruby -v: 2.0.0dev

Description
OWASP doesn't recommend it
https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet#RULE_.231_-_HTML_Escape_Before_Inserting_Untrusted_Data_into_HTML_Element_Content
and ' is not a valid in HTML4
http://www.w3.org/TR/html4/sgml/entities.html

I've made a Pull Request on github too
https://github.com/ruby/ruby/pull/154

Related issues:
Related to Ruby master - Bug #5485: ERB html_escape should follow OWASP recom... Closed 10/26/2011

Associated revisions
Revision 745ada86 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36692 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

Revision 36692 - 08/14/2012 03:03 AM - xibbar (Takeyuki FUJIOKA)
Tue Aug 14 11:55:37 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML): ' is not recommended. [Bug #6850]

History
#1 - 08/10/2012 11:01 AM - xibbar (Takeyuki FUJIOKA)
- Assignee set to xibbar (Takeyuki FUJIOKA)

#2 - 08/10/2012 11:01 AM - xibbar (Takeyuki FUJIOKA)
- Status changed from Open to Assigned

#3 - 08/14/2012 01:15 AM - spastorino (Santiago Pastorino)
I've just updated the pull request to take in consideration https://bugs.ruby-lang.org/projects/ruby-trunk/repository/revisions/36687

#4 - 08/14/2012 12:03 PM - xibbar (Takeyuki FUJIOKA)
- Status changed from Assigned to Closed
- % Done changed from 0 to 100

This issue was solved with changeset r36692.
Santiago, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

Tue Aug 14 11:55:37 2012  Takeyuki FUJIOKA  xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI::escapeHTML); ` is not recommended. [Bug #6850]