Ruby master - Bug #6850

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

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

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>xibbar (Takeyuki FUJIOKA)</td>
</tr>
<tr>
<td>Target version:</td>
<td>2.0.0</td>
</tr>
<tr>
<td>ruby -v:</td>
<td>2.0.0dev</td>
</tr>
<tr>
<td>Backport:</td>
<td></td>
</tr>
</tbody>
</table>
| 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](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/sqml/entities.html](http://www.w3.org/TR/html4/sqml/entities.html)  
I've made a Pull Request on github too [https://github.com/ruby/ruby/pull/154](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]

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]

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**

08/06/2021
I've just updated the pull request to take in consideration https://bugs.ruby-lang.org/projects/ruby-trunk/repository/revisions/36687

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.

* lib/cgi/util.rb (CGI::escapeHTML): `\` is not recommended. [Bug #6850]