Ruby master - Feature #6620
Add &apos; to CGI's HTML escaping
06/22/2012 07:53 AM - drbrain (Eric Hodel)

<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>
</tbody>
</table>

Description:
From https://github.com/ruby/ruby/pull/52

Patch by Igor Sales: https://github.com/ruby/ruby/pull/52.diff

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

Associated revisions
Revision 07132e06 - 07/03/2012 11:32 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 4 08:24:28 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
  * lib/cgi/util.rb: Add ` to CGI's HTML escaping.[Feature #6620]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36299 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 36299 - 07/03/2012 11:32 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 4 08:24:28 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
  * lib/cgi/util.rb: Add ` to CGI's HTML escaping.[Feature #6620]

Revision 36299 - 07/03/2012 11:32 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 4 08:24:28 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
  * lib/cgi/util.rb: Add ` to CGI's HTML escaping.[Feature #6620]

Revision 36299 - 07/03/2012 11:32 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 4 08:24:28 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
  * lib/cgi/util.rb: Add ` to CGI's HTML escaping.[Feature #6620]

Revision 36299 - 07/03/2012 11:32 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 4 08:24:28 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
  * lib/cgi/util.rb: Add ` to CGI's HTML escaping.[Feature #6620]

Revision 36299 - 07/03/2012 11:32 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 4 08:24:28 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
  * lib/cgi/util.rb: Add ` to CGI's HTML escaping.[Feature #6620]

Revision 36299 - 07/03/2012 11:32 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 4 08:24:28 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
  * lib/cgi/util.rb: Add ` to CGI's HTML escaping.[Feature #6620]

Revision c47cca2f - 07/17/2012 11:04 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 18 07:59:29 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
  * lib/cgi/util.rb (CGI.escapeHTML,unescapeHTML): Add ` for HTML5 escaping. [Feature #6620]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36422 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

09/23/2021
Revision 36422 - 07/17/2012 11:04 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 18 07:59:29 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI.escapeHTML,unescapeHTML): Add ' for HTML5 escaping. [Feature #6620]

Revision 36422 - 07/17/2012 11:04 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 18 07:59:29 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI.escapeHTML,unescapeHTML): Add ' for HTML5 escaping. [Feature #6620]

Revision 36422 - 07/17/2012 11:04 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 18 07:59:29 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI.escapeHTML,unescapeHTML): Add ' for HTML5 escaping. [Feature #6620]

Revision 36422 - 07/17/2012 11:04 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 18 07:59:29 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI.escapeHTML,unescapeHTML): Add ' for HTML5 escaping. [Feature #6620]

Revision 36422 - 07/17/2012 11:04 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 18 07:59:29 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI.escapeHTML,unescapeHTML): Add ' for HTML5 escaping. [Feature #6620]

Revision 36422 - 07/17/2012 11:04 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 18 07:59:29 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI.escapeHTML,unescapeHTML): Add ' for HTML5 escaping. [Feature #6620]

Revision 36422 - 07/17/2012 11:04 PM - xibbar (Takeyuki FUJIOKA)
Wed Jul 18 07:59:29 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb (CGI.escapeHTML,unescapeHTML): Add ' for HTML5 escaping. [Feature #6620]

History

#1 - 07/04/2012 05:48 AM - xibbar (Takeyuki FUJIOKA)
- Status changed from Open to Assigned

#2 - 07/04/2012 08:32 AM - xibbar (Takeyuki FUJIOKA)
- Status changed from Assigned to Closed
- % Done changed from 0 to 100

This issue was solved with changeset r36299.
Eric, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

Wed Jul 4 08:24:28 2012 Takeyuki FUJIOKA xibbar@ruby-lang.org
- lib/cgi/util.rb: Add ' to CGI's HTML escaping.[Feature #6620]

#3 - 07/04/2012 01:44 PM - xibbar (Takeyuki FUJIOKA)
- Status changed from Closed to Rejected

' is not html but xml specification.

#4 - 07/09/2012 01:26 PM - moxley (Moxley Stratton)
' is a valid entity for both XHML (http://www.w3.org/TR/xhtml1/dtds.html) and HTML5 (http://www.w3.org/TR/2011/WD-html5-20110525/syntax.html#attributes-0), and is supported by all mainstream browsers. It is a potential security risk not to escape the apostrophe character, because the apostrophe is a valid quote character for attribute values. For example:

```
name = "' href='javascript:doSomethingBad()"
"Foo"
```

The above creates a link to "javascript:doSomethingBad()", not "/foo". At the very least, the apostrophe should be escaped to its numeric entity, ' because it is part of HTML syntax.

09/23/2021 2/3
#5 - 07/10/2012 10:33 AM - xibbar (Takeyuki FUJIOKA)
- Status changed from Rejected to Assigned

Sorry, I confirmed this specification in HTML5. I will import ` later. Please wait.

#6 - 07/18/2012 08:04 AM - xibbar (Takeyuki FUJIOKA)
- Status changed from Assigned to Closed

This issue was solved with changeset r36422.
Eric, thank you for reporting this issue. Your contribution to Ruby is greatly appreciated. May Ruby be with you.