Ruby trunk - Bug #12791

Don't allow ,-separator for cookie

09/27/2016 03:11 AM - naruse (Yui NARUSE)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:		**Backport:**	2.1: UNKNOWN, 2.2: UNKNOWN, 2.3: UNKNOWN

Description

RFC2965 allowed both ; and , as a separator for cookie, but RFC6265 only allows ;.

Moreover CVE-2016-7401 uses , as a separator to overwrite CSRF-token.
https://gist.github.com/mala/457a25650950d4daf4144f98159802cc

Associated revisions

Revision 5f33c6b0 - 09/27/2016 03:17 AM - naruse (Yui NARUSE)

- lib/cgi/cookie.rb (parse): don't allow , as a separator. [Bug #12791]
- lib/webrick/cookie.rb (parse): ditto.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@56262 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 56262 - 09/27/2016 03:17 AM - naruse (Yui NARUSE)

- lib/cgi/cookie.rb (parse): don't allow , as a separator. [Bug #12791]
- lib/webrick/cookie.rb (parse): ditto.

Revision 56262 - 09/27/2016 03:17 AM - naruse (Yui NARUSE)

- lib/cgi/cookie.rb (parse): don't allow , as a separator. [Bug #12791]
- lib/webrick/cookie.rb (parse): ditto.

Revision 56262 - 09/27/2016 03:17 AM - naruse (Yui NARUSE)

- lib/cgi/cookie.rb (parse): don't allow , as a separator. [Bug #12791]
- lib/webrick/cookie.rb (parse): ditto.

Revision 56262 - 09/27/2016 03:17 AM - naruse (Yui NARUSE)

- lib/cgi/cookie.rb (parse): don't allow , as a separator. [Bug #12791]
- lib/webrick/cookie.rb (parse): ditto.

History

#1 - 09/27/2016 03:17 AM - naruse (Yui NARUSE)

- Status changed from Open to Closed

Applied in changeset r56262.

- lib/cgi/cookie.rb (parse): don't allow , as a separator. [Bug #12791]
- lib/webrick/cookie.rb (parse): ditto.