Ruby master - Bug #5022

WEBrick returns improper response for malformed HTTP Request

07/13/2011 03:25 PM - felixalias (Felix Jodoin)

Status:	Closed		
Priority:	Normal		
Assignee:	tenderlovemaking (Aaron Patterson)		
Target version:	1.9.3		
ruby -v:	ruby 1.9.2p180 (2011-02-18 revision 30909) [x86_64-darwin10.7.0]	**Backport:**	

Description

=begin

When sending an improper HTTP request in the form of:

GET /\n

(with any valid or invalid HTTP verb), WEBrick returns:

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN">

Internal Server Error

Internal Server Error
undefined method `each' for nil:NilClass

WEBrick/1.3.1 (Ruby/1.9.2/2011-02-18) at
localhost:3000

and then closes the connection, without sending any HTTP status headers or printing a correct '400 Bad Request' error page. This is because the @header variable wasn't set up properly, so @header is nil when a message is passed to it when handling the request. WEBrick's log on the server console will read similar to:

[2011-07-13 00:49:40] ERROR NoMethodError: undefined method each' for nil:NilClass
/Users/x/.rvm/rubies/ruby-1.9.2-p180/lib/ruby/1.9.1/webrick/httprequest.rb:154:ineach'
/Users/x/.rvm/rubies/ruby-1.9.2-p180/lib/ruby/1.9.1/webrick/httprequest.rb:231:in meta_vars'
/Users/x/.rvm/gems/ruby-1.9.2-p180/gems/rack-1.3.0/lib/rack/handler/webrick.rb:34:inservice'
/Users/x/.rvm/rubies/ruby-1.9.2-p180/lib/ruby/1.9.1/webrick/httpserver.rb:111:in service'
/Users/x/.rvm/rubies/ruby-1.9.2-p180/lib/ruby/1.9.1/webrick/httpserver.rb:70:inrun'
/Users/x/.rvm/rubies/ruby-1.9.2-p180/lib/ruby/1.9.1/webrick/server.rb:183:in `block in start_thread'

(Where line 34 of rack/handler/webrick.rb is a simple env = req.meta_vars)

This is reproducible in both 1.8.7 and 1.9.2.

A simple patch is attached to WEBrick's httprequest.rb that will allow the request to continue processing, fixing the 500 internal server error (and let the app decide how to handle the malformed request). In my testing with rack 1.3.0 & sinatra 1.2.6, this patch allowed the request complete normally.

=end

Associated revisions

Revision 2dfc9e16 - 07/21/2011 08:27 AM - naruse (Yui NARUSE)

- lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each): Allow HTTP/0.9 request which doesn't has any header or body. patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32593 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 32593 - 07/21/2011 08:27 AM - naruse (Yui NARUSE)

- lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each): Allow HTTP/0.9 request which doesn't has any header or body. patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]

Revision 32593 - 07/21/2011 08:27 AM - naruse (Yui NARUSE)

- lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each): Allow HTTP/0.9 request which doesn't has any header or body. patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]

Revision 32593 - 07/21/2011 08:27 AM - naruse (Yui NARUSE)

- lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each): Allow HTTP/0.9 request which doesn't has any header or body. patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]

Revision 32593 - 07/21/2011 08:27 AM - naruse (Yui NARUSE)

- lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each): Allow HTTP/0.9 request which doesn't has any header or body. patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]

Revision 32593 - 07/21/2011 08:27 AM - naruse (Yui NARUSE)

- lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each): Allow HTTP/0.9 request which doesn't has any header or body. patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]

Revision 32593 - 07/21/2011 08:27 AM - naruse (Yui NARUSE)

- lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each): Allow HTTP/0.9 request which doesn't has any header or body. patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]

Revision 11b4be8e - 07/22/2011 12:49 PM - naruse (Yui NARUSE)

merge revision(s) 32593:

```
    * lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each):
      Allow HTTP/0.9 request which doesn't has any header or body.
      patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@32625 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 07/13/2011 03:39 PM - tenderlovemaking (Aaron Patterson)

Can you add a test?

Also, I'm not sure that this should be an error. In section 4.1 of RFC 1945, it says that simple requests are OK. Simple requests do not require an http version:

Simple-Request = "GET" SP Request-URI CRLF

#2 - 07/13/2011 04:56 PM - felixalias (Felix Jodoin)

- File webrick_test_httprequest_case.patch added

Aaron Patterson wrote:

> Can you add a test?
>
> Also, I'm not sure that this should be an error. In section 4.1 of RFC 1945, it says that simple requests are OK. Simple requests do not require an http version:
>
> Simple-Request = "GET" SP Request-URI CRLF

Hi, yes, this should not be a 400 bad request at all (I was incorrect in labeling it as a malformed HTTP request) - however, it is still broken without my patch since it returns a 500 instead of passing the request. Rather than erroring when the meta_vars are accessed, it should be prepared for a nil

header (as RFC 1945 specifies headers should not exist with an HTTP/0.9 simple request). With my original patch applied, meta_vars will work as intended.

The attached test case will illustrate this (patches test/webrick/test_httprequest.rb).

#3 - 07/13/2011 05:30 PM - nobu (Nobuyoshi Nakada)

- Category set to lib

- Assignee set to tenderlovemaking (Aaron Patterson)

- Target version set to 1.9.3

assert(hash) does not seem nice.
assert_equal({}, hash) would be better.

#4 - 07/14/2011 02:40 AM - felixalias (Felix Jodoin)

Nobuyoshi Nakada wrote:

> assert(hash) does not seem nice.
> assert_equal({}, hash) would be better.

Has to be assert_nothing_raised { } at least, since meta_vars won't be empty with no headers.

Improved test case:

def test_simple_request
msg = <<-end_of_message
GET /
end_of_message

```
req = WEBrick::HTTPRequest.new(WEBrick::Config::HTTP)
req.parse(StringIO.new(msg.gsub(/^ {6}/, '')))

# assertion fails if @header was not initialized and iteration is attempted on the nil reference
assert_nothing_raised('req.meta_vars should be available with HTTP/0.9 simple request') { req.meta_vars }
```

end

#5 - 07/21/2011 02:30 PM - kosaki (Motohiro KOSAKI)

- Status changed from Open to Assigned

#6 - 07/21/2011 05:27 PM - naruse (Yui NARUSE)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r32593.
Felix, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- lib/webrick/httprequest.rb (WEBrick::HTTPRequest#each): Allow HTTP/0.9 request which doesn't has any header or body. patched by Felix Jodoin. [ruby-core:38040] [Bug #5022]

Files

webrick_httprequest_header_fix.patch	323 Bytes	07/13/2011	felixalias (Felix Jodoin)
webrick_test_httprequest_case.patch	676 Bytes	07/13/2011	felixalias (Felix Jodoin)