

## Backport193 - Backport #7325

### Marshal#load taints classes if they are referenced in a marshaled object

11/10/2012 10:00 PM - urielka (Uriel Katz)

<b>Status:</b>	Closed
<b>Priority:</b>	Normal
<b>Assignee:</b>	usa (Usaku NAKAMURA)
<b>Description</b>	
<pre>=begin = Reproducing steps: ruby taint.rb  = Output of this script in my computer running 1.9.3-p327: Before marshal is tainted?: false After marshal is tainted?: true Safe level when calling tainted method using call: 4 Safe level when calling tainted method directly: 0  = Expected: MyObject#test shouldn't be tainted as it was defined in my own source and what was saved into the file is just a reference to MyObject class ("\u0004\bcrMyObject")  = Actual: MyObject#test is tainted and calling it using Method#call will make it run in safe-level 4.  = Some background on how I got to this issue: I wrote some RPC code that accepts a class and method name and does the invocation,the way I call the method is getting the method from the instance using something like: "cls_instance.method(method_name).call"  I used Rails.cache with FileStore (which uses Marshal#load from file) to cache a object that had references to classes.  After reading from the cache all other requests saw the classes as tainted and when calling the methods they ran at \$SAFE=4 which caused it to fail (even puts doesn't work at that level :)  This issue also made me understand that there is 2 potential bugs in Rails. =end</pre>	

#### Associated revisions

##### Revision 0ac361f5 - 12/13/2012 05:12 AM - shugo (Shugo Maeda)

- marshal.c (r\_entry0): don't taint classes and modules because Marshal.load just return the dumped classes and modules. [Bug #7325] [ruby-core:49198]
- test/ruby/test\_marshal.rb: related test.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@38357 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

##### Revision 38357 - 12/13/2012 05:12 AM - shugo (Shugo Maeda)

- marshal.c (r\_entry0): don't taint classes and modules because Marshal.load just return the dumped classes and modules. [Bug #7325] [ruby-core:49198]
- test/ruby/test\_marshal.rb: related test.

**Revision 38357 - 12/13/2012 05:12 AM - shugo (Shugo Maeda)**

- marshal.c (r\_entry0): don't taint classes and modules because Marshal.load just return the dumped classes and modules. [Bug #7325] [ruby-core:49198]
- test/ruby/test\_marshal.rb: related test.

**Revision 38357 - 12/13/2012 05:12 AM - shugo (Shugo Maeda)**

- marshal.c (r\_entry0): don't taint classes and modules because Marshal.load just return the dumped classes and modules. [Bug #7325] [ruby-core:49198]
- test/ruby/test\_marshal.rb: related test.

**Revision 38357 - 12/13/2012 05:12 AM - shugo (Shugo Maeda)**

- marshal.c (r\_entry0): don't taint classes and modules because Marshal.load just return the dumped classes and modules. [Bug #7325] [ruby-core:49198]
- test/ruby/test\_marshal.rb: related test.

**Revision 38357 - 12/13/2012 05:12 AM - shugo (Shugo Maeda)**

- marshal.c (r\_entry0): don't taint classes and modules because Marshal.load just return the dumped classes and modules. [Bug #7325] [ruby-core:49198]
- test/ruby/test\_marshal.rb: related test.

**Revision 38357 - 12/13/2012 05:12 AM - shugo (Shugo Maeda)**

- marshal.c (r\_entry0): don't taint classes and modules because Marshal.load just return the dumped classes and modules. [Bug #7325] [ruby-core:49198]
- test/ruby/test\_marshal.rb: related test.

**Revision 60e7104f - 12/19/2012 12:13 PM - usa (Usaku NAKAMURA)**

merge revision(s) 38357,38363: [Backport #7325]

```
* marshal.c (r_entry0): don't taint classes and modules because
  Marshal.load just return the dumped classes and modules.
  [Bug #7325] [ruby-core:49198]
```

```
* test/ruby/test_marshal.rb: related test.
  Marshal.load just returns the dumped classes and modules.
```

**Revision 38468 - 12/19/2012 12:13 PM - usa (Usaku NAKAMURA)**

merge revision(s) 38357,38363: [Backport #7325]

```
* marshal.c (r_entry0): don't taint classes and modules because
  Marshal.load just return the dumped classes and modules.
  [Bug #7325] [ruby-core:49198]
```

```
* test/ruby/test_marshal.rb: related test.
  Marshal.load just returns the dumped classes and modules.
```

**History**

---

**#1 - 11/25/2012 12:11 PM - mame (Yusuke Endoh)**

- Status changed from Open to Assigned
- Assignee set to shugo (Shugo Maeda)
- Target version set to 2.0.0

Summarized:

```
p Integer.tainted? #=> false
Marshal.load(Marshal.dump(Integer).taint)
p Integer.tainted? #=> expected: false, actual: true
```

Indeed, it looks weird. Shugo-san, what do you think?

--

Yusuke Endoh [mame@tsq.ne.jp](mailto:mame@tsq.ne.jp)

**#2 - 12/13/2012 02:12 PM - shugo (Shugo Maeda)**

- Status changed from Assigned to Closed
- % Done changed from 0 to 100

This issue was solved with changeset r38357.  
Uriel, thank you for reporting this issue.  
Your contribution to Ruby is greatly appreciated.  
May Ruby be with you.

- 
- marshal.c (r\_entry0): don't taint classes and modules because  
 Marshal.load just return the dumped classes and modules.  
 [Bug [#7325](#)] [ruby-core:49198]
  - test/ruby/test\_marshal.rb: related test.

**#3 - 12/14/2012 05:33 PM - usa (Usaku NAKAMURA)**

- Tracker changed from Bug to Backport
- Project changed from Ruby master to Backport193
- Status changed from Closed to Assigned
- Assignee changed from shugo (Shugo Maeda) to usa (Usaku NAKAMURA)
- Target version deleted (2.0.0)

**#4 - 12/14/2012 05:35 PM - usa (Usaku NAKAMURA)**

memo: r38357 is also related.

**#5 - 12/19/2012 09:13 PM - usa (Usaku NAKAMURA)**

- Status changed from Assigned to Closed

This issue was solved with changeset [r38468](#).  
Uriel, thank you for reporting this issue.  
Your contribution to Ruby is greatly appreciated.

May Ruby be with you.

---

merge revision(s) 38357,38363: [Backport [#7325](#)]

```
* marshal.c (r_entry0): don't taint classes and modules because
  Marshal.load just return the dumped classes and modules.
  [Bug #7325] [ruby-core:49198]

* test/ruby/test_marshal.rb: related test.
  Marshal.load just returns the dumped classes and modules.
```

---

## Files

taint.rb	458 Bytes	11/10/2012	urielka (Uriel Katz)
----------	-----------	------------	----------------------