

## Ruby master - Bug #884

### Insecure operation: -r

12/15/2008 08:06 PM - znz (Kazuhiro NISHIYAMA)

<b>Status:</b> Closed	
<b>Priority:</b> Normal	
<b>Assignee:</b> ko1 (Koichi Sasada)	
<b>Target version:</b>	
<b>ruby -v:</b>	<b>Backport:</b>
<b>Description</b> =begin #####-r#####  % ruby-trunk -ve '\$SAFE=4;open("")' ruby 1.9.1 (2008-12-14 revision 20736) [i686-linux] -e:1:in open': Insecure operation: -r (SecurityError) from -e:1:in' % =end	

#### Associated revisions

##### Revision aebfdbeea573c031ea690ee93f816a53ac27ca51 - 12/27/2008 07:22 AM - ko1 (Koichi Sasada)

- eval.c (rb\_frame\_callee, rb\_frame\_caller): rb\_frame\_callee() should return method id on current frame. add rb\_frame\_caller() to get method id on parent frame. Bug #884 [ruby-dev:37446]
- eval.c (rb\_f\_method\_name): use rb\_frame\_caller() instead of rb\_frame\_callee().

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@21093 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

##### Revision aebfdbee - 12/27/2008 07:22 AM - ko1 (Koichi Sasada)

- eval.c (rb\_frame\_callee, rb\_frame\_caller): rb\_frame\_callee() should return method id on current frame. add rb\_frame\_caller() to get method id on parent frame. Bug #884 [ruby-dev:37446]
- eval.c (rb\_f\_method\_name): use rb\_frame\_caller() instead of rb\_frame\_callee().

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@21093 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

##### Revision 21093 - 12/27/2008 07:22 AM - ko1 (Koichi Sasada)

- eval.c (rb\_frame\_callee, rb\_frame\_caller): rb\_frame\_callee() should return method id on current frame. add rb\_frame\_caller() to get method id on parent frame. Bug #884 [ruby-dev:37446]
- eval.c (rb\_f\_method\_name): use rb\_frame\_caller() instead of rb\_frame\_callee().

##### Revision 21093 - 12/27/2008 07:22 AM - ko1 (Koichi Sasada)

- eval.c (rb\_frame\_callee, rb\_frame\_caller): rb\_frame\_callee() should return method id on current frame. add rb\_frame\_caller() to get method id on parent frame. Bug #884 [ruby-dev:37446]
- eval.c (rb\_f\_method\_name): use rb\_frame\_caller() instead of rb\_frame\_callee().

##### Revision 21093 - 12/27/2008 07:22 AM - ko1 (Koichi Sasada)

- eval.c (rb\_frame\_callee, rb\_frame\_caller): rb\_frame\_callee() should return method id on current frame. add rb\_frame\_caller() to get method id on parent frame. Bug #884 [ruby-dev:37446]
- eval.c (rb\_f\_method\_name): use rb\_frame\_caller() instead of rb\_frame\_callee().

##### Revision 21093 - 12/27/2008 07:22 AM - ko1 (Koichi Sasada)

- eval.c (rb\_frame\_callee, rb\_frame\_caller): rb\_frame\_callee() should return method id on current frame. add rb\_frame\_caller() to get method id on parent frame. Bug #884 [ruby-dev:37446]
- eval.c (rb\_f\_method\_name): use rb\_frame\_caller() instead of rb\_frame\_callee().



Yukihiro Matsumoto wrote::

```
|
|
| % ruby-trunk -ve '$SAFE=4;open("")'
| ruby 1.9.1 (2008-12-14 revision 20736) [i686-linux]
| -e:1:in open': Insecure operation: -r (SecurityError)
|   from -e:1:in'
| %
```

```
rb_check_safe_obj()
rb_frame_callee() NULL
```

```
rb_check_safe_obj()
(-r)
```

```
rb_frame_callee() caller
rb_f_method_name() rb_frame_caller()
rb_frame_callee()
```

Index: eval.c

=====

--- eval.c (20968)

+++ eval.c

@@ -750,6 +750,12 @@ rb\_frame\_this\_func(void)

ID

rb\_frame\_callee(void)

{

- return frame\_func\_id(GET\_THREAD()->cfp); +} +static ID +rb\_frame\_caller(void) +{ rb\_thread\_t th = GET\_THREAD(); rb\_control\_frame\_t \*prev\_cfp = RUBY\_VM\_PREVIOUS\_CONTROL\_FRAME(th->cfp); /\* check if prev\_cfp can be accessible \*/ @@ -1105,7 +1111,7 @@ rb\_f\_local\_variables(void) static VALUE rb\_f\_method\_name(void) {
- ID fname = rb\_frame\_callee();

- ID fname = rb\_frame\_caller(); /\* need caller ID \*/

```
if (fname) {
return ID2SYM(fname);
```

--

// SASADA Koichi at atdot dot net

=end

**#4 - 12/27/2008 04:27 PM - ko1 (Koichi Sasada)**

- Status changed from Open to Closed

- % Done changed from 0 to 100

=begin

Applied in changeset r21093.

=end