Ruby - Bug #9588

program name variables tainted

03/03/2014 09:09 AM - jrusnack (Jan Rusnacko)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	1.8.7, 1.9.3, 2.0.0	**Backport:**	

Description

I have noticed inconsistency in taint flag of program name:

```
[jrusnack@dhcp-31-42 ruby-safe]$ cat tainted.rb
#!/usr/bin/env ruby
puts "$0:            #{$0}, tainted? #{$0.tainted?}"
puts "__FILE__:      #{__FILE__}, tainted? #{__FILE__.tainted?}"
puts "$PROGRAM_NAME: #{$PROGRAM_NAME}, tainted? #{$PROGRAM_NAME.tainted?}"

[jrusnack@dhcp-31-42 ruby-safe]$ rvm use 1.8.7
Using /home/jrusnack/.rvm/gems/ruby-1.8.7-p374

[jrusnack@dhcp-31-42 ruby-safe]$ ./tainted.rb
$0:            ./tainted.rb, tainted? true
__FILE__:      ./tainted.rb, tainted? false
$PROGRAM_NAME: ./tainted.rb, tainted? true

[jrusnack@dhcp-31-42 ruby-safe]$ rvm use 1.9.3
Using /home/jrusnack/.rvm/gems/ruby-1.9.3-p484

[jrusnack@dhcp-31-42 ruby-safe]$ ./tainted.rb
$0:            ./tainted.rb, tainted? false
__FILE__:      ./tainted.rb, tainted? true
$PROGRAM_NAME: ./tainted.rb, tainted? false

[jrusnack@dhcp-31-42 ruby-safe]$ rvm use 2.0.0
Using /home/jrusnack/.rvm/gems/ruby-2.0.0-p353

[jrusnack@dhcp-31-42 ruby-safe]$ ./tainted.rb
$0:            ./tainted.rb, tainted? false
__FILE__:      ./tainted.rb, tainted? true
$PROGRAM_NAME: ./tainted.rb, tainted? false
```

Related issues:

Related to Ruby - Feature #16131: Remove $SAFE, taint and trust	**Closed**

History

#1 - 03/03/2014 09:59 AM - shugo (Shugo Maeda)

Jan Rusnacko wrote:

```
[jrusnack@dhcp-31-42 ruby-safe]$ ./tainted.rb
$0:            ./tainted.rb, tainted? false
__FILE__:      ./tainted.rb, tainted? true
$PROGRAM_NAME: ./tainted.rb, tainted? false
```

I guess it's a regression introduced in r20656.
Or did you mean not to taint $0, Yugui?

#2 - 03/03/2014 10:59 AM - shyouhei (Shyouhei Urabe)

My expectation to tainted.rb output is what 1.8.7 outputs. This seems like a regression to me.

#3 - 07/12/2019 02:01 AM - jeremyevans0 (Jeremy Evans)

- Backport deleted (1.9.3: UNKNOWN, 2.0.0: UNKNOWN, 2.1: UNKNOWN)

It looks like $0, __FILE__, and $PROGRAM_NAME have been not tainted since 2.1. I'm not sure if this is still considered a bug or not.

#4 - 09/02/2019 05:33 AM - nobu (Nobuyoshi Nakada)

- Description updated

#5 - 09/02/2019 05:36 AM - ko1 (Koichi Sasada)

- Related to Feature #16131: Remove $SAFE, taint and trust added

#6 - 10/13/2019 05:19 PM - jeremyevans0 (Jeremy Evans)

- Status changed from Open to Closed

As tainting will be removed from Ruby 2.7, this can be closed.