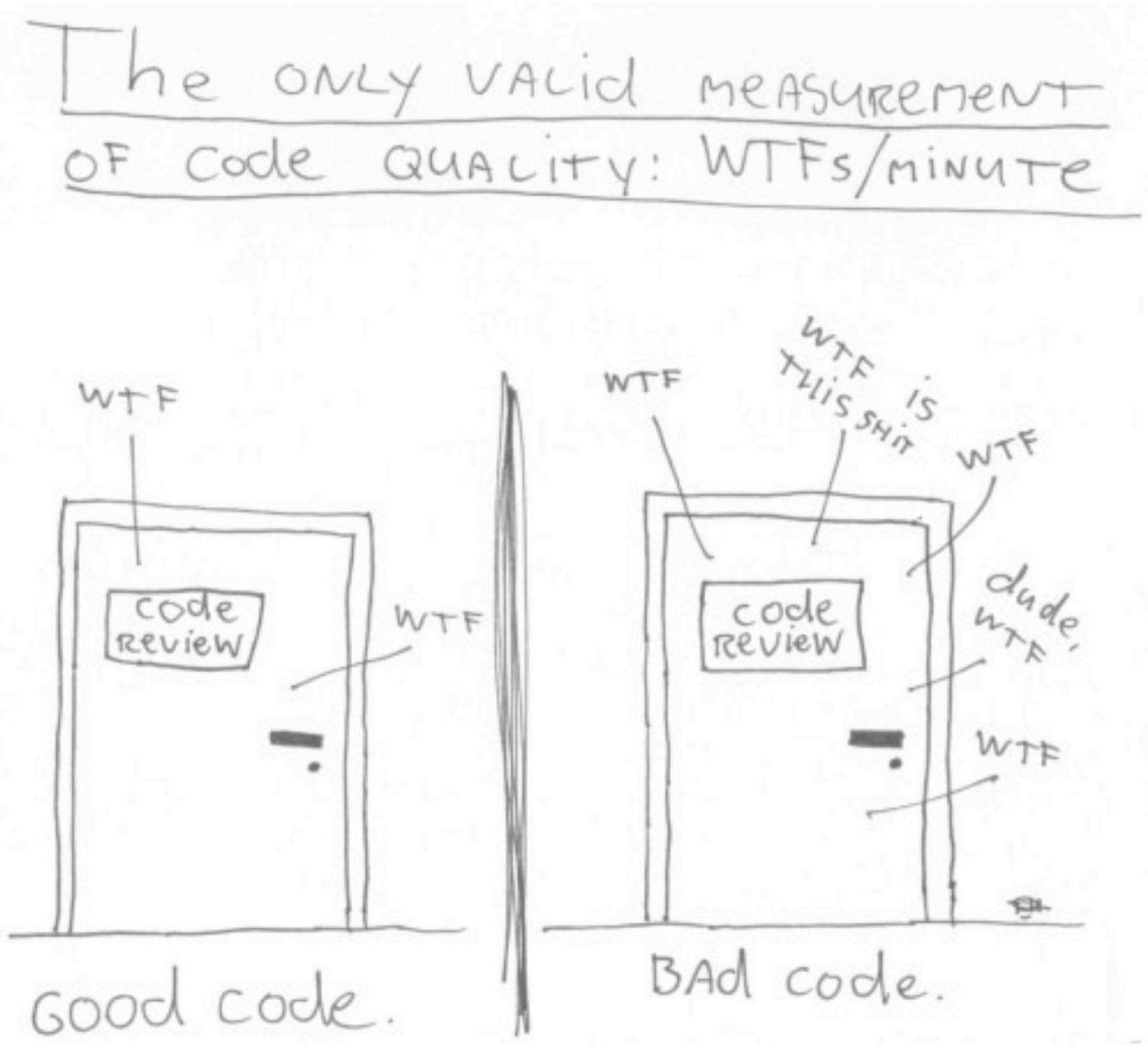
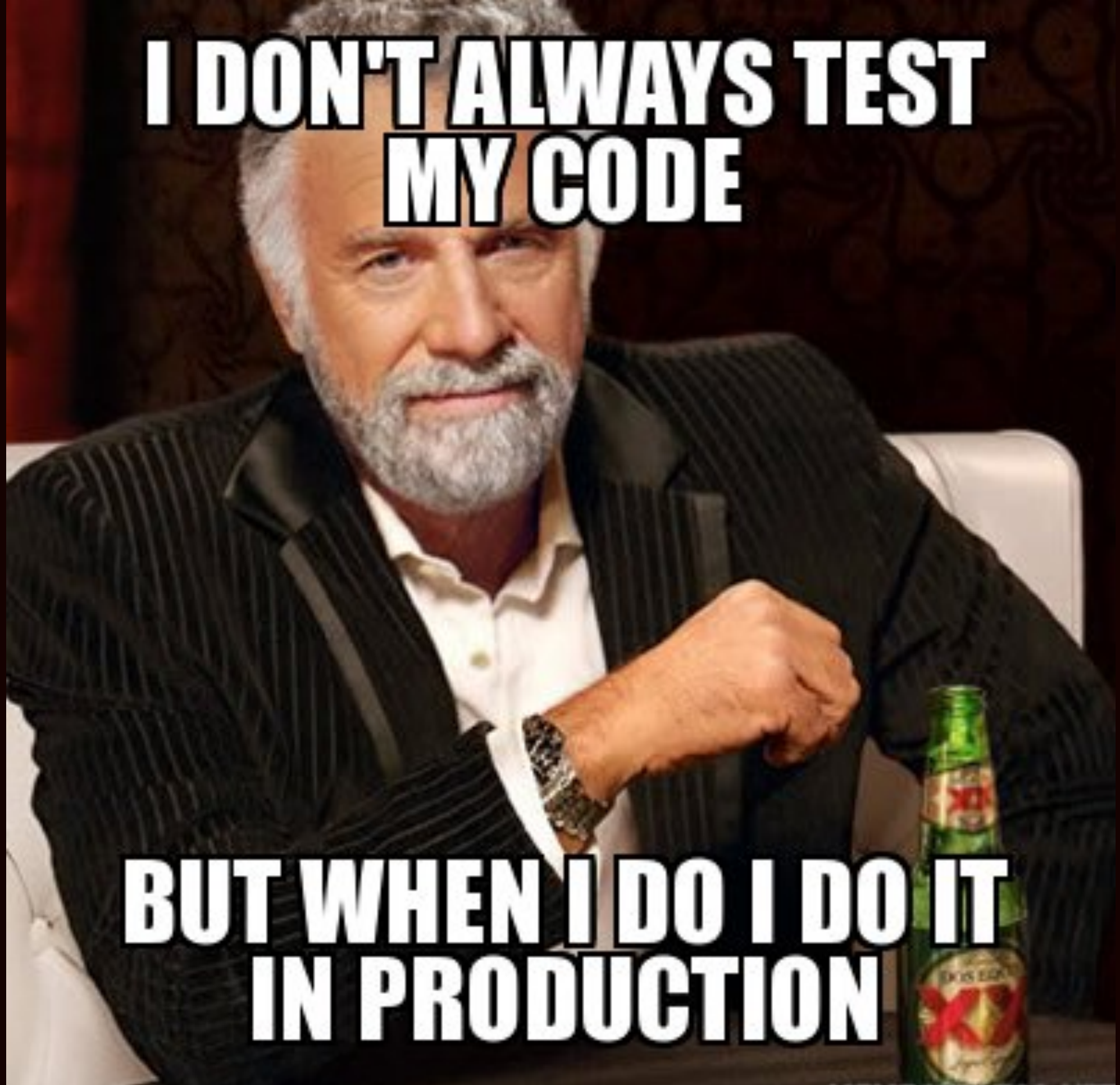
Code Quality: Tools & Services




I DON'T ALWAYS TEST
MY CODE
BUT WHEN I DO I DO IT
IN PRODUCTION

What don't I know about my code?

- Did I test all my code?
- Is my code any good?
- Is my code secure?


I WILL BREAK YOU
A PIECE OF MY KIT-KAT SO WE CAN SHARE IT

OKAY, FINE! #eval IS EVIL! I GET IT!

About metric_fu 2.1.0

Metric_fu is a set of rake tasks that make it easy to generate metrics reports. It uses Saikuro, Flog, Flay, Rcov, Reek, Roodi, Churn, RailsBestPractices, Subversion, Git, and Rails built-in stats task to create a series of reports. It's designed to integrate easily with CruiseControl.rb by placing files in the Custom Build Artifacts folder.

In 2.1.0 there are a lot of bug fixes, Check the HISTORY file for complete details. There's a verbose mode (config.verbose = true) that's helpful for debugging (from Dan Sinclair), the ability to opt out of TextMate (from Kakutani Shintaro) opening your files (config.darwin_txmt_protocol_no_thanks = true), and super cool annotations on the Hotspots page so you can see your code problems in-line with the file contents (also from Dan Sinclair).

jscruggs / metric_fu

Watch

Code | Network | Pull Requests 8 | Issues 28

A fist full of code metrics — Read more

http://metric-fu.rubyforge.org/

Clone in Mac | ZIP | HTTP | SSH | Git Read-Only | git://github.com/jscruggs/metric_fu.git

branch: **master** | **Files** | Commits | Branches 3

metric_fu /

updating docs for 2.1.1 release

jscruggs authored 2 years ago

config	2 years ago	Adding in config/roodi_config.yml to ignore assignment in an if c
home_page	2 years ago	updating docs for 2.1.1 release [jscruggs]
lib	2 years ago	Syntax highlighting is now optional [jscruggs]

metric_fu equivalent for ruby 1.9.x

9

metric_fu doesn't seem to be supported in the latest ruby kernel (1.9.2 | 1.9.3). Are there any gems which offer equivalent functionality.

ruby-on-rails-3 metric-fu

share | edit | retag | flag

asked **Mar 3 at 5:58**

priya
824 1 14
73% accept rate

add comment

start a bounty

2 Answers

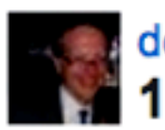
active oldest **votes**

1

Checkout Metrical, last time I looked it still wasn't 100% but that was months ago.

share | edit | flag

answered **Mar 3 at 7:38**



dogenpunk
1,565 3 13

metrical /

35 commits

Metrical is deprecated. Give up on trying to install metrical without… ···

iain authored 8 months ago — latest commit `dfd01e732c`

bin	10 months ago	Add a couple of specs for running metrical [iain]
lib	10 months ago	Release version 0.1.0 [iain]
spec	10 months ago	Add RSpec rake task [iain]
.gitignore	a year ago	Don't ignore Gemfile.lock, it contains debug info. [iain]
.metrics	10 months ago	More specs [iain]
.rspec	10 months ago	More specs [iain]
.travis.yml	10 months ago	Remove unsupported versions from Travis [iain]
Gemfile	a year ago	Use bundler as gem builder [iain]
Gemfile.lock	10 months ago	Trying to solve RCov incompatibility issues, refs #12 [iain]
README.md	8 months ago	Metrical is deprecated. Give up on trying to install metrical without… [iain]
Rakefile	10 months ago	Add RSpec rake task [iain]
metrical.gemspec	10 months ago	Trying to solve RCov incompatibility issues, refs #12 [iain]

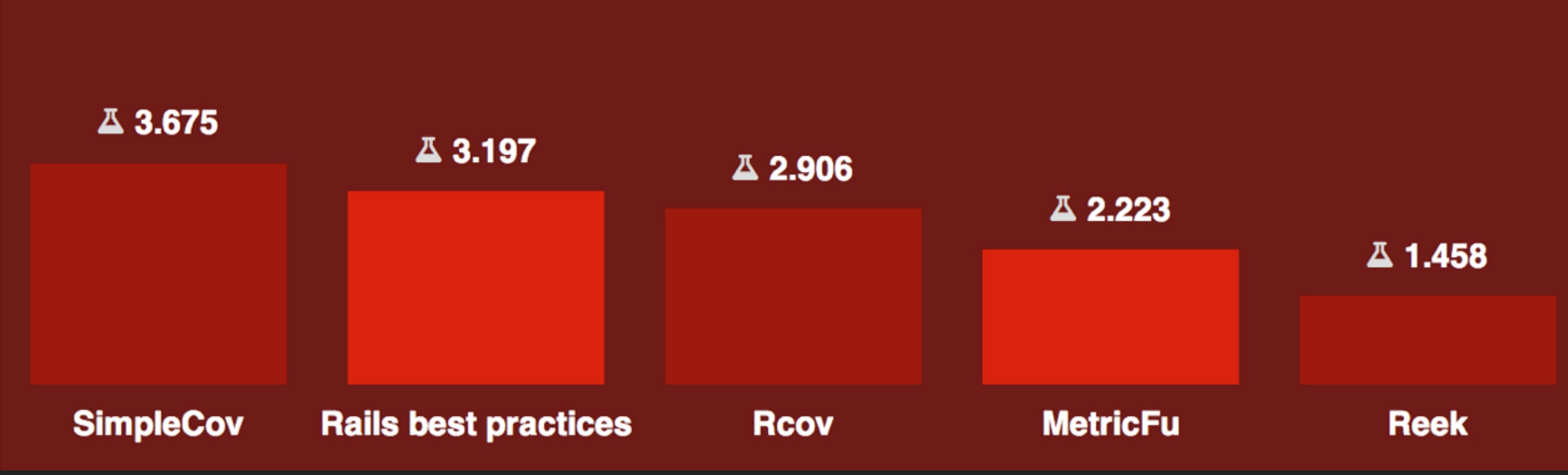
README.md

Warning: This gem is not being maintained anymore!

I work exclusively with Ruby 1.9, and most tools included don't (fully) support it. If you want to take over the project, fork the project, and open an issue stating your intentions.

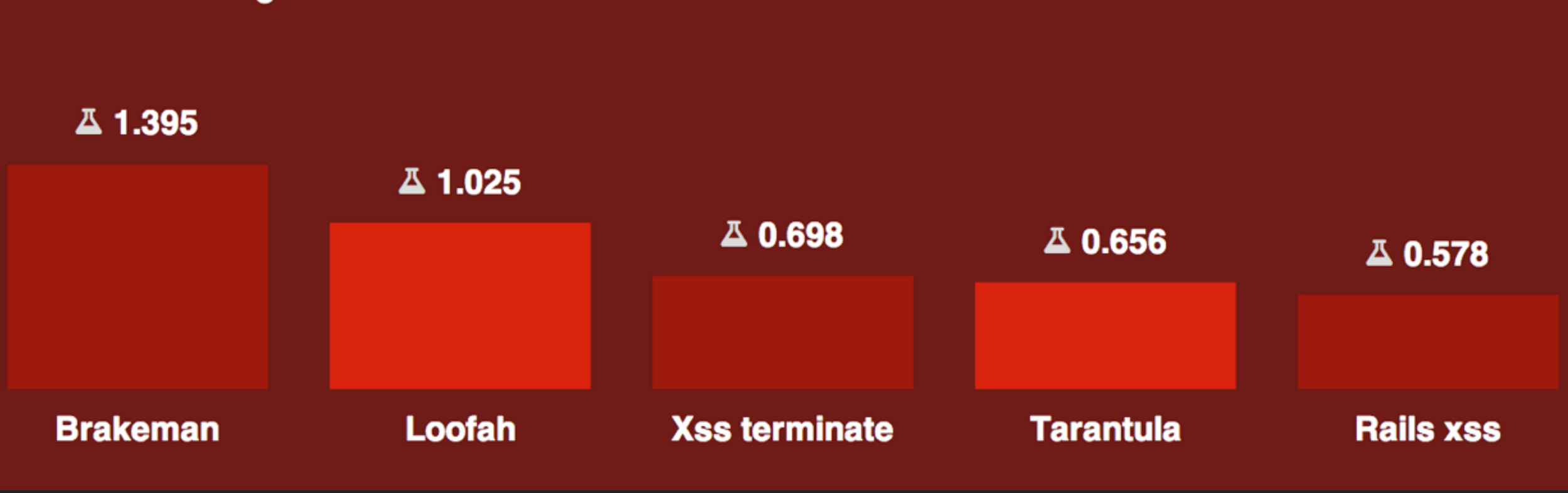
The Ruby Toolbox

Code Metrics



The Ruby Toolbox

Security Tools



Services

- Code Climate
- Gemnasium
- Travis CI

colszowka / simplecov

Watch | Star 993

Code | Network | Pull Requests 4 | Issues 34

Code coverage for Ruby 1.9 with a powerful configuration library and automatic merging of coverage across test suites — Read more

https://www.ruby-toolbox.com/projects/simplecov

Clone in Mac | ZIP | HTTP | SSH | Git Read-Only | `git://github.com/colszowka/simplecov.git` | Read-O

branch: **master** | **Files** | Commits | Branches 2

simplecov /

Merge pull request #181 from semanticart/master ···

colszowka authored 22 days ago — latest co

features	24 days ago	Run cukes on 1.9 and up [colszowka]
gemfiles	24 days ago	Appraisal changed their naming scheme [colszowka]
lib	22 days ago	Merge pull request #181 from semanticart/master [colszowka]
test	22 days ago	Adds command guessing support for Rails 4 functional tests [semanticart]
.gitignore	3 months ago	Removed appraisal gemfile locks from git [colszowka]
.travis.yml	24 days ago	Also added rbx-19mode (for now allowing failures) as per #164 [colszowka]
.yardopts	7 months ago	.yardopts to include all .md files in Documentation [colszowka]

Installation

Gemfile

```
group :test do
  gem ‘simplecov’, require: false
end
```

spec_helper.rb

```
require ‘simplecov’
Simplecov.start ‘rails’
```

~/ruby_projects/credit_card_checker

```
[credit_card_checker (master)]$ rspec spec/
 10/10 |========================== 100 ==========================>| Time: 00:00:00

Finished in 0.02192 seconds
10 examples, 0 failures
Coverage report generated for RSpec to /Users/paul/Documents/SoftwareEngineering
/MyProgramming/ruby_projects/credit_card_checker/coverage. 98 / 139 LOC (70.5%)
covered.
[credit_card_checker (master)]$
```

All Files (70.5%)

All Files (70.5% covered at 0.99 hits/line)

11 files in total. **139** relevant lines. **98** lines covered and **41** lines missed

Search:

File	% covered	Lines	Relevant Lines	Lines covered
spec/support/utilities.rb	50.0 %	103	24	12
lib/credit_card_checker/checker.rb	51.85 %	50	27	14
lib/credit_card_checker/cli.rb	65.52 %	59	29	19
lib/credit_card_checker/card_number_validator.rb	66.67 %	25	12	8
lib/credit_card_checker/checker_helper.rb	75.0 %	33	4	3
lib/credit_card_checker/credit_card.rb	87.5 %	18	8	7
lib/credit_card_checker.rb	100.0 %	4	4	4
spec/checker_spec.rb	100.0 %	162	13	13
spec/cli_spec.rb	100.0 %	28	8	8
spec/credit_card_checker_spec.rb	100.0 %	8	5	5
spec/credit_card_spec.rb	100.0 %	45	5	5

Showing 1 to 11 of 11 entries

lib/credit_card_checker/card_number_validator.rb

66.67 % covered

12 relevant lines. 8 lines covered and 4 lines missed.

```
1.  require 'active_model'                                          1
2.
3.  module CreditCardChecker                                        1
4.    # Validator for credit card numbers using the Luhn algorithm
5.    class CardNumberValidator                                     1
6.      include ActiveModel::Validations                            1
7.
8.      attr_reader :number_array                                   1
9.
10.     def initialize(number)                                      1
11.       @number_array = number.chars.map(&:to_i)                  4
12.     end
13.
14.     def number_valid?                                           1
15.       check = @number_array.pop
16.
17.       sum = @number_array.reverse.each_slice(2).map do |left_num, right_num|
18.         [(left_num * 2).divmod(10), right_num]
19.       end.push(check).flatten.compact.inject(:+)
20.
21.       sum % 10 == 0
22.     end
23.
24.   end
25. end
```

All Files (100.0%)

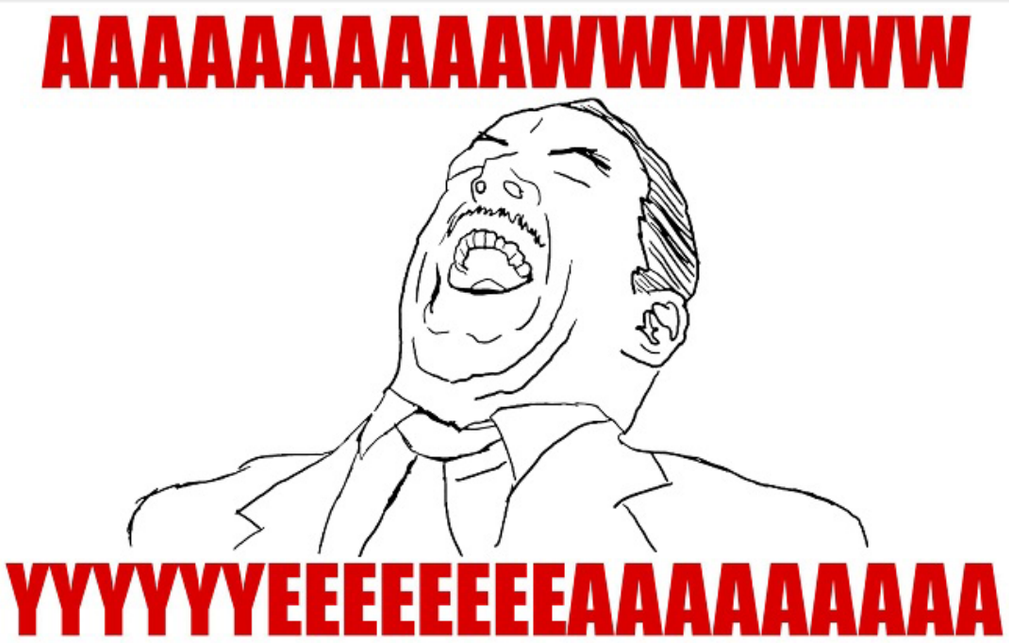
All Files (100.0% covered at 168.73 hits/line)

11 files in total. **246** relevant lines. **246** lines covered and **0** lines missed

Search:

File	% covered	Lines	Relevant Lines	Lines covered
lib/credit_card_checker.rb	100.0 %	4	4	4
lib/credit_card_checker/card_number_validator.rb	100.0 %	25	12	12
lib/credit_card_checker/checker.rb	100.0 %	50	27	27
lib/credit_card_checker/checker_helper.rb	100.0 %	33	4	4
lib/credit_card_checker/cli.rb	100.0 %	59	29	29
lib/credit_card_checker/credit_card.rb	100.0 %	18	8	8
spec/checker_spec.rb	100.0 %			
spec/cli_spec.rb	100.0 %			
spec/credit_card_checker_spec.rb	100.0 %			
spec/credit_card_spec.rb	100.0 %			
spec/support/utilities.rb	100.0 %			

Showing 1 to 11 of 11 entries



All Files (100.0%)

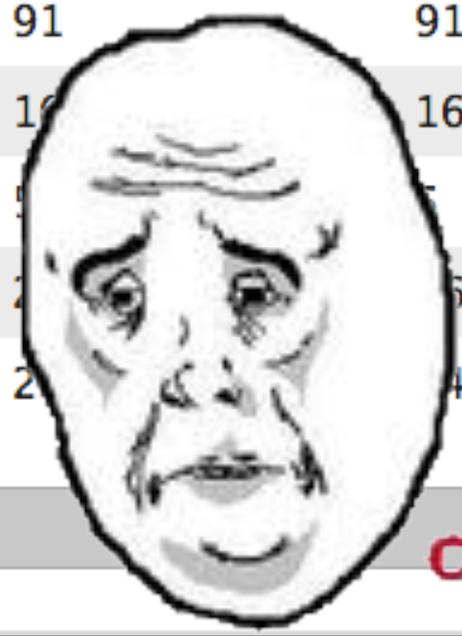
All Files (100.0% covered at 168.73 hits/line)

11 files in total. **246** relevant lines. **246** lines covered and **0** lines missed

Search:

File	% covered	Lines	Relevant Lines	Lines covered
lib/credit_card_checker.rb	100.0 %	4	4	4
lib/credit_card_checker/card_number_validator.rb	100.0 %	25	12	12
lib/credit_card_checker/checker.rb	100.0 %	50	27	27
lib/credit_card_checker/checker_helper.rb	100.0 %	33	4	4
lib/credit_card_checker/cli.rb	100.0 %	59	29	29
lib/credit_card_checker/credit_card.rb	100.0 %	18	8	8
spec/checker_spec.rb	100.0 %	162	91	91
spec/cli_spec.rb	100.0 %	28	16	16
spec/credit_card_checker_spec.rb	100.0 %	8	5	5
spec/credit_card_spec.rb	100.0 %	45	26	26
spec/support/utilities.rb	100.0 %	103	24	24

Showing 1 to 11 of 11 entries



All Files (100.0%)

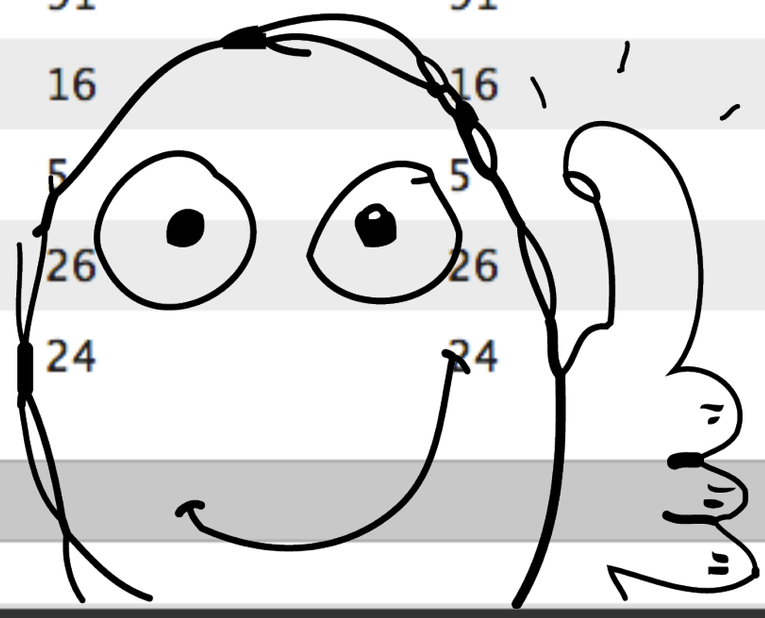
All Files (100.0% covered at 168.73 hits/line)

11 files in total. **246** relevant lines. **246** lines covered and **0** lines missed

Search:

File	% covered	Lines	Relevant Lines	Lines covered
lib/credit_card_checker.rb	100.0 %	4	4	4
lib/credit_card_checker/card_number_validator.rb	100.0 %	25	12	12
lib/credit_card_checker/checker.rb	100.0 %	50	27	27
lib/credit_card_checker/checker_helper.rb	100.0 %	33	4	4
lib/credit_card_checker/cli.rb	100.0 %	59	29	29
lib/credit_card_checker/credit_card.rb	100.0 %	18	8	8
spec/checker_spec.rb	100.0 %	162	91	91
spec/cli_spec.rb	100.0 %	28	16	16
spec/credit_card_checker_spec.rb	100.0 %	8	5	5
spec/credit_card_spec.rb	100.0 %	45	26	26
spec/support/utilities.rb	100.0 %	103	24	24

Showing 1 to 11 of 11 entries



Rails Best Practices

Follow The Rails Best Practices Here

Share Your Rails Best Practices Here

SUBSCRIBE TO OUR RSS FEED

Rails Best Practices

Share

Created | Votes | Comments | Implemented

31 votes
15611 views

Use Observer

Observer serves as a connection point between models and some other subsystem whose functionality is used by some of other classes, such as email notification. It is loose coupling in contract with model callback.

model observer

7 Comments and 0 Reactions

implemented

by ihower

31 votes
4476 views

Double-check your migrations

When you generate a new migration, try it forwards and backwards to ensure it has no errors

sanity checks migration

by jaimeiniesta

Installation

Gemfile

```
group :development do
  gem "rails_best_practices"
end
```

```
[sample_app (master)]$ rails_best_practices
Source Codes:  100% |oooooooooooooooooooooooooooo| Time:    0:00:01
./app/controllers/application_controller.rb:11 - remove unused meth
ods (ApplicationController#url_options)
./app/helpers/sessions_helper.rb:3 - remove unused methods (Session
sHelper#sign_in)
./app/helpers/sessions_helper.rb:13 - remove unused methods (Sessio
nsHelper#signed_in_user)
./app/helpers/sessions_helper.rb:25 - remove unused methods (Sessio
nsHelper#current_user=)
./app/helpers/sessions_helper.rb:33 - remove unused methods (Sessio
nsHelper#sign_out)
./app/helpers/sessions_helper.rb:39 - remove unused methods (Sessio
nsHelper#redirect_back_or)

Please go to http://rails-bestpractices.com to see more useful Rail
s Best Practices.

Found 6 warnings.
[sample_app (master)]$
```

rails_best_practices output

Please go to http://rails-bestpractices.com to see more useful Rails Best Practices.

Found 2287 warnings.

- [ ] Always Add Db Index
- [ ] Check Save Return Value
- [ ] Isolate Seed Data
- [x] Law Of Demeter
- [x] Move Code Into Controller
- [x] Move Code Into Helper
- [x] Move Code Into Model
- [x] Move Finder To Named Scope
- [x] Move Model Logic Into Model
- [x] Not Use Default Route
- [x] Overuse Route Customizations
- [x] Protect Mass Assignment
- [x] Remove Empty Helpers
- [x] Remove Unused Methods In Controllers
- [x] Remove Unused Methods In Helpers
- [x] Remove Unused Methods In Models
- [x] Replace Complex Creation With Factory Method
- [x] Replace Instance Variable With Local Variable
- [x] Restrict Auto Generated Routes
- [x] Simplify Render In Controllers
- [x] Simplify Render In Views
- [x] Use Model Association
- [x] Use Multipart Alternative As Content Type Of Email
- [x] Use Query Attribute
- [x] Use Say With Time In Migrations
- [x] Use Scope Access

Check all | Uncheck all

Filename	Line Number	Warning Message
app/controllers/app_settings_controller.rb	218	law of demeter
app/controllers/services_controller.rb	589	law of demeter
app/controllers/services_controller.rb	590	law of demeter
app/controllers/services_controller.rb	591	law of demeter
app/controllers/services_controller.rb	592	law of demeter
app/controllers/services_controller.rb	593	law of demeter
app/controllers/services_controller.rb	594	law of demeter
app/controllers/services_controller.rb	595	law of demeter
app/controllers/services_controller.rb	596	law of demeter
app/controllers/services_controller.rb	597	law of demeter

the Law of Demeter

19

Posted by ihower on July 24, 2010

According to the law of demeter, a model should only talk to its immediate association, don't talk to the association's association and association's property, it is a case of loose coupling.

Bad Smell

```
class Invoice < ActiveRecord::Base
  belongs_to :user
end

<%= @invoice.user.name %>
<%= @invoice.user.address %>
<%= @invoice.user.cellphone %>
```

In this example, invoice model calls the association(user)'s property(name, address and cellphone), which violates the law of demeter. We should add some wrapper methods.

Refactor

```
class Invoice < ActiveRecord::Base
  belongs_to :user
  delegate :name, :address, :cellphone, :to => :user, :prefix => true
end

<%= @invoice.user_name %>
<%= @invoice.user_address %>
<%= @invoice.user_cellphone %>
```

Luckily, rails provides a helper method delegate which utilizes the DSL way to generates the wrapper methods. Besides the loose coupling, delegate also prevents the error call method on nil object if you add option :allow_nil

Public Repositories

iscore-rails	#78
Duration: 17 secs , Finished: about 17 hours ago	
Lab201	#4
Duration: 6 secs , Finished: 1 day ago	
finance	#9
Duration: 8 secs , Finished: 2 days ago	
game_of_life	#8
Duration: 10 secs , Finished: 2 days ago	
rails-brakeman.com	#46
Duration: 12 secs , Finished: 3 days ago	
railsbp.com	#178
Duration: 27 secs , Finished: 3 days ago	
diputados	#60
Duration: 7 secs , Finished: 4 days ago	
sa	#5
Duration: 41 secs , Finished: 5 days ago	
ruby-china	#90
Duration: 37 secs , Finished: 5 days ago	
deadline_camp	#21
Duration: 15 secs , Finished: 6 days ago	

What's Railsbp?

Railsbp is short for rails best practices, it provides online rails projects code quality check service. It works based on rails_best_practices gem.

Why Railsbp?

Railsbp.com helps you to follow rails best practices and gives you some suggestions to improve your rails projects code quality.

Features

Automatic to analyze source codes. Every time you push to github, the code check service will be executed automatically.

Easy to share analyze result with collaborators. You can easily share the analyze result to your team collaborators, then talk and discuss together.

Easy to track builds history. Railsbp keeps each analyze result, you can track if your code quality is improved or not.

No worry about ruby version. rails_best_practices gem doesn't work well for ruby 1.8.7, jruby, etc., but using railsbp.com, you don't need to worry about what ruby version you are developing your rails project.

Configure what to review. You can also configure what to review, like if you don't want to always add db index for foreign key, you can disable that checker.

[Railsbp] paulfioravanti/sample_app build #147, warnings count 5

notification@rails-bestpractices.com 12/6/12

to me

Repository	paulfioravanti/sample_app
Build #147	http://railsbp.com/repositories/197-paulfioravanti-sample_app/builds/2311
Warning Count	5
Commit	2d93e81 (master)
Message	Update gems
Duration	22 secs

paulfioravanti/sample_app

Current | History | Build #147

Build	147	**Duration**	22 secs
Branch	master	**Finished**	27 days ago
Commit	2d93e81	**Message**	Update gems

Analyze Result

Warning count: 5

Customize Checks

Filename	Line Number	Warning Message
dac75b/sample_app/app/controllers/application_controller.rb	11	remove unused methods (ApplicationController#url_options)
dac75b/sample_app/app/helpers/sessions_helper.rb	3	remove unused methods (SessionsHelper#sign_in)
dac75b/sample_app/app/helpers/sessions_helper.rb	25	remove unused methods (SessionsHelper#current_user=)
dac75b/sample_app/app/helpers/sessions_helper.rb	33	remove unused methods (SessionsHelper#sign_out)
dac75b/sample_app/app/helpers/sessions_helper.rb	39	remove unused methods (SessionsHelper#redirect_back_or)

Options
Collaborators
Service Hooks
Deploy Keys

AVAILABLE SERVICE HOOKS

- WebHook URLs (0)
- ActiveCollab
- Acunote
- AgileBench
- AgileZen
- AmazonSNS
- AMQP
- Apoio
- AppHarbor
- Asana
- Backlog
- Bamboo
- BasecampClassic
- Basecamp
- Boxcar
- buddycloud (GitHub plugin)
- BugHerd
- Bugly
- Bugzilla

Railsbp Url

http://railsbp.com

Token

Sup4_53kR!+_P45sw0|2d_z0mG

☑ Active

Test Hook | Update Settings

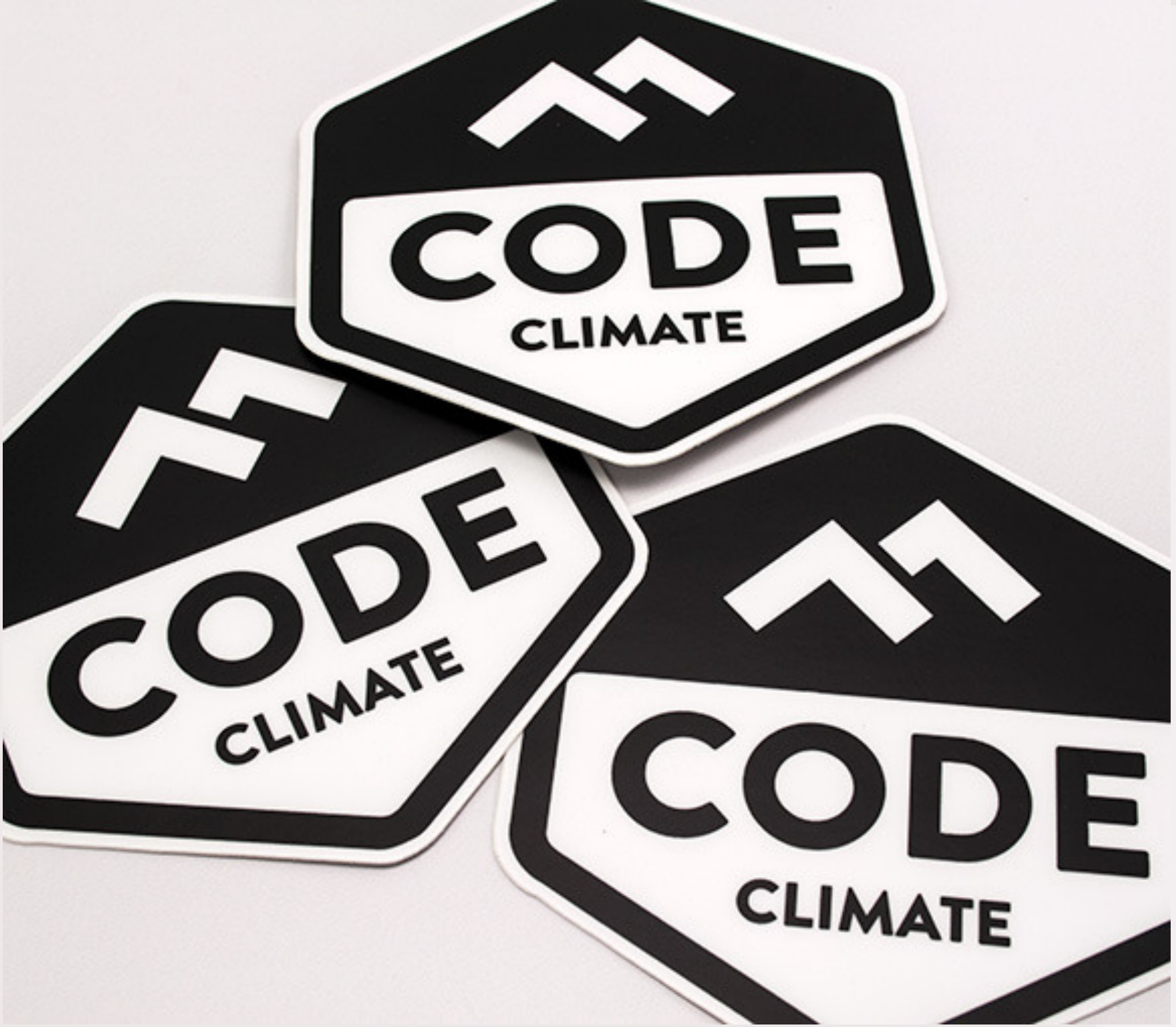
Railsbp

Railsbp - a code analyzer service for rails projects.

Install Notes

1. Create an account on railsbp.com (just sign in with GitHub)
2. Create a repository on railsbp.com
3. Enter your token
   - the token which you can find on repository edit page on railsbp.com
4. Enter your railsbp_url if you deploy the proxy on your own server
5. Check the "Active" checkbox and click "Update Settings"

For more details about Railsbp, go to https://railsbp.com

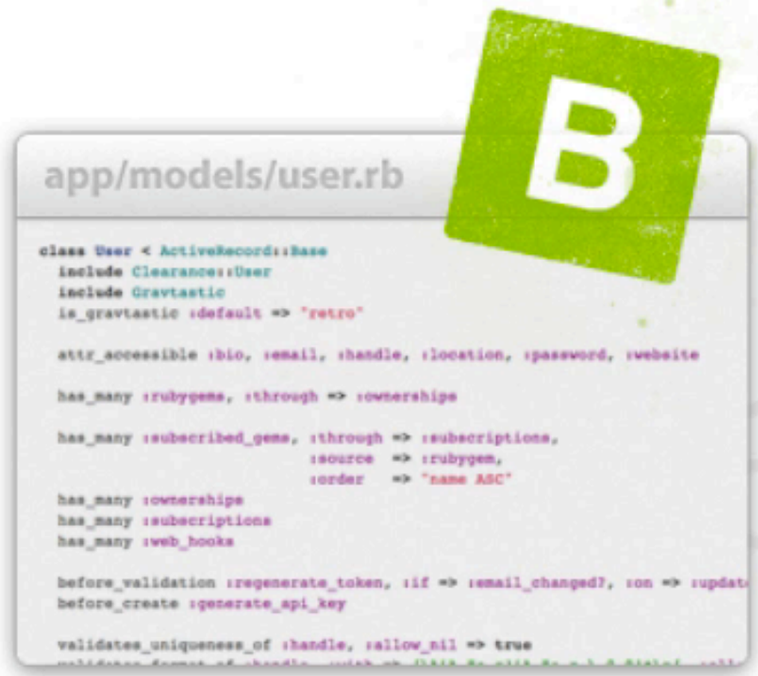

CODE
CLIMATE
CODE
CLIMATE
CODE
CLIMATE

CODE CLIMATE

How it Works Features Pricing Start a Free Trial Login

SHIP QUALITY RUBY CODE. FASTER.

Hosted software metrics for Ruby apps. Get control of your technical debt today.



Get Metrics

Immediate Feedback
Notifications are triggered by Git pushes.

Faster Code Reviews
Lets you focus on the most significant commits.

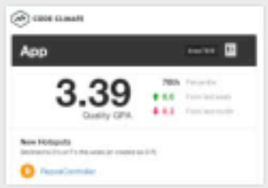
Set Goals & Track Progress
Work with your team to improve ratings over time.

Try Code Climate Free

14-day Trial - No credit card required. Or see Pricing.

Activity Feeds
Track quality in real-time.

Drill-down Analysis
Pinpoint and resolve issues.



Email Reports
Summarize recent changes.

CODE CLIMATE

Select Repository Type

Private

- **14-day free trial.**
- You choose who can view.
- Supports any Git repository.

Create Account

Public

- **Free forever.**
- Anyone can view metrics.
- Supports public GitHub repos.

Add Repository

user/some_repo

Feed | Classes | Smells | Trends | Search by class name

Summary of **December 24th - 30th**
70 files changed, 3,103 insertions, 3,072 deletions

Summary of **December 17th - 23rd**
60 files changed, 1,102 insertions, 1,031 deletions

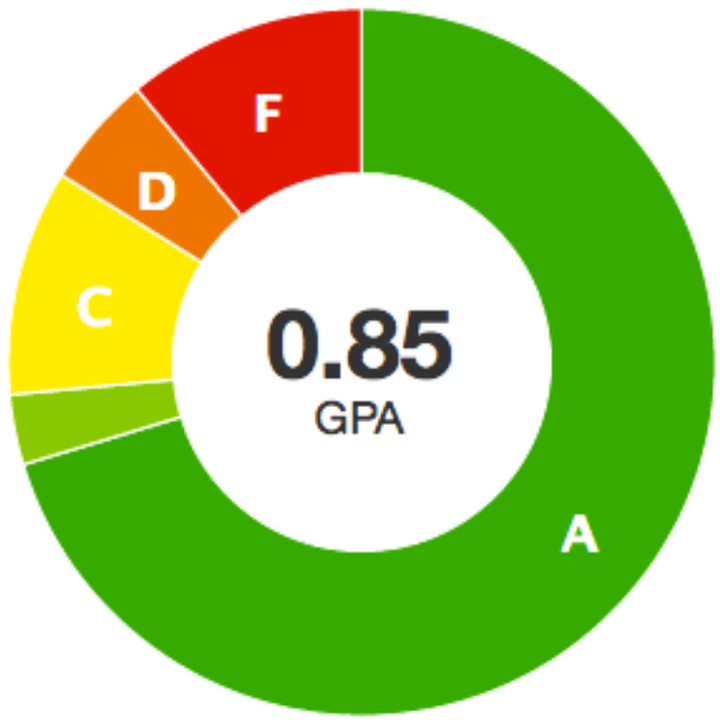
Summary of **December 10th - 16th**
1 file changed, 1 insertion, 1 deletion

Summary of **December 3rd - 9th**
91 files changed, 2,455 insertions, 2,245 deletions

Summary of **November 26th - December 2nd**
4 files changed, 47 insertions, 45 deletions

Summary of **November 19th - 25th**
57 files changed, 839 insertions, 793 deletions

Classes by Rating



Hotspots

F ServicesController

F SpeakersController

F ExhibitorsController

user/some_repo

Feed | Classes | Smells | Trends

Search by class name

Smell	Location
High overall complexity	ServicesController
Complex method	ServicesController#get_app_data
Complex method	ServicesController#get_widget_data
High overall complexity	UserAssetsController
Complex method	ServicesController#get_all_designs
Similar code in two :defn nodes	ExhibitorsController
Similar code in two :defn nodes	SpeakersController
Identical code in two :block nodes	ServicesController

user/some_repo Feed | Classes | Smells | Trends | Search by class name | Tweet | e6b92953

F User

Updated 8 months ago.

207 Complexity	364 Duplication	149 Lines	7 Methods
29.5 Complexity / M	48 Churn	108 Lines of Code	15 LOC / Method

✖ Total Complexity | ✖ Method Complexity 2 | ✖ Duplication 1

High overall complexity

The grand total complexity of all of the code in this class is 207.

app/models/user.rb — View on GitHub »

```
1  require 'net/https'
2  require 'uri'
3  class User < ActiveRecord::Base
4    Radix = 36
5    # Include default devise modules. Others available are:
6    # :token_authenticatable, :encryptable, :confirmable, :lockable, :timeoutable and :omniauthable
7    devise :database_authenticatable, :registerable,
8           :recoverable, :rememberable, :trackable, :validatable, :confirmable
9
10   # Setup accessible (or protected) attributes for your model
11   attr_accessible :email, :password, :password_confirmation, :remember_me, :first_name, :last_name, :parent_id, :domain_name, :active
12   #validates :domain_name, :presence => true, :uniqueness => true
13   #has_many :roles
14   #has_many :roles_users, :through => :roles
15
16   has_many :roles_users
17   has_many :roles, :through => :roles_users
```

troessner / reek

Watch | Unstar

Code | Network | Pull Requests 2 | Issues 30 | Wiki

Code smell detector for Ruby — Read more

http://wiki.github.com/troessner/reek

Clone in Mac | ZIP | HTTP | SSH | Git Read-Only | git://github.com/troessner/reek.git

branch: master | Files | Commits | Branches 5

reek /

Bump version to 1.2.13.

troessner authored 25 days ago

bin	7 months ago	Change the link to the reek github repositroy [andywenk]
config	a year ago	relaxed strict cucumber runs while we get 1.9.2 passing [kevinrutherford]
features	7 months ago	Allow cucumber feature to match old and new syntax error messages. [mvz]
lib	25 days ago	Bump version to 1.2.13. [troessner]
quality	2 years ago	Added some missing newlines at ends of files [kevinrutherford]
spec	25 days ago	Update to rspec2. [troessner]

Example

Imagine a source file `demo.rb` containing:

```
class Dirty
  # This method smells of :reek:NestedIterators but ignores them
  def awful(x, y, offset = 0, log = false)
    puts @screen.title
    @screen = widgets.map {|w| w.each {|key| key += 3}}
    puts @screen.contents
  end
end
```

Reek will report the following code smells in this file:

```
$ reek demo.rb
spec/samples/demo/demo.rb -- 6 warnings:
  Dirty has no descriptive comment (IrresponsibleModule)
  Dirty#awful has 4 parameters (LongParameterList)
  Dirty#awful has boolean parameter 'log' (ControlCouple)
  Dirty#awful has the parameter name 'x' (UncommunicativeName)
  Dirty#awful has the parameter name 'y' (UncommunicativeName)
  Dirty#awful has the variable name 'w' (UncommunicativeName)
```

Code Smells

Smells are indicators of where your code might be hard to read, maintain or evolve, rather than things that are specifically *wrong*. Naturally this means that Reek is looking towards your code's future (and that can make its reports seem somewhat subjective, of course).

Reek currently includes very naive checks for the following smells:

- Attribute (disabled by default)
- Class Variable
- Control Couple, including
  - Boolean Parameter
- Data Clump
- Duplication
- Irresponsible Module
- Large Class
- Long Method
- Long Parameter List
- Low Cohesion, including
  - Feature Envy
  - Utility Function
- Nested Iterators
- Simulated Polymorphism
- Uncommunicative Name, including
  - Uncommunicative Method Name
  - Uncommunicative Module Name
  - Uncommunicative Parameter Name
  - Uncommunicative Variable Name

BRAKEMAN

Installation

Gemfile

```
group :development do
  gem "brakeman"
end
```

Public Repositories

iscore-rails #78
Duration: 4 secs ,
Finished: about 20 hours ago

rails-brakeman.com #48
Duration: 2 secs ,
Finished: 3 days ago

railsbp.com #33
Duration: 15 secs ,
Finished: 3 days ago

SetupMeetup #22
Duration: 2 secs ,
Finished: 8 days ago

sample_app #183
Duration: 5 secs ,
Finished: 8 days ago

R3TMS #33
Duration: 4 secs ,

What's rails-brakeman.com?

rails-brakeman.com is an online service to find security issues in your rails projects. It works based on Justin's great gem brakeman

Why rails-brakeman.com?

rails developers always write code fast, but sometimes they leave some security issues in their rails project.

rails-brakeman.com is aimed to help them find out the security issues.

Features

Automatic to analyze source codes. Every time you push to github, the service will be executed automatically.

Easy to share analysis with collaborators. You can easily share the analysis to your team collaborators, then talk and discuss together.

Screenshot

Confidence	Class	Method	Warning Type	Message
High	PostsController	create	Mass Assignment	Unprotected mass assignment near line 43: Post.new(params[:post])
High	PostsController	update	Mass Assignment	Unprotected mass assignment near line 63: Post.find(params[:id]).update_attributes(params[:post])
High	UsersController	create	Mass Assignment	Unprotected mass assignment near line 43: User.new(params[:user])
High	UsersController	update	Mass Assignment	Unprotected mass assignment near line 62: User.find(params[:id]).update_attributes(params[:user])
Medium			Cross Site Scripting	Rails 3.2.1 has a vulnerabilty in SafeBuffer. Upgrade to 3.2.2 or apply patches.
Weak	PostsController	update	Redirect	Possible unprotected redirect near line 64: redirect_to(Post.find(params[:id]), :notice => "Post was ...
Weak	UsersController	update	Redirect	Possible unprotected redirect near line 63:

[rails-brakeman] paulfioravanti/sample_app build #180 warnings count 0

Inbox x

notification@rails-bestpractices.com 12/22/12 (11 days ago)

to me

Repository	paulfioravanti/sample_app
Build #180	http://rails-brakeman.com/paulfioravanti/sample_app/builds/1177
Warnings count	0
Commit	52daa5e (master)
Message	Clean up config
Duration	13 secs

Brakeman Report

Application Path	Rails Version	Brakeman Version	Report Time	Checks Performed
/Users/paul/Documents/SoftwareEngineering/MyProgramming/rails_projects/test	3.1.3	1.9.0	2012-12-27 14:45:51 +1030 24.400161 seconds	BasicAuth, ContentTag, CrossSiteScripting, DefaultRoutes, DigestDoS, EscapeFunction, Evaluation, Execute, FileAccess, FilterSkipping, ForgerySetting, LinkTo, LinkToHref, MailTo, MassAssignment, ModelAttributes, NestedAttributes, QuoteTableName, Redirect, Render, ResponseSplitting, SQL, SafeBufferManipulation, SelectTag, SelectVulnerability, Send, SendFile, SessionSettings, SingleQuotes, SkipBeforeFilter, StripTags, TranslateBug, ValidationRegex, WithoutProtection

Summary

Scanned/Reported	Total
Controllers	56
Models	73
Templates	256
Errors	0
Security Warnings	352 (166)

Warning Type	Total
Attribute Restriction	1
Cross Site Scripting	31
Default Routes	1
Denial of Service	1
Dynamic Render Path	1
File Access	48
Mass Assignment	234
Redirect	32
SQL Injection	3

Security Warnings

Confidence	Class	Method	Warning Type	Message
High			Default Routes	All public methods in controllers are available as actions in routes.rb near line 401
High	Admin::CategoriesController	create	Mass Assignment	Unprotected mass assignment near line 20: Category.new(params[:category])

Summary

Scanned/Reported	Total
Controllers	56
Models	73
Templates	256
Errors	0
Security Warnings	352 (166)

Warning Type	Total
Attribute Restriction	1
Cross Site Scripting	31
Default Routes	1
Denial of Service	1
Dynamic Render Path	1
File Access	48
Mass Assignment	234
Redirect	32
SQL Injection	3

Security Warnings

Confidence	Class	Method	Warning Type	Message
High			Default Routes	All public methods in controllers are available as actions in routes.rb near line 401
High	Admin::CategoriesController	create	Mass Assignment	Unprotected mass assignment near line 20: Category.new(params[:category])
High	Admin::CodeBasesController	create	Mass Assignment	Unprotected mass assignment near line 42: CodeBasis.new(params[:code_basis])
Medium			Cross Site Scripting	Rails 3.1.3 has a vulnerabilty in SafeBuffer. Upgrade to 3.1.4 or apply patches.
Medium	PluginsController	open_window	Dynamic Render Path	Render path contains parameter value near line 13: render(partial => "plugins/#{params[:type]}", {})
Weak	AppSettingsController	redirect_app	Redirect	Possible unprotected redirect near line 246: redirect_to(("/app_settings/app_data/" + params[:m_id]))...
Weak	AppSettingsController	redirect_app	Redirect	Possible unprotected redirect near line 248: redirect_to(("/app_settings/publish/" + params[:m_id]))
Weak			Denial of Service	Vulnerability in digest authentication (CVE-2012-3424). Upgrade to Rails version 3.1.7

View Warnings

Confidence	Template	Warning Type	Message
Medium	admin/categories/index (Admin::CategoriesController#index)	Cross Site Scripting	Unsafe model attribute in link_to href near line 18: link_to("Delete", ("/admin/categories/destroy/" ...
Medium	admin/data_connectors/index (Admin::DataConnectorsController#index)	Cross Site Scripting	Unsafe model attribute in link_to href near line 20: link_to("Destroy", ("/admin/data_connectors/dest...
Medium	admin/features/show (Admin::FeaturesController#show)	Cross Site Scripting	Unsafe model attribute in link_to href near line 39: link_to("Delete", ("/admin/features/destroy/" + ...

				{FileSection.new(pa...
High	UserUploadsController	destroy	Redirect	Possible unprotected redirect near line 390: re {FileSection.find(p...
High	WidgetsController	create	Redirect	Possible unprotected redirect near line 137: re {Widget.new(params[...
High	WidgetsController	create	Redirect	Possible unprotected redirect near line 135: re {Widget.new(par...
High	WidgetsController	create_widget_attribute	Redirect	Possible unprotected redirect near line 311: re {Widget.find...
High	WidgetsController	update_widget_attribute	Redirect	Possible unprotected redirect near line 447: re {Widget.find...
High	WidgetsController	destroy	Redirect	Possible unprotected redirect near line 455: re {Widget.find(params...
High	WidgetsController	add_data_to_widget	Redirect	Possible unprotected redirect near line 492: re {Widget.find(pa...
High	WidgetsController	add_data_to_widget	Redirect	Possible unprotected redirect near line 494: re {Widget.find...
High	WidgetsController	remove_artist	Redirect	Possible unprotected redirect near line 509: re {Widget.find(pa...
High	WidgetsController	remove_artist	Redirect	Possible unprotected redirect near line 511: re {Widget.find...
High			SQL Injection	All versions of Rails before 3.0.13, 3.1.5, and Vulnerability: C...
High			SQL Injection	All versions of Rails before 3.0.13, 3.1.5, and CVE-2012...
High			SQL Injection	All versions of Rails before 3.0.14, 3.1.6, and CVE-2012...
Medium			Cross Site Scripting	Rails 3.1.3 has a vulnerabilty in SafeBuffer. U
Medium	PluginsController	open_window	Dynamic Render Path	Render path contains parameter value near line {})

add_data_to_widget	Redirect	Possible unprotected redirect near line 492: redirect_to("/widgets/add_custom_fields/#{Widget.find(params[:id]).id}")

app/controllers/widgets_controller.rb

```
487         artist_widget.save!
488       end
489     end
490     #  expire_fragment(:controller => '/services', :action => 'get_all_data',:format => 'json
491     if params[:act] == "add_custom_fields"
492       redirect_to "/widgets/add_custom_fields/#{@widget.id}"
493     else
494       redirect_to "/widgets/update_custom_fields/#{@widget.id}"
495     end
496   end
```

add_data_to_widget	Redirect	Possible unprotected redirect near line 494: redirect_to("/widgets/update_custom_fields/#{Widget.find...
remove_artist	Redirect	Possible unprotected redirect near line 509: redirect_to("/widgets/add_custom_fields/#{Widget.find(pa...
remove_artist	Redirect	Possible unprotected redirect near line 511: redirect_to("/widgets/update_custom_fields/#{Widget.find...
	SQL Injection	All versions of Rails before 3.0.13, 3.1.5, and 3.2.5 contain a SQL Query Generation Vulnerability: C...
	SQL Injection	All versions of Rails before 3.0.13, 3.1.5, and 3.2.5 contain a SQL Injection Vulnerability: CVE-2012...
	SQL Injection	All versions of Rails before 3.0.14, 3.1.6, and 3.2.6 contain SQL Injection Vulnerabilities: CVE-2012...
	Cross Site Scripting	Rails 3.1.3 has a vulnerabilty in SafeBuffer. Upgrade to 3.1.4 or apply patches.
open_window	Dynamic Render Path	Render path contains parameter value near line 13: render(partial => "plugins/#{params[:type]}", {}
import_artist	File Access	Model attribute value used in file name near line 216: File.read("#{Rails.root}/public#{("" or Asset....

Brakeman - Rails Security Scanner

Static analysis security scanner for Ruby on Rails

Redirect

Unvalidated redirects and forwards are #10 on the OWASP Top Ten.

Redirects which rely on user-supplied values can be used to "spoof" websites or hide malicious links in otherwise harmless-looking URLs. They can also allow access to restricted areas of a site if the destination is not validated.

Brakeman will raise warnings whenever `redirect_to` appears to be used with a user-supplied value that may allow them to change the `:host` option.

Rails Brakeman SQL injection warning when using Arel syntax

0

In my Rails 3.2 app, Brakeman 1.8.3 raises a High confidence SQL injection warning for the following code in a model:

micropost.rb

```
def self.from_users_followed_by(user)
  followed_user_ids = Relationship.select(:followed_id).
                      where("follower_id = :user_id").
                      to_sql
  where("user_id IN (#{followed_user_ids}) OR user_id = :user_id",
        user_id: user.id)
end
```

However, when I change the code to not use Arel syntax, no warning is raised:

```
def self.from_users_followed_by(user)
  followed_user_ids = "SELECT followed_id FROM relationships
                       WHERE follower_id = :user_id"
  where("user_id IN (#{followed_user_ids}) OR user_id = :user_id",
        user_id: user.id)
end
```

Is this a false positive, or something to do with Arel syntax or the `to_sql` method...? I don't understand what the difference is between the actual code that gets executed in the two examples that would warrant the warning.

ruby-on-rails | ruby-on-rails-3 | sql-injection | arel | brakeman

share | edit | close | delete | flag

asked Nov 29 '12 at 11:33
Paul Fioravanti
1,200 • 4 • 20
100% accept rate

add comment

1 Answer

active oldest votes

1

It's a false positive.

In this situation, Brakeman knows `Relationship` is a model, and that `select` and `where` are query methods. So it assumes `Relationship.select(...).where(...).to_sql` is a record attribute (and potentially dangerous). It shouldn't, though, since `to_sql` just generates the SQL code for the query as you mentioned. I'll fix this.

The second version of course does not warn because you are interpolating a string literal.

share | edit | flag

answered Nov 29 '12 at 15:09

Justin
116 •3

Best answer I could have hoped for! Thanks very much! – Paul Fioravanti Nov 29 '12 at 23:29

1 Glad to help. Fix is here. – Justin Nov 30 '12 at 2:42

add comment

Creator of Brakeman

paulfioravanti/sample_app

dependencies out-of-date

On GitHub

Dependencies

	Locked	Requirement	Stable	Prerelease	
annotate	2.5.0	= 2.5.0	2.5.0		
bcrypt-ruby	3.0.1	= 3.0.1	3.0.1		
best_in_place	2.0.2	= 2.0.2	2.0.2		
bootstrap-sass	2.2.2.0	= 2.2.2.0	2.2.2.0		
bootstrap-will_paginate	0.0.9	= 0.0.9	0.0.9		
brakeman	1.9.0.pre1	= 1.9.0.pre1	1.9.0		
bullet	4.2.0	= 4.2.0	4.3.0		
capybara	2.0.1	= 2.0.1	2.0.2		
coffee-rails	3.2.2	= 3.2.2	3.2.2		
cucumber-rails	1.3.0	= 1.3.0	1.3.0		
database_cleaner	0.9.1	= 0.9.1	0.9.1		
debugger	1.2.2	= 1.2.2	1.2.3		
factory_girl_rails	4.1.0	= 4.1.0	4.1.0		
faker	1.1.2	= 1.1.2	1.1.2		
figaro	0.5.0	= 0.5.0	0.5.0		
font-awesome-sass-rails	2.0.0.0	= 2.0.0.0	2.0.0.0		
fuubar	1.1.0	= 1.1.0	1.1.0		

New ruby_parser version

Inbox x

Gemnasium <app@gemnasium.com>

12/20/12 (13 days ago)

to me

There's a new **patch** version of **ruby_parser**. 3.1.0 ⇢ **3.1.1**

Gemnasium

ruby_parser 3.1.1

Big news!

There's a new **patch** version of **ruby_parser**.

3.1.0 ⇢ **3.1.1**

You have 1 ruby_parser dependency:

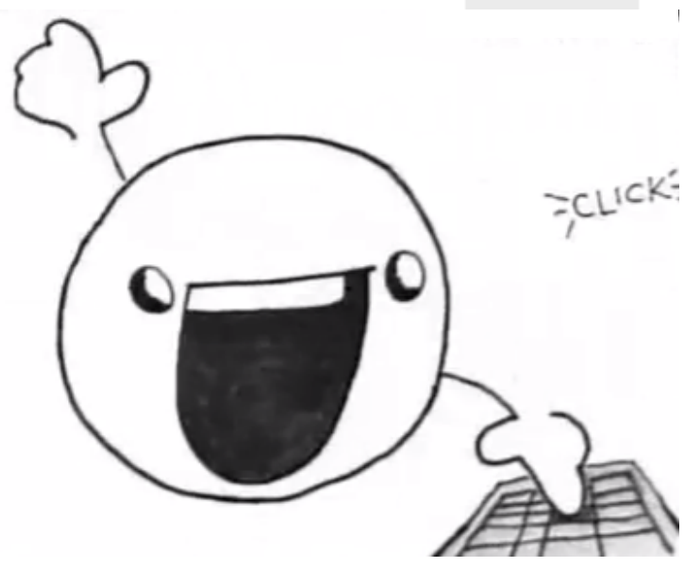
paulfioravanti/sample_app = 2.3.1

Cheers!
Gemnasium

On RubyGems

On GitHub

Stop notifications



travis Home Stats Blog Docs Paul Fioravanti

Recent My Repositories

- bigeasy/timezone 351
  Duration: 39 sec, Finished: -
- enthought/pyql 26
  Duration: 6 min 54 sec, Finished: -
- middleman/middleman 552
  Duration: 7 min 8 sec, Finished: -
- square/okhttp 123
  Duration: 56 sec, Finished: 3 minu…
- ekmett/lens 1435
  Duration: 2 min 49 sec, Finished: l…

paulfioravanti/sample_app

Ruby on Rails Tutorial sample application (plus mods)

Current | Build History | Pull Requests | Branch Summary

Build	209	Commit	c188ca4 (master)
state	Passed	Compare	1a7a27cc40c0...c188ca49c7a0
Finished	9 days ago	Author	Paul Fioravanti
Duration	7 min 33 sec	Committer	Paul Fioravanti
Message	Comment out code that trips up Rails Breakman for now. When the service upgrades to 1.9.0, then can swap the code back in		
Config	Rvm: 1.9.3, Env: DB=postgresql HEROKU_API_KEY=[secure]		

```
1 Using worker: ruby1.worker.travis-ci.org:ruby-6
2
3 $ cd ~/builds
4 $ export DB=postgresql
5 $ export HEROKU_API_KEY=[secure]
6 $ git clone --branch=master --depth=100 --quiet
    git://github.com/paulfioravanti/sample_app.git paulfioravanti/sample_app
```

README.md

Ruby on Rails Tutorial: sample application

This is the sample application for *Ruby on Rails Tutorial: Learn Rails by Example* by Michael Hartl

- This code is currently deployed here using Heroku
- Translation keys are currently being managed here with Localeapp.

If you find this repo useful, please help me level-up on Coderwall with an 

Travis CI

Gemnasium

Brakeman

Code Climate

Recap

- SimpleCov - code test coverage gem
- Rails Best Practices - coding quality gem/ service
- Code Climate - code metrics service
- Reek - code smells gem
- Brakeman - app security gem/service
- Gemnasium - gem manager service
- Travis CI - continuous integration (and deployment) service