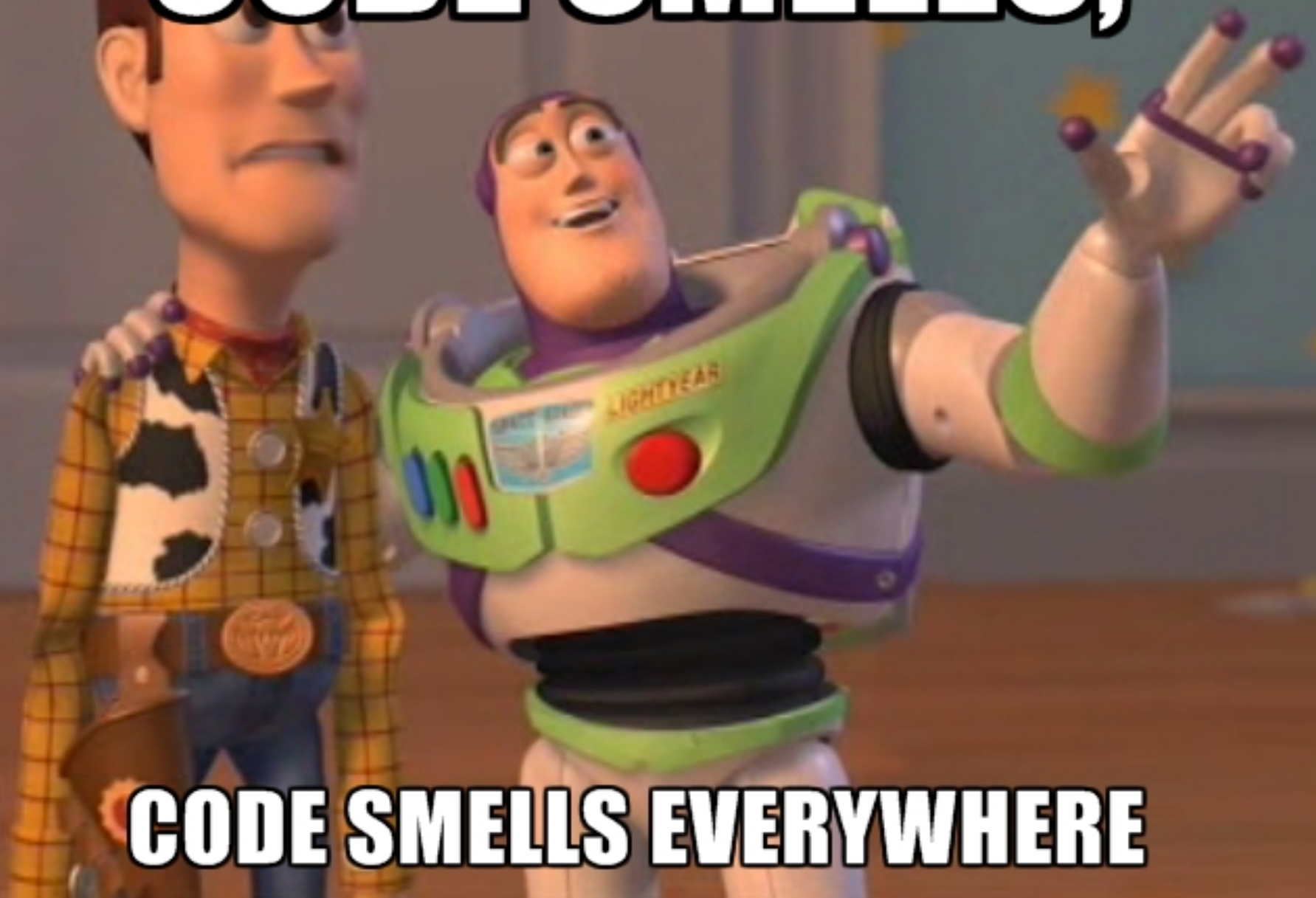


Ruby Code Analysis

Tools and Practices

CODE SMELLS,



CODE SMELLS EVERYWHERE

Well known smells

- long methods and large classes

Well known smells

- long methods and large classes
- duplicated code

Well known smells

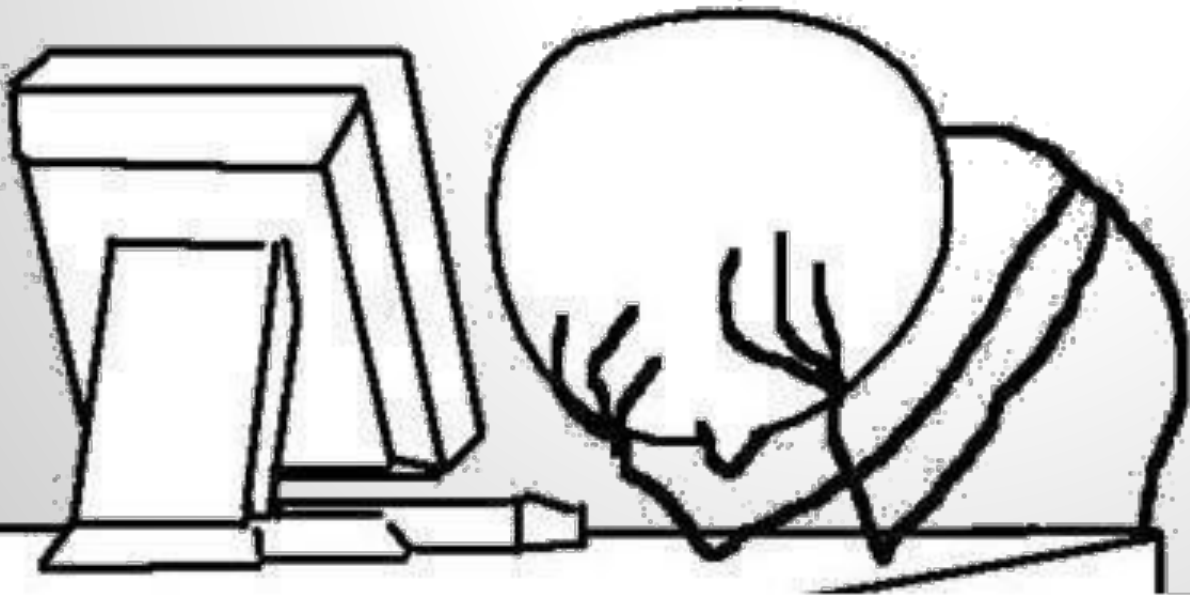
- long methods and large classes
- duplicated code
- too many parameters

Well known smells

- long methods and large classes
- duplicated code
- too many parameters
- conditional complexity

Well known smells

- long methods and large classes
- duplicated code
- too many parameters
- conditional complexity
- etc...

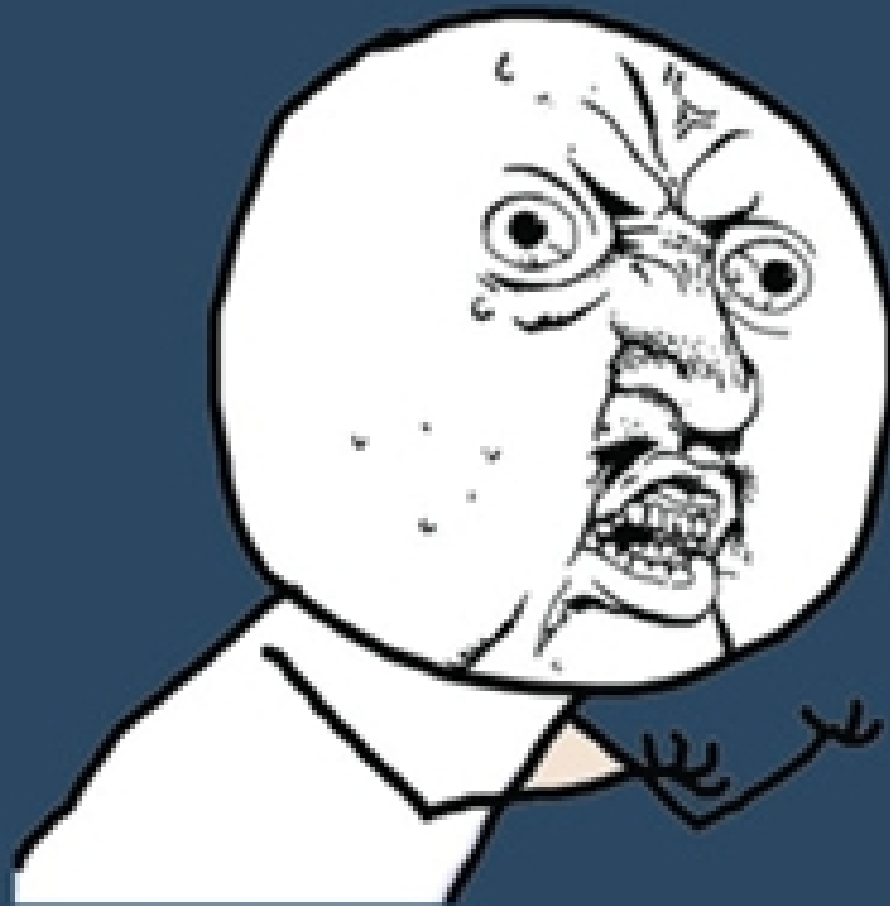


REFACTOR



ALL THE THINGS!

RUBY



Y U SO DYNAMIC?

ruby -w

ruby -w

```
$ ruby -w script.rb
```

ruby -w

```
$ ruby -w script.rb
```



enables verbose mode of ruby interpreter

ruby -w

```
$ ruby -w script.rb
```



enables verbose mode of ruby interpreter

```
script.rb:4: warning: assigned but unused variable -  
file
```

```
script.rb:11: warning: mismatched indentations at  
'end' with 'def' at 7
```

ruby -w

What about  ?

ruby -w

```
$ RUBYOPT=-w rails server 2>&1 | grep appname/app
```

ruby -w

```
$ RUBYOPT=-w rails server 2>&1 | grep errbit/app
```

```
errbit/app/models/issue_trackers/github_issues_tracker.rb:38: warning: assigned  
but unused variable - options  
errbit/app/models/notice.rb:138: warning: shadowing outer local variable - h  
errbit/app/models/user.rb:6: warning: `*' interpreted as argument prefix  
errbit/app/models/watcher.rb:16: warning: method redefined; discarding old  
watcher_type  
errbit/app/controllers/apps_controller.rb:90: warning: mismatched indentations  
at 'end' with 'def' at 83  
errbit/app/helpers/notices_helper.rb:72: warning: assigned but unused variable  
- file
```

<http://tinyurl.com/shelrtv-errbit-ruby-verbose>

flog

flog

```
$ flog app.rb
```

flog

```
$ flog app.rb
```

```
311.4: flog total
```

```
13.6: flog/method average
```

```
73.4: App#none
```

```
65.9: App#notify      app.rb:124
```

```
42.1: App#attributes  app.rb:142
```

flog

```
$ flog app.rb
```

```
  311.4: flog total
```

```
    13.6: flog/method average
```

```
    73.4: App#none
```

```
    65.9: App#notify      app.rb:124
```

```
    42.1: App#attributes  app.rb:142
```

flog

```
$ flog app.rb
```

```
311.4: flog total
```

```
13.6: flog/method average
```

```
73.4: App#none
```

```
65.9: App#notify      app.rb:124
```

```
42.1: App#attributes  app.rb:142
```

flog

```
$ flog app.rb
```

```
311.4: flog total
```

```
13.6: flog/method average
```

```
73.4: App#none
```

```
65.9: App#notify      app.rb:124
```

```
42.1: App#attributes  app.rb:142
```

flog

```
$ flog -g appname/app
```

or

```
$ flog -g appname/app/models
```

flog

```
$ flog -g errbit/app/models
```

```
1690.0: flog total
```

```
11.1: flog/method average
```

```
219.3: App total
```

```
88.4: App#none
```

```
60.5: App#notification_recipients      errbit/app/models/app.rb:144
```

```
48.8: App#copy_attributes_from          errbit/app/models/app.rb:153
```

```
21.7: App#check_issue_tracker           errbit/app/models/app.rb:178
```

<http://tinyurl.com/shelrtv-errbit-flog>

flay

analyzes code for similarities

flay

```
$ flay app.rb
```

flay

```
$ flay app.rb
```

```
Total score (lower is better) = 266
```

1) IDENTICAL code found in :iter (mass*2 = 152)

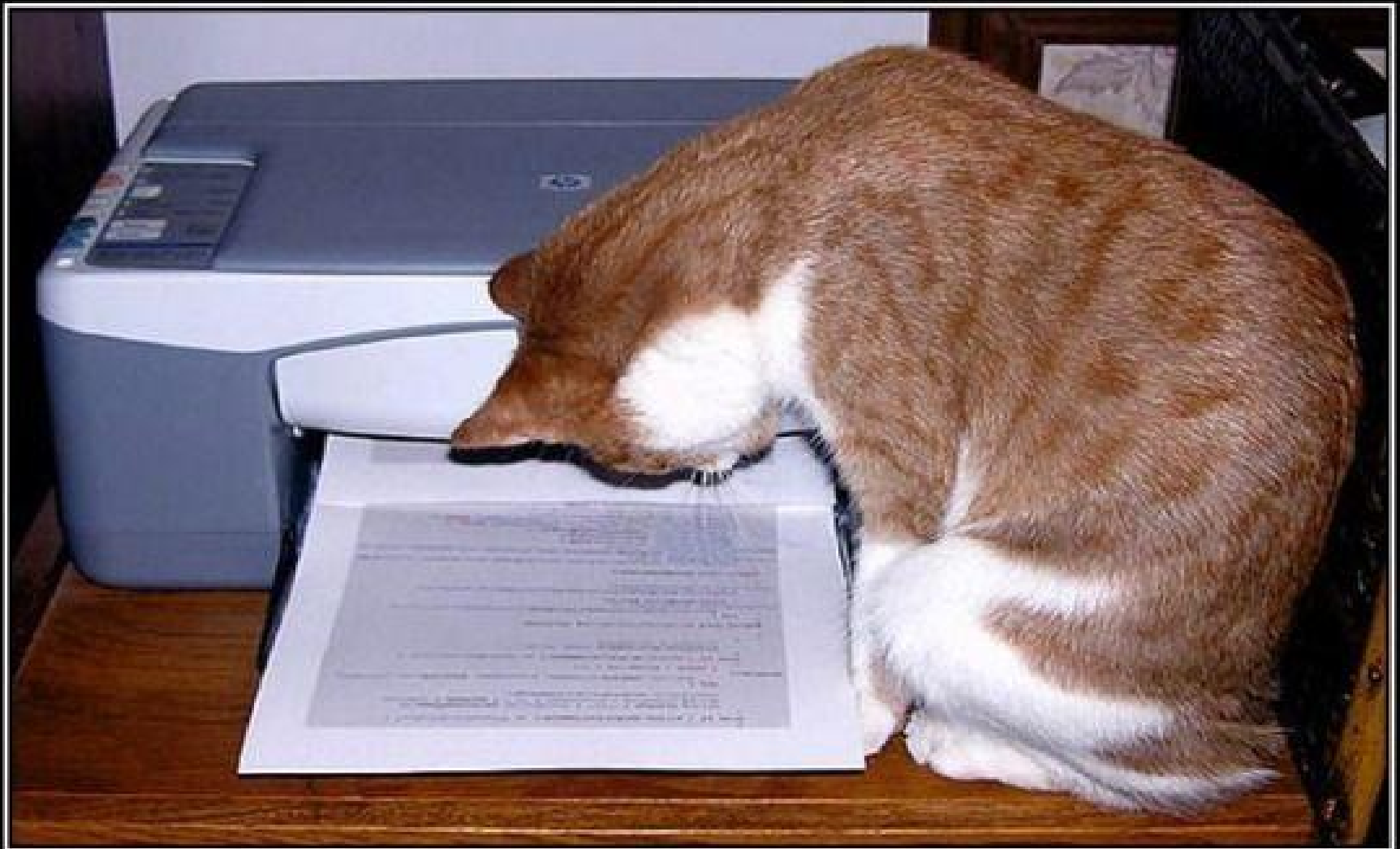
```
app.rb:16
```

```
app.rb:31
```

2) Similar code found in :defn (mass = 114)

```
app.rb:74
```

```
app.rb:83
```



CODE REVIEWS

An essential step to ensure code quality.



BRAKEMAN

brakeman warning types

- Command Injection

```
`ls #{params[:file]}`
```

brakeman warning types

- Command Injection
- SQL Injection

```
username=params[:user][:name].downcase
```

```
password=params[:user][:password]
```

```
User.first.where("username = '" + username + "'  
AND password = '" + password + "'")
```

brakeman warning types

- Command Injection
- SQL Injection
- Mass Assignment

brakeman warning types

- Command Injection
- SQL Injection
- Mass Assignment
- Default Routes

```
match ':controller(/:action(/:id(.:format)))'
```

brakeman warning types

- Command Injection
- SQL Injection
- Mass Assignment
- Default Routes
- File Access

```
File.open("/tmp/#{cookie[:file]}")
```

brakeman warning types

- Command Injection
- SQL Injection
- Mass Assignment
- Default Routes
- File Access
- Dangerous Send

```
method = params[:method]
```

```
@result = User.send(method.to_sym)
```

brakeman warning types

- Command Injection
- SQL Injection
- Mass Assignment
- Default Routes
- File Access
- Dangerous Send

See more in documentation.

Scanned/Reported	Total
Controllers	6
Models	2
Templates	44
Errors	1
Security Warnings	7 (0)

```
$ brakeman shelr.tv -o report.html
```

Warning Type	Total
Cross Site Scripting	2
Dynamic Render Path	5

Exceptions raised during the analysis (click to see them)

Security Warnings

Confidence	Class	Method	Warning Type	Message
Medium			Cross Site Scripting	Rails 3.2.6 does not escape single quotes (CVE-2012-3464). Upgrade to 3.2.8

View Warnings

Confidence	Template	Warning Type	Message
Weak	users/show (UserController#show)	Cross Site Scripting	Unescaped parameter value near line 24: find_and_preserve(Haml::Filters::Escaped.render_with_options("gem install shelr shelr setup # {UserDecorator.find(params[:id]).api_key} shelr record shelr push last ", _hamlout.options))
			app/views/users/show.html.haml
			19 %h2.alert-heading Start sharing now!
			20 %pre
			21 %code
			22 = preserve do
			23 :escaped

security status failing

rails-brakeman.com

rails_best_practices

rails-bestpractices.com

18 votes
10625 views

Not use time_ago_in_words

It's very common for a rails developer to use `time_ago_in_words` to display time like "5 minutes ago", but it's too expensive to calculate the time in server side, you should utilize client cpu to calculate the time ago.

[helper](#)

[javascript](#)

10 Comments and 0 Reactions

by [flyerhzm](#)



implemented

rails-bestpractices.com advices

- Protect mass assignment
- Not use `time_ago_in_words`
- Remove empty helpers
- Always add DB index
- Use Observer
- Remove trailing whitespace

Filename	Line Number	Warning Message
db/migrate/20110422152027_move_notices_to_separate_collection.rb	18	isolate seed data
db/migrate/20110905134638_link_errs_to_problems.rb	15	isolate seed data
app/views/kaminari/_paginator.html.haml	12	move code into model (page use_count > 2)
app/views/problems/_table.html.haml	42	move code into model (problem use_count > 2)
app/controllers/api/v1/problems_controller.rb	14	move finder to named_scope
app/controllers/api/v1/notices_controller.rb	14	move finder to named_scope
app/controllers/apps_controller.rb	6	move model logic into model (@problems use_count > 4)
app/controllers/apps_controller.rb	102	move model logic into model (app use_count > 4)
config/routes.rb	30	needless deep nesting (nested_count > 2)
config/routes.rb	31	needless deep nesting (nested_count > 2)
app/views/problems/_table.html.haml	38	not use time_ago_in_words
app/views/problems/show.html.haml	34	not use time_ago_in_words
config/routes.rb	17	overuse route customizations (customize_count > 3)
app/controllers/application_controller.rb	9	remove unused methods (ApplicationController#stored_location_for)
app/controllers/apps_controller.rb	98	remove unused methods (AppsController#interpolation_options)
app/models/user.rb	43	remove unused methods (User#password_required?)
app/models/problem.rb	64	remove unused methods (Problem#unresolve!)
app/models/problem.rb	85	remove unused methods (Problem#merged?)
app/models/problem.rb	89	remove unused methods (Problem#unmerge!)
app/models/problem.rb	113	remove unused methods (Problem#in_date_range)
app/models/watcher.rb	24	remove unused methods (Watcher#address)
app/models/app.rb	85	remove unused methods (App#find_by_id!)
app/views/users/_fields.html.haml	1	replace instance variable with local variable
app/views/apps/_fields.html.haml	1	replace instance variable with local variable

R_p^b
railsbp.com

What else

- performance
- tests and code coverage
- codeclimate

Resume

ruby -w + flog + flay + brakeman = 

Thank you



@proghat



github.com/proghat



dima.zhlobo@gmail.com

