

[3SCALE HACKATON 2015]

@RAI & @TONI

AS...

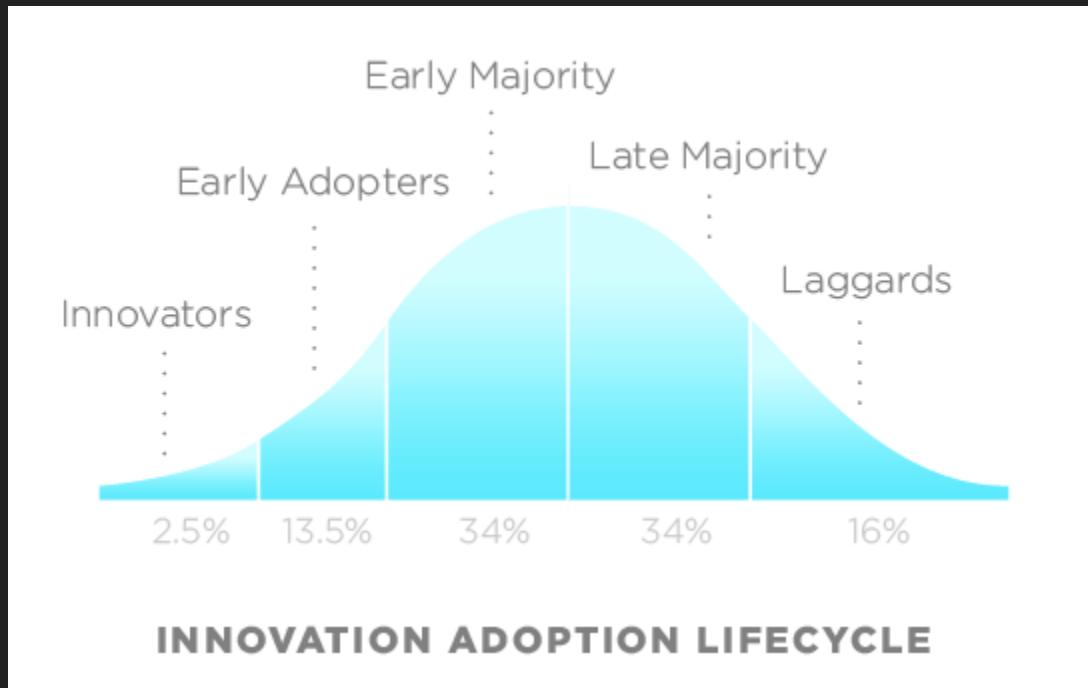
TENERIFE HAACKING TEAM



CAPITAN CANARIO

presenting:

INNOVATION



BUT THIS COMES AT A COST...

- Explosion of adoption
- Adopters from different areas
- Adopters of different knowledge
- Not Invented Here syndrome

RUBY DRAMA

We illustrate our examples with Ruby because it's our main language

- Indentation: Spaces vs Tabs; Two spaces vs Four spaces
- Parens or no parens
- or and || && operators
 - HOLA: @michal, @wojciech, @alex :-)
- limit chars per line (80chars)
- Align parameters
- negative conditions
- etc

API DRAMA

- Different formats: XML vs JSON
- REST or NO REST
- Versioning
 - No versioning
 - Version in uri path
 - Version in headers
- Backwards compatibility
- Different ways to represent resources
- URI paths
- ADD HERE YOUR PERSONAL NIGHTMARE

CONVERGENCE

- Standardization of styles.
- Follow best practices
- Recognized authorities
- Enforced laws
- Official committee

WE'RE THERE (KINDA)

- Ruby has its own style guide (powered by thoughtbot)
- SCSS has it too
- js has it too (airbnb)
- Scientific publications have it too
- APIs have it too (provided by heroku, but still settling)

AND WE GOT SMARTER...

So we made it automatic, so apps can check code looking for code red flags.

- Rubocop: Automatic Ruby style checking tool.



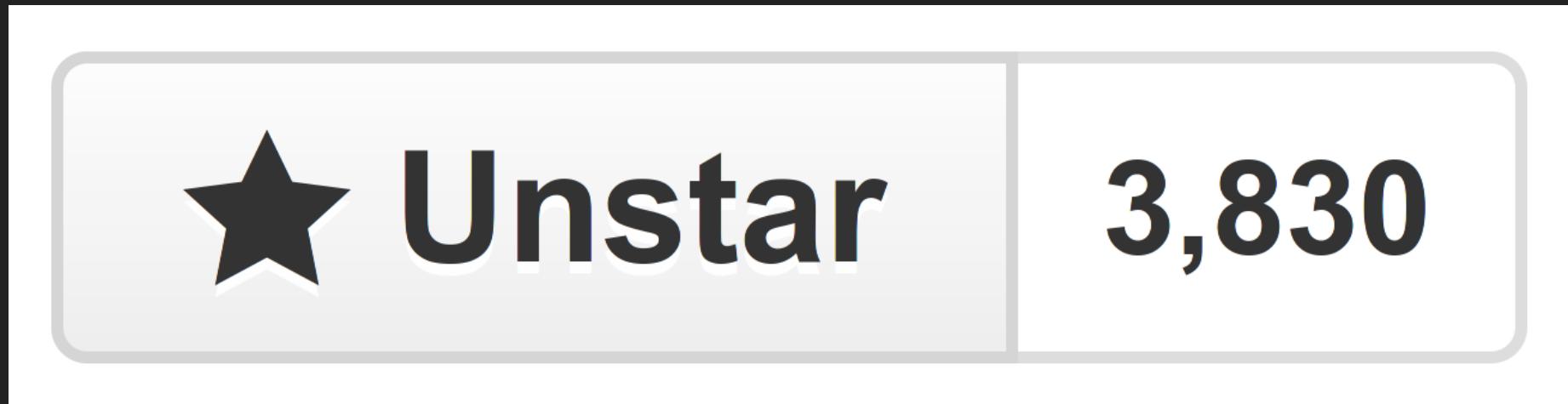
RuboCop

Role models are important.
-- Officer Alex J. Murphy / RoboCop

RuboCop is a Ruby static code analyzer. Out of the box it will enforce many of the guidelines outlined in the community [Ruby Style Guide](#).

Most aspects of its behavior can be tweaked via various [configuration options](#).

EH!!



BUT! NO CHECKER FOR APIs...

Until now....

APILINT (ZAPP BRANNIGAN)

Given a collection of request-response pairs, automatically detects red flags or warns about bad practices on that API.

♩ ♩ ♩ It's got to beeeeeee perfect ♩ ♩ ♩

APILINT (ZAPP BRANNINGAN)

Ways to collect HTTP requests & responses:

- Apitools
- Apicast
- Swagger spec
- Ruby Rack Middleware
- rspec_api_documentation

APILINT (ZAPP BRANNIGAN)

Lints are the individual checkers for each style element.

- It's easy to create your own lints

```
module Apilint
  module Lint
    class DowncasePath < Linter
      MSG = 'Use downcased and dash-separated path names, for alignment with hostnames'

      def check(request, response)
        if request.uri =~ /[A-Z]/
          add_offense(request, response, :uri)
        end
      end
    end
  end
end
```

APILINT (ZAPP BRANNIGAN)

- Which are configurable, and also activable/deactivable

```
DowncasePath:  
  Enabled: true  
  
DeepPath:  
  Enabled: true  
  Prefix: '/admin/api'  
  MaxDepth: 3  
  
RateLimitStatus:  
  Enabled: true  
  
MinifiedJson:  
  Enabled: false
```

-:--- apilint-config.yml All L13

PRAY FOR THE DEMO GODS

- Command line interface:
 - Usage:

```
~/development/3scale-hackaton $ apilint
Commands:
  apilint check FILE      # Check FILE containing your API requests
  apilint help [COMMAND]  # Describe available commands or one specific command
```

- Help:

```
~/development/3scale-hackaton $ apilint help check
Usage:
  apilint check FILE

Options:
  -c, [--config-file=CONFIG_FILE]

Check FILE containing your API requests
```

PRAY FOR THE DEMO GODS

- Command line interface:
 - Results by Lint type:

```
~/development/3scale-hackaton $ apilint check MT-traffic.json -c apilint-config.yml
Checking MT-traffic.json...

-----
DowncasePath - Use downcased and dash-separated path names, for alignment with
hostnames
-----

- /admin/api/accounts/:param/APPLICATIONS/:param/keys/app-key-1.json
  URI: "/admin/api/accounts/247/APPLICATIONS/436/keys/app-key-1.json":
  Offense in uri: "/admin/api/accounts/247/APPLICATIONS/436/keys/app-key-1.json"

-----
DeepPath - Limit nesting depth by preferring to locate resources at the root path.

-----

- /admin/api/accounts/:param/APPLICATIONS/:param/keys/app-key-1.json
  URI: "/admin/api/accounts/247/APPLICATIONS/436/keys/app-key-1.json":
  Offense in uri: "/admin/api/accounts/247/APPLICATIONS/436/keys/app-key-1.json"

- /admin/api/accounts/:param/applications/:param/keys.xml
  URI: "/admin/api/accounts/250/applications/441/keys.xml":
  Offense in uri: "/admin/api/accounts/250/applications/441/keys.xml"

- /admin/api/accounts/:param/applications/:param/keys/app-key-2.xml
  URI: "/admin/api/accounts/253/applications/446/keys/app-key-2.xml":
  Offense in uri: "/admin/api/accounts/253/applications/446/keys/app-key-2.xml"
```

PRAY FOR THE DEMO GODS

- Command line interface:
 - Results by Lint type:

```
-----  
RateLimitStatus - Return the remaining number of request tokens with each request in the 'RateLimit-Remaining' response header.  
-----  
- /admin/api/accounts/:param/APPLICATIONS/:param/keys/app-key-1.json  
  URI: "/admin/api/accounts/247/APPLICATIONS/436/keys/app-key-1.json":  
    Offense in headers: "{\"X-Frame-Options\"=>"DENY", \"X-XSS-Protection\"=>"1; mode=block", \"X-Content-Type-Options\"=>"no  
-f"}"  
  
- /admin/api/accounts/:param/applications/:param/keys.xml  
  URI: "/admin/api/accounts/250/applications/441/keys.xml":  
    Offense in headers: "{\"X-Frame-Options\"=>"DENY", \"X-XSS-Protection\"=>"1; mode=block", \"X-Content-Type-Options\"=>"no  
-f", \"Location\"=>"http://example.org/admin/api/accounts/250/applications/441/keys?id=11"}"  
  
- /admin/api/accounts/:param/applications/:param/keys/app-key-2.xml  
  URI: "/admin/api/accounts/253/applications/446/keys/app-key-2.xml":  
    Offense in headers: "{\"X-Frame-Options\"=>"DENY", \"X-XSS-Protection\"=>"1; mode=block", \"X-Content-Type-Options\"=>"no  
-f"}"  
  
- /admin/api/accounts/:param/applications/:param/referrer_filters.json  
  URI: "/admin/api/accounts/280/applications/503/referrer_filters.json":  
    Offense in headers: "{\"X-Frame-Options\"=>"DENY", \"X-XSS-Protection\"=>"1; mode=block", \"X-Content-Type-Options\"=>"no  
-f", \"Location\"=>"http://example.org/admin/api/accounts/280/applications/503/referrer_filters?id=9"}"
```

PRAY FOR THE DEMO GODS

- Command line interface:
 - Results by Lint type:

```
-----  
IncludeTimestamps - Provide 'created_at' and 'updated_at' timestamps for resources by default  
-----  
- /admin/api/accounts/:param/applications/:param/change_plan.xml  
  URI: "/admin/api/accounts/367/applications/653/change_plan.xml":  
    Offense in body: "<?xml version='1.0' encoding='UTF-8'?><plan custom='false' default='false'><id>770</id><n/></name><type>application_plan</type><state>hidden</state><service_id>373</service_id><end_user_required>false</end_user_requ<fee>0.0</setup_fee><cost_per_month>0.0</cost_per_month><trial_period_days>0</trial_period_days><cancellation_period>0</canc<iod></plan>"  
  
- /admin/api/accounts/:param/applications/:param/decustomize_plan.xml  
  URI: "/admin/api/accounts/371/applications/660/decustomize_plan.xml":  
    Offense in body: "<?xml version='1.0' encoding='UTF-8'?><plan custom='false' default='false'><id>776</id><n/></name><type>application_plan</type><state>hidden</state><service_id>378</service_id><end_user_required>false</end_user_requ<fee>0.0</setup_fee><cost_per_month>0.0</cost_per_month><trial_period_days>0</trial_period_days><cancellation_period>0</canc<iod></plan>"
```

PRAY FOR THE DEMO GODS

- Command line interface:
 - Total number of results:

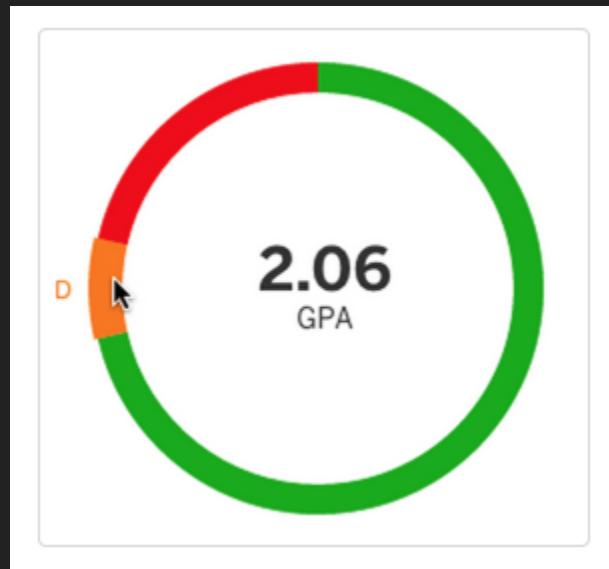
```
--> 39 requests inspected, 82 offenses detected
```

INTEGRATIONS (FUTURE WORK)

- 3SCALE API DOCS PROXY
- 3SCALE REQUEST LOGS
- APINATOR ?

INTEGRATIONS (FUTURE WORK)

- imagine:
 - 3SCALE widget/badges with info about your API quality



INTEGRATIONS (FUTURE WORK)

- imagine:
 - 3SCALE section (ala codeclimate) with general recommendations about API design and info about your real traffic API

Complexity	2340
Duplication	2011
Security	946
Style	1838
Clarity	5367

Feed Code Issues Security Branches Trends Settings c1b037d6

High total complexity (complexity = 5736)
Found in [core/assets/vendor/jquery.ui/ui/jquery-ui.custom.js](#)

High total complexity (complexity = 1418)
Found in [core/assets/vendor/jquery.ui/external/jshint.js](#)

High total complexity (complexity = 992)
Found in [core/assets/vendor/jquery.ui/ui/jquery.ui.datepicker.js](#)

High total complexity (complexity = 619)
Found in [core/assets/vendor/jquery.ui/external/qunit.js](#)

High total complexity (complexity = 548)
Found in [core/modules/ckeditor/js/ckeditor.admin.js](#)

High total complexity (complexity = 510)
Found in [core/assets/vendor/jquery.ui/ui/jquery.ui.sortable.js](#)

THANKS

- <http://kidd.github.io/apilint> [WEB]
- <http://github.com/kidd/apilint> [GH]
- Q & A