Drifting Ruby

EPISODE #62

Security and Static Code Analyzers

Gemfile | users_controller.rb

```
1  source 'https://rubygems.org'
2  gem 'rails', '5.0.0'
3  gem 'sqlite3'
4  gem 'puma', '~> 3.0'
5  gem 'sass-rails', '~> 5.0'
6  gem 'uglifier', '>= 1.3.0'
7  gem 'coffee-rails', '~> 4.1.0'
8  gem 'jquery-rails'
9  gem 'turbolinks', '~> 5.x'
10 gem 'jbuilder', '~> 2.0'
11 group :development, :test do
12   gem 'byebug', platform: :mri
13 end
14
15 group :development do
16   gem 'web-console'
17   gem 'listen', '~> 3.0.5'
18   gem 'spring'
19   gem 'spring-watcher-listen', '~> 2.0.0'
20   gem 'better_errors'
21   gem 'rails_layout'
22 end
23
24 gem 'tzinfo-data', platforms: [:mingw, :mswin, :x64_mingw, :jruby]
25
26 gem 'bootstrap-sass'
27 gem 'simple_form'
28
```

```
1  source 'https://rubygems.org'
2  gem 'rails', '5.0.0.1'
3  gem 'sqlite3'
4  gem 'puma', '~> 3.0'
5  gem 'sass-rails', '~> 5.0'
6  gem 'uglifier', '>= 1.3.0'
7  gem 'coffee-rails', '~> 4.1.0'
8  gem 'jquery-rails'
9  gem 'turbolinks', '~> 5.x'
10 gem 'jbuilder', '~> 2.0'
11 group :development, :test do
12   gem 'byebug', platform: :mri
13 end
14
15 group :development do
16   gem 'web-console'
17   gem 'listen', '~> 3.0.5'
18   gem 'spring'
19   gem 'spring-watcher-listen', '~> 2.0.0'
20   gem 'better_errors'
21   gem 'rails_layout'
22 end
23
24 gem 'tzinfo-data', platforms: [:mingw, :mswin, :x64_mingw, :jruby]
25
26 gem 'bootstrap-sass'
27 gem 'simple_form'
28
```

Brakeman - Rails Security Scanner

Static analysis security scanner for Ruby on Rails

NOV 2ND, 2016

Brakeman 3.4.1 Released

- Configurable engines path (Jason Yeo)
- Check CSRF setting in direct subclasses of `ActionController::Base` (Jason Yeo)
- Pull Ruby version from `.ruby-version` or Gemfile
- Use Ruby version to turn off SymbolDoS check (#928)
- Fix ignoring link interpolation not at beginning of string (#939)
- Show action help at start of interactive ignore (#949)
- Avoid warning about `where_values_hash` in SQLi (#942)

Brakeman is an open source vulnerability scanner specifically designed for Ruby on Rails applications. It statically analyzes Rails application code to find security issues at any stage of development.

Brakeman Pro is the commercial version of Brakeman which offers a GUI, test integration, deeper analysis, and more.

Code Updates

Merge pull request #981 from presidentbeef/add_check_name_to_reports

```
➜  062-security-and-static-code-analyzers git:(master) ✗ gem install brakeman
```

```
➜  062-security-and-static-code-analyzers git:(master) ✗ gem install brakeman
Successfully installed brakeman-3.4.1
1 gem installed
➜  062-security-and-static-code-analyzers git:(master) ✗ brakeman
```

2. kobaltz@TardisPro: ~/drifting_ruby/062-security-and-static-code-analyzers (zsh)

```
inders, EscapeFunction, Evaluation, Execute, FileAccess, FileDisclosure, FilterSkipping, ForgerySetting, HeaderDoS, I18nXSS, JRubyXML, JSONEncoding, JSONPars
ing, LinkTo, LinkToHref, MailTo, MassAssignment, MimeTypeDoS, ModelAttrAccessible, ModelAttributes, ModelSerialize, NestedAttributes, NestedAttributesBypass,
 NumberToCurrency, QuoteTableName, Redirect, RegexDoS, Render, RenderDoS, RenderInline, ResponseSplitting, RouteDoS, SQL, SQLCVEs, SSLVerify, SafeBufferManip
ulation, SanitizeMethods, SelectTag, SelectVulnerability, Send, SendFile, SessionManipulation, SessionSettings, SimpleFormat, SingleQuotes, SkipBeforeFilter,
 StripTags, SymbolDoSCVE, TranslateBug, UnsafeReflection, ValidationRegex, WithoutProtection, XMLDoS, YAMLParsing


+SUMMARY+

+-------------------+-------+
| Scanned/Reported  | Total |
+-------------------+-------+
| Controllers       | 3     |
| Models            | 2     |
| Templates         | 11    |
| Errors            | 0     |
| Security Warnings | 3 (2) |
+-------------------+-------+

+----------------------+-------+
| Warning Type         | Total |
+----------------------+-------+
| Cross Site Scripting | 1     |
| Mass Assignment      | 1     |
| SQL Injection        | 1     |
+----------------------+-------+


+SECURITY WARNINGS+

+------------+-----------------+-------------+----------------------+----------------------------------------------------------------------------------->>
| Confidence | Class           | Method      | Warning Type         | Message                                                                           >>
+------------+-----------------+-------------+----------------------+----------------------------------------------------------------------------------->>
| High       |                 |             | Cross Site Scripting | Rails 5.0.0 content_tag does not escape double quotes in attribute values (CVE-2016-6>>
| High       | UsersController | set_user    | SQL Injection        | Possible SQL injection near line 68: User.where("ID = #{+params[:id]+}")          >>
| Medium     | UsersController | user_params | Mass Assignment      | Parameters should be whitelisted for mass assignment near line 74: params.require(:us>>
+------------+-----------------+-------------+----------------------+----------------------------------------------------------------------------------->>

➜ 062-security-and-static-code-analyzers git:(master) ✗
```

```
inders, EscapeFunction, Evaluation, Execute, FileAccess, FileDisclosure, FilterSkipping, ForgerySetting, HeaderDoS, I18nXSS, JRubyXML, JSONEncoding, JSONPars
ing, LinkTo, LinkToHref, MailTo, MassAssignment, MimeTypeDoS, ModelAttrAccessible, ModelAttributes, ModelSerialize, NestedAttributes, NestedAttributesBypass,
 NumberToCurrency, QuoteTableName, Redirect, RegexDoS, Render, RenderDoS, RenderInline, ResponseSplitting, RouteDoS, SQL, SQLCVEs, SSLVerify, SafeBufferManip
ulation, SanitizeMethods, SelectTag, SelectVulnerability, Send, SendFile, SessionManipulation, SessionSettings, SimpleFormat, SingleQuotes, SkipBeforeFilter,
 StripTags, SymbolDoSCVE, TranslateBug, UnsafeReflection, ValidationRegex, WithoutProtection, XMLDoS, YAMLParsing


+SUMMARY+

+------------------+-------+
| Scanned/Reported | Total |
+------------------+-------+
| Controllers      | 3     |
| Models           | 2     |
| Templates        | 11    |
| Errors           | 0     |
| Security Warnings | 3 (2) |
+------------------+-------+

+----------------------+-------+
| Warning Type         | Total |
+----------------------+-------+
| Cross Site Scripting | 1     |
| Mass Assignment      | 1     |
| SQL Injection        | 1     |
+----------------------+-------+


+SECURITY WARNINGS+

+----------+----------------+------------+---------------------+-------------------------------------------------------------------------------------->>
| Confidence | Class          | Method     | Warning Type        | Message                                                                                >>
+----------+----------------+------------+---------------------+-------------------------------------------------------------------------------------->>
| High     |                |            | Cross Site Scripting | Rails 5.0.0 content_tag does not escape double quotes in attribute values (CVE-2016-6>>
| High     | UsersController | set_user   | SQL Injection       | Possible SQL injection near line 68: User.where("ID = #{+params[:id]+}")               >>
| Medium   | UsersController | user_params | Mass Assignment     | Parameters should be whitelisted for mass assignment near line 74: params.require(:us>>
+----------+----------------+------------+---------------------+-------------------------------------------------------------------------------------->>

➜ 062-security-and-static-code-analyzers git:(master) ✗
```

```
inders, EscapeFunction, Evaluation, Execute, FileAccess, FileDisclosure, FilterSkipping, ForgerySetting, HeaderDoS, I18nXSS, JRubyXML, JSONEncoding, JSONPars
ing, LinkTo, LinkToHref, MailTo, MassAssignment, MimeTypeDoS, ModelAttrAccessible, ModelAttributes, ModelSerialize, NestedAttributes, NestedAttributesBypass,
 NumberToCurrency, QuoteTableName, Redirect, RegexDoS, Render, RenderDoS, RenderInline, ResponseSplitting, RouteDoS, SQL, SQLCVEs, SSLVerify, SafeBufferManip
ulation, SanitizeMethods, SelectTag, SelectVulnerability, Send, SendFile, SessionManipulation, SessionSettings, SimpleFormat, SingleQuotes, SkipBeforeFilter,
 StripTags, SymbolDoSCVE, TranslateBug, UnsafeReflection, ValidationRegex, WithoutProtection, XMLDoS, YAMLParsing


+SUMMARY+

+------------------+-------+
| Scanned/Reported | Total |
+------------------+-------+
| Controllers      | 3     |
| Models           | 2     |
| Templates        | 11    |
| Errors           | 0     |
| Security Warnings | 3 (2) |
+------------------+-------+

+----------------------+-------+
| Warning Type         | Total |
+----------------------+-------+
| Cross Site Scripting | 1     |
| Mass Assignment      | 1     |
| SQL Injection        | 1     |
+----------------------+-------+


+SECURITY WARNINGS+

+----------+----------------+------------+---------------------+-------------------------------------------------------------------------------->>
| Confidence | Class          | Method     | Warning Type        | Message                                                                        >>
+----------+----------------+------------+---------------------+-------------------------------------------------------------------------------->>
| High     |                |            | Cross Site Scripting | Rails 5.0.0 content_tag does not escape double quotes in attribute values (CVE-2016-6>>
| High     | UsersController | set_user   | SQL Injection       | Possible SQL injection near line 68: User.where("ID = #{+params[:id]+}")       >>
| Medium   | UsersController | user_params | Mass Assignment     | Parameters should be whitelisted for mass assignment near line 74: params.require(:us>>
+----------+----------------+------------+---------------------+-------------------------------------------------------------------------------->>

➜ 062-security-and-static-code-analyzers git:(master) ✗ brakeman -o brakeman.html
```

```
 - CheckModelAttributes
 - CheckModelSerialize
 - CheckNestedAttributes
 - CheckNestedAttributesBypass
 - CheckNumberToCurrency
 - CheckQuoteTableName
 - CheckRedirect
 - CheckRegexDoS
 - CheckRender
 - CheckRenderDoS
 - CheckRenderInline
 - CheckResponseSplitting
 - CheckRouteDoS
 - CheckSafeBufferManipulation
 - CheckSanitizeMethods
 - CheckSelectTag
 - CheckSelectVulnerability
 - CheckSend
 - CheckSendFile
 - CheckSessionManipulation
 - CheckSessionSettings
 - CheckSimpleFormat
 - CheckSingleQuotes
 - CheckSkipBeforeFilter
 - CheckSQL
 - CheckSQLCVEs
 - CheckSSLVerify
 - CheckStripTags
 - CheckSymbolDoSCVE
 - CheckTranslateBug
 - CheckUnsafeReflection
 - CheckValidationRegex
 - CheckWithoutProtection
 - CheckXMLDoS
 - CheckYAMLParsing
Checks finished, collecting results...
Generating report...
Report saved in 'brakeman.html'
➜ 062-security-and-static-code-analyzers git:(master) ✗
```

Brakeman Report

file:///Users/kobaltz/OneDrive/Drifting%20Ruby/Rails/062-security-and-static-code-analyzers/brakeman.html

Brakeman Report

Application Path	Rails Version	Brakeman Version	Report Time	Checks Performed
/Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-analyzers	5.0.0	3.4.1	2017-01-08 20:12:54 -0500 0.212439 seconds	BasicAuth, BasicAuthTimingAttack, ContentTag, CreateWith, CrossSiteScripting, DefaultRoutes, Deserialize, DetailedExceptions, DigestDoS, DynamicFinders, EscapeFunction, Evaluation, Execute, FileAccess, FileDisclosure, FilterSkipping, ForgerySetting, HeaderDoS, I18nXSS, JRubyXML, JSONEncoding, JSONParsing, LinkTo, LinkToHref, MailTo, MassAssignment, MimeTypeDoS, ModelAttrAccessible, ModelAttributes, ModelSerialize, NestedAttributes, NestedAttributesBypass, NumberToCurrency, QuoteTableName, Redirect, RegexDoS, Render, RenderDoS, RenderInline, ResponseSplitting, RouteDoS, SQL, SQLCVEs, SSLVerify, SafeBufferManipulation, SanitizeMethods, SelectTag, SelectVulnerability, Send, SendFile, SessionManipulation, SessionSettings, SimpleFormat, SingleQuotes, SkipBeforeFilter, StripTags, SymbolDoSCVE, TranslateBug, UnsafeReflection, ValidationRegex, WithoutProtection, XMLDoS, YAMLParsing

Summary

Scanned/Reported	Total
Controllers	3

/Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-analyzers	5.0.0	3.4.1	20:12:54 -0500 0.212439 seconds	NestedAttributes, NestedAttributesBypass, NumberToCurrency, QuoteTableName, Redirect, RegexDoS, Render, RenderDoS, RenderInline, ResponseSplitting, RouteDoS, SQL, SQLCVEs, SSLVerify, SafeBufferManipulation, SanitizeMethods, SelectTag, SelectVulnerability, Send, SendFile, SessionManipulation, SessionSettings, SimpleFormat, SingleQuotes, SkipBeforeFilter, StripTags, SymbolDoSCVE, TranslateBug, UnsafeReflection, ValidationRegex, WithoutProtection, XMLDoS, YAMLParsing

Summary

Scanned/Reported	Total
Controllers	3
Errors	0
Ignored Warnings	0
Models	2
Security Warnings	3 (2)
Templates	11

Warning Type	Total
Cross Site Scripting	1
Mass Assignment	1
SQL Injection	1

Scanned/Reported	Total
Controllers	3
Errors	0
Ignored Warnings	0
Models	2
Security Warnings	3 (2)
Templates	11

Warning Type	Total
Cross Site Scripting	1
Mass Assignment	1
SQL Injection	1

Security Warnings

Confidence	Class	Method	Warning Type	Message
High	UsersController	set_user	SQL Injection	Possible SQL injection near line 68: User.where("ID = #{params[:id]}")
High			Cross Site Scripting	Rails 5.0.0 content_tag does not escape double quotes in attribute values (CVE-2016-6316). Upgrade to...
Medium	UsersController	user_params	Mass Assignment	Parameters should be whitelisted for mass assignment near line 74: params.require(:user).permit!

Warning Type	Total
Cross Site Scripting	1
Mass Assignment	1
SQL Injection	1

Security Warnings

Confidence	Class	Method	Warning Type	Message
High	UsersController	set_user	SQL Injection	Possible SQL injection near line 68: User.where("ID = #{params[:id app/controllers/users_controller.rb 64 private 65 # Use callbacks to share common setup or constraints betw 66 def set_user 67 # @user = User.find(params[:id]) 68 @user = User.where("ID = #{params[:id]}").first 69 end 71 # Never trust parameters from the scary internet, only a 72 def user_params 73 # params.require(:user).permit(:first_name, :last_name
High			Cross Site Scripting	Rails 5.0.0 content_tag does not escape double quotes in attribute Upgrade to...
Medium	UsersController	user_params	Mass Assignment	Parameters should be whitelisted for mass assignment near line 74: params.require(:user).permit!

High	UsersController	set_user	SQL Injection	app/controllers/users_controller.rb

```
64    private
65      # Use callbacks to share common setup or constraints betv
66      def set_user
67        # @user = User.find(params[:id])
68        @user = User.where("ID = #{params[:id]}").first
69      end
71      # Never trust parameters from the scary internet, only al
72      def user_params
73        # params.require(:user).permit(:first_name, :last_name,
```

High			Cross Site Scripting	Rails 5.0.0 content_tag does not escape double quotes in attribute
Upgrade to 5.0.0 near line 97

Gemfile.lock

```
92        mini_portile2 (~> 2.1.0)
93      puma (3.6.2)
94      rack (2.0.1)
95      rack-test (0.6.3)
96        rack (>= 1.0)
97      rails (5.0.0)
98        actioncable (= 5.0.0)
99        actionmailer (= 5.0.0)
100       actionpack (= 5.0.0)
101       actionview (= 5.0.0)
102       activejob (= 5.0.0)
```

Medium	UsersController	user_params	Mass Assignment	Parameters should be whitelisted for mass assignment near line 74:
params.require(:user).permit!

Scanned/Reported	Total
Controllers	3
Errors	0
Ignored Warnings	0
Models	2
Security Warnings	3 (2)
Templates	11

Warning Type	Total
Cross Site Scripting	1
Mass Assignment	1
SQL Injection	1

Security Warnings

Confidence	Class	Method	Warning Type	Message
High	UsersController	set_user	SQL Injection	Possible SQL injection near line 68: User.where("ID = #{params[:id]}")
High			Cross Site Scripting	Rails 5.0.0 content_tag does not escape double quotes in attribute values (CVE-2016-6316). Upgrade to...
Medium	UsersController	user_params	Mass Assignment	Parameters should be whitelisted for mass assignment near line 74: params.require(:user).permit!

unpleasant outcomes.

Brakeman focuses on ActiveRecord methods dealing with building SQL statements.

A basic (Rails 2.x) example looks like this:

```
User.first(:conditions => "username = '#{params[:username]}'")
```

Brakeman would produce a warning like this:

```
Possible SQL injection near line 30: User.first(:conditions => ("username = '#{params
```

The safe way to do this query is to use a parameterized query:

```
User.first(:conditions => ["username = ?", params[:username]])
```

Brakeman also understands the new Rails 3.x way of doing things (and local variables and concatentation):

Code Updates

Merge pull request #981 from presidentbeef/add_check_name_to_reports

Add check name to text and JSON reports

Recent Posts

Brakeman 3.4.1 Released

Brakeman 3.4.0 Released

Brakeman 3.3.4/3.3.5 Released

Brakeman 3.3.3 Released

Brakeman 3.3.2 Released

Latest Tweets

Tweets by @brakeman

Brakeman Scanner Retweeted

```
➜  062-security-and-static-code-analyzers git:(master) ✗ gem install bundler-audit
Successfully installed bundler-audit-0.5.0
1 gem installed
➜  062-security-and-static-code-analyzers git:(master) ✗
```

```
➜  062-security-and-static-code-analyzers git:(master) ✗ gem install bundler-audit
Successfully installed bundler-audit-0.5.0
1 gem installed
➜  062-security-and-static-code-analyzers git:(master) ✗ bundle-audit
```

```
➜ 062-security-and-static-code-analyzers git:(master) ✗ gem install bundler-audit
Successfully installed bundler-audit-0.5.0
1 gem installed
➜ 062-security-and-static-code-analyzers git:(master) ✗ bundle-audit
Name: actionview
Version: 5.0.0
Advisory: CVE-2016-6316
Criticality: Unknown
URL: https://groups.google.com/forum/#!topic/rubyonrails-security/I-VWr034ouk
Title: Possible XSS Vulnerability in Action View
Solution: upgrade to ~> 3.2.22.3, ~> 4.2.7.1, >= 5.0.0.1

Vulnerabilities found!
➜ 062-security-and-static-code-analyzers git:(master) ✗
```

```
➜ 062-security-and-static-code-analyzers git:(master) ✗ gem install bundler-audit
Successfully installed bundler-audit-0.5.0
1 gem installed
➜ 062-security-and-static-code-analyzers git:(master) ✗ bundle-audit
Name: actionview
Version: 5.0.0
Advisory: CVE-2016-6316
Criticality: Unknown
URL: https://groups.google.com/forum/#!topic/rubyonrails-security/I-VWr034ouk
Title: Possible XSS Vulnerability in Action View
Solution: upgrade to ~> 3.2.22.3, ~> 4.2.7.1, >= 5.0.0.1

Vulnerabilities found!
➜ 062-security-and-static-code-analyzers git:(master) ✗
```

Gemfile | users_controller.rb

```
1  source 'https://rubygems.org'
2  gem 'rails', '5.0.0.1'
3  gem 'sqlite3'
4  gem 'puma', '~> 3.0'
5  gem 'sass-rails', '~> 5.0'
6  gem 'uglifier', '>= 1.3.0'
7  gem 'coffee-rails', '~> 4.1.0'
8  gem 'jquery-rails'
9  gem 'turbolinks', '~> 5.x'
10 gem 'jbuilder', '~> 2.0'
11 group :development, :test do
12   gem 'byebug', platform: :mri
13 end
14
15 group :development do
16   gem 'web-console'
17   gem 'listen', '~> 3.0.5'
18   gem 'spring'
19   gem 'spring-watcher-listen', '~> 2.0.0'
20   gem 'better_errors'
21   gem 'rails_layout'
22 end
23
24 gem 'tzinfo-data', platforms: [:mingw, :mswin, :x64_mingw, :jruby]
25
26 gem 'bootstrap-sass'
27 gem 'simple_form'
28
```

```
➜ 062-security-and-static-code-analyzers git:(master) ✗ gem install bundler-audit
Successfully installed bundler-audit-0.5.0
1 gem installed
➜ 062-security-and-static-code-analyzers git:(master) ✗ bundle-audit
Name: actionview
Version: 5.0.0
Advisory: CVE-2016-6316
Criticality: Unknown
URL: https://groups.google.com/forum/#!topic/rubyonrails-security/I-VWr034ouk
Title: Possible XSS Vulnerability in Action View
Solution: upgrade to ~> 3.2.22.3, ~> 4.2.7.1, >= 5.0.0.1

Vulnerabilities found!
➜ 062-security-and-static-code-analyzers git:(master) ✗ bundle update rails
```

```
Using nokogiri 1.7.0.1
Using rack-test 0.6.3
Using sprockets 3.7.1
Using websocket-driver 0.6.4
Using mime-types 3.1
Using autoprefixer-rails 6.6.1
Using uglifier 3.0.4
Using better_errors 2.1.1
Using coffee-script 2.4.1
Using rb-inotify 0.9.7
Using turbolinks 5.0.1
Using activesupport 5.0.0.1 (was 5.0.0)
Using loofah 2.0.3
Using mail 2.6.4
Using bootstrap-sass 3.3.7
Using listen 3.0.8
Using rails-dom-testing 2.0.2
Using globalid 0.3.7
Using activemodel 5.0.0.1 (was 5.0.0)
Using jbuilder 2.6.1
Using spring 2.0.0
Using rails-html-sanitizer 1.0.3
Installing activejob 5.0.0.1 (was 5.0.0)
Installing activerecord 5.0.0.1 (was 5.0.0)
Using spring-watcher-listen 2.0.1
Using actionview 5.0.0.1 (was 5.0.0)
Using actionpack 5.0.0.1 (was 5.0.0)
Installing actioncable 5.0.0.1 (was 5.0.0)
Installing actionmailer 5.0.0.1 (was 5.0.0)
Installing railties 5.0.0.1 (was 5.0.0)
Using sprockets-rails 3.2.0
Using simple_form 3.4.0
Using coffee-rails 4.1.1
Using jquery-rails 4.2.2
Using web-console 3.4.0
Installing rails 5.0.0.1 (was 5.0.0)
Using sass-rails 5.0.6
Bundle updated!
➜  062-security-and-static-code-analyzers git:(master) ✗
```

```
Using nokogiri 1.7.0.1
Using rack-test 0.6.3
Using sprockets 3.7.1
Using websocket-driver 0.6.4
Using mime-types 3.1
Using autoprefixer-rails 6.6.1
Using uglifier 3.0.4
Using better_errors 2.1.1
Using coffee-script 2.4.1
Using rb-inotify 0.9.7
Using turbolinks 5.0.1
Using activesupport 5.0.0.1 (was 5.0.0)
Using loofah 2.0.3
Using mail 2.6.4
Using bootstrap-sass 3.3.7
Using listen 3.0.8
Using rails-dom-testing 2.0.2
Using globalid 0.3.7
Using activemodel 5.0.0.1 (was 5.0.0)
Using jbuilder 2.6.1
Using spring 2.0.0
Using rails-html-sanitizer 1.0.3
Installing activejob 5.0.0.1 (was 5.0.0)
Installing activerecord 5.0.0.1 (was 5.0.0)
Using spring-watcher-listen 2.0.1
Using actionview 5.0.0.1 (was 5.0.0)
Using actionpack 5.0.0.1 (was 5.0.0)
Installing actioncable 5.0.0.1 (was 5.0.0)
Installing actionmailer 5.0.0.1 (was 5.0.0)
Installing railties 5.0.0.1 (was 5.0.0)
Using sprockets-rails 3.2.0
Using simple_form 3.4.0
Using coffee-rails 4.1.1
Using jquery-rails 4.2.2
Using web-console 3.4.0
Installing rails 5.0.0.1 (was 5.0.0)
Using sass-rails 5.0.6
Bundle updated!
➜  062-security-and-static-code-analyzers git:(master) ✗
```

```
Using rack-test 0.6.3
Using sprockets 3.7.1
Using websocket-driver 0.6.4
Using mime-types 3.1
Using autoprefixer-rails 6.6.1
Using uglifier 3.0.4
Using better_errors 2.1.1
Using coffee-script 2.4.1
Using rb-inotify 0.9.7
Using turbolinks 5.0.1
Using activesupport 5.0.0.1 (was 5.0.0)
Using loofah 2.0.3
Using mail 2.6.4
Using bootstrap-sass 3.3.7
Using listen 3.0.8
Using rails-dom-testing 2.0.2
Using globalid 0.3.7
Using activemodel 5.0.0.1 (was 5.0.0)
Using jbuilder 2.6.1
Using spring 2.0.0
Using rails-html-sanitizer 1.0.3
Installing activejob 5.0.0.1 (was 5.0.0)
Installing activerecord 5.0.0.1 (was 5.0.0)
Using spring-watcher-listen 2.0.1
Using actionview 5.0.0.1 (was 5.0.0)
Using actionpack 5.0.0.1 (was 5.0.0)
Installing actioncable 5.0.0.1 (was 5.0.0)
Installing actionmailer 5.0.0.1 (was 5.0.0)
Installing railties 5.0.0.1 (was 5.0.0)
Using sprockets-rails 3.2.0
Using simple_form 3.4.0
Using coffee-rails 4.1.1
Using jquery-rails 4.2.2
Using web-console 3.4.0
Installing rails 5.0.0.1 (was 5.0.0)
Using sass-rails 5.0.6
Bundle updated!
➜  062-security-and-static-code-analyzers git:(master) ✗ bundle-audit
```

```
Using sprockets 3.7.1
Using websocket-driver 0.6.4
Using mime-types 3.1
Using autoprefixer-rails 6.6.1
Using uglifier 3.0.4
Using better_errors 2.1.1
Using coffee-script 2.4.1
Using rb-inotify 0.9.7
Using turbolinks 5.0.1
Using activesupport 5.0.0.1 (was 5.0.0)
Using loofah 2.0.3
Using mail 2.6.4
Using bootstrap-sass 3.3.7
Using listen 3.0.8
Using rails-dom-testing 2.0.2
Using globalid 0.3.7
Using activemodel 5.0.0.1 (was 5.0.0)
Using jbuilder 2.6.1
Using spring 2.0.0
Using rails-html-sanitizer 1.0.3
Installing activejob 5.0.0.1 (was 5.0.0)
Installing activerecord 5.0.0.1 (was 5.0.0)
Using spring-watcher-listen 2.0.1
Using actionview 5.0.0.1 (was 5.0.0)
Using actionpack 5.0.0.1 (was 5.0.0)
Installing actioncable 5.0.0.1 (was 5.0.0)
Installing actionmailer 5.0.0.1 (was 5.0.0)
Installing railties 5.0.0.1 (was 5.0.0)
Using sprockets-rails 3.2.0
Using simple_form 3.4.0
Using coffee-rails 4.1.1
Using jquery-rails 4.2.2
Using web-console 3.4.0
Installing rails 5.0.0.1 (was 5.0.0)
Using sass-rails 5.0.6
Bundle updated!
➜  062-security-and-static-code-analyzers git:(master) ✗ bundle-audit
No vulnerabilities found
➜  062-security-and-static-code-analyzers git:(master) ✗
```

```
Using mime-types 3.1
Using autoprefixer-rails 6.6.1
Using uglifier 3.0.4
Using better_errors 2.1.1
Using coffee-script 2.4.1
Using rb-inotify 0.9.7
Using turbolinks 5.0.1
Using activesupport 5.0.0.1 (was 5.0.0)
Using loofah 2.0.3
Using mail 2.6.4
Using bootstrap-sass 3.3.7
Using listen 3.0.8
Using rails-dom-testing 2.0.2
Using globalid 0.3.7
Using activemodel 5.0.0.1 (was 5.0.0)
Using jbuilder 2.6.1
Using spring 2.0.0
Using rails-html-sanitizer 1.0.3
Installing activejob 5.0.0.1 (was 5.0.0)
Installing activerecord 5.0.0.1 (was 5.0.0)
Using spring-watcher-listen 2.0.1
Using actionview 5.0.0.1 (was 5.0.0)
Using actionpack 5.0.0.1 (was 5.0.0)
Installing actioncable 5.0.0.1 (was 5.0.0)
Installing actionmailer 5.0.0.1 (was 5.0.0)
Installing railties 5.0.0.1 (was 5.0.0)
Using sprockets-rails 3.2.0
Using simple_form 3.4.0
Using coffee-rails 4.1.1
Using jquery-rails 4.2.2
Using web-console 3.4.0
Installing rails 5.0.0.1 (was 5.0.0)
Using sass-rails 5.0.6
Bundle updated!
➜ 062-security-and-static-code-analyzers git:(master) ✗ bundle-audit
No vulnerabilities found
➜ 062-security-and-static-code-analyzers git:(master) ✗ brakeman -o brakeman.html
Loading scanner...
```

Summary

Scanned/Reported	Total
Controllers	3
Errors	0
Ignored Warnings	0
Models	2
Security Warnings	2 (1)
Templates	11

Warning Type	Total
Mass Assignment	1
SQL Injection	1

Security Warnings

Confidence	Class	Method	Warning Type	Message
High	UsersController	set_user	SQL Injection	Possible SQL injection near line 68: User.where("ID = #{params[:id]}")
Medium	UsersController	user_params	Mass Assignment	Parameters should be whitelisted for mass assignment near line 74: params.require(:user).permit!

Security Warnings	2 (1)
Templates	11

Warning Type	Total
Mass Assignment	1
SQL Injection	1

Security Warnings

Confidence	Class	Method	Warning Type	Message
High	UsersController	set_user	SQL Injection	Possible SQL injection near line 68: User.where("ID = #{params[:id app/controllers/users_controller.rb 64 private 65 # Use callbacks to share common setup or constraints betw 66 def set_user 67 # @user = User.find(params[:id]) 68 @user = User.where("ID = #{params[:id]}").first 69 end 71 # Never trust parameters from the scary internet, only al 72 def user_params 73 # params.require(:user).permit(:first_name, :last_name,
Medium	UsersController	user_params	Mass Assignment	Parameters should be whitelisted for mass assignment near line 74: params.require(:user).permit!

Security Warnings

Confidence	Class	Method	Warning Type	Message
High	UsersController	set_user	SQL Injection	Possible SQL injection near line 68: User.where("ID = #{params[:id]}").first app/controllers/users_controller.rb 64 private 65 # Use callbacks to share common setup or constraints betw 66 def set_user 67 # @user = User.find(params[:id]) 68 @user = User.where("ID = #{params[:id]}").first 69 end 71 # Never trust parameters from the scary internet, only a 72 def user_params 73 # params.require(:user).permit(:first_name, :last_name
Medium	UsersController	user_params	Mass Assignment	Parameters should be whitelisted for mass assignment near line 74 params.require(:user).permit! app/controllers/users_controller.rb 69 end 71 # Never trust parameters from the scary internet, only a 72 def user_params 73 # params.require(:user).permit(:first_name, :last_name 74 params.require(:user).permit! 75 end 76 end

```
➜  062-security-and-static-code-analyzers git:(master) ✗ gem install guard guard-brakeman
```

```
➜  062-security-and-static-code-analyzers git:(master) ✗ gem install guard guard-brakeman
Successfully installed guard-2.14.0
Successfully installed guard-brakeman-0.8.3
2 gems installed
➜  062-security-and-static-code-analyzers git:(master) ✗
```

```
➜ 062-security-and-static-code-analyzers git:(master) ✗ gem install guard guard-brakeman
Successfully installed guard-2.14.0
Successfully installed guard-brakeman-0.8.3
2 gems installed
➜ 062-security-and-static-code-analyzers git:(master) ✗ guard init
Warning: you have a Gemfile, but you're not using bundler or RUBYGEMS_GEMDEPS
Expected string default value for '--listen-on'; got false (boolean)
20:30:38 - INFO - Writing new Guardfile to /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-analyzers/Guardfile
20:30:39 - INFO - brakeman guard added to Guardfile, feel free to edit it
➜ 062-security-and-static-code-analyzers git:(master) ✗
```

```
➜ 062-security-and-static-code-analyzers git:(master) ✗ gem install guard guard-brakeman
Successfully installed guard-2.14.0
Successfully installed guard-brakeman-0.8.3
2 gems installed
➜ 062-security-and-static-code-analyzers git:(master) ✗ guard init
Warning: you have a Gemfile, but you're not using bundler or RUBYGEMS_GEMDEPS
Expected string default value for '--listen-on'; got false (boolean)
20:30:38 - INFO - Writing new Guardfile to /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-analyzers/Guardfile
20:30:39 - INFO - brakeman guard added to Guardfile, feel free to edit it
➜ 062-security-and-static-code-analyzers git:(master) ✗ vi Gua
```

```
# A sample Guardfile
# More info at https://github.com/guard/guard#readme

## Uncomment and set this to only include directories you want to watch
# directories %w(app lib config test spec features) \
#  .select{|d| Dir.exists?(d) ? d : UI.warning("Directory #{d} does not exist")}

## Note: if you are using the `directories` clause above and you are not
## watching the project directory ('.'), then you will want to move
## the Guardfile to a watched dir and symlink it back, e.g.
#
#  $ mkdir config
#  $ mv Guardfile config/
#  $ ln -s config/Guardfile .
#
# and, you'll have to watch "config/Guardfile" instead of "Guardfile"

guard 'brakeman', :run_on_start => true do
  watch(%r{^app/.+\.(erb|haml|rhtml|rb)$})
  watch(%r{^config/.+\.rb$})
  watch(%r{^lib/.+\.rb$})
  watch('Gemfile')
end
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"Guardfile" 23L, 797C
```

```
# A sample Guardfile
# More info at https://github.com/guard/guard#readme

## Uncomment and set this to only include directories you want to watch
# directories %w(app lib config test spec features) \
#  .select{|d| Dir.exists?(d) ? d : UI.warning("Directory #{d} does not exist")}

## Note: if you are using the `directories` clause above and you are not
## watching the project directory ('.'), then you will want to move
## the Guardfile to a watched dir and symlink it back, e.g.
#
#  $ mkdir config
#  $ mv Guardfile config/
#  $ ln -s config/Guardfile .
#
# and, you'll have to watch "config/Guardfile" instead of "Guardfile"

guard 'brakeman', :run_on_start => true do
  watch(%r{^app/.+\.(erb|haml|rhtml|rb)$})
  watch(%r{^config/.+\.rb$})
  watch(%r{^lib/.+\.rb$})
  watch('Gemfile')
end
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"Guardfile" 23L, 797C
```

```
➜ 062-security-and-static-code-analyzers git:(master) ✗ gem install guard guard-brakeman
Successfully installed guard-2.14.0
Successfully installed guard-brakeman-0.8.3
2 gems installed
➜ 062-security-and-static-code-analyzers git:(master) ✗ guard init
Warning: you have a Gemfile, but you're not using bundler or RUBYGEMS_GEMDEPS
Expected string default value for '--listen-on'; got false (boolean)
20:30:38 - INFO - Writing new Guardfile to /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-analyzers/Guardfile
20:30:39 - INFO - brakeman guard added to Guardfile, feel free to edit it
➜ 062-security-and-static-code-analyzers git:(master) ✗ vi Guardfile
➜ 062-security-and-static-code-analyzers git:(master) ✗ guard
```

```
 - CheckRegexDoS
 - CheckRender
 - CheckRenderDoS
 - CheckRenderInline
 - CheckResponseSplitting
 - CheckRouteDoS
 - CheckSafeBufferManipulation
 - CheckSanitizeMethods
 - CheckSelectTag
 - CheckSelectVulnerability
 - CheckSend
 - CheckSendFile
 - CheckSessionManipulation
 - CheckSessionSettings
 - CheckSimpleFormat
 - CheckSingleQuotes
 - CheckSkipBeforeFilter
 - CheckSQL
 - CheckSQLCVEs
 - CheckSSLVerify
 - CheckStripTags
 - CheckSymbolDoSCVE
 - CheckTranslateBug
 - CheckUnsafeReflection
 - CheckValidationRegex
 - CheckWithoutProtection
 - CheckXMLDoS
 - CheckYAMLParsing
Checks finished, collecting results...
20:31:54 - INFO -
> [#6bc124893672] ------ brakeman warnings --------
> [#6bc124893672]
20:31:54 - INFO - 2 brakeman findings
20:31:54 - INFO - High - SQL Injection - Possible SQL injection near line 68 in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-anal
yzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}")
20:31:54 - INFO - Medium - Mass Assignment - Parameters should be whitelisted for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Rails
/062-security-and-static-code-analyzers/app/controllers/users_controllerrb: params.require(:user).permit!
20:31:54 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-analyzers'
[1] guard(main)>
```

```
# A sample Guardfile
# More info at https://github.com/guard/guard#readme

## Uncomment and set this to only include directories you want to watch
# directories %w(app lib config test spec features) \
#  .select{|d| Dir.exists?(d) ? d : UI.warning("Directory #{d} does not exist")}

## Note: if you are using the `directories` clause above and you are not
## watching the project directory ('.'), then you will want to move
## the Guardfile to a watched dir and symlink it back, e.g.
#
#  $ mkdir config
#  $ mv Guardfile config/
#  $ ln -s config/Guardfile .
#
# and, you'll have to watch "config/Guardfile" instead of "Guardfile"

guard 'brakeman', run_on_start: true, quiet: true do
  watch(%r{^app/.+\.(erb|haml|rhtml|rb)$})
  watch(%r{^config/.+\.rb$})
  watch(%r{^lib/.+\.rb$})
  watch('Gemfile')
end

```

2. guard (zsh)

```
 - CheckSSLVerify
 - CheckStripTags
 - CheckSymbolDoSCVE
 - CheckTranslateBug
 - CheckUnsafeReflection
 - CheckValidationRegex
 - CheckWithoutProtection
 - CheckXMLDoS
 - CheckYAMLParsing
Checks finished, collecting results...
20:31:54 - INFO -
> [#6bc124893672] ------ brakeman warnings --------
> [#6bc124893672]
20:31:54 - INFO - 2 brakeman findings
20:31:54 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:31:54 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:31:54 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
[1] guard(main)> quit

20:32:06 - INFO - Bye bye...
➜  062-security-and-static-code-analyzers git:(master) ✗ guard
Warning: you have a Gemfile, but you're not using bundler or RUBYGEMS_GEMDEPS
Expected string default value for '--listen-on'; got false (boolean)
20:32:52 - INFO - Guard here! It looks like your project has a Gemfile, yet y
ou are running
> [#] `guard` outside of Bundler. If this is your intent, feel free to ignore
 this
> [#] message. Otherwise, consider using `bundle exec guard` to ensure your
> [#] dependencies are loaded correctly.
> [#] (You can run `guard` with --no-bundler-warning to get rid of this messa
ge.)
```

Guardfile — 062-security-and-static-code-analyzers

FOLDERS

- 062-security-and-stat
  - app
    - assets
    - channels
    - controllers
      - concerns
      - application_con
      - users_controller
      - visitors_controll
    - helpers
    - jobs
    - mailers
    - models
    - views
  - bin
  - config
  - db
  - lib
  - log
  - public
  - test
  - tmp
  - vendor
  - .gitignore
  - brakeman.html
  - config.ru
  - Gemfile
  - Gemfile.lock
  - Guardfile
  - Rakefile
  - README.md

Gemfile | Guardfile | users_controller.rb

```
1  # A sample Guardfile
2  # More info at https://github.com/guard/guard#
3
4  ## Uncomment and set this to only include dire
5  # directories %w(app lib config test spec feat
6  #  .select{|d| Dir.exists?(d) ? d : UI.warning
7
8  ## Note: if you are using the `directories` cl
9  ## watching the project directory ('.'), then
10 ## the Guardfile to a watched dir and symlink
11 #
12 #  $ mkdir config
13 #  $ mv Guardfile config/
14 #  $ ln -s config/Guardfile .
15 #
16 # and, you'll have to watch "config/Guardfile"
17
18 guard 'brakeman', run_on_start: true, quiet: t
19   watch(%r{^app/.+\.(erb|haml|rhtml|rb)$})
20   watch(%r{^config/.+\.rb$})
21   watch(%r{^lib/.+\.rb$})
22   watch('Gemfile')
23 end
24
```

Line 18, Column 50 | Spaces: 2 | Ruby

```
2. guard (fsevent_watch)
20:31:54 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:31:54 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:31:54 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
[1] guard(main)> quit

20:32:06 - INFO - Bye bye...
➜ 062-security-and-static-code-analyzers git:(master) ✗ guard
Warning: you have a Gemfile, but you're not using bundler or RUBYGEMS_GEMDEPS
Expected string default value for '--listen-on'; got false (boolean)
20:32:52 - INFO - Guard here! It looks like your project has a Gemfile, yet y
ou are running
> [#] `guard` outside of Bundler. If this is your intent, feel free to ignore
 this
> [#] message. Otherwise, consider using `bundle exec guard` to ensure your
> [#] dependencies are loaded correctly.
> [#] (You can run `guard` with --no-bundler-warning to get rid of this messa
ge.)
20:32:53 - INFO - rocessed
> [#fbc8b2fa513c] ------ brakeman warnings --------
> [#fbc8b2fa513c]
20:32:53 - INFO - 2 brakeman findings
20:32:53 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:32:53 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:32:53 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
[1] guard(main)>
```

Guardfile — 062-security-and-static-code-analyzers

FOLDERS

- 062-security-and-stat
  - app
    - assets
    - channels
    - controllers
      - concerns
      - application_con
      - users_controller
      - visitors_controll
    - helpers
    - jobs
    - mailers
    - models
    - views
  - bin
  - config
  - db
  - lib
  - log
  - public
  - test
  - tmp
  - vendor
  - .gitignore
  - brakeman.html
  - config.ru
  - Gemfile
  - Gemfile.lock
  - Guardfile
  - Rakefile
  - README.md

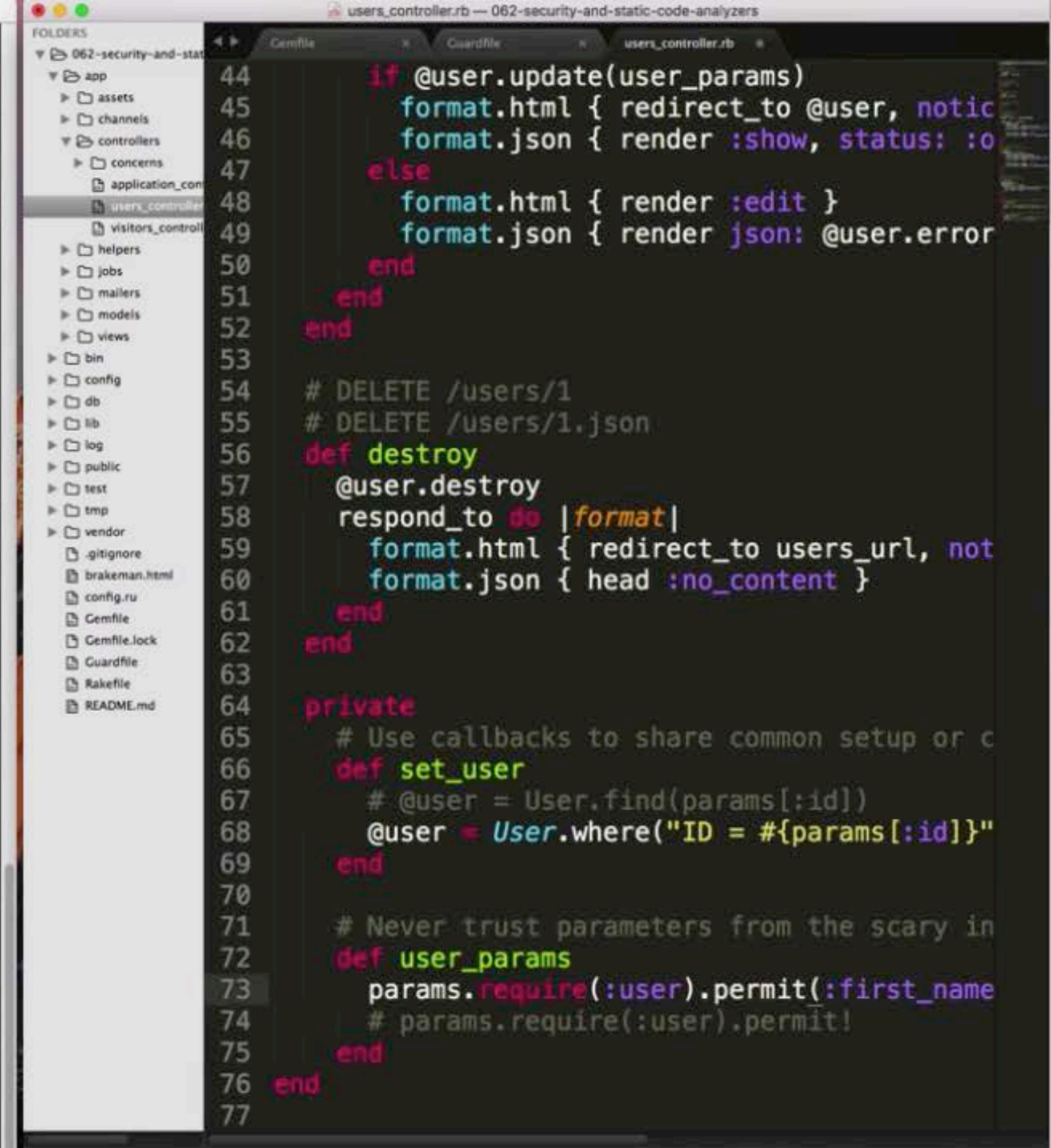
Gemfile | Guardfile | users_controller.rb

```
1  # A sample Guardfile
2  # More info at https://github.com/guard/guard#
3
4  ## Uncomment and set this to only include dire
5  # directories %w(app lib config test spec feat
6  #  .select{|d| Dir.exists?(d) ? d : UI.warning
7
8  ## Note: if you are using the `directories` cl
9  ## watching the project directory ('.'), then
10 ## the Guardfile to a watched dir and symlink
11 #
12 #  $ mkdir config
13 #  $ mv Guardfile config/
14 #  $ ln -s config/Guardfile .
15 #
16 # and, you'll have to watch "config/Guardfile"
17
18 guard 'brakeman', run_on_start: true, quiet: t
19   watch(%r{^app/.+\.(erb|haml|rhtml|rb)$})
20   watch(%r{^config/.+\.rb$})
21   watch(%r{^lib/.+\.rb$})
22   watch('Gemfile')
23 end
24
```

Line 18, Column 50 | Spaces: 2 | Ruby

```
20:31:54 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:31:54 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:31:54 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
[1] guard(main)> quit

20:32:06 - INFO - Bye bye...
➜ 062-security-and-static-code-analyzers git:(master) ✗ guard
Warning: you have a Gemfile, but you're not using bundler or RUBYGEMS_GEMDEPS
Expected string default value for '--listen-on'; got false (boolean)
20:32:52 - INFO - Guard here! It looks like your project has a Gemfile, yet y
ou are running
> [#] `guard` outside of Bundler. If this is your intent, feel free to ignore
 this
> [#] message. Otherwise, consider using `bundle exec guard` to ensure your
> [#] dependencies are loaded correctly.
> [#] (You can run `guard` with --no-bundler-warning to get rid of this messa
ge.)
20:32:53 - INFO - rocessed
> [#fbc8b2fa513c] ------ brakeman warnings --------
> [#fbc8b2fa513c]
20:32:53 - INFO - 2 brakeman findings
20:32:53 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:32:53 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:32:53 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
[1] guard(main)>
```



```
20:31:54 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:31:54 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:31:54 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
[1] guard(main)> quit

20:32:06 - INFO - Bye bye...
➜  062-security-and-static-code-analyzers git:(master) ✗ guard
Warning: you have a Gemfile, but you're not using bundler or RUBYGEMS_GEMDEPS
Expected string default value for '--listen-on'; got false (boolean)
20:32:52 - INFO - Guard here! It looks like your project has a Gemfile, yet y
ou are running
> [#] `guard` outside of Bundler. If this is your intent, feel free to ignore
 this
> [#] message. Otherwise, consider using `bundle exec guard` to ensure your
> [#] dependencies are loaded correctly.
> [#] (You can run `guard` with --no-bundler-warning to get rid of this messa
ge.)
20:32:53 - INFO - rocessed
> [#fbc8b2fa513c] ------ brakeman warnings --------
> [#fbc8b2fa513c]
20:32:53 - INFO - 2 brakeman findings
20:32:53 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:32:53 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:32:53 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
[1] guard(main)>
```

FOLDERS

- 062-security-and-stat
  - app
    - assets
    - channels
    - controllers
      - concerns
      - application_con
      - users_controller
      - visitors_controll
    - helpers
    - jobs
    - mailers
    - models
    - views
  - bin
  - config
  - db
  - lib
  - log
  - public
  - test
  - tmp
  - vendor
  - .gitignore
  - brakeman.html
  - config.ru
  - Gemfile
  - Gemfile.lock
  - Guardfile
  - Rakefile
  - README.md

users_controller.rb — 062-security-and-static-code-analyzers

Gemfile | Guardfile | users_controller.rb

```
44        if @user.update(user_params)
45          format.html { redirect_to @user, notic
46          format.json { render :show, status: :o
47        else
48          format.html { render :edit }
49          format.json { render json: @user.error
50        end
51      end
52    end
53
54    # DELETE /users/1
55    # DELETE /users/1.json
56    def destroy
57      @user.destroy
58      respond_to do |format|
59        format.html { redirect_to users_url, not
60        format.json { head :no_content }
61      end
62    end
63
64    private
65      # Use callbacks to share common setup or c
66      def set_user
67        # @user = User.find(params[:id])
68        @user = User.where("ID = #{params[:id]}"
69      end
70
71      # Never trust parameters from the scary in
72      def user_params
73        params.require(:user).permit(:first_name
74        # params.require(:user).permit!
75      end
76  end
77
```

Line 73, Column 36 | Spaces: 2 | Ruby

```
ou are running
> [#] `guard` outside of Bundler. If this is your intent, feel free to ignore
 this
> [#] message. Otherwise, consider using `bundle exec guard` to ensure your
> [#] dependencies are loaded correctly.
> [#] (You can run `guard` with --no-bundler-warning to get rid of this messa
ge.)
20:32:53 - INFO - rocessed
> [#fbc8b2fa513c] ------ brakeman warnings --------
> [#fbc8b2fa513c]
20:32:53 - INFO - 2 brakeman findings
20:32:53 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:32:53 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:32:53 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
20:33:13 - INFO -
> [#]
> [#] rescanning ["app/controllers/users_controller.rb"], running all checks
20:33:13 - INFO -
> [#] ------ brakeman warnings --------
> [#]
20:33:13 - INFO - 1 fixed warning
20:33:13 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:33:13 - INFO - 1 previous warning
20:33:13 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)

[1] guard(main)>
```

users_controller.rb — 062-security-and-static-code-analyzers

FOLDERS

- 062-security-and-stat
  - app
    - assets
    - channels
    - controllers
      - concerns
      - application_con
      - users_controller
      - visitors_controll
    - helpers
    - jobs
    - mailers
    - models
    - views
  - bin
  - config
  - db
  - lib
  - log
  - public
  - test
  - tmp
  - vendor
  - .gitignore
  - brakeman.html
  - config.ru
  - Gemfile
  - Gemfile.lock
  - Guardfile
  - Rakefile
  - README.md

Gemfile | Guardfile | users_controller.rb

```
44        if @user.update(user_params)
45          format.html { redirect_to @user, notic
46          format.json { render :show, status: :o
47        else
48          format.html { render :edit }
49          format.json { render json: @user.error
50        end
51      end
52    end
53
54    # DELETE /users/1
55    # DELETE /users/1.json
56    def destroy
57      @user.destroy
58      respond_to do |format|
59        format.html { redirect_to users_url, not
60        format.json { head :no_content }
61      end
62    end
63
64    private
65      # Use callbacks to share common setup or c
66      def set_user
67        # @user = User.find(params[:id])
68        @user = User.where("ID = #{params[:id]}"
69      end
70
71      # Never trust parameters from the scary in
72      def user_params
73        params.require(:user).permit(:first_name
74        # params.require(:user).permit!
75      end
76  end
77
```

Line 73, Column 36 — Spaces: 2 — Ruby

```
ou are running
> [#] `guard` outside of Bundler. If this is your intent, feel free to ignore
 this
> [#] message. Otherwise, consider using `bundle exec guard` to ensure your
> [#] dependencies are loaded correctly.
> [#] (You can run `guard` with --no-bundler-warning to get rid of this messa
ge.)
20:32:53 - INFO - rocessed
> [#fbc8b2fa513c] ------ brakeman warnings --------
> [#fbc8b2fa513c]
20:32:53 - INFO - 2 brakeman findings
20:32:53 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:32:53 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:32:53 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
20:33:13 - INFO -
> [#]
> [#] rescanning ["app/controllers/users_controller.rb"], running all checks
20:33:13 - INFO -
> [#] ------ brakeman warnings --------
> [#]
20:33:13 - INFO - 1 fixed warning
20:33:13 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:33:13 - INFO - 1 previous warning
20:33:13 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)

[1] guard(main)>
```

users_controller.rb — 062-security-and-static-code-analyzers

FOLDERS

- 062-security-and-stat
  - app
    - assets
    - channels
    - controllers
      - concerns
      - application_con
      - users_controller
      - visitors_controll
    - helpers
    - jobs
    - mailers
    - models
    - views
  - bin
  - config
  - db
  - lib
  - log
  - public
  - test
  - tmp
  - vendor
  - .gitignore
  - brakeman.html
  - config.ru
  - Gemfile
  - Gemfile.lock
  - Guardfile
  - Rakefile
  - README.md

Gemfile | Guardfile | users_controller.rb

```
44        if @user.update(user_params)
45          format.html { redirect_to @user, notic
46          format.json { render :show, status: :o
47        else
48          format.html { render :edit }
49          format.json { render json: @user.error
50        end
51      end
52    end
53
54    # DELETE /users/1
55    # DELETE /users/1.json
56    def destroy
57      @user.destroy
58      respond_to do |format|
59        format.html { redirect_to users_url, not
60        format.json { head :no_content }
61      end
62    end
63
64    private
65      # Use callbacks to share common setup or c
66      def set_user
67        # @user = User.find(params[:id])
68        @user = User.where("ID = #{params[:id]}"
69      end
70
71      # Never trust parameters from the scary in
72      def user_params
73        params.require(:user).permit(:first_name
74        # params.require(:user).permit!
75      end
76  end
77
```

31 characters selected — Spaces: 2 — Ruby

```
2. [1 Warning fixed.] 1 fixed warning, 1 previous warning (fsevent_watch)
ge.)
20:32:53 - INFO - rocessed
> [#fbc8b2fa513c] ------ brakeman warnings --------
> [#fbc8b2fa513c]
20:32:53 - INFO - 2 brakeman findings
20:32:53 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)
20:32:53 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:32:53 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
Ruby/Rails/062-security-and-static-code-analyzers'
20:33:13 - INFO -
> [#]
> [#] rescanning ["app/controllers/users_controller.rb"], running all checks
20:33:13 - INFO -
> [#] ------ brakeman warnings --------
> [#]
20:33:13 - INFO - 1 fixed warning
20:33:13 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
: params.require(:user).permit!
20:33:13 - INFO - 1 previous warning
20:33:13 - INFO - High - SQL Injection - Possible SQL injection near line 68
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
)

20:33:46 - INFO -
> [#]
> [#] rescanning ["app/controllers/users_controller.rb"], running all checks
20:33:46 - INFO -
> [#] ------ brakeman warnings --------
> [#]
[1] guard(main)>
```

users_controller.rb — 062-security-and-static-code-analyzers

FOLDERS

- 062-security-and-stat
  - app
    - assets
    - channels
    - controllers
      - concerns
      - application_con
      - users_controller
      - visitors_controll
    - helpers
    - jobs
    - mailers
    - models
    - views
  - bin
  - config
  - db
  - lib
  - log
  - public
  - test
  - tmp
  - vendor
  - .gitignore
  - brakeman.html
  - config.ru
  - Gemfile
  - Gemfile.lock
  - Guardfile
  - Rakefile
  - README.md

Gemfile | Guardfile | users_controller.rb

```
44        if @user.update(user_params)
45          format.html { redirect_to @user, notic
46          format.json { render :show, status: :o
47        else
48          format.html { render :edit }
49          format.json { render json: @user.error
50        end
51      end
52    end
53
54    # DELETE /users/1
55    # DELETE /users/1.json
56    def destroy
57      @user.destroy
58      respond_to do |format|
59        format.html { redirect_to users_url, not
60        format.json { head :no_content }
61      end
62    end
63
64    private
65      # Use callbacks to share common setup or c
66      def set_user
67        @user = User.find(params[:id])
68        # @user = User.where("ID = #{params[:id]
69      end
70
71      # Never trust parameters from the scary in
72      def user_params
73        params.require(:user).permit(:first_name
74        # params.require(:user).permit!
75      end
76  end
77
```

Line 67, Column 1; Saved ~/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-analyzers/app/controllers/users_controller.rb (UTF-8)

Spaces

Brakeman - Rails Security Scanner

Static analysis security scanner for Ruby on Rails

NOV 2ND, 2016

Brakeman 3.4.1 Released

- Configurable engines path (Jason Yeo)
- Check CSRF setting in direct subclasses of `ActionController::Base` (Jason Yeo)
- Pull Ruby version from `.ruby-version` or Gemfile
- Use Ruby version to turn off SymbolDoS check (#928)
- Fix ignoring link interpolation not at beginning of string (#939)
- Show action help at start of interactive ignore (#949)
- Avoid warning about `where_values_hash` in SQLi (#942)

Brakeman is an open source vulnerability scanner specifically designed for Ruby on Rails applications. It statically analyzes Rails application code to find security issues at any stage of development.

Brakeman Pro is the commercial version of Brakeman which offers a GUI, test integration, deeper analysis, and more.

Code Updates

Merge pull request #981 from presidentbeef/add_check_name_to_reports

Drifting Ruby

WWW.DRIFTINGRUBY.COM