

Drifting Ruby

Security and Static Code Analyzers

```
FOLDERS
♥ 🕞 062-security-and-static-code-analyzers
 A 🕒 abb
  ► 🗀 assets
  ₹ ⊜ controllers
    application_controller.rb
      nusers_controller.rb
      yisitors_controller.rb
  ► D Jobs
  ► □ models
  ► 🗀 views
 ▶ 🗀 bin
 ► □ config
 ▶ (3) db
 ► D Nb
 ► 🗀 log
 ▶ □ public
 ₽ 🗀 test
 ► □ tmp
 ▶ □ vendor
   gitignore.
   config.ru
   Cemfile.lock
   Rakefile
   README.md
```

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

🔲 Line 28, Column 1

Ruby

```
FOLDERS
♥ № 062-security-and-static-code-analyzers
 ₩ 🕞 app
   ► 🗀 assets
   ► 🗀 channels
   ₹ 😂 controllers
    ► 🗀 concerns
       application_controller.rb
       users_controller.rb
       yisitors_controller.rb

▶ □ jobs

   ► 🗀 mailers

▶ □ models
   ► 🗀 views
 ▶ 🗀 bin
 ► □ config
 Þ □ db
 ► D Nb
 ▶ 🗀 log

▶ □ public
 ▶ 🗀 test
 ► 🗀 tmp
 ► □ vendor
    gitignore.
    config.ru
    Cemfile.lock
    Rakefile
    README.md
```

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

Ruby

NOV 2ND, 2016

Brakeman 3.4.1 Released

- Configurable engines path (<u>Jason Yeo</u>)
- 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 repor

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

→ 062-security-and-static-code-analyzers git:(master) × gem install brakeman

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

- → 062-security-and-static-code-analyzers git:(master) x gem install brakeman Successfully installed brakeman-3.4.1
- 1 gem installed
- → 062-security-and-static-code-analyzers git:(master) x brakeman

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

Scanned/Reported	ï	To	ot	al	ï	
+	-+				+	
Controllers	1	3			1	
Models	1	2			1	
1 Templates	1	1	1		1	
l Errors	1	0			1	
I Security Warnings	1	3	((2)	1	
1	-4				+	
*						
4			+-			-
+			+-	Tot	tal	
+ Warning Type +			+-	To	tal	-
Warning Type	in		+-	Tot	tal	-
Cross Site Script	in		† - 		tal	+ - +
Cross Site Script	in		- 	1	tal	1 - +

| Confidence | Class

| Method

| Warning Type

+SUMMARY+

High			Rails 5.0.0 content_tag does not escape double quotes in attribute values (CVE-2016-6>>
I 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>>
+	+	-+	+>>
252			
→ 062-secu	rity-and-static-code-analyzers gi	t:(master) X	

Message

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

Scanned/Reported	То	tal	i
Controllers	3		+
	2		i
Templates	11		i
Errors	0		ĭ
		(2)	i
eccui tey maintings	_		
+			-+
+			-+
+	-+		-+ tal
+	-+	То	tal
+	-+	To	-+ tal
+	-+	To:	-+ tal
+	-+	To	tal

Confidence | Class

Method

Warning Type

+SUMMARY+

Message

0 0 0	2. kobaltz@TardisPro; -/drifting_ruby/062-security-and-static-code-analyzers (zsh)
ing, LinkTo, LinkTol NumberToCurrency, (ulation, SanitizeMe	ion, Evaluation, Execute, FileAccess, FileDisclosure, FilterSkipping, ForgerySetting, HeaderDoS, I18nXSS, JRubyXML, JSONEncoding, JSONPars Href, MailTo, MassAssignment, MimeTypeDoS, ModelAttrAccessible, ModelAttributes, ModelSerialize, NestedAttributes, NestedAttributesBypass, QuoteTableName, Redirect, RegexDoS, Render, RenderDoS, RenderInline, ResponseSplitting, RouteDoS, SQL, SQLCVEs, SSLVerify, SafeBufferManip thods, SelectTag, SelectVulnerability, Send, SendFile, SessionManipulation, SessionSettings, SimpleFormat, SingleQuotes, SkipBeforeFilter, oSCVE, TranslateBug, UnsafeReflection, ValidationRegex, WithoutProtection, XMLDoS, YAMLParsing
+SUMMARY+	
Scanned/Reported	Total
Controllers	13
Models Templates	2
1 Errors	

+SECURITY WARNINGS+

| Security Warnings | 3 (2) |

→ 062-security-and-static-code-analyzers git:(master) x 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) X

Brakeman Report

□ □ □ 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, Il8nXSS, 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

Brakeman Report ×				Dav
file:///Users/kobaltz/OneDrive/Drifting%20Ruby/Rails/062-secur	rity-and-static-code-	analyzers/brakeman.html		Q t O 2
Ruby/Rails/062-security-and- static-code-analyzers	5.0.0	3.4.1	-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

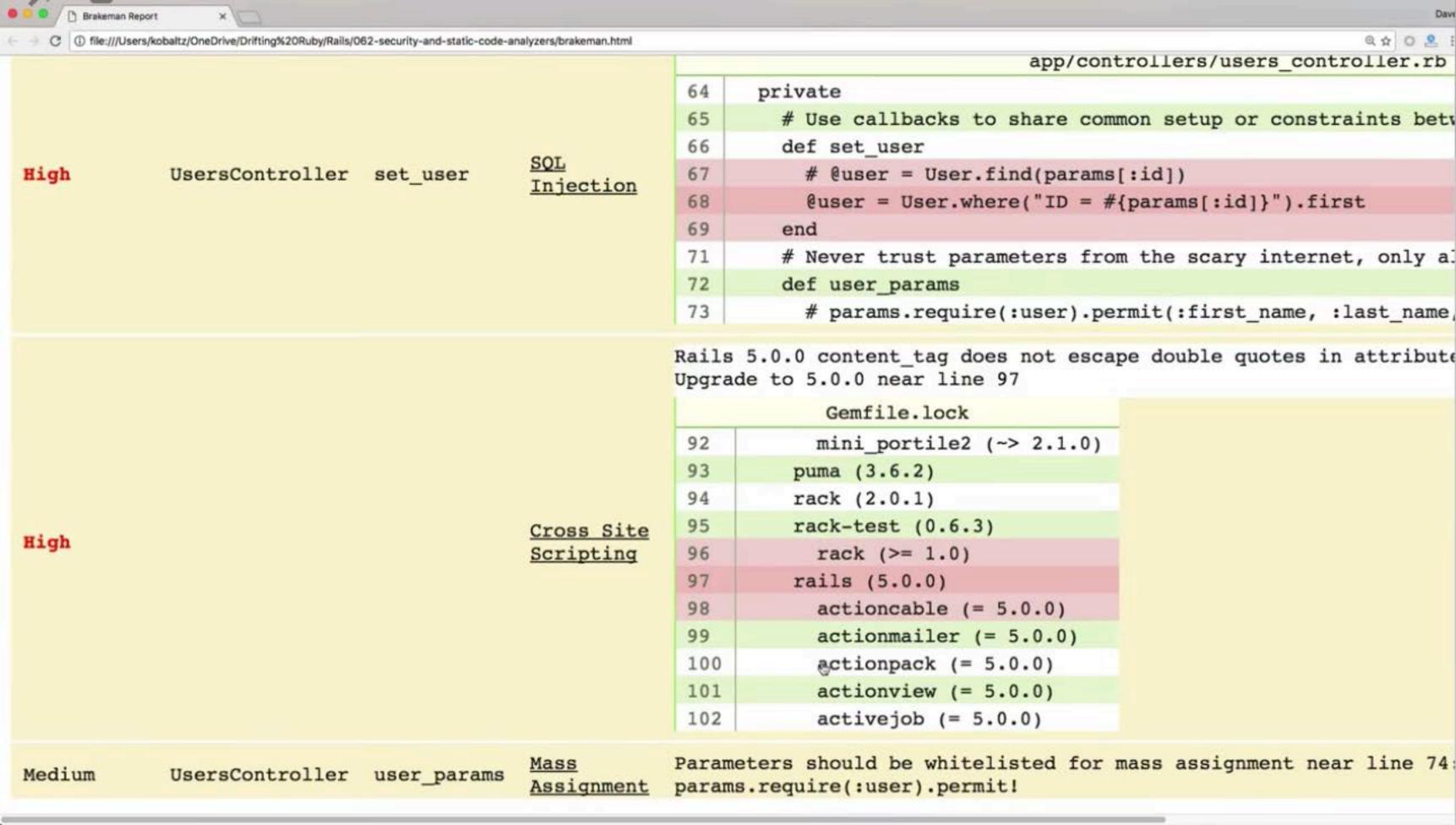
Dave

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

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

Confidence	Class	Method	warning Type	Message
			SQL Injection	Possible SQL injection near line 68: User.where("ID = #{params[:ic
				app/controllers/users_controller.rb
High				64 private
	UsersController	set_user		# Use callbacks to share common setup or constraints bety
				66 def set_user
				<pre># @user = User.find(params[:id])</pre>
				<pre>68 @user = User.where("ID = #{params[:id]}").first</pre>
				69 end
				71 # Never trust parameters from the scary internet, only a:
				72 def user_params
				# 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!



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

Confidence	Class	Method	Warning Type	Message
High	UsersController	set_user	SOL Injection	<pre>Possible SQL injection near line 68: User.where("ID = # {params[:id]}")</pre>
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!

unpreasant outcomes.

C D brakemanscanner.org/docs/warning_types/sql_injection/

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 repor ts

Add check name to text and JSON reports



Recent Posts

Brakeman 3.4.1 Released

Brakeman 3.4.0 Released

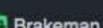
Brakeman 3.3.4/3.3.5 Released

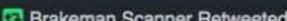
Brakeman 3.3.3 Released

Brakeman 3.3.2 Released

Latest Tweets

Tweets by @brakeman





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

- → 062-security-and-static-code-analyzers git:(master) x gem install bundler-audit Successfully installed bundler-audit-0.5.0
- 1 gem installed
- → 062-security-and-static-code-analyzers git:(master) X

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

- 1 gem installed
- → 062-security-and-static-code-analyzers git:(master) x bundle-audit

```
A 15 A
```

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

```
@ IE @
```

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

```
FOLDERS
                              Gemfile
▼ 25 062-security-and-static-code-analyzers
                              source 'https://rubygems.org'
 A 😂 abb
  ► 🗀 assets
                                    'rails', '5.0.0.1'
  'sqlite3'
  ₹ 🖰 controllers
                                    'puma', '~> 3.0'
   ► 🗀 concerns
    application_controller.rb
                                    'sass-rails', '~> 5.0'
    users_controller.rb
                                    'uglifier', '>= 1.3.0'
    yisitors_controller.rb
  'coffee-rails', '~> 4.1.0'
  ► D Jobs
                                    'jquery-rails'
  8
  ► 🗀 models
                                    'turbolinks', '~> 5.x'
                           9
  ► 🗀 views
                                    'jbuilder', '~> 2.0'
                          10
 ▶ 🗀 bin
 ► □ config
                              group :development, :test
 Þ □ db
                          12
                                       'byebug', platform: :mri
 ► (C) 16b
 ► 🗀 log
                          13
 ▶ □ public
                          14
 ▶ 🗀 test
 ► 🗀 tmp
                          15
                              group :development
 ▶ 🗀 vendor
                          16
                                       'web-console'
  3 gitignore
                                       'listen', '~> 3.0.5'
  brakeman.html
                          17
  Config.ru
                          18
                                       'spring'
                                       'spring-watcher-listen', '~> 2.0.0'
                          19
  Gemfile.lock
  Rakefile
                                       'better_errors'
                          20
  E README.md
                          21
                                       'rails_layout'
                          22
                          23
                          24
                                    'tzinfo-data', platforms: [:mingw, :mswin, :x64_mingw, :jruby]
                          25
                          26
                                    'bootstrap-sass'
                          27
                                    'simple_form'
                          28
```

3 characters selected

```
→ 062-security-and-static-code-analyzers git:(master) x gem install bundler-audit Successfully installed bundler-audit-0.5.0
1 gem installed
→ 062-security-and-static-code-analyzers git:(master) x bundle-audit
Name: actionview
Version: 5.0.0
```

https://groups.google.com/forum/#!topic/rubyonrails-security/I-VWr034ouk

CVE-2016-6316 Ly: Unknown

→ 062-security-and-static-code-analyzers git:(master) x bundle update rails

~> 3.2.22.3, ~> 4.2.7.1, >= 5.0.0.1

Possible XSS Vulnerability in Action View

```
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 active support 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 active model 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) X
```

```
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 active model 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) X
```

```
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 active model 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 jauery-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) x 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 active support 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 active model 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) x bundle-audit
No vulnerabilities found
→ 062-security-and-static-code-analyzers git:(master) X
```

```
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 active support 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 active model 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 active job 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) x bundle-audit
No vulnerabilities found
→ 062-security-and-static-code-analyzers git:(master) x brakeman -o brakeman.html
Loading scanner...
```

Summary

Brakeman Report

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

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

11

Warning Type Total Mass Assignment 1 SQL Injection

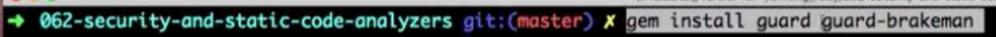
Security Warnings

Templates

Confidence	Class	Method	Warning Type	Message
	UsersController	set_user	SQL Injection	Possible SQL injection near line 68: User.where("ID = #{params[:ic
				app/controllers/users_controller.rb
				64 private
				# Use callbacks to share common setup or constraints bety
				66 def set_user
High				<pre># @user = User.find(params[:id])</pre>
				68 @u@er = User.where("ID = #{params[:id]}").first
				69 end
				71 # Never trust parameters from the scary internet, only a:
				72 def user_params
				# 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!

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

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



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

```
→ 062-security-and-static-code-analyzers git:(master) x 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) X

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

→ 062-security-and-static-code-analyzers git:(master) x gem install guard guard-brakeman
Successfully installed guard-brakeman-0.8.3
2 gems installed
→ 062-security-and-static-code-analyzers git:(master) x 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) X

8 E 8

```
→ 062-security-and-static-code-analyzers git:(master) x 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) x 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) x 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)$})
 watch(%r{\land config/.+\.rb})
 watch(%r{^lib/.+\.rb$})
 watch('Gemfile')
end
```

"Guardfile" 23L, 797C

```
2. vi Guardfile (vim)
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

2. guard (zsh)

```
→ 062-security-and-static-code-analyzers git:(master) x 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) x 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) x vi Guardfile
→ 062-security-and-static-code-analyzers git:(master) x guard
```

```
Guardfile — 062-security-and-static-code-analyzers
FOLDERS
▼ 25 062-security-and-static-code-analyzers
                            # A sample Guardfile
 # B app

► □ assets
                            # More info at https://github.com/guard/guard#readme

► □ channels
                          3
  T (3) controllers
   ## Uncomment and set this to only include directories you want to watch
    application_controller.rb
                            # directories %w(app lib config test spec features) \
    (h) users_controller.rb
    h visitors_controller.rb
                                .select{|d| Dir.exists?(d) ? d : UI.warning("Directory #{d} does not exist")}
 ▶ □ helpers
  ▶ □ Jobs
  ## Note: if you are using the 'directories' clause above and you are not

► □ models
                            ## watching the project directory ('.'), then you will want to move
 ► 🗀 views
                             ## the Guardfile to a watched dir and symlink it back, e.g.
 ▶ 🗀 bin
 ► □ config
                         11
 db C3 4
                         12
                                $ mkdir config
 ► (3 lib
 ► D log
                                $ mv Guardfile config/
 ▶ □ public
                                $ ln -s config/Guardfile .
 ≥ D test
 ► □ tmp
                         15
 ▶ □ vendor
                             # and, you'll have to watch "config/Guardfile" instead of "Guardfile"
                         16
  gitignore.
  brakeman.html
                         17
  config.ru
                             guard 'brakeman', run_on_start: true, quiet: true
  Cemfile.
                               watch(%r{^app/.+\.(erb|haml|rhtml|rb)$})
                         19
  Gemfile.lock
                         20
                               watch(%r{^config/.+\.rb$})
  Rakefile
                        21
                               watch(%r{^lib/.+\.rb$})
  README.md
                         22
                               watch('Gemfile')
                        23
                        24
```

☐ Line 18, Column 50

2. guard (zsh) **FOLDERS** - CheckSSLVerify Gemfile V 6 062-security-and-stat CheckStripTags ₹ 🕞 app CheckSymbolDoSCVE ► □ channels CheckTranslateBug * (3) controllers CheckUnsafeReflection ► Concerns CheckValidationRegex application_conf - CheckWithoutProtection yisitors_controll CheckXMLDoS CheckYAMLParsing ▶ □ jobs ▶ □ mailers Checks finished, collecting results... ▶ □ models 20:31:54 - INFO -► □ views > [#6bc124893672] ----- brakeman warnings ------▶ 🗀 bin ► □ config > [#6bc124893672] 11 ▶ □ db 20:31:54 - INFO - 2 brakeman findings 12 > □ 1b 20:31:54 - INFO - High - SQL Injection - Possible SQL injection near line 68 ▶ 🗀 log ▶ 🗀 public in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a ► □ test nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}" ▶ 🗀 tmp 15 ▶ □ vendor -gitignore 20:31:54 - INFO - Medium - Mass Assignment - Parameters should be whitelisted B brakeman.html 17 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra config.ru Ch Gemfile ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb Gemfile.lock : params.require(:user).permit! 20 20:31:54 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting Rakefile 21 P README.md Ruby/Rails/062-security-and-static-code-analyzers' 22 [1] quard(main)> quit 23 24 20:32:06 - INFO - Bye bye... → 062-security-and-static-code-analyzers git:(master) x 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.) Line 18, Column 50

```
1 # A sample Guardfile
  # More info at https://github.com/guard/guard# ***
  ## Uncomment and set this to only include dire
 # directories %w(app lib config test spec feat
  # .select{|d| Dir.exists?(d) ? d : UI.warning
 ## Note: if you are using the `directories` cl
 ## watching the project directory ('.'), then
  ## the Guardfile to a watched dir and symlink
     $ mkdir config
     $ mv Guardfile config/
    $ In -s config/Guardfile .
  # and, you'll have to watch "config/Guardfile"
  guard 'brakeman', run_on_start: true, quiet: t
    watch(%r{^app/.+\ (erb|haml|rhtml|rb)$})
    watch(%r{^config/.+\.rb$})
    watch(%r{^lib/.+\.rb$})
    watch('Gemfile')
```

Spaces: 2

Ruby

Guardfile - 062-security-and-static-code-analyzen

2. guard (fsevent_watch) Guardfile - 062-security-and-static-code-analyzer FOLDERS 20:31:54 - INFO - High - SQL Injection - Possible SQL injection near line 68 V 3 062-security-and-sta in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a 1 # A sample Guardfile Y B app nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}" ▶ 🗀 assets # More info at https://github.com/guard/guard# *** ► C channels # 25 controllers 20:31:54 - INFO - Medium - Mass Assignment - Parameters should be whitelisted ► Concerns ## Uncomment and set this to only include dire for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra application_con # directories %w(app lib config test spec feat users_controller ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb yisitors_controll # .select{|d| Dir.exists?(d) ? d : UI.warning : params.require(:user).permit! ▶ □ helpers 20:31:54 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting ▶ □ jobs ▶
 mailers ## Note: if you are using the 'directories' cl Ruby/Rails/062-security-and-static-code-analyzers' ▶ □ models ## watching the project directory ('.'), then [1] guard(main)> quit ► □ views ## the Guardfile to a watched dir and symlink ▶ 🗀 bin ► 🗀 config 11 20:32:06 - INFO - Bye bye... ▶ □ db → 062-security-and-static-code-analyzers git:(master) x guard 12 \$ mkdir config ► D Nb Warning: you have a Gemfile, but you're not using bundler or RUBYGEMS_GEMDEPS ▶ □ log \$ mv Guardfile config/ ▶ □ public Expected string default value for '--listen-on'; got false (boolean) \$ In -s config/Guardfile . ▶ □ test 20:32:52 - INFO - Guard here! It looks like your project has a Gemfile, yet y ▶ 🗀 tmp 15 ▶ □ vendor ou are running # and, you'll have to watch "config/Guardfile" gitignore. > [#] `guard` outside of Bundler. If this is your intent, feel free to ignore brakeman.html 17 this config.ru guard 'brakeman', run_on_start: true, quiet: t Cemfile. > [#] message. Otherwise, consider using `bundle exec guard` to ensure your watch(%r{^app/.+\.(erb|haml|rhtml|rb)\$}) Gemfile.lock > [#] dependencies are loaded correctly. watch(%r{^config/.+\.rb\$}) 20 > [#] (You can run `guard` with --no-bundler-warning to get rid of this messa A Rakefile watch(%r{^lib/.+\.rb\$}) 21 README.md ge.) watch('Gemfile') 20:32:53 - INFO - rocessed 23 > [#fbc8b2fa513c] ----- brakeman warnings -----24 > [#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)> Line 18, Column 50

Spaces: 2

Ruby

```
2. [1 Warning fixed.] 1 fixed warning, 1 previous warning (fsevent watch)
                                                                                                             users_controller.rb — 062-security-and-static-code-analyzers
                                                                                     FOLDERS.
                                                                                      V 3 062-security-and-stat
20:32:53 - INFO - rocessed
                                                                                                                    @user.update(user_params)
                                                                                                    44
                                                                                      Y & app
> [#fbc8b2fa513c] ----- brakeman warnings ------
                                                                                       ► 🗀 assets
                                                                                                                   format.html { redirect_to @user, notic
                                                                                                    45

▶ □ channels
> [#fbc8b2fa513c]
                                                                                                                   format.json { render :show, status: :o
                                                                                                    46
                                                                                       Y S controllers
20:32:53 - INFO - 2 brakeman findings
                                                                                        ► 🗀 concerns
                                                                                                    47
20:32:53 - INFO - High - SQL Injection - Possible SQL injection near line 68
                                                                                          application_con
                                                                                                                   format.html { render :edit }
                                                                                                    48
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
                                                                                          yisitors_control
                                                                                                                   format.json { render json: @user.error
                                                                                                    49
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
                                                                                       ▶ □ helpers
                                                                                                    50
                                                                                       ▶ □ Jobs
                                                                                                    51
                                                                                       20:32:53 - INFO - Medium - Mass Assignment - Parameters should be whitelisted

▶ □ models
                                                                                                    52
 for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
                                                                                       ► □ views
                                                                                                    53
                                                                                      ▶ 🗀 bin
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
                                                                                      ► 🗀 config
: params.require(:user).permit!
                                                                                                    54
                                                                                                           # DELETE /users/1
                                                                                      ► D db
20:32:53 - INFO - Guard is now watching at '/Users/kobaltz/OneDrive/Drifting
                                                                                                    55
                                                                                                           # DELETE /users/1.json
                                                                                      1 0 1b
                                                                                      ▶ □ log
Ruby/Rails/062-security-and-static-code-analyzers'
                                                                                                    56
                                                                                                                destroy
                                                                                      ▶ □ public
20:33:13 - INFO -
                                                                                                    57
                                                                                                              @user.destroy
                                                                                      ▶ 🗀 test
> [#]
                                                                                      ▶ 🗀 tmp
                                                                                                    58
                                                                                                              respond to
                                                                                                                                format
                                                                                      ▶ □ vendor
> [#] rescanning ["app/controllers/users_controller.rb"], running all checks
                                                                                                                 format.html { redirect_to users_url, not
                                                                                                    59
                                                                                        gitignore.
20:33:13 - INFO -
                                                                                        h brakeman.html
                                                                                                    60
                                                                                                                 format.json { head :no content }
> [#] ----- brakeman warnings -----
                                                                                        config.ru
                                                                                                    61
                                                                                        C Gemfile
> [#]
                                                                                                    62
                                                                                        Gemfile.lock
20:33:13 - INFO - 1 fixed warning
                                                                                        Cuardfile
                                                                                                    63
20:33:13 - INFO - Medium - Mass Assignment - Parameters should be whitelisted
                                                                                        Rakefile
                                                                                                    64
                                                                                        Th README.md
for mass assignment near line 74 in /Users/kobaltz/OneDrive/Drifting Ruby/Ra
                                                                                                    65
                                                                                                              # Use callbacks to share common setup or c
ils/062-security-and-static-code-analyzers/app/controllers/users_controllerrb
                                                                                                    66
                                                                                                                   set_user
: params.require(:user).permit!
                                                                                                    67
                                                                                                                @user = User.find(params[:id])
20:33:13 - INFO - 1 previous warning
20:33:13 - INFO - High - SQL Injection - Possible SQL injection near line 68
                                                                                                    68
                                                                                                                 # @user = User.where("ID = #{params[:id]
in /Users/kobaltz/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-a
                                                                                                    69
nalyzers/app/controllers/users_controllerrb: User.where("ID = #{params[:id]}"
                                                                                                    70
                                                                                                    71
                                                                                                              # Never trust parameters from the scary in
                                                                                                    72
                                                                                                                   user_params
20:33:46 - INFO -
                                                                                                     73
                                                                                                                                 e(:user).permit(:first_name
                                                                                                                 params. Te
> [#]
                                                                                                     74
                                                                                                                 # params.require(:user).permit!
> [#] rescanning ["app/controllers/users_controller.rb"], running all checks
20:33:46 - INFO -
                                                                                                    76
> [#] ----- brakeman warnings ------
> [#]
[1] guard(main)>
                                                                                     Line 67, Column 1; Saved ~/OneDrive/Drifting Ruby/Rails/062-security-and-static-code-analyzers/app/controllers/users_controller.rb (UTF-8)
```



NOV 2ND, 2016

Brakeman 3.4.1 Released

- Configurable engines path (<u>Jason Yeo</u>)
- 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.

<u>Brakeman Pro</u> 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 repor



Drifting Ruby

WWW.DRIFTINGRUBY.COM