

Ruby/Rails Security



ebay



YAHOO!

Forbes



patreon



TARGET

Gmail

MINECRAFT

SONY



ASHLEY
MADISON[®].COM

The logo for Ashley Madison is displayed on a red rectangular background. The word "ASHLEY" is on top in a large serif font, and "MADISON" is below it in a larger, bold sans-serif font. A registered trademark symbol (®) is positioned above the letter "N" in "MADISON". Below "MADISON" is ".COM" in a smaller sans-serif font.

Sources: <https://haveibeenpwned.com/PwnedWebsites>
<http://betanews.com/2014/12/17/the-top-10-worst-security-breaches-of-2014/>

WINTER

Adobe	Poor Encryption
Sony	SQL Injection + OnSite Breach / Stolen Credentials
Dominos	Weak MD5 password Hashing
Snapchat	Brute force enumeration of phone numbers
Yahoo	SQL Injection
Target	Stolen HVAC credentials & pivoted into POS system
eBay	Stolen employee credentials
Ashley Madison	Internal data dump

Source: <http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>
<http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12>

Gavin Miller

@gavingmiller
gavinmiller.io

Cisco

Advanced Malware Protection (AMP)

[we're also hiring Sr. Rails devs]

The dashboard displays a timeline from May 27 08:02 to Nov 4 21:04, showing device trajectories for multiple hosts. A yellow shaded area highlights a period of high activity between late October and early November.

Device Trajectory for Demo_SFElcar:

- System: DellOptiPlex 5090 (Intel)
- IP: 10.0.10.100 [PXE]
- OS: Windows 10 Pro [PXE]
- Ports: 10-19 [PXE]
- Process: 40002198...400044 [D12]
- File: 2 [PXE]
- Services: 4000178...40001798 [PXE]
- Connections: 40001798...40001808 [PXE]
- Network: 40001808...40001818 [D12]
- File: 40001818...40001828 [PXE]
- Process: 40001828...40001838 [PXE]

Indicators of Compromise:

- Demo_ZAccess
- Threat Detected , Java compromise , Executed malware , Potential Dropper Infection

Hosts Detecting Malware (7 days):

Computer	Count
Demo_ZAccess	29
Demo_SFElcar	19
Demo_Ramnit	14
Demo_TDSS	13
Demo_Zbot	13

Hosts Detecting Network Threats (7 days):

Computer	Count
Demo_Stabuniq	4
Demo_Tinba	2
Demo_Zbot	1

Malware Threats (7 days):

Detection Name	Count
W32.ZAccess.L5inf	26
W32.Ramnit.A	14
ZBot.FakeAlert-tpd	13
Eldorado:Alureon-tpd	12
Win32.DemoMal.Rat.Client	12

Network Threats (7 days):

Remote IP	Count
82.165.37.127	2
205.234.252.212	2
75.102.25.76	2
178.19.25.52	1

Recent Malware Threats:

Computer	Detection Name
Demo_TDSS	Eldorado:Alureon-tpd
Demo_TDSS	Alureon.Olmarik.tpd
Demo_TDSS	Eldorado:Alureon-tpd
Demo_TDSS	Eldorado:Alureon-tpd
Demo_TDSS	Eldorado:Alureon-tpd

Recent Network Threats:

Computer	Detection Name	Remote IP
Demo_Tinba	DFC.CustomIPList	82.165.37.127
Demo_Tinba	DFC.CustomIPList	82.165.37.127
Demo_Zbot	DFC.CustomIPList	178.19.25.52
Demo_Stabuniq	DFC.CustomIPList	75.102.25.76
Demo_Stabuniq	DFC.CustomIPList	75.102.25.76

Filter Options:

- THREAT TYPE: create, copy, move, execute, open, connection, scan-detection, exec-block, compromised?, self-exe, refresh, task, file-update, policy-update, connector-update, task-schedule, uninstall
- EVENT POSITION: design, multiple, unknown
- EVENT Flags: none, warning, audit-only
- FILE TYPE: executable, ms-office (file), pdf, ms-cabinet, Ram, zip-archive, other, unknown

Search... Select All Clear All

Goals

Could my business/project be
breached like that?

Glimpse into how hackers operate

~~Pee your pants a little~~

Scare you a tiny bit

Beginner/Intermediate Security

- Attacks:
 - SQL Injection, Timing Attacks
- Tools:
 - sqlmap, Shodan
- Prevention:
 - Brakeman, CVES, Process

SQL Injection



Sign In to Online Banking

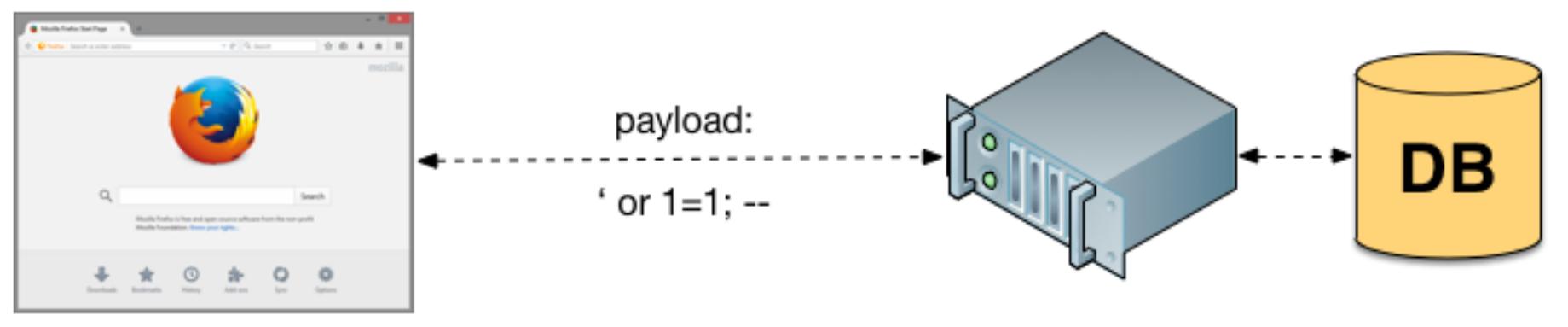
Client Card/Username: [Recover Client Card/Username](#)

Remember My Client Card/Username [Help With Sign-In](#)

Password: **Sign In >**

[Recover Password](#)

SQL Injection



Demo



VOLUME 1

1 6

8

10

11

VOLUME

1 6

0

11



For media inquiries please email media@ashleymadison.com
or call 1.866.205.7525 (Toll-free) / 1.647.558.3526 (Local)



Statement from Avid Life Media – August 19, 2015

Archive

Aug 19, 2015

3025

Statement from Avid Life Media – August 19, 2015

Toronto, ON August 19, 2015 – No current or past members' full credit card numbers were stolen from Avid Life Media. Any statements to the contrary are false. Avid Life Media has never stored members' full credit card numbers.

Source: <http://www.troyhunt.com/2015/09/good-news-your-credit-card-is-fine-and.html>

Quiz Time

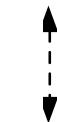


Timing Attacks

- Work by exploiting early-exits in comparison algorithms

```
1 class String
2   def self.==(obj)
3     0.upto(length).each do |index|
4       return false unless self[index] == obj[index]
5     end
6     true
7   end
8 end
```

	0	1	2	3	4	5	6	7				
Input	P	A	S	S	W	O	R	D				



	0	1	2	3	4	5	6	7				
Password	P	A	S	S	W	O	R	D				

	0	1	2	3	4	5	6	7				
Input	P	A	S	S	W	O	R	D				



	0	1	2	3	4	5	6	7				
Password	P	A	S	S	W	O	R	D				

	0	1	2	3	4	5	6	7				
Input	P	A	S	S	W	O	R	D				



	0	1	2	3	4	5	6	7				
Password	P	A	S	S	W	O	R	D				

Input

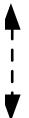
0	1	2	3	4	5	6	7				
P	A	S	S	W	O	R	D				



Password

0	1	2	3	4	5	6	7				
P	A	S	S	W	O	R	D				

	0	1	2	3	4	5	6	7				
Input	P	A	S	S	W	O	R	D				



	0	1	2	3	4	5	6	7				
Password	P	A	S	S	W	O	R	D				

Exploitable?

Ruby comparison takes 0.840ns/byte
(effectively per character)

Can measure a 30 μ s difference over the internet

Which means you can't exploit a timing attack over the internet ... (in Ruby)

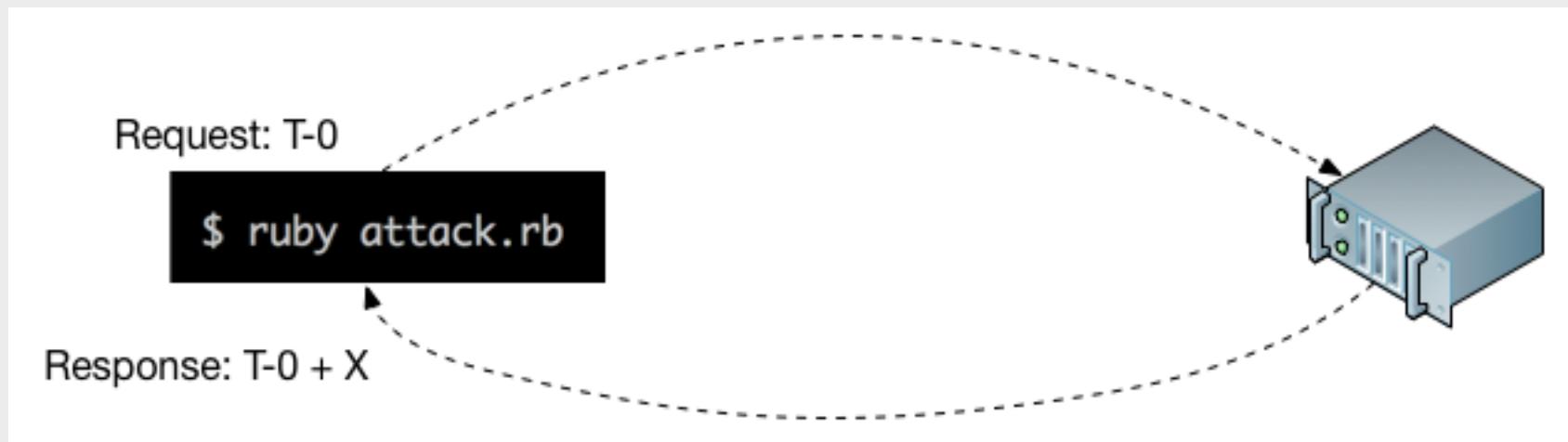
Exploitable!

So get closer...

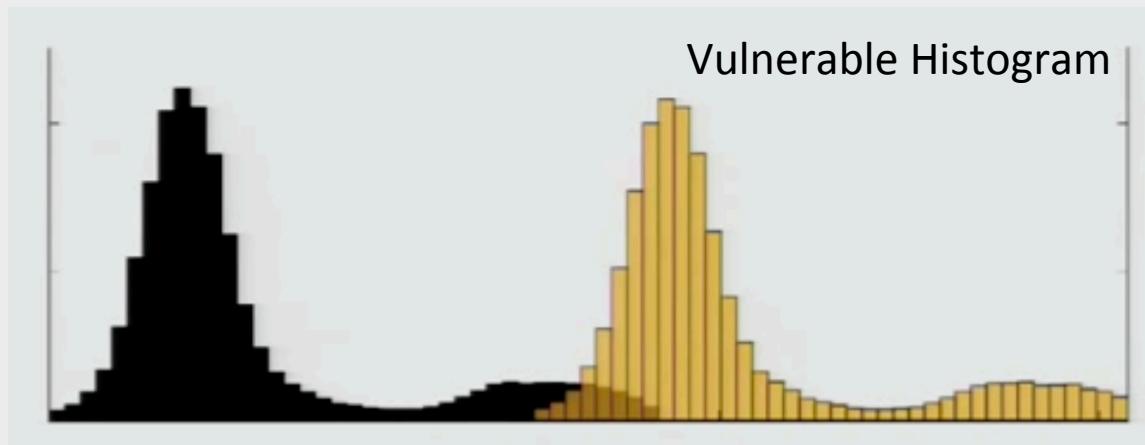
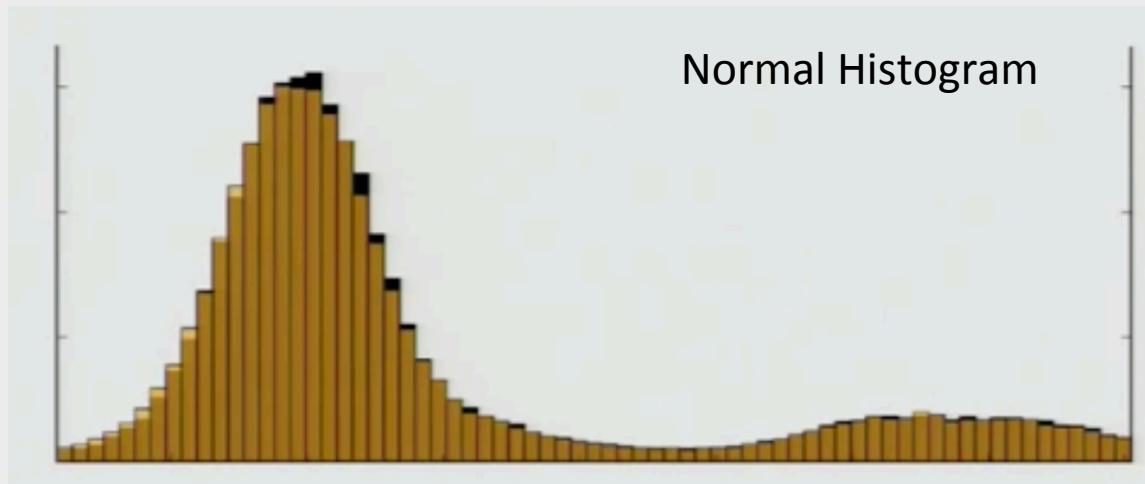
EC2 to EC2 can measure a 15-400ns difference.

Bingo!

How?



How?

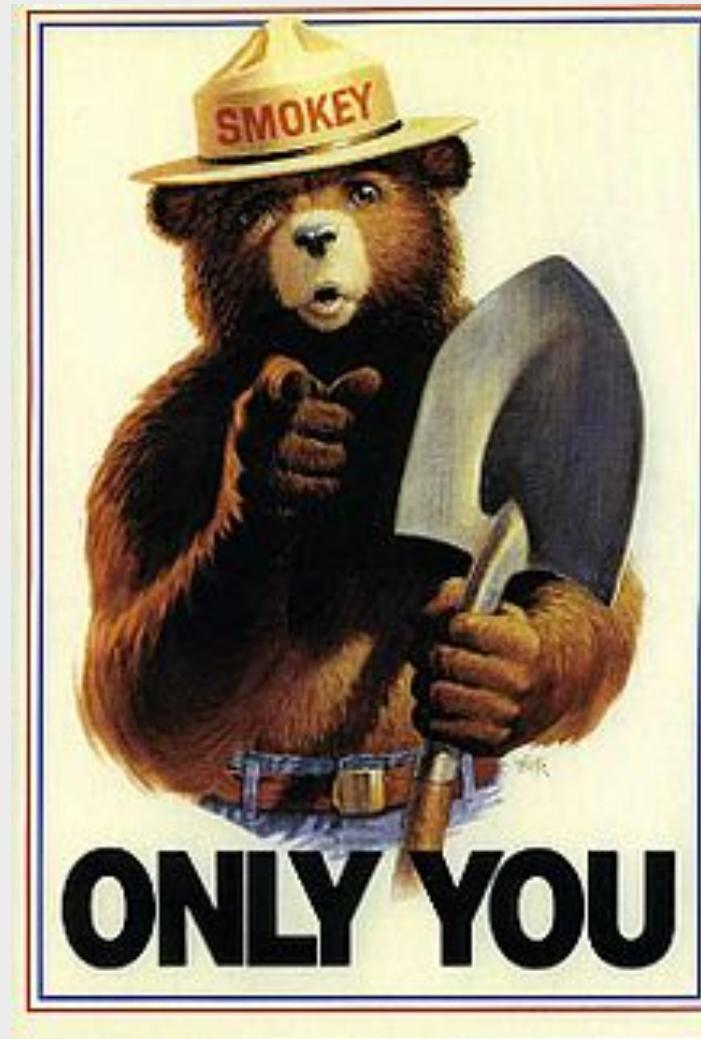


MOAR!

DEMOS!



Prevention



~~Copy-Paste Coding~~

```
SqlCommand cmd = new SqlCommand("Update logintable set password_change_status=1  
where email='" + txtemail.Text + "'", con);
```

Process

"Put someone on your team in charge of tracking your dependencies (C libraries, Ruby gems, Python easy_install thingies) and have a process by which you periodically check to make sure you're capturing upstream security fixes.

You should run your service aware of the fact that major vulnerabilities in third-party library code are often fixed without fanfare or advisories; when maintainers don't know exactly who's affected how, the whole announcement might happen in a git commit."

- tptacek (Thomas Ptacek)

<https://news.ycombinator.com/item?id=3940286>

Mailing Lists & CVEs

- Ruby Security List
 - <https://groups.google.com/forum/#!forum/ruby-security-ann>
- Rails Security List
 - <https://groups.google.com/forum/?fromgroups#!forum/rubyonrails-security>
- CVE Databases
 - <https://www.cvedetails.com/>



Patrick McKenzie

@patio11



Following

Heard about a vulnerability? The adversary is not a stressed human like you. It's a for loop. The vuln is not secret; after all, you know.

2013 Rails YAML CVE

SHODAN X-Powered-By: Phusion Passenger Explore Contact Us

Exploits Maps

TOP COUNTRIES



Country	Count
United States	54,848
Germany	5,563
Japan	5,350
Ireland	3,759
United Kingdom	3,633

Showing results 1 - 10 of 106,906

2406:da00:ff00::36eb:c5b3

Added on 2016-01-04 01:35:20 GMT

[Details](#)

HTTP/1.1 301 Moved Permanently
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Date: Mon, 04 Jan 2016 01:35:09 GMT
Location: https://[2406:
Server: nginx/1.6.2 + Phusion Passenger 4.0.59
Status: 301 Moved Permanently
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIG...

107.23.239.165

ec2-107-23-239-165.compute-1.amazonaws.com

Amazon.com

Added on 2016-01-04 01:35:18 GMT

 United States, Ashburn

[Details](#)

HTTP/1.1 302 Found
cache-control: no-cache
Content-Type: text/html; charset=utf-8
Date: Mon, 04 Jan 2016 01:24:20 GMT
location: http://107.23.239.165/session/new
Server: nginx + Phusion Passenger
Set-Cookie: _OneCallNowRails_session=dHhp6Nmhb2VsYlRqSHYwQ3QxSksBkJNDUxc31WZUQzUVZVMH10QVmzNU...

2406:da00:ff00::36eb:d48f

Added on 2016-01-04 01:35:09 GMT

[Details](#)

HTTP/1.1 301 Moved Permanently
Bluegreen-Enabled: false
Bluegreen-Percent: 0
Content-Type: text/html
Date: Mon, 04 Jan 2016 01:34:59 UTC
Location: http://bleacherreport.com/
Server: nginx/1.2.6 + Phusion Passenger 4.0.0.rc6
Set-Cookie: site_version=old; domain=.bleacherreport.com; path=/...

94.245.36.28

h5ef5241c.wireless.dyn.perspektivbredband.net

Perspektiv Bredband AB

Added on 2016-01-04 01:35:05 GMT

 Sweden

[Details](#)

HTTP/1.1 303 See Other
Date: Mon, 04 Jan 2016 01:35:02 GMT
Server: Apache/2.2.9 (Debian) Phusion_Passenger/2.2.9
X-Powered-By: Phusion Passenger (mod_rails/mod_rack) 2.2.9
X-Runtime: 0
Cache-Control: no-cache

/security



Security policy

Rails takes web security very seriously.
If you found a vulnerability in Ruby on Rails, follow
these steps to safely report the issue to the core team.

Supported versions

Support of the Rails framework is divided into four groups: New features, bug fixes, security issues, and severe security issues. They are handled as follows:

New Features

New Features are only added to the master branch and will not be made available in point releases.

Bug fixes

Only the latest release series will receive bug fixes. When enough bugs are fixed and its deemed worthy to release a new gem, this is the branch it happens from.

- Current release series: 4.2.x

Security issues:

The current release series and the next most recent one will receive patches and new versions in case of a security issue.

- Current release series: 4.2.x
- Next most recent release series: 4.1.x

Severe security issues:

For severe security issues we will provide new versions as above, and also the last major release series will receive patches and new versions. The classification of the security issue is judged by the core team.

/security

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1

```
mQENBFZnMMgBCADYrScTgbKQAS/ciju4PUp5TUp sXovmlsSc/b0Zx0iFlhpRy5z4
TSi2bLh4UlGTtkI1+CrrxEt+Xf3XUzes10+j24yZUdKKNJQUmPrSLjLM5rT5tdrV
lhEbXVKs rP1RfjL0oKvGN9tvylGuGBm/SAW1KZR00E3jT3WX27G9Ru6j4xYojYZK
bHDx/SVNi3fBppv4egybxLfcq+zKJ9vqFzbxE6mgv3PCiWfwrR0pw6lnRUwr52BK
bjIuZVbEscpa68acx7esB5Wm6An13pKBGuxrGkue51L7GiebfzqbrL88hX2Jjm0u
18tMQU8KJh lNXSEv j07/dms je0UEy0Ynxrq9ABEBAAG0IkVyaW4gUHRhY2VrIDxl
cmluQHN0YXJmaWdodGVycy5pbz6JAT4EEwECACgFA1ZnMMgCGwMFCQPCZwAGCwkI
BwMCBhUIAgkKCwQWA gMBAh4BAheAAAoJEH+dNeH0Ci1M6TwH/1c5LTZ4YLJ9VNrc
20Lqfv rKbw37dAaQd70MTw+1XMu h2AKWAUzAoym0mfCMvSivHfFs zYohKzx+xCKb
LUh2bcjTq3sWbPhdFgHHxzkN5Zr5RSLW4dXlzd6u+M/7JZdUi xYdA1dvRkWNdkSK
opYY/qjYo3JEa+Yooiw7L045W+Mjcd1CP+9pW/nT+KAbjyLTxUF/3Q/WhboSYIqR
jSMuPYHoq0YamTuhJt3wAbBLQf5y13/WYQ5IZE/wSEdM1xvxbVi4DNdBGbtzfonm
y1JWG45yySI+QEJR+t0M3LNKTjMSf9v0fVkwjYOPDF4CrdtNXM6F8vwiCJ5cuLhZ
Cj+c2A65AQ0EVmcwyAEIAK0RebEwVZDgMme fGF1Ns b4qEd9fJguJ6Ws xgvuPfP1Q
qseRfQfuGwIRE8eW0+Ux5V/qVK+qr8Xsjfb42FBNjhibKyJZ2xXgza fA06/YNhgcP
65I90bNCNb kXzuaqt bFfcQL56k2W20UgfEPvfj2Isieqzlt16ws g00QGOND9nLXD
+vzXvc lll036EujMxd6ykJ4ba0fNHBaDcxLVPkj4e2/oagas/dT73cy0Pdhacf3
wq0XqeR2o5Stv61x7Mj jZy7bIwB7WAfn5x0EnDoKZ9Y CtGaXJrmG4fLEgudNm fQL
q5rrzX79k4GCxnu4RhdYc8i+7kJJQbslyXhf7elUIA0AEQEAAYkBjQQYAQIAdwUC
VmcwyAIbDAUJA8JnAAAKCRB/nTXhzgotTPuRB/4oM+wsBVq901jmc3NWMrLzHsWl
1zZPsS2vkg/U4e66A0J0KLIQbtXI Kya8SAAhjXYyh1R6TqVqp3CoIaFCwm2jAU5h
S0HeCzHUn4wt nr6arTgiN75qaNnaRaHMhMSWwUc6J6AG3A7dWsQ4i8ywatHa4QL
Y5qiBsPWJwWHxhxye1m+Wt fev/Ee3j rNadc46rW+2iKNDzVxnJtLbrXzui8zZHGS
JmiTYYH8mR4vw/GlouGGnT+bsV04MngAubBvnfMj/fE34aRMROZpWq4sxMUo+Lz6
Huj7tJ6MQ92qTvFgj2ZaG8gQy8H0W2PGhL Aw9JEL9zq0jMPLmoLsK VpSqg1
=l1qj
-----END PGP PUBLIC KEY BLOCK-----
```

bundle outdated

```
Outdated gems included in the bundle:
```

```
* activerecord-deprecated_finders (newest 1.0.4, installed 1.0.3) in group "default"
* activesupport (newest 4.2.5, installed 4.2.0) in group "default"
* aws-sdk (newest 2.2.8, installed 1.61.0) in group "default"
* axlsx_rails (newest 0.4.0, installed 0.3.0) in group "default"
* backup (newest 4.2.2, installed 3.0.27, requested ~> 3.0.0) in group "default"
* bootstrap-datepicker-rails (newest 1.5.0, installed 1.3.1.1) in group "default"
* bootstrap-sass (newest 3.3.6, installed 3.3.3) in group "default"
* bourbon (newest 4.2.6, installed 3.2.4) in group "default"
* brakeman (newest 3.1.4, installed 1.5.3) in group "development"
* bullet (newest 4.14.10, installed 4.14.2) in group "development"
* capistrano-rails (newest 1.1.5, installed 1.1.3, requested ~> 1.1.1) in group "default"
* capistrano-rbenv (newest 2.0.4, installed 2.0.3, requested ~> 2.0) in group "default"
* coffee-rails (newest 4.1.1, installed 4.1.0, requested ~> 4.1.0) in group "assets"
* daemons (newest 1.2.3, installed 1.1.9) in group "default"
* dalli (newest 2.7.5, installed 2.7.2) in group "default"
* date_validator (newest 0.8.1, installed 0.7.1) in group "default"
* delayed_job (newest 4.1.1, installed 4.0.6) in group "default"
* delayed_job_active_record (newest 4.1.0, installed 4.0.3) in group "default"
* delayed_paperclip (newest 2.9.1, installed 2.9.0) in group "default"
* devise (newest 3.5.3, installed 3.4.1) in group "default"
* draper (newest 2.1.0, installed 1.4.0) in group "default"
* geocoder (newest 1.2.14, installed 1.2.6) in group "default"
* gmaps4rails (newest 2.1.2, installed 1.5.6, requested = 1.5.6) in group "default"
* guard-rspec (newest 4.6.4, installed 4.5.0) in groups "test, development"
* hirb (newest 0.7.3, installed 0.7.2) in group "default"
* identity_cache (newest 0.2.5, installed 0.2.3) in group "default"
* jquery-rails (newest 4.0.5, installed 4.0.3) in group "default"
* judge (newest 2.1.1, installed 2.0.5) in group "default"
* kaminari (newest 0.16.3, installed 0.16.2) in group "default"
```

bundle-audit check

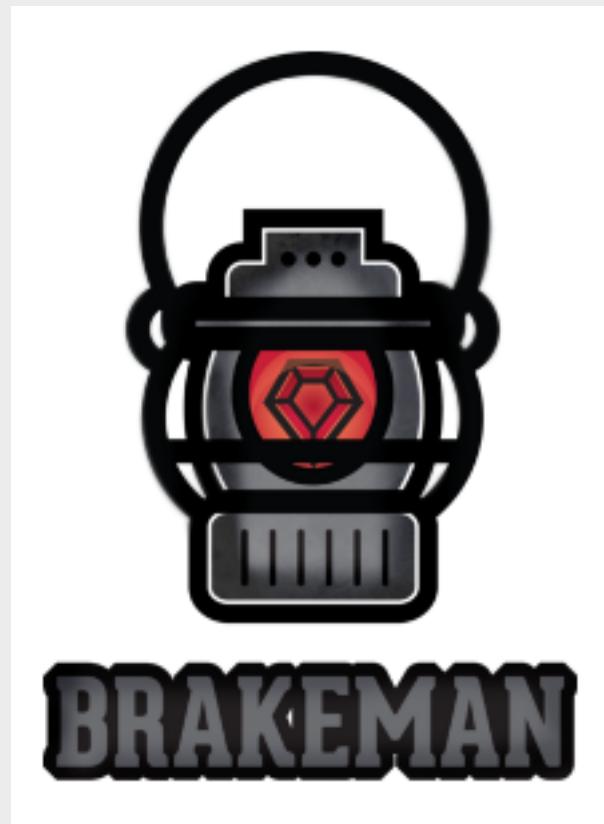
```
Name: jquery-rails
Version: 4.0.3
Advisory: CVE-2015-1840
Criticality: Medium
URL: https://groups.google.com/forum/#!topic/ruby-security-ann/XIZPbobuwaY
Title: CSRF Vulnerability in jquery-rails
Solution: upgrade to >= 4.0.4, ~> 3.1.3
```

```
Name: nokogiri
Version: 1.6.6.1
Advisory: CVE-2015-1819
Criticality: Unknown
URL: https://github.com/sparklemotion/nokogiri/issues/1374
Title: Nokogiri gem contains several vulnerabilities in libxml2 and libxslt
Solution: upgrade to ~> 1.6.6.4, >= 1.6.7.rc4
```

```
Name: nokogiri
Version: 1.6.6.1
Advisory: CVE-2015-5312
Criticality: High
URL: https://groups.google.com/forum/#!topic/ruby-security-ann/aSbgDiwb24s
Title: Nokogiri gem contains several vulnerabilities in libxml2
Solution: upgrade to >= 1.6.7.1
```

```
Name: paperclip
Version: 4.2.1
Advisory: CVE-2015-2963
Criticality: Medium
URL: https://robots.thoughtbot.com/paperclip-security-release
Title: Paperclip Gem for Ruby vulnerable to content type spoofing
```

Brakeman



Brakeman

+SUMMARY+

Scanned/Reported	Total
Controllers	27
Models	91
Templates	84
Errors	0
Security Warnings	98 (22)

Warning Type	Total
Attribute Restriction	22
Cross Site Scripting	9
Cross-Site Request Forgery	1
Denial of Service	1
Mass Assignment	62
Redirect	3

+SECURITY WARNINGS+

Confidence	Class	Method	Warning Type	Message
High			Cross Site Scripting	Rails 4.2.0 does not encode JSON keys (CVE-2015-3226). Upgrade to Rails version 4.2.1 or greater.
Medium			Denial of Service	Rails 4.2.0 is vulnerable to denial of service via XML parsing (CVE-2015-3227). Upgrade to Rails version 4.2.1 or greater.
Weak	[REDACTED]	set_value	Redirect	Possible unprotected redirect near line 140: redirect_to("/[REDACTED]/" + +Pro
Weak	[REDACTED]::[REDACTED]	create	Redirect	Possible unprotected redirect near line 48: redirect_to([REDACTED]::[REDACTED].new(+pa
Weak	[REDACTED]::[REDACTED]	update	Redirect	Possible unprotected redirect near line 64: redirect_to([REDACTED]::[REDACTED].find(+pa

Model Warnings:

Confidence	Model	Warning Type	Message
High	[REDACTED]	Attribute Restriction	Mass assignment is not restricted using attr_accessible
High	[REDACTED]	Attribute Restriction	Mass assignment is not restricted using attr_accessible
High	[REDACTED]	Attribute Restriction	Mass assignment is not restricted using attr_accessible
Medium	[REDACTED]	Attribute Restriction	attr_accessible is recommended over attr_protected near line 7
Weak	[REDACTED]	Mass Assignment	Potentially dangerous attribute available for mass assignment: :[REDACTED]
Weak	[REDACTED]	Mass Assignment	Potentially dangerous attribute available for mass assignment: :[REDACTED]

Thanks :)

Make good decisions