

Ruby/Rails Security



TARGET



SONY

ASHLEY
MADISON[®].COM

RECEIVED

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

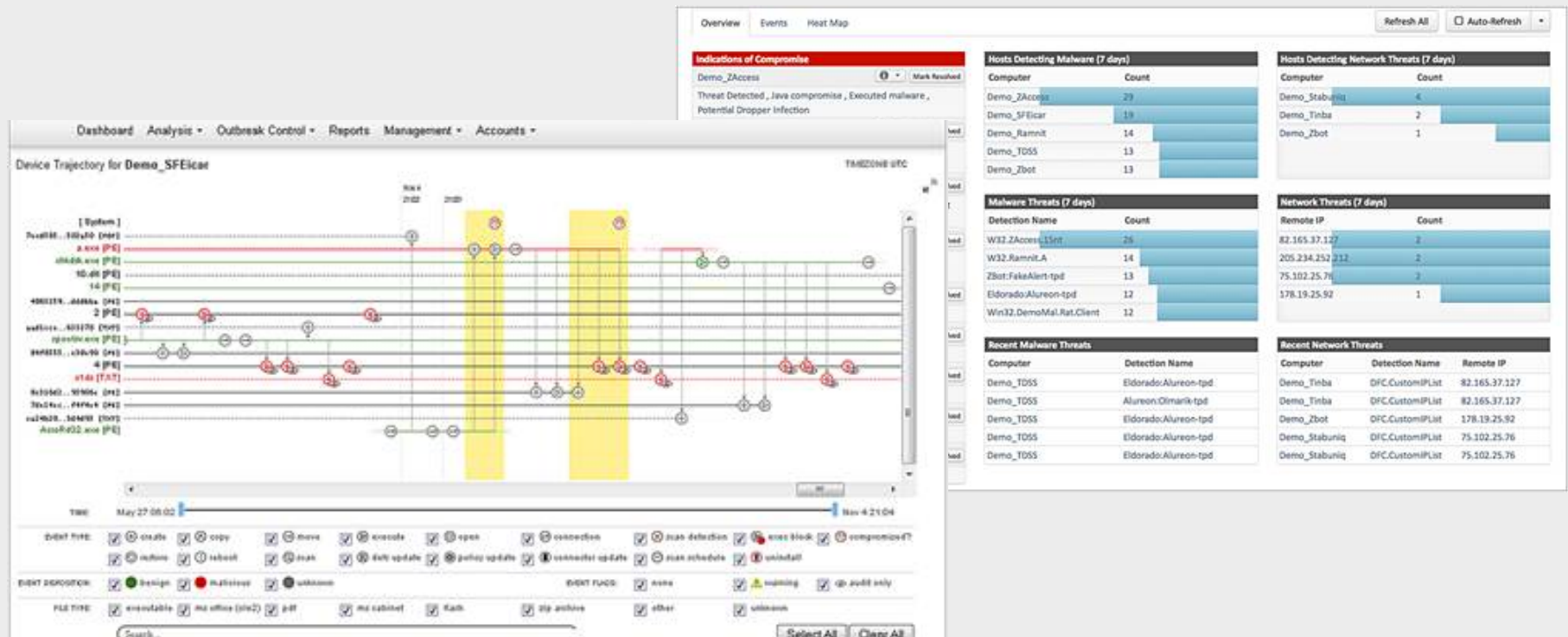
Gavin Miller

@gavingmiller
gavinmiller.io

Cisco

Advanced Malware Protection (AMP)

[we're also hiring Sr. Rails devs]



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:

' or 1=1;

▶ [Recover Client Card/
Username](#)

☐ Remember My Client Card/Username

▶ [Help With Sign-In](#) 

Password:

▶ [Recover Password](#)

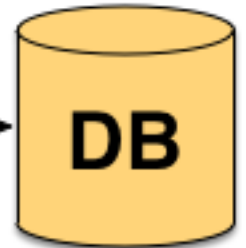
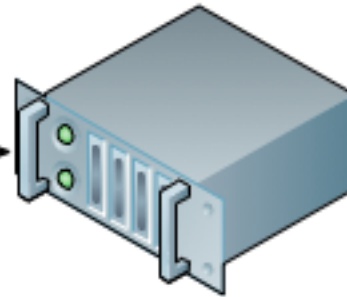
Sign In >



SQL Injection



payload:
' or 1=1; --



Demo





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>

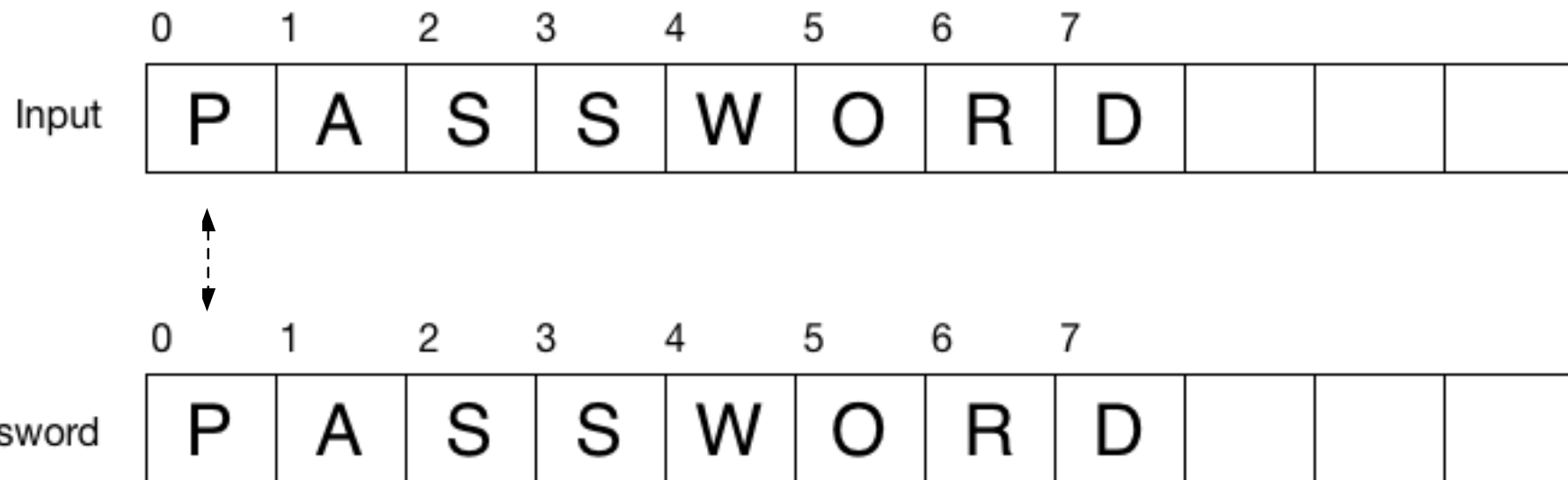
Quiz Time

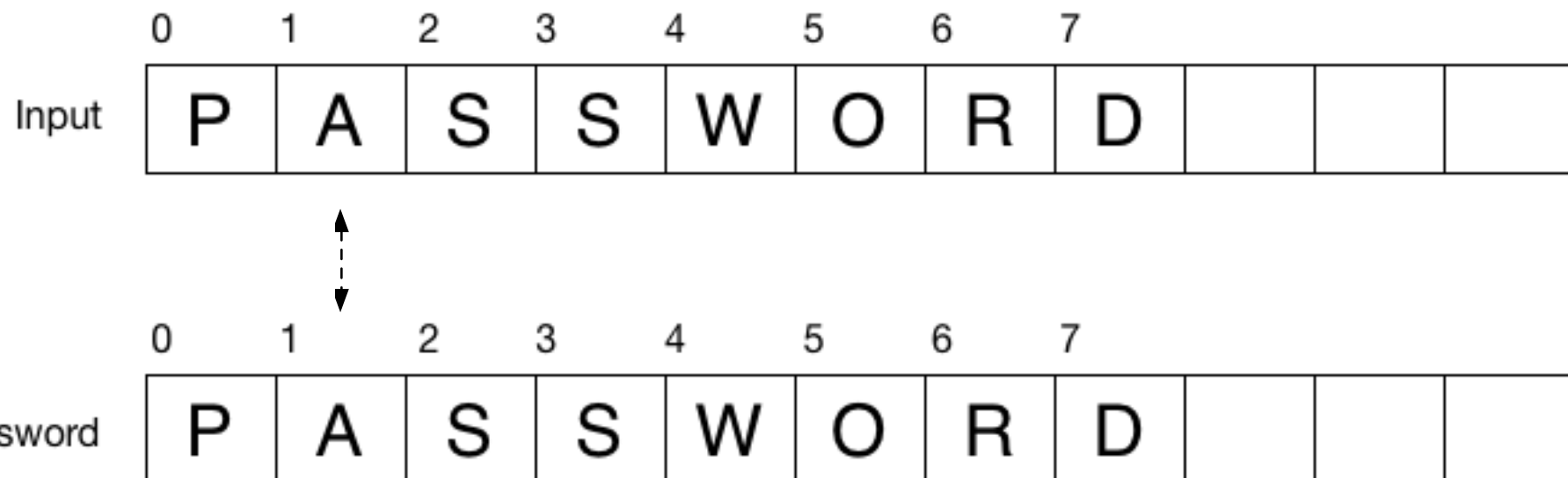


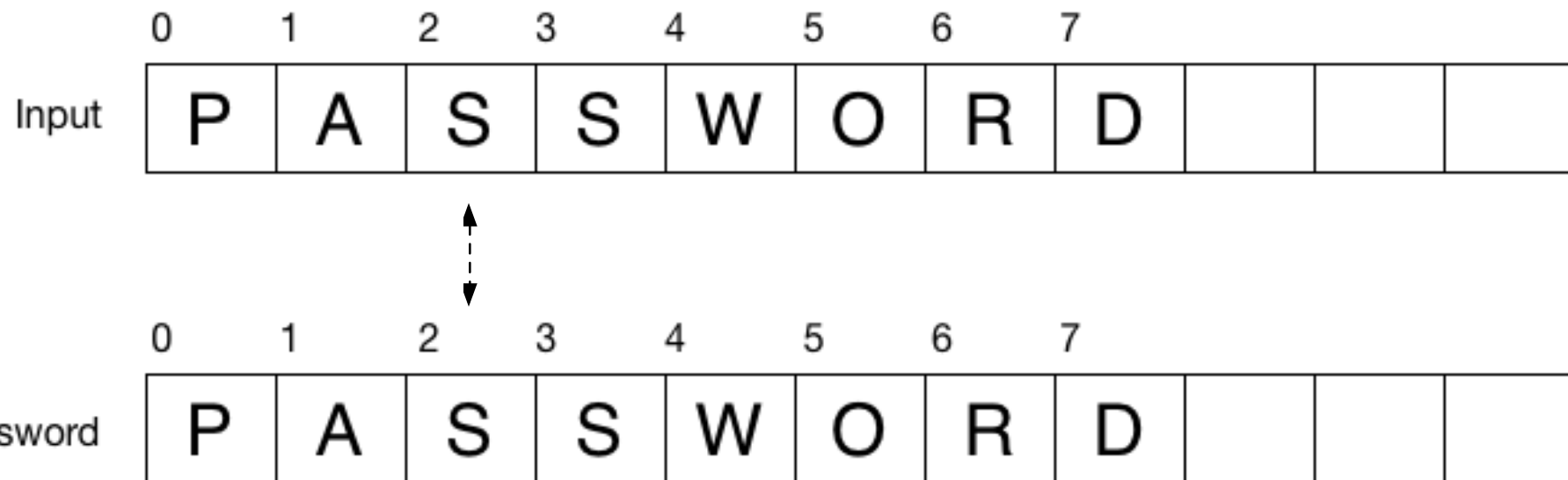
Timing Attacks

- 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
```

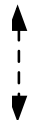







Input

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

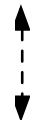


Password

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

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			

Exploitable?

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

Can measure a 30μs difference over the
internet

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

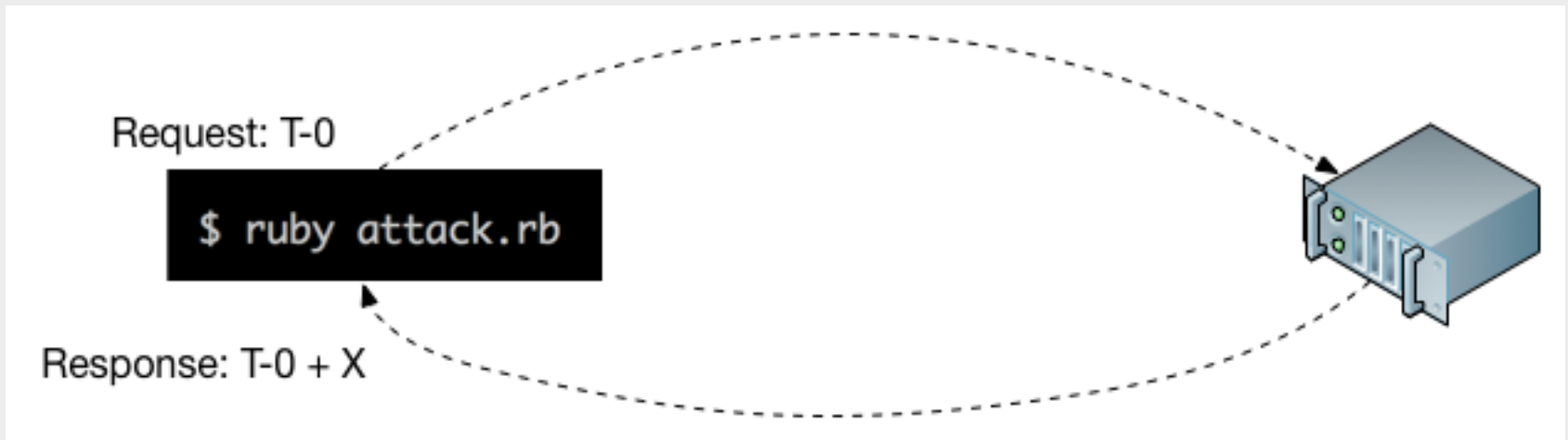
Exploitable!

So get closer...

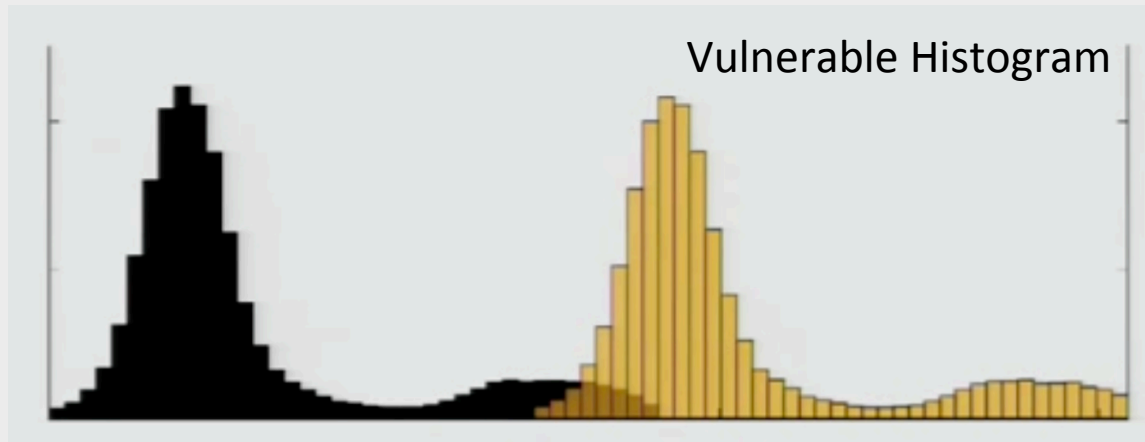
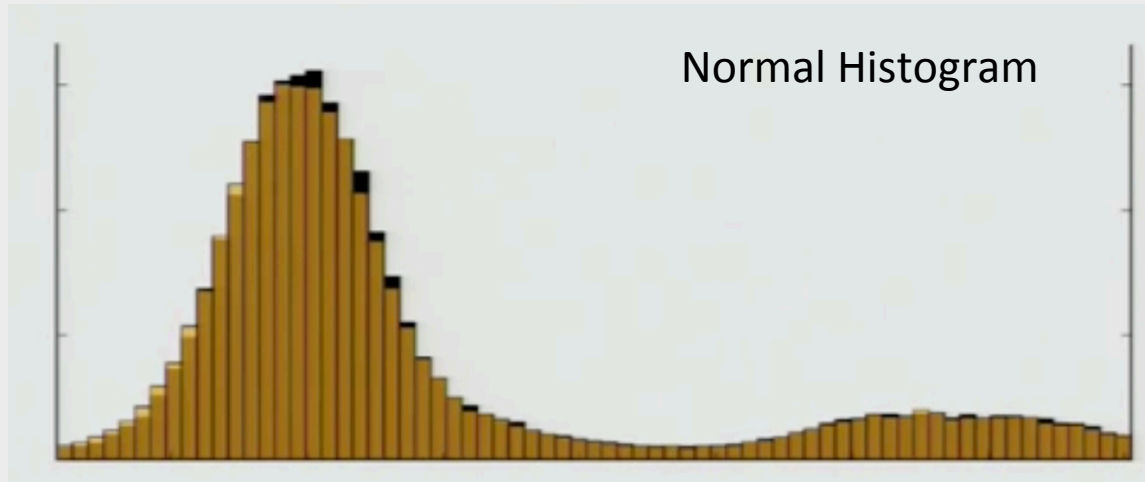
EC2 to EC2 can measure a 15-400ns difference.

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



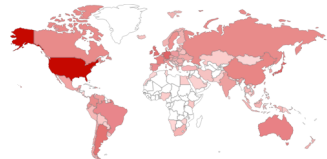
Explore

Contact Us

 Exploits

 Maps

TOP COUNTRIES



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

TOP SERVICES

HTTP	57,118
HTTPS	41,238
HTTP (8080)	3,390
HTTP (81)	1,422
Puppet Master	734

TOP ORGANIZATIONS

Amazon.com	30,497
Digital Ocean	5,848
AMAZON	4,596
Linode	3,695
DigitalOcean	1,812

TOP OPERATING SYSTEMS

Linux 3.x	637
Linux 2.6.x	206
FreeBSD 8.x	61
Linux 2.4-2.6	5
Windows 7 or 8	3

TOP PRODUCTS

Apache httpd	52,808
nginx	44,227
cloudflare-noinx	54

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=dHp6Nmhb2VsY1RqSHYwQ3QxSkxSbkJBNDUxc3lWZUQzUUVZVMH10QVMzNU...

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=.2bleacherreport.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/ciju4PUp5TUpSxovmlsSc/b0Zx0iFlhpRy5z4
TSi2bLh4UlGTtkI1+CrrxEt+Xf3XUzes1Q+j24yZudKKNJQUmPrSLjLM5rT5tdrV
lhEbXVKsrP1RfjL0oKvGN9tvylGuGBm/SAW1KZR00E3jT3WX27G9Ru6j4xYojYZK
bHDx/SVNi3fBppv4egybxLfcq+zKJ9vqFzbxE6mgv3PCiWfwrR0pw6lnRUwr52BK
bjIuZVbEscpa68acx7esB5Wm6An13pKBGuxrGkue51L7GiebfzqbrL88hX2Jjm0u
18tMQU8KJhLNXSEvj07/dmsje0UEy0Ynxrq9ABEBAAG0IkVyaw4gUHRhY2VrIDxl
cmLuQHN0YXJmaWdodGVycy5pbz6JAT4EEwECACgFAlZnMMgCGwMFCQPCZwAGCwkI
BwMCMbUIAgkKCwQWAgMBAh4BAheAAAJEH+dNeH0Ci1M6TwH/1c5LTZ4YLJ9VNrc
20LqfvrKbw37dAaQd70MTw+LXMuh2AKWAUzAoym0mfCMvSivHfFszYohKzx+xCKb
LUh2bcjTq3sWbPhdFgHHxzKN5Zr5RSLW4dXld6u+M/7JZdUixYdA1dvRkWNdkSK
opYY/qjYo3JEa+Yooiw7L045W+Mjcd1CP+9pW/nT+KAbjyLTxUF/3Q/WhboSYIqR
jSMuPYHoq0YamTuhJt3wAbBLQf5y13/WYQ5IZE/wSEdM1xvxbVi4DNdBGbtzfonm
yLJWG45yySI+QEJR+tOM3LNKTjMSf9v0fVkwjY0PDF4CrdtNXM6F8vwiCJ5cuLhZ
Cj+c2A65AQ0EVmcwyAEIAK0RebEwVZDgMmefGF1Nsb4qEd9fJguJ6WsxgvuPfP1Q
qseRfQfuGwIRE8eW0+Ux5V/qVK+qr8Xsjfb42FBNjhibKyJZ2xXgzfA06/YNhgcp
65I90bNCNbkXzuaqtbFfcQL56k2W20UgfEPvfj2Isieqzlt16wsg00QGOND9nLXD
+vzXvclll036EujMxd6ykJ4ba0fNHBAcXLPKj4e2/oagas/dT73cy0Pdhacft3
wq0XqeR2o5STv61x7MjjZy7bIwB7Wafn5x0EnDoKZ9YctGaXJrmG4fLEgudNmFQL
q5rrzX79k4GCxnu4RhdYc8i+7kJJQbslyXh7eLUIA0AEQEAAyKBJQQYAQIADwUC
VmcwyAIbDAUJA8JnAAAKCRB/nTXhzgotTPuRB/4oM+wsBVq901jmc3NWMrLzHsWl
lzZPsS2vkg/U4e66A0J0KLIQbtXIKya8SAAhjXYyh1R6TqVqp3CoIaFCwm2jAU5h
S0HeCzHUn4wtnr6arTgin75qaNnaRaHMHMSWwUc6J6AG3A7dwsQ4i8ywatHa4QL
Y5qiBsPWJwWHxhxye1m+Wtfev/Ee3jrNadc46rW+2iKNDzVxnJtLbrXzui8zZHGS
JmiTYyH8mR4vw/GlouGGnT+bsV04MngAubBvnfmj/fE34aRMR0ZpWq4sxMUo+Lz6
Huj7tJ6MQ92qQtvFgj2ZaG8gQy8H0W2PGhLaw9JEL9zq0jMPLmoLsKVpSqq1
=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

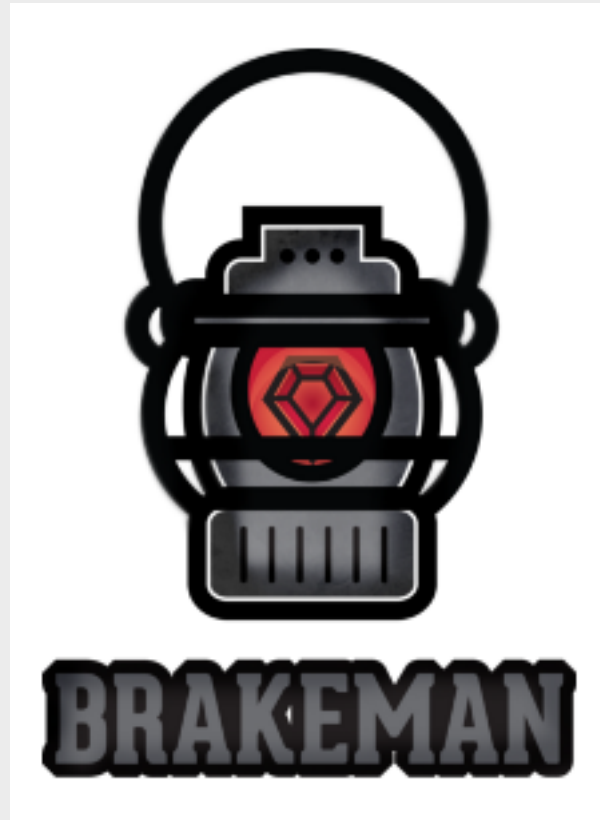
Name: jquery-rails
Version: 4.0.3
Advisory: CVE-2015-1840
Criticality: Medium
URL: <https://groups.google.com/forum/#!topic/ruby-security-ann/XIZPbobuwaY>
Title: CSRF Vulnerability in jquery-rails
Solution: upgrade to >= 4.0.4, ~> 3.1.3

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 ver
Medium			Denial of Service	Rails 4.2.0 is vulnerable to denial of service via XML parsing (CVE-2015-32
Weak		set_value	Redirect	Possible unprotected redirect near line 140: redirect_to((" / " + +Pro
Weak		create	Redirect	Possible unprotected redirect near line 48: redirect_to(:: .new(+pa
Weak		update	Redirect	Possible unprotected redirect near line 64: redirect_to(:: .find

Model Warnings:

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

Thanks :)

Make good decisions