

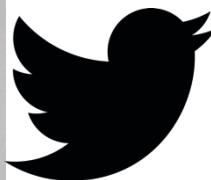
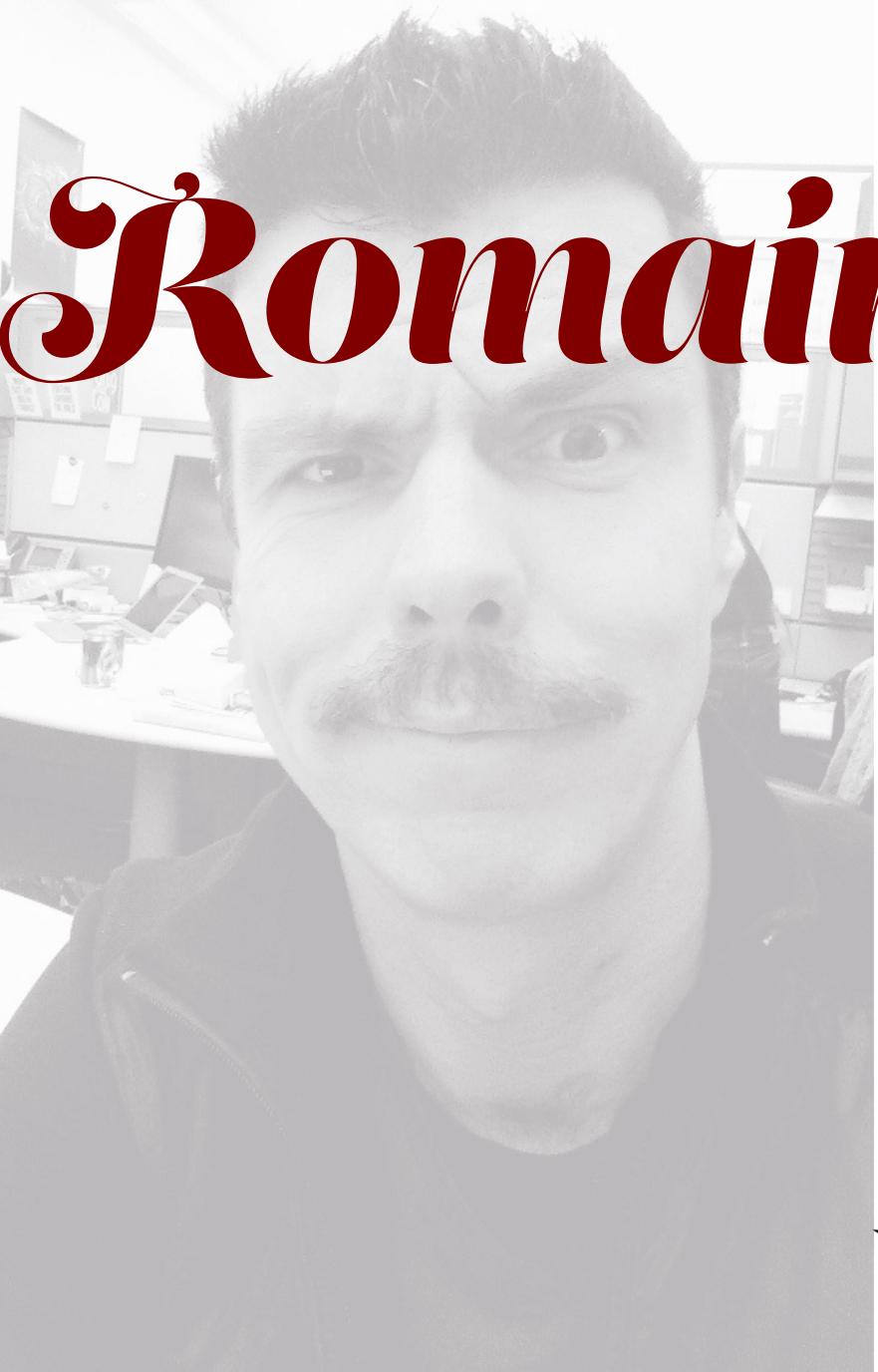


Barbus & Barbares

#barbusdevoxx

DEVOXX™ France

Romain



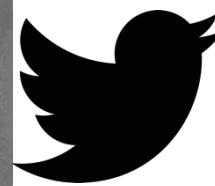
@rpelisse

DEVOXX™ France

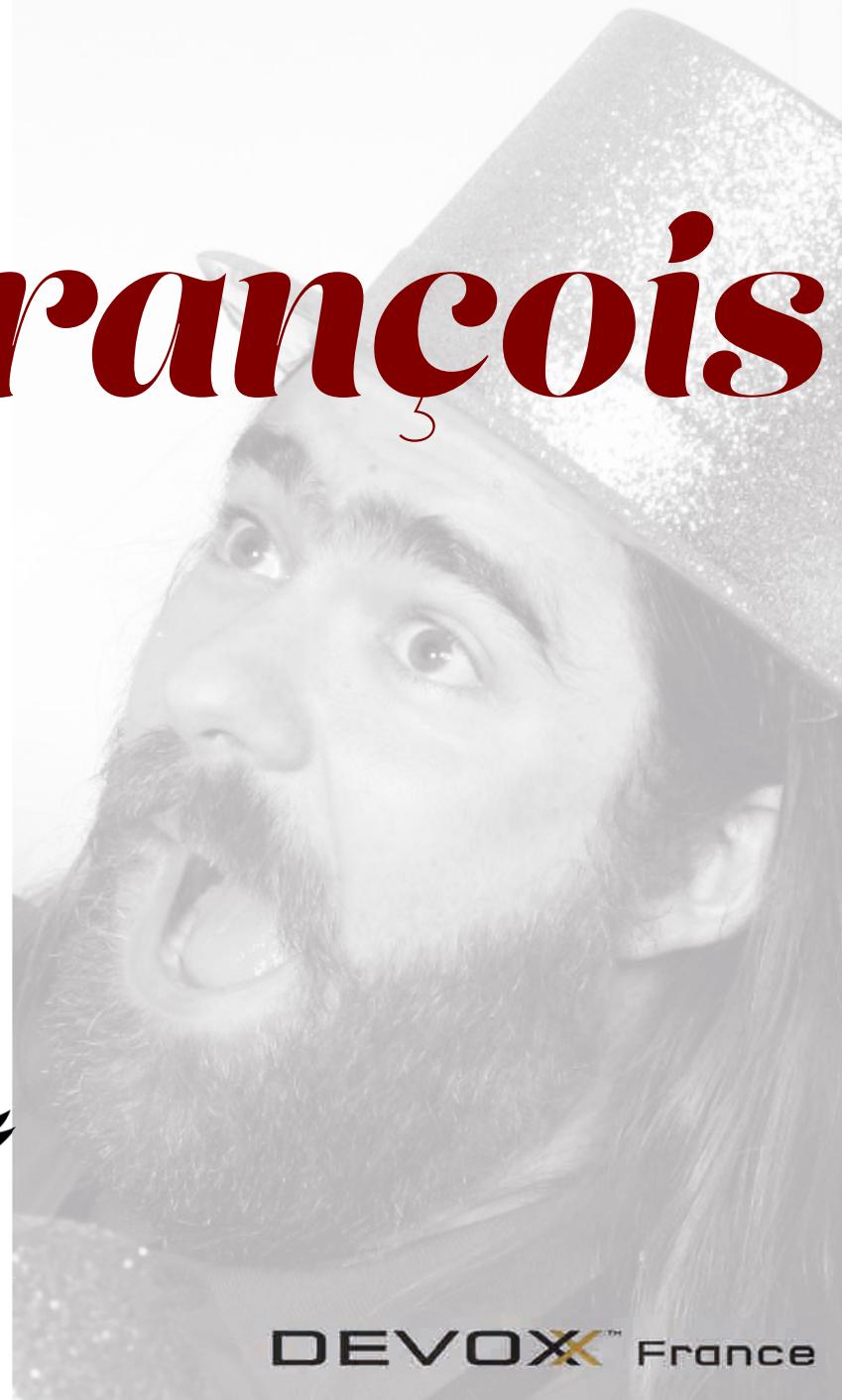




@francoisledroff



François



DEVOX™ France

Un Audit de sécurité ?

- Audit

Non

- ~~Audit ?~~

La Sécurité c'est toi

SEC-UR-IT-Y



Quelles Menaces ?

Threat Modeling

#barbusdevoxx

DEVOXX™ France

Identifier les menaces

STRIDE

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Prioritiser les menaces

DREAD

- *D*amage Potential
- *R*eproducibility
- *E*xloitability
- *A*ffected Users
- *D*iscoverability

Notre Cas d'étude

jHipster



<https://jhipster.github.io/>

Yo jHipster

```
~/workspace/github/devoxx2015 ⌚ 13:51:19
```

```
$ yo jhipster
```

JHipster Generator
JHipster
JHipster Generator
JHipster Generator



Welcome to the JHipster Generator

```
? May JHipster anonymously report usage statistics to improve the tool over time? Yes
? (1/13) What is the base name of your application? barbus
? (2/13) What is your default Java package name? org.devoxx.barbus
? (3/13) Do you want to use Java 8? No (use Java 7)
? (4/13) Which *type* of authentication would you like to use? OAuth2 Authentication (stateless, with an OAuth2 server)
? (5/13) Which *type* of database would you like to use? NoSQL (MongoDB)
? (6/13) Which *production* database would you like to use? MongoDB
? (7/13) Which *development* database would you like to use? MongoDB
? (8/13) Do you want to use Hibernate 2nd level cache? No (this not possible with the NoSQL option)
? (9/13) Do you want to use clustered HTTP sessions? No
? (10/13) Do you want to use WebSockets? No
? (11/13) Would you like to use Maven or Gradle for building the backend? Maven (recommended)
? (12/13) Would you like to use Grunt or Gulp.js for building the frontend? Grunt (recommended)
? (13/13) Would you like to use the Compass CSS Authoring Framework? No
  create package.json
  create bower.json
#DEVOXXFRANCE
```

Spring Security

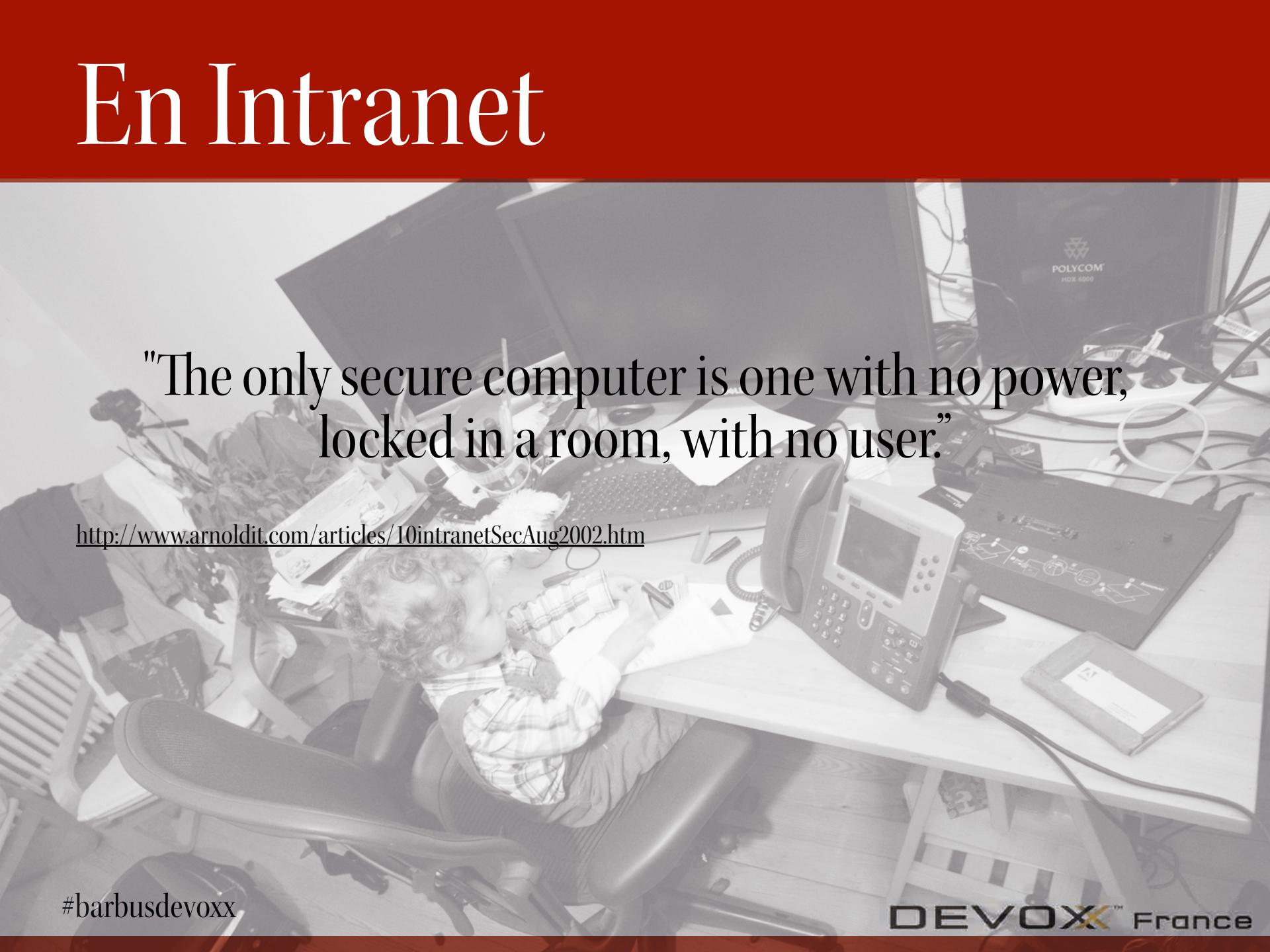
- Various Auth support
 - OAuth1 & OAuth 2
 - SAML
 - Kerberos
 - etc
- Role
- HSTS
- XFrame Option / XSS
- CSRF Protection
- Security Auditor

En Intranet

#barbusdevoxx

DEVOXX™ France

En Intranet



"The only secure computer is one with no power,
locked in a room, with no user."

<http://www.arnoldit.com/articles/10intranetSecAug2002.htm>

Firewall



#barbusdevoxx

Muraille ?
ligne Maginot ?

DEVOX™ France

Reverse Proxy



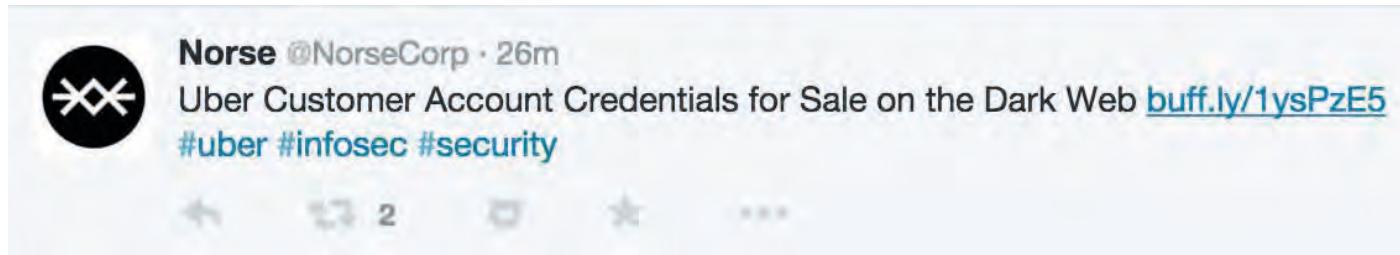
Le grand
nettoyage

#barbusdevoxx

DEVOX™ France

Nos Données

Nos données?



- PII
- Internal
- Confidential
- Restricted

Y a plus qu'à chiffrer

Chiffrer le front

https & SSL c'est bien... mais

- les clefs
 - doivent être
 - protégées
 - longues
 - peuvent être
 - cassées
 - subtilisées
- choisis tes algos
 - Heard of POODLE ?
- les clients
 - de confiance ?

Norse (@NorseCorp) Following
Researchers Find RSA Encryption Keys Duplicated Thousands of Times
buff.ly/1DxFAEk #infosec #security

Jeremiah Grossman (@jeremiahg) Follow
'Google warns of unauthorized TLS cert trusted by almost all OSes'
arstechnica.com/security/2015/... <we're really really gonna need replacement system

Chiffrer le back

- Sécuriser Mongo
 - Authentication
 - Role Based Access Control
 - <https://github.com/jhipster/generator-jhipster/issues/733>
 - Audit
- SSL with Mongo

Mohit Kumar (@unix_root) Follow

40,000 unprotected MongoDB databases, 8 million telecommunication customer records exposed
[thehackernews.com/2015/02/mongod... |](http://thehackernews.com/2015/02/mongod...)

Chiffrage au repos

Chiffrer

- au niveau de l'applicatif
- au niveau du stockage

Auth *Authentification &* *Autorisation*

#barbusdevoxx

DEVOXX™ France

A screenshot of a web browser window titled "barbus". The address bar shows "barbus.et.barbares.com:8080/#/login". The page content is a login form with a red ribbon banner on the left reading "Development".

Authentication

Login

Your login

Password

Your password

Authenticate

You don't have an account
Register a new account

This is your footer

Sign-up as a speaker

Sign-up as speaker for Devoxx FR 2015 CFP and propose one or more subjects.

Sign-up

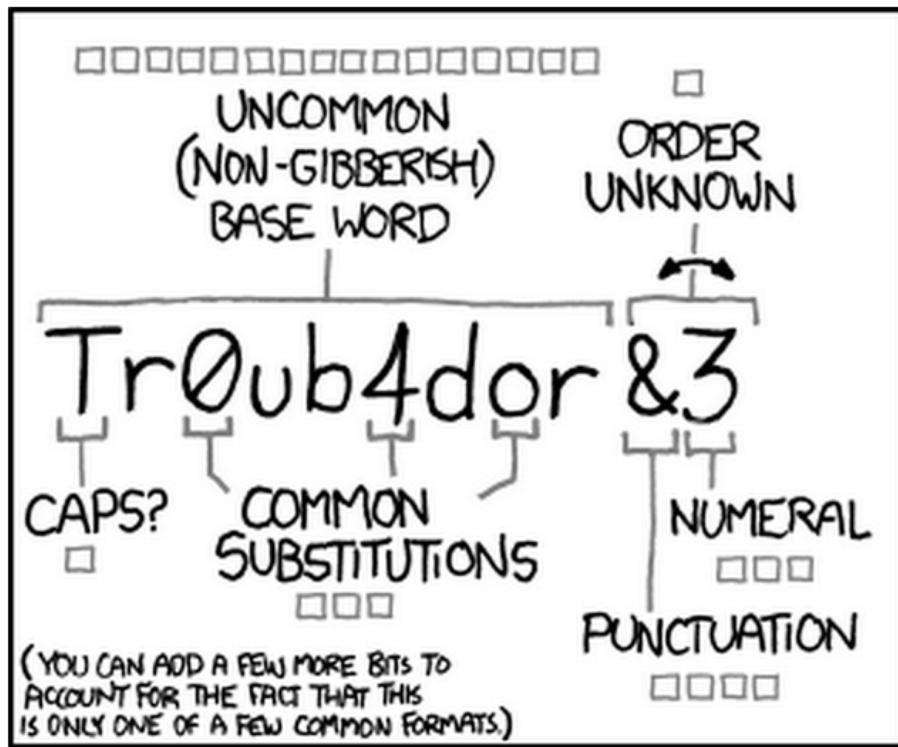
Sign-up with one of your social profile in 5 seconds. No password needed.

Github

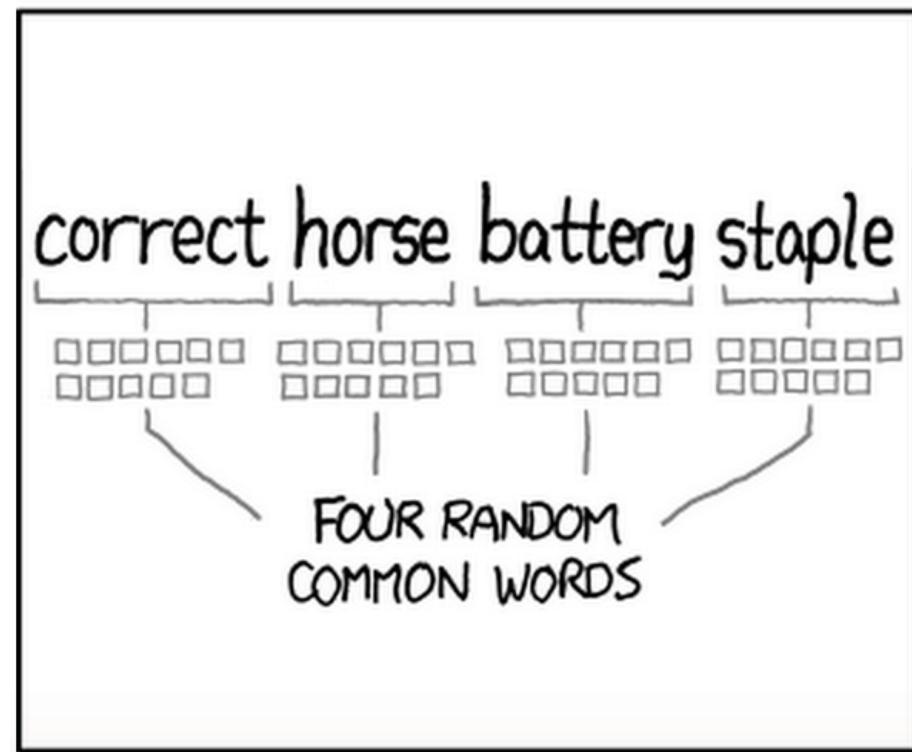
Google

LinkedIn

Votre mot de Passe ?



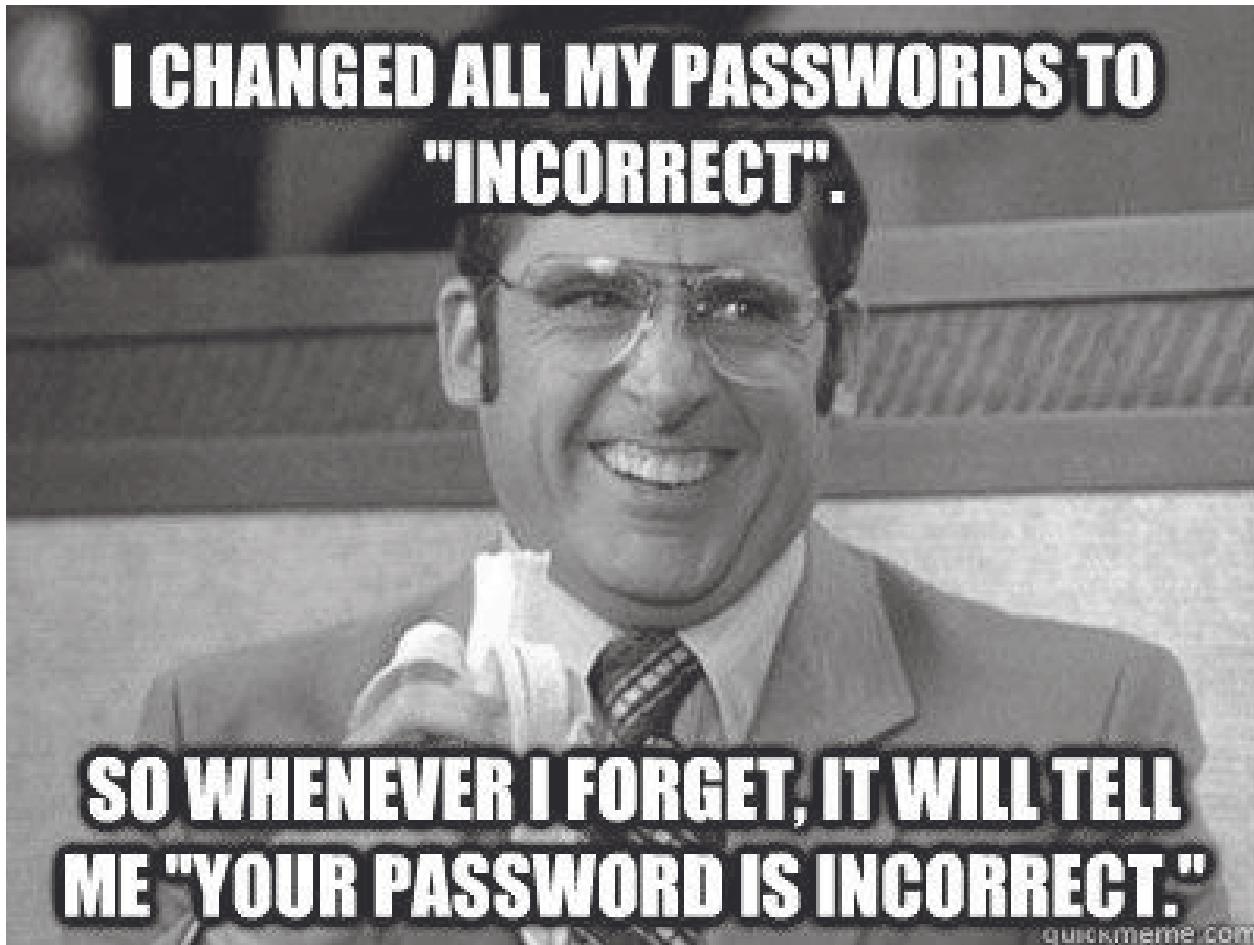
$$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$$



$$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$$

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

1 Mot de Passe ?



**I CHANGED ALL MY PASSWORDS TO
"INCORRECT".**

**SO WHENEVER I FORGET, IT WILL TELL
ME "YOUR PASSWORD IS INCORRECT."**

quickmeme.com

156 mots de passe ?

The screenshot shows a software interface with a sidebar on the left containing icons for 'Files', 'Phone Numbers', 'Serial Numbers', and 'Web Logins'. The 'Web Logins' item is highlighted with a blue bar and has the number '156' displayed next to it. To the right of this sidebar is a vertical list of 156 entries, each preceded by a small globe icon. The entries are:

- postman chrome extension
- puk
- rallydev
- runkeeper
- salesForce
- salesforce poc renault
- sap hx
- sap-d2
- sap-d4
- sap-prod
- sap-s2
- sap-s4
- scoleo.fr
- sedif veoliaeau

1 chien ?



#barbusdevoxx

DEVOXX™ France

Des secrets ?



Norse follows

Cytegic @Cytegic · Mar 2

160,000 #Facebook pages are hacked a day #infosec #privacy
nyp.st/1aGb3bh via @nypost



1



1

...

[View summary](#)



IT Security News @IT_securitynews · Mar 17

Minimizing Damage From J.P. Morgan's Data Breach: How did a mega bank like J.P. Morgan get #hacked? It all... goo.gl/fb/vxIeNv #infosec



...

[View summary](#)



Le Gorafi and 1 other follow

Alexandre Pouchard @AlexPouchard · Feb 23

[View translation](#)

Pourquoi la #NSA et le #GCHQ ont volé des clés de chiffrement de cartes SIM
lemonde.fr/pixels/article... #Gemalto

100%

*100% des attaques en 2014
impliquent des mots de passe dérobés*

<http://www.idtheftcenter.org/>

Notre but :

- N'être qu'un fournisseur de service
- Identifier un fournisseur d'identité, de confiance
- S'y interfaçer

1 IDP ?

Barbus & Barbares devoxx 2015

Barbus & Barbares

Home

Prouve ton identité à travers notre *Identity Provider*

Barbus & Barbares devoxx 2015 - git branch: \${env.GIT_BRANCH} commit: \${env.GIT_COMMIT}

#barbusdevoxx

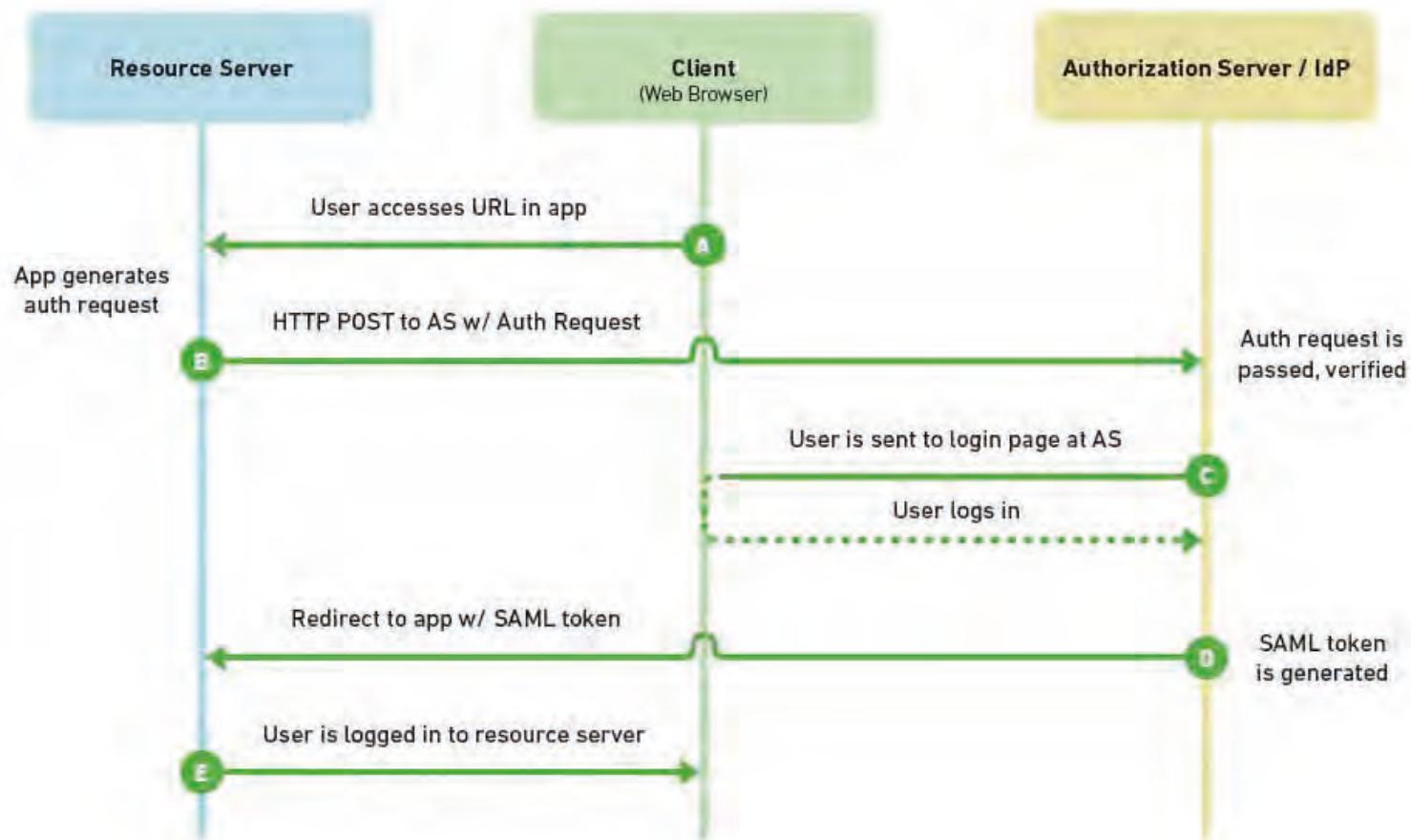
DEVOXX™ France

SAML

- SAML
 - un standard
 - SSO du navigateur
 - <http://www.ssocircle.com>
 - Juste un standard

SAML

SAML 2.0 Flow



SAML & JHipster

- Support dans Spring Security
- Pas de Support dans JHipster
 - #695
 - Francois à quand un PR ?

Click?

A screenshot of a web browser window displaying the homepage of "Barbus & Barbares". The browser interface includes standard controls like back, forward, and search, along with a URL bar showing the address <https://barbus.et.barbares.com/index.html>. The main content area features two profile pictures of men, one with a mustache and one with a beard. The title "Barbus & Barbares" is prominently displayed in large, bold, black font. Below it, a button reads "Prouve ton identité à travers notre *Identity Provider*". At the bottom of the page, a footer note states "Barbus & Barbares devoxx 2015 - git branch: \${env.GIT_BRANCH} commit: \${env.GIT_COMMIT}".

#barbusdevoxx

DEVOXX™ France

Adobe Stage Env - Sign In

https://adobe-stage.okta.com/app/template_saml_2_0/kzancf07QRTJSEYSKJGT/sso/saml

Please sign in below to access Adobe Hub

okta

Sign In

Username: ledroff

Password:

Sign In Remember me

Your security image



Forgot password? | Help

Powered by Okta | Privacy Policy

Adobe Systems Inc - Extra ... * +

https://adobe.okta.com/login/do-login

François Le Droff [Sign Out](#)

Adobe

Enter your text message verification code

Your computer or mobile device has not been verified, or a previous verification has expired.

Need assistance? Call support at 6-4357

Enter code

Remember device



Powered by Okta

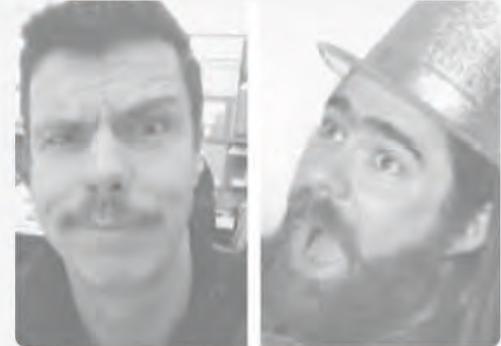
Barbus & Barbares

https://barbus.et.barbares.com/index.html

Search

Home Hub API Account Administration

Barbus & Barbares devoxx 2015



Barbus & Barbares

Home

You are currently logged-in as "ledroff".
[Log out](#)

Barbus & Barbares devoxx 2015 - git branch: \${env.GIT_BRANCH} commit: \${env.GIT_COMMIT}



Michael Neale

@michaelneale



Follow

1. App requires 2FA login. 2. get phone from pants 3. Distracted by 100s of notifications on it 3. Back to computer. Repeat.



Norse

@NorseCorp



Following

Executive Priorities: Balancing Security and Usability bit.ly/1GNBN3x via @Wh1t3Rabbit
#infosec #security





<http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>



francoisaleadroff retweeted



Alain Buzzacaro @abuzzacaro · 24h

"Vous, développeurs, avez une grande responsabilité car les portes d'entrée de la surveillance sont des bugs!" Eric Filiol à #DevoxxFR



17



6



Henri Gomez @hgomez · 3h

"@vinzniv: comment faire une attaque "élaborée" chez #tv5monde ? mots de passe affichés sur mur " cc @JJBourdin_RMC



2FA twofactorauth.org

Category		Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation	
Developer								
 Atail		✓	✓	✓		✓	✓	
 Arbitrake					✗ TELL THEM TO SUPPORT 2FA			
 atech Media		✓				✓	✓	
 Balsamiq					✗ TELL THEM TO SUPPORT 2FA			
 Bitbucket					✗ TELL THEM TO SUPPORT 2FA			
 Cloud9					✗ TELL THEM TO SUPPORT 2FA			
 Code Climate		✓				✓		
 Coverity					✗ TELL THEM TO SUPPORT 2FA			
 Compositional		✓	✓			✓		
 Docker					✗ TELL THEM TO SUPPORT 2FA			
 Erl		✓				✓		
 GitHub		✓	✓			✓		
Finance								
 ASAP					✗ TELL THEM TO SUPPORT 2FA			
 Check Inc					✗ TELL THEM TO SUPPORT 2FA			
 Fintech					✗ TELL THEM TO SUPPORT 2FA			
 HelloWallet					✗ TELL THEM TO SUPPORT 2FA			
 Intuit TurboTax					✗ TELL THEM TO SUPPORT 2FA			
 Kiva					✗ TELL THEM TO SUPPORT 2FA			
 LevelUp					✗ TELL THEM TO SUPPORT 2FA			
 Mint					✗ TELL THEM TO SUPPORT 2FA			
 Ticketmaster		✓				✓		
 Quicken Online					✗ TELL THEM TO SUPPORT 2FA			
Email								
 Hot Mail					✗ TELL THEM TO SUPPORT 2FA			
 FastMail		✓	✓		✓	✓	✓	
 Gmail		✓	✓	✓		✓	✓	
Health								
 3bandMe						✗ TELL THEM TO SUPPORT 2FA		
 antiviro			✓				✓	
 Drug.com						✗ IN PROGRESS		
 HHS.gov						✗ TELL THEM TO SUPPORT 2FA		
 HealthVault (Microsoft Account)			✓	✓			✓	
 myfitnesspal						✗ TELL THEM TO SUPPORT 2FA		
 WebMD						✗ TELL THEM TO SUPPORT 2FA		
 Winklevoss						✗ TELL THEM TO SUPPORT 2FA		
Payments								
 Amazon Payments						✗ TELL THEM TO SUPPORT 2FA		
 BuyCraft		✗	✓	✓			✓	
 Budu						✗ TELL THEM TO SUPPORT 2FA		
 GoCardless						✗ TELL THEM TO SUPPORT 2FA		
 Google Wallet		✓	✓	✓		✓	✓	
 Lilith & Co						✗ TELL THEM TO SUPPORT 2FA		
 Paytometer						✗ THANK THEM FOR WORKING ON 2FA		
 PayPal		✗	✓	✓			✓	
 Skill		✓				✓		
 Skrill						✗ TELL THEM TO SUPPORT 2FA		
Social								
 about.me						✗ TELL THEM TO SUPPORT 2FA		
 App.net		✓					✓	
 Bliby			✗		✓			
 Buffer		✓	✓				✓	
 Facebook		✓	✓	✓			✓	
 Google+		✓	✓	✓		✓	✓	

#barbusdevoxx

DEVOX™ France

SAML2 + OAuth2

- SAML v2
 - enterprise SSO
- OAuth v2
 - Autoriser l'accès à des données, à une API
 - Etablir une chaîne de confiance entre une app et un fournisseur de service

A screenshot of a web browser window titled "Barbus & Barbares". The address bar shows the URL <https://barbus.et.barbares.com/index>. The main content area displays the heading "Barbus & Barbares devoxx 2015" and a large title "oAuth Tokens for [ledroff]". Below this, a table lists OAuth token details:

ClientId	User ID	Scope
ledroff_hub_oauth_client	ledroff@adobe.com	write read

A blue "Revoke" button is located in the bottom right corner of the table row.

Autres options

- OAuth 1.0
- Kerberos
- Radius
- X509 auth
- Combinations of the above
 - including SAML & OAuth 2.0

Intégration Continue

&

Gestion des Secrets

Ségrégation des secrets?

The screenshot shows a GitHub search interface with the query 'secret'. The results are displayed in three sections:

- Code:** Shows a snippet from `src/main/webapp/scripts/components/auth/provider/oauth.oauth2.service.js` containing a JavaScript function with a red box around the word `client_secret`.

```
var data = "username=" + credentials.username + "&password=" + credentials.password + "&grant_type=password&scope=read%20write&" + "client_secret=mySecretOAuthSecret&client_id=barbusapp";
```
- Issues:** Shows a snippet from `src/main/resources/config/application.yml` containing a YAML configuration with a red box around the key `secret`.

```
# security configuration (this key should be unique for your application, and kept secret)
jhipster.security.rememberme.key: Sa57975ee65e8bda3dca253cd835dff90883a19d

messageSource:
cacheSeconds: 1

authentication:
auth:
  clientid: barbusapp
  secret: my SecretOAuthSecret
```
- Search all of GitHub:** Shows a snippet from `src/test/resources/config/application.yml` containing a YAML configuration with a red box around the key `secret`.

```
# security configuration (this key should be unique for your application, and kept secret)
jhipster.security.rememberme.key: Sa57975ee65e8bda3dca253cd835dff90883a19d
```

<https://github.com/francoisledroff/devoxx2015/search?utf8=%E2%9C%93&q=secret>

https://www.google.ie/search?q=%22.git%22+intitle:%22Index+of%22&gws_rd=cr,ssl&ei=hTMRVfHtONbXapDogrgG

#barbusdevoxx

DEVOX™ France

Ségrégation des secrets?



Marco Abis

@capotribu



Follow

My \$2375 Amazon EC2 Mistake
bit.ly/13RfcFI < "my key had been spotted by
a bot that continually searches GitHub for
API keys"

<https://twitter.com/capotribu/status/550079317368381441>

<http://www.devfactor.net/2014/12/30/2375-amazon-mistake/>

Gestion des Secrets

 **Overheard By**
@jtimberman

Managing secrets: still the hardest problem in operations.

2 RETWEETS 8 FAVORITES



8:07 PM - 18 Feb 2015

 Reply to @jtimberman

 **DiggityBiscuits** @grubernaut · Feb 18
@jtimberman doing it well is the biggest secret

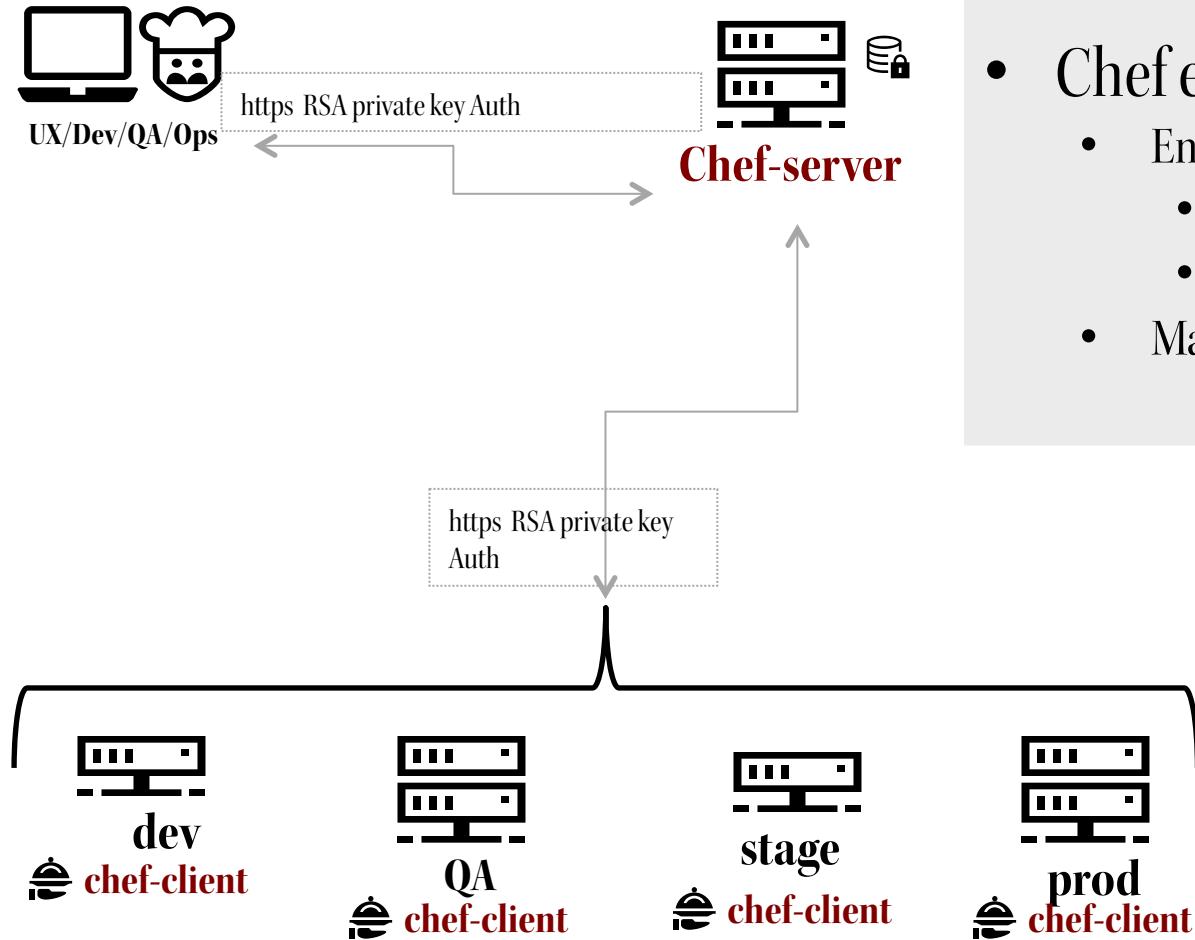
1 RETWEET 1 FAVORITE

<https://twitter.com/jtimberman/status/568124542553423872>

#barbusdevoxx

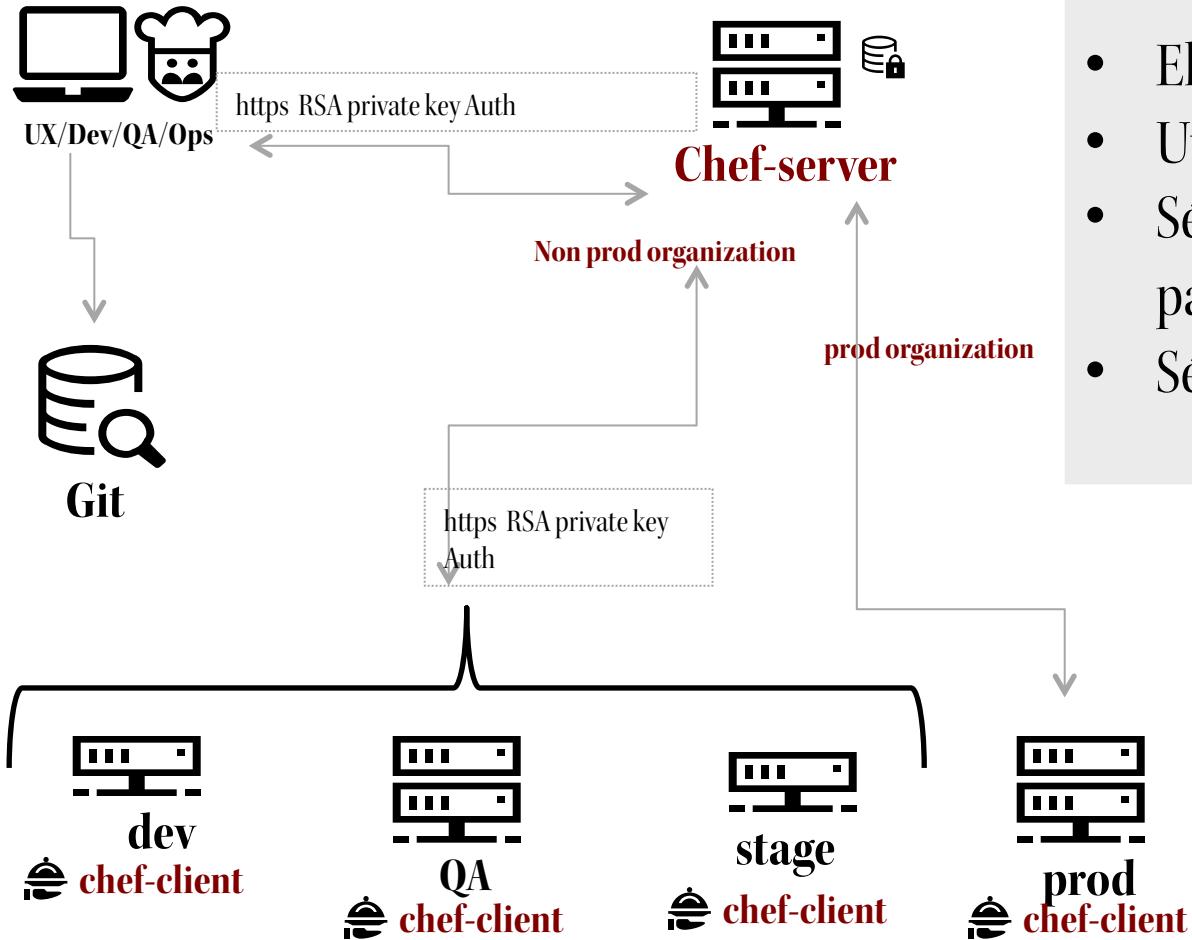
DEVOX™ France

Chef-vault



- Chef encrypted data bags
 - Encrypted for
 - admin users
 - whitelisted nodes
 - Managed by **chef-vault ruby gem**

Chef-vault ?



- Elasticité ?
- Utiliser des repo git privés ?
- Ségrégation de la production par organisation ?
- Sécuriser le Chef Server

Jenkins sécurisé

- Sécurise tes jenkins
 - SAML est aussi une option
- Cloudbees
- Automatise
 - *Short live*



Jean-Laurent Morlhon

@morlhon

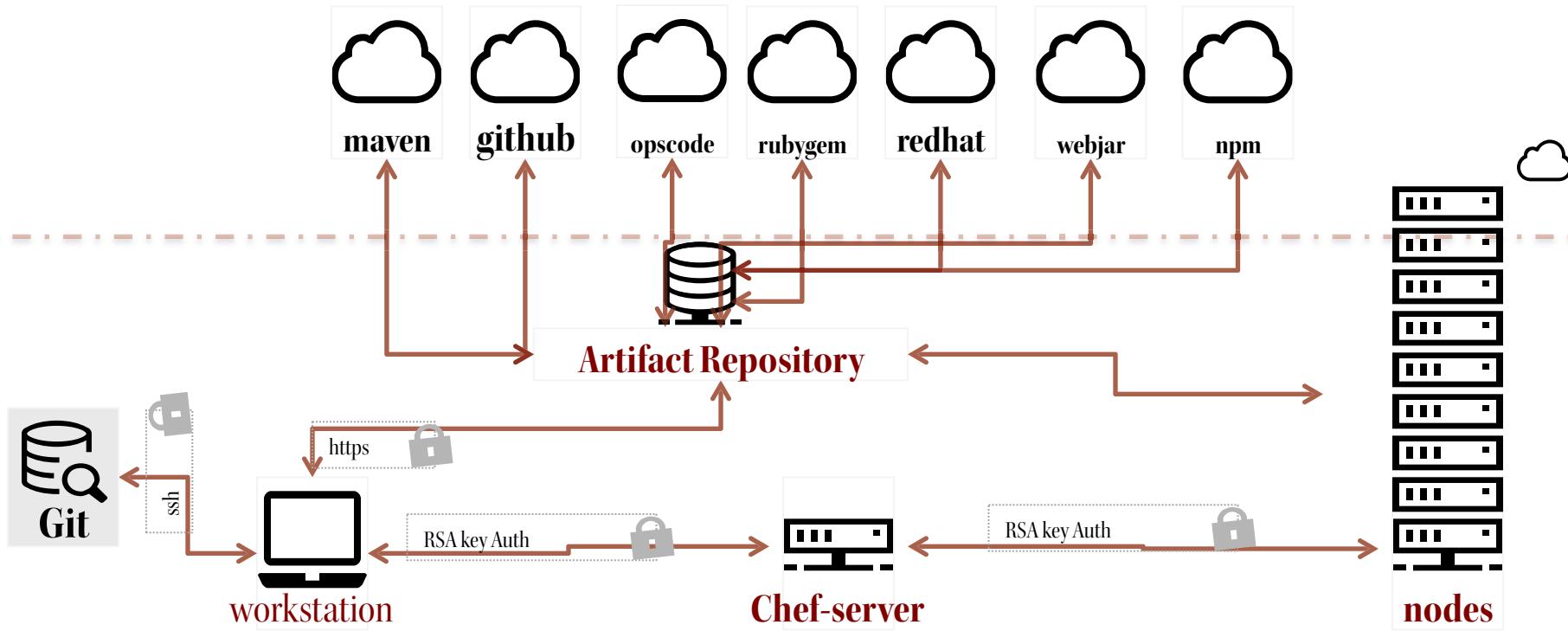


Following

A must-read : [@paulgreg](#): interesting slide on security of your webapp "DevOoops" by [@carnalOwnage](#) #devops #hacking [slideshare.net/chrisgates/las...](#)"

<https://twitter.com/morlhon/status/554899543150850048>

Gestion sécurisée des dépendances

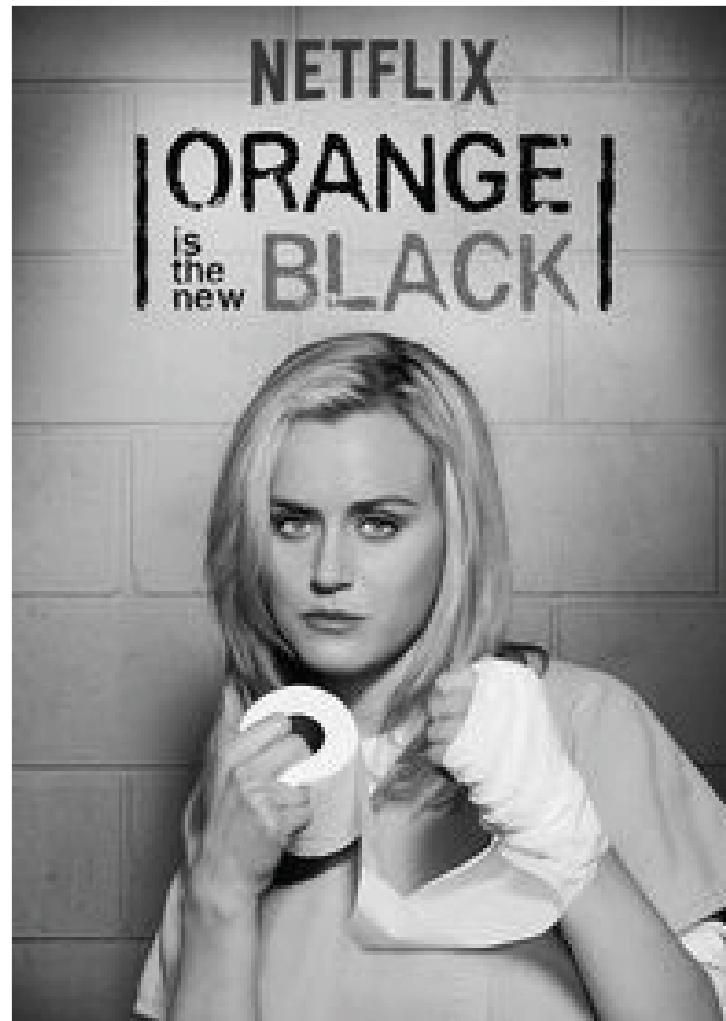




Et le Cloud ?



DEVOX France



Prêt à te faire hacker?

Allo les pompiers ?

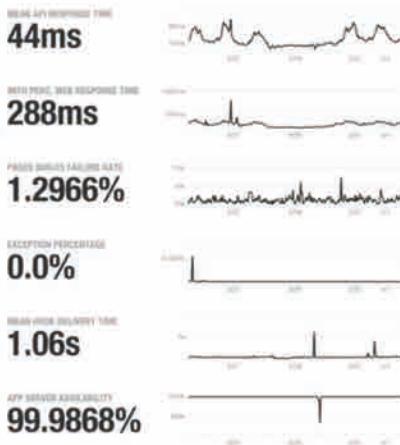


GitHub Status @githubstatus · Mar 26
We are currently experiencing some minor service outages.

Olivier Bazoud and 8 others follow

GitHub Status @githubstatus · Mar 27
We are investigating increased error rates as an incoming DDoS amplifies their attack.

Rewritten 483 times.
GitHub Status @githubstatus · 13h
After 113 hours of sustained DDoS attacks our defenses are holding. We will keep our status at yellow until the threat has subsided.



#barbusdevoxx

DEVOX™ France

Y a la maison qui brûle



#barbusdevoxx

Détecteur de fumée

- HSM
- IDS
- Porte coupe-feu
- SELinux
- SecurityManager

De DevOps à DevSec



#barbusdevoxx

DEVOXX™ France

Ce qu'il fallait retenir

Ce qu'il fallait retenir

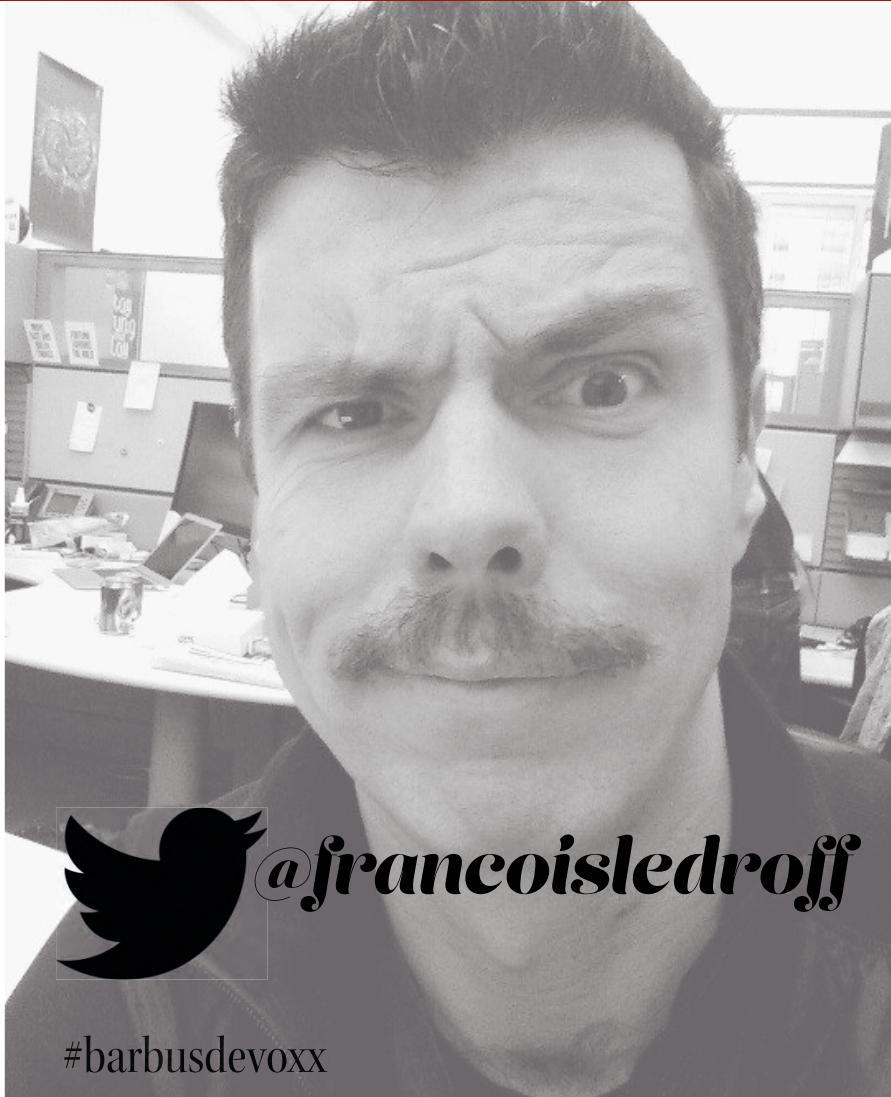
- La sécurité c'est toi
- Penses-y
- T'es jamais à l'abri
 - tes données non plus
- Gère tes secrets
- Passe à l'authentication forte

Ce qu'il fallait retenir

- l'expérience utilisateur n'est pas un prétexte pour une mauvaise sécurité
- n'oublie pas l'extension du domaine de la lutte
- traite tes serveurs comme du bétail
- sois prêt(e) à combattre le feu

Des questions ? Vraiment ?

Pourtant c'était clair non ?



@francoisledroff

#barbusdevoxx



@rpelisse

DEVOXX™ France