
Barbus
&
Barbares
#barbusdevoxx
DEVOXX France

Romain

@rpelisse

DEVOXX France

François

@francoisledroff

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

- **S**poofing Identity
- **T**ampering with Data
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

Prioritiser les menaces

DREAD

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability

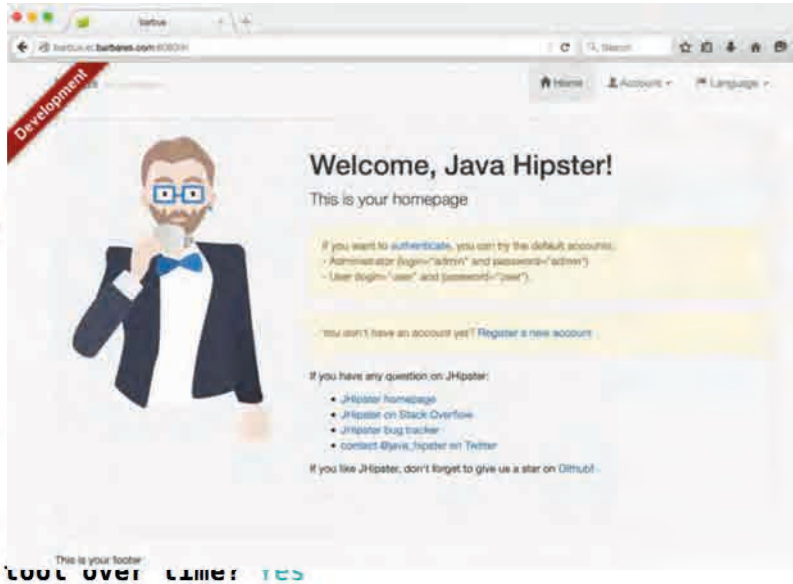
Notre Cas d'étude

jHipster

https://jhipster.github.io/

Yo jHipster

```
~/workspace/github/devoxx2015 13:51:19
$ yo jhipster
```




```
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
```

Spring Security

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

En Intranet

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

Muraille ?

ligne Maginot ?

Reverse Proxy

Le grand nettoyage

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 ?

Chiffrer le back

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

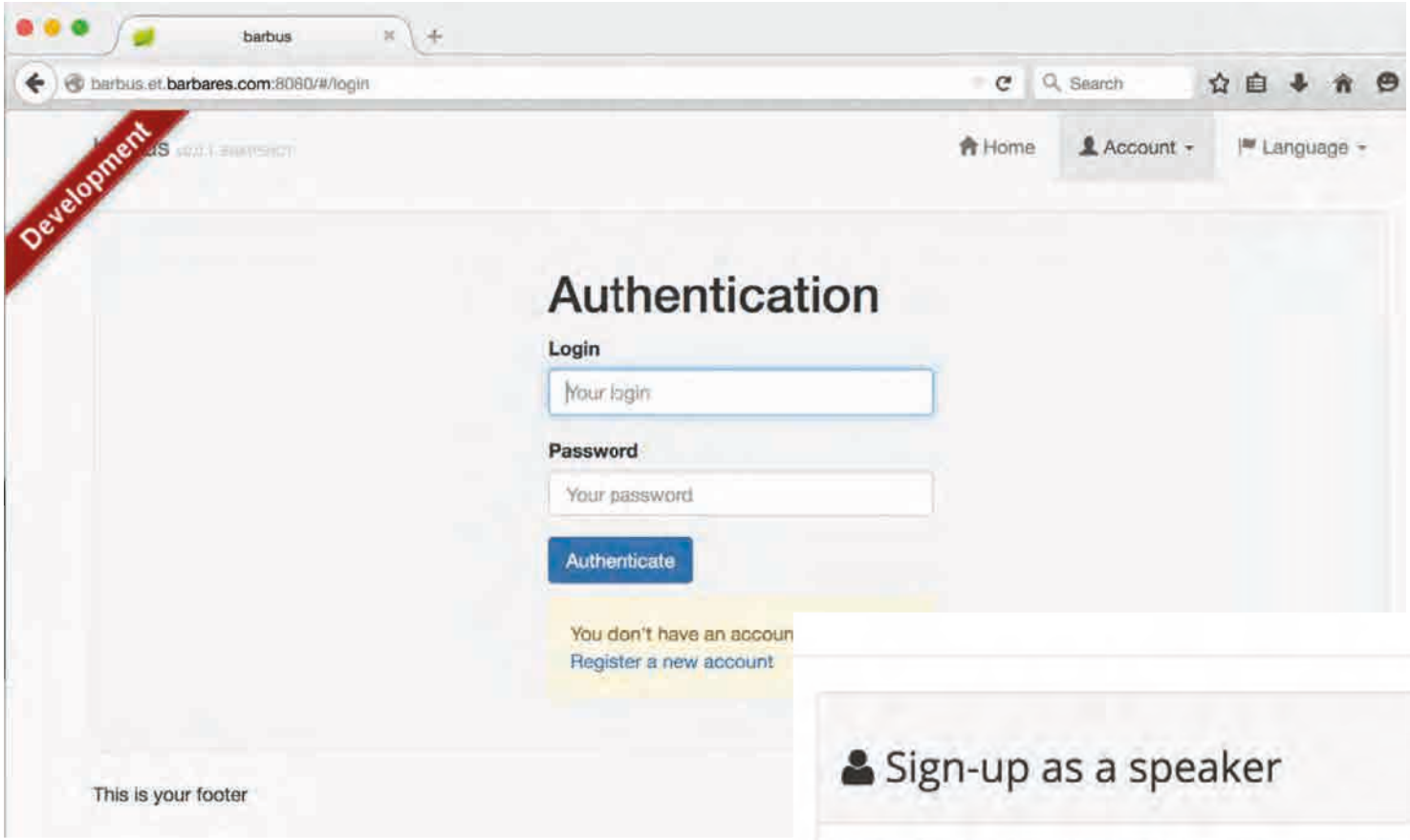
Chiffrage au repos

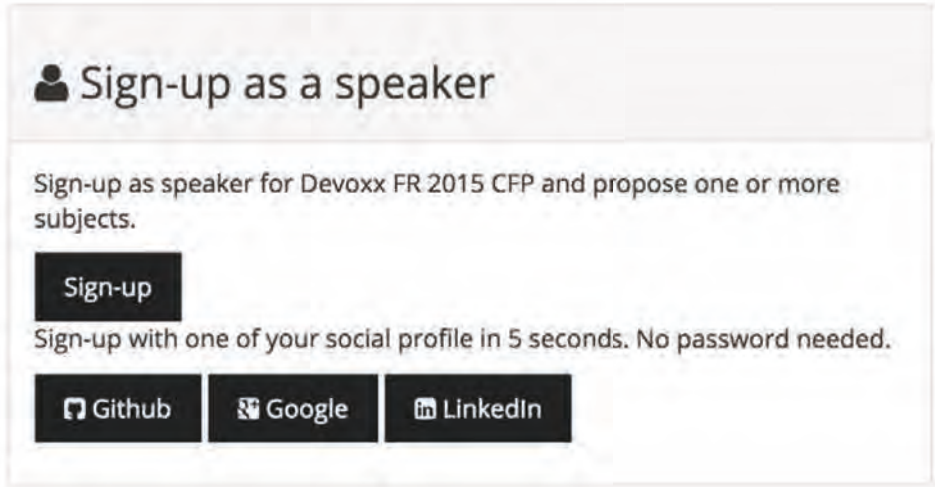
Chiffrer

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

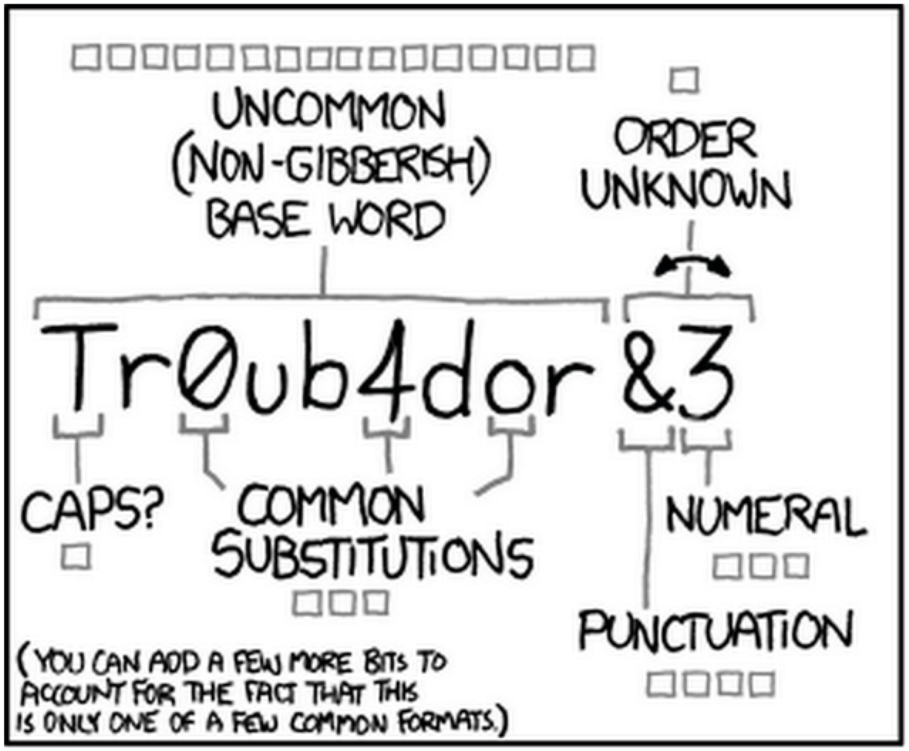
Auth

Authentification & Autorisation

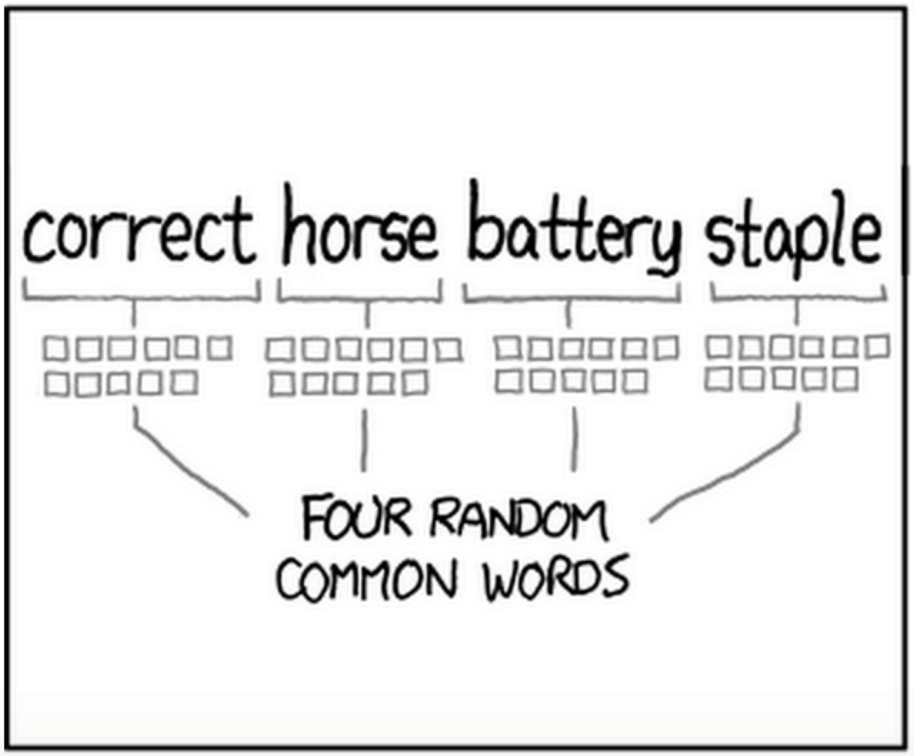

barbus
barbus.et.barbares.com:8080/#/login
Search
Development
Home
Account
Language
Authentication
Login
Your login
Password
Your password
Authenticate
You don't have an accoun
Register a new account
This is your footer


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 DAYS AT 1000 GUESSES/SEC



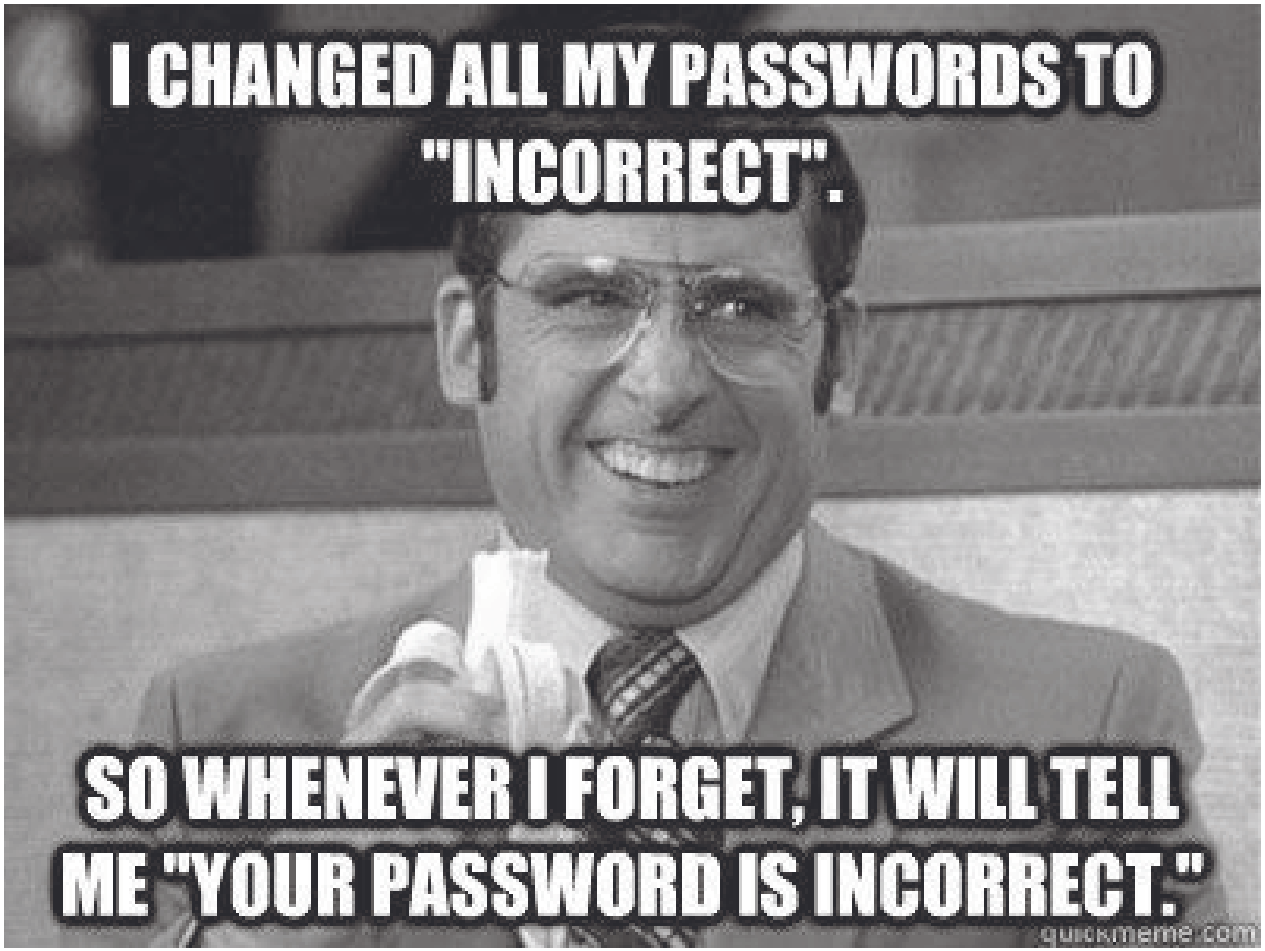
2^{44} = 550 YEARS AT 1000 GUESSES/SEC

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.

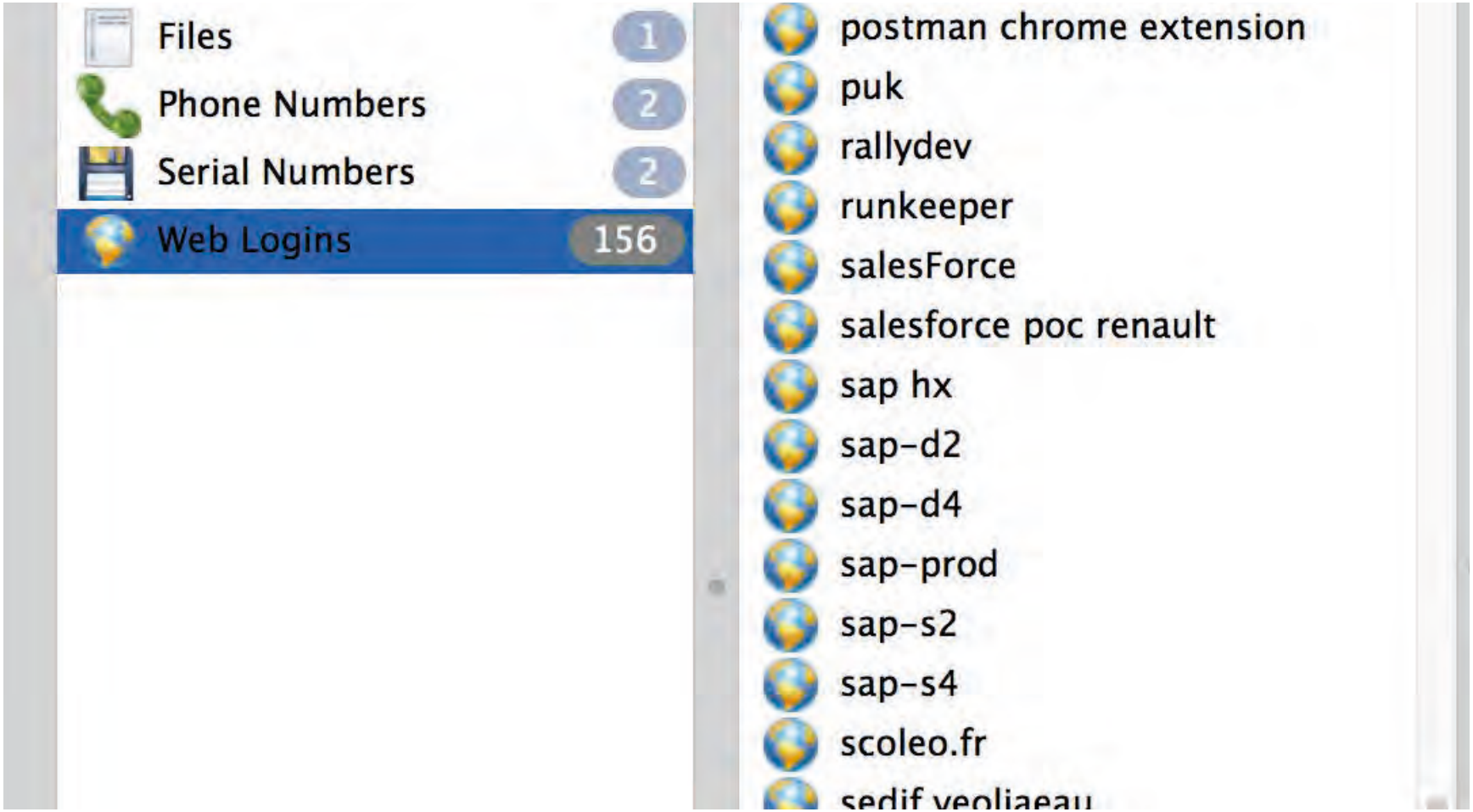
http://xkcd.com/936/

#barbusdevoxx

1 Mot de Passe ?



156 mots de passe ?



1 chien ?

#barbusdevoxx

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/vxleNv **#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%

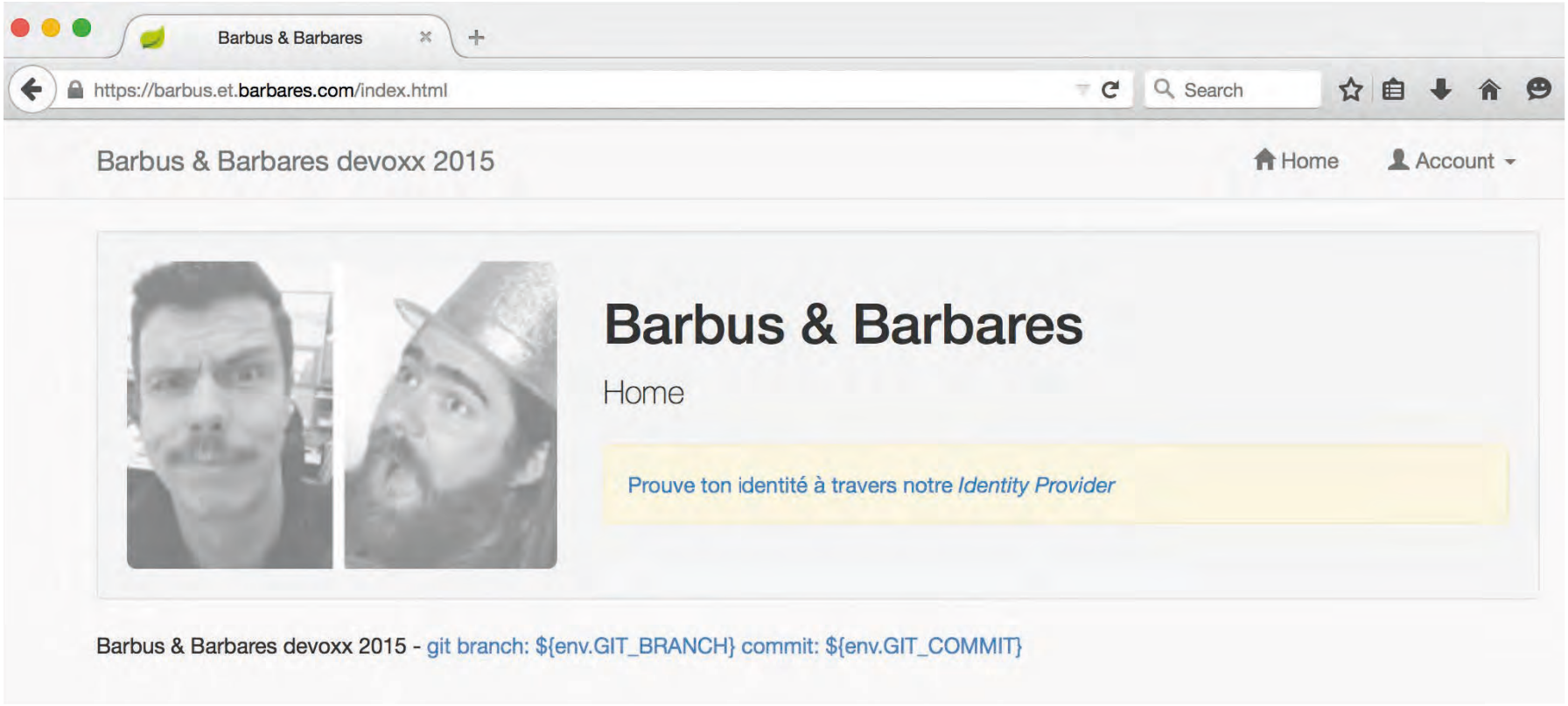
100% des attaques en 2014
impliquent des mots de passe dérobés

http://www.idtheftcenter.org/

Notre but :

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

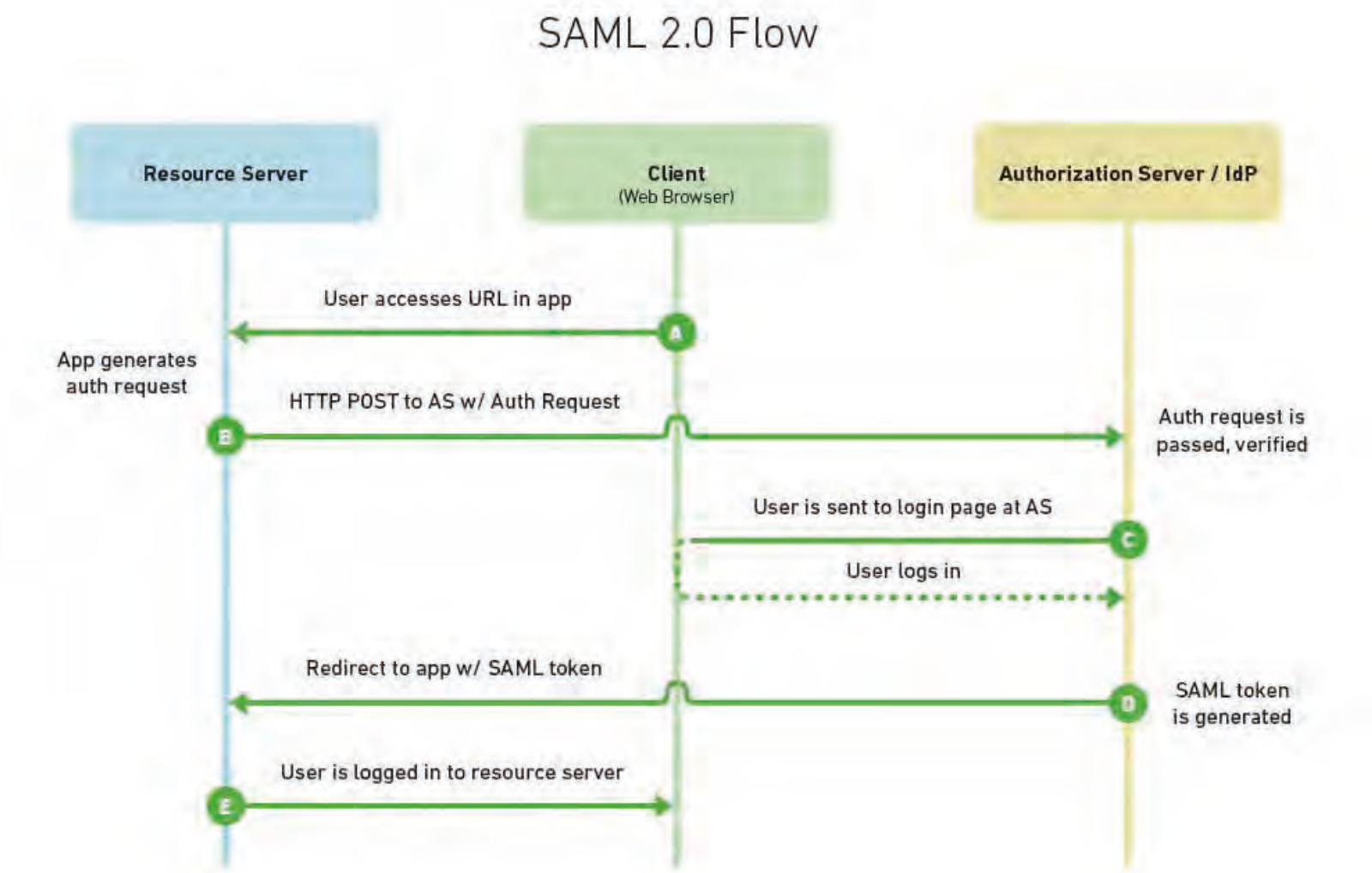
1 IDP ?


Barbus & Barbares
https://barbus.et.barbares.com/index.html
Search
Barbus & Barbares devoxx 2015
Home
Account
Barbus & Barbares
Home
Prouve ton identité à travers notre *Identity Provider*
Barbus & Barbares devoxx 2015 - git branch: ${env.GIT_BRANCH} commit: ${env.GIT_COMMIT}

SAML

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

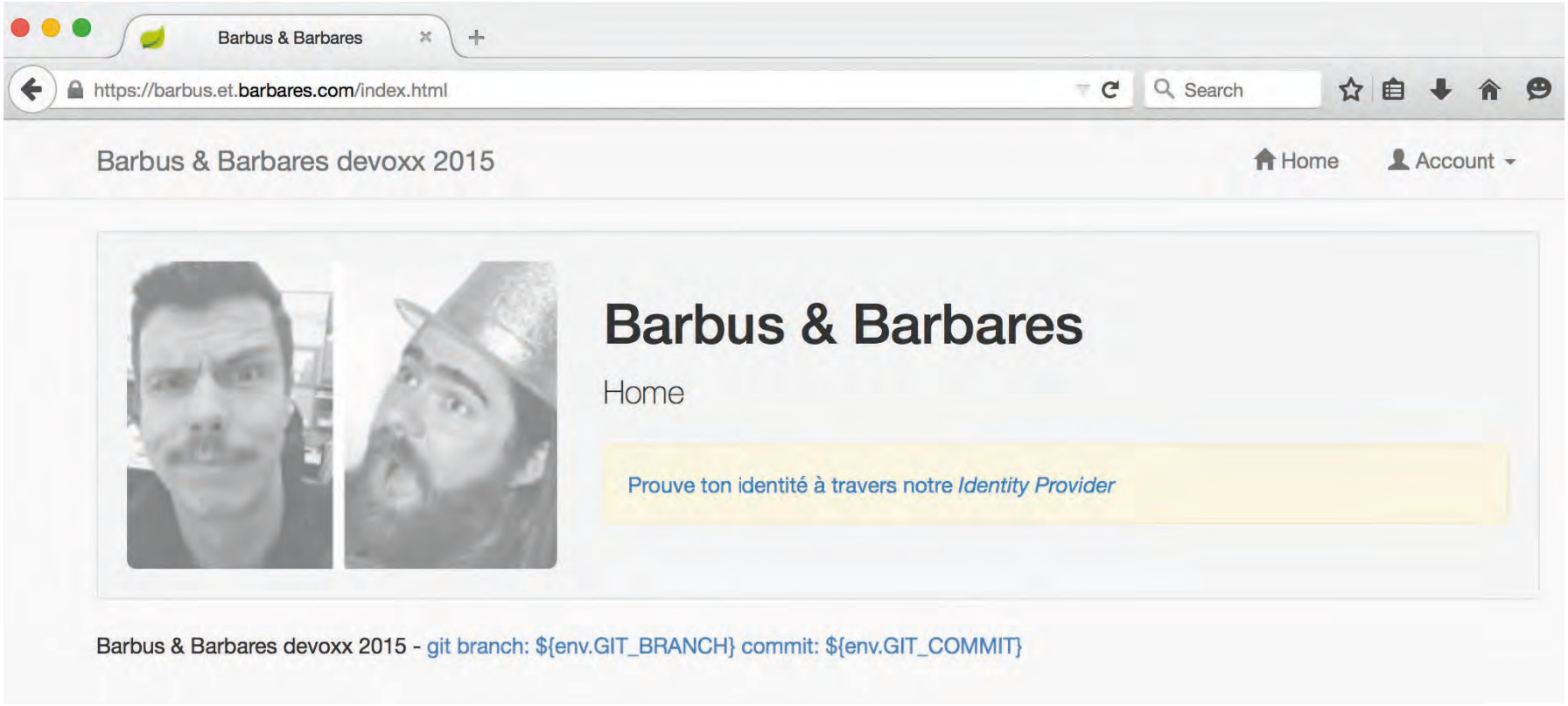
SAML


SAML 2.0 Flow
Resource Server
Client
(Web Browser)
Authorization Server / IdP
User accesses URL in app
A
App generates
auth request
HTTP POST to AS w/ Auth Request
B
Auth request is
passed, verified
User is sent to login page at AS
C
User logs in
Redirect to app w/ SAML token
D
SAML token
is generated
User is logged in to resource server
E

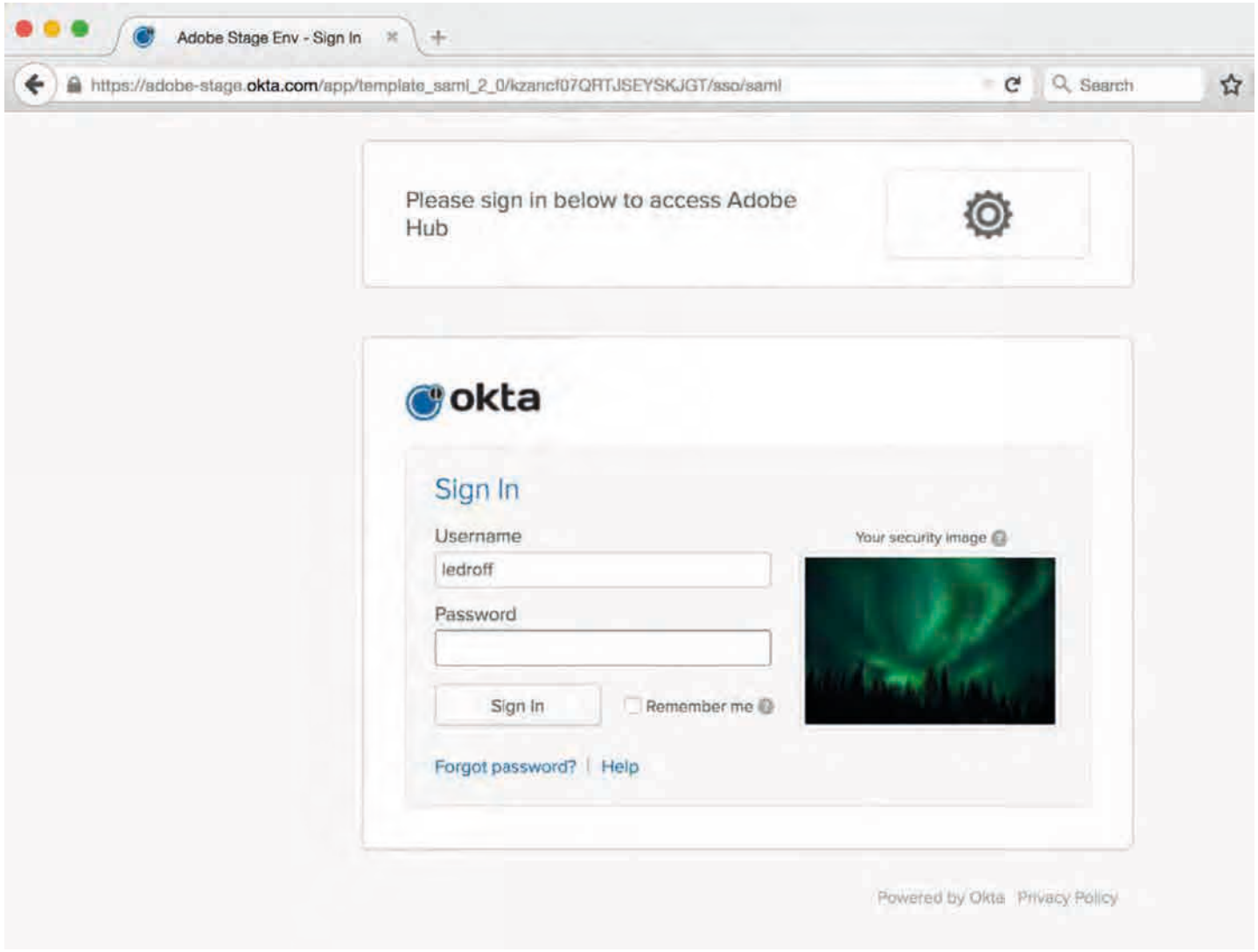
SAML & JHipster

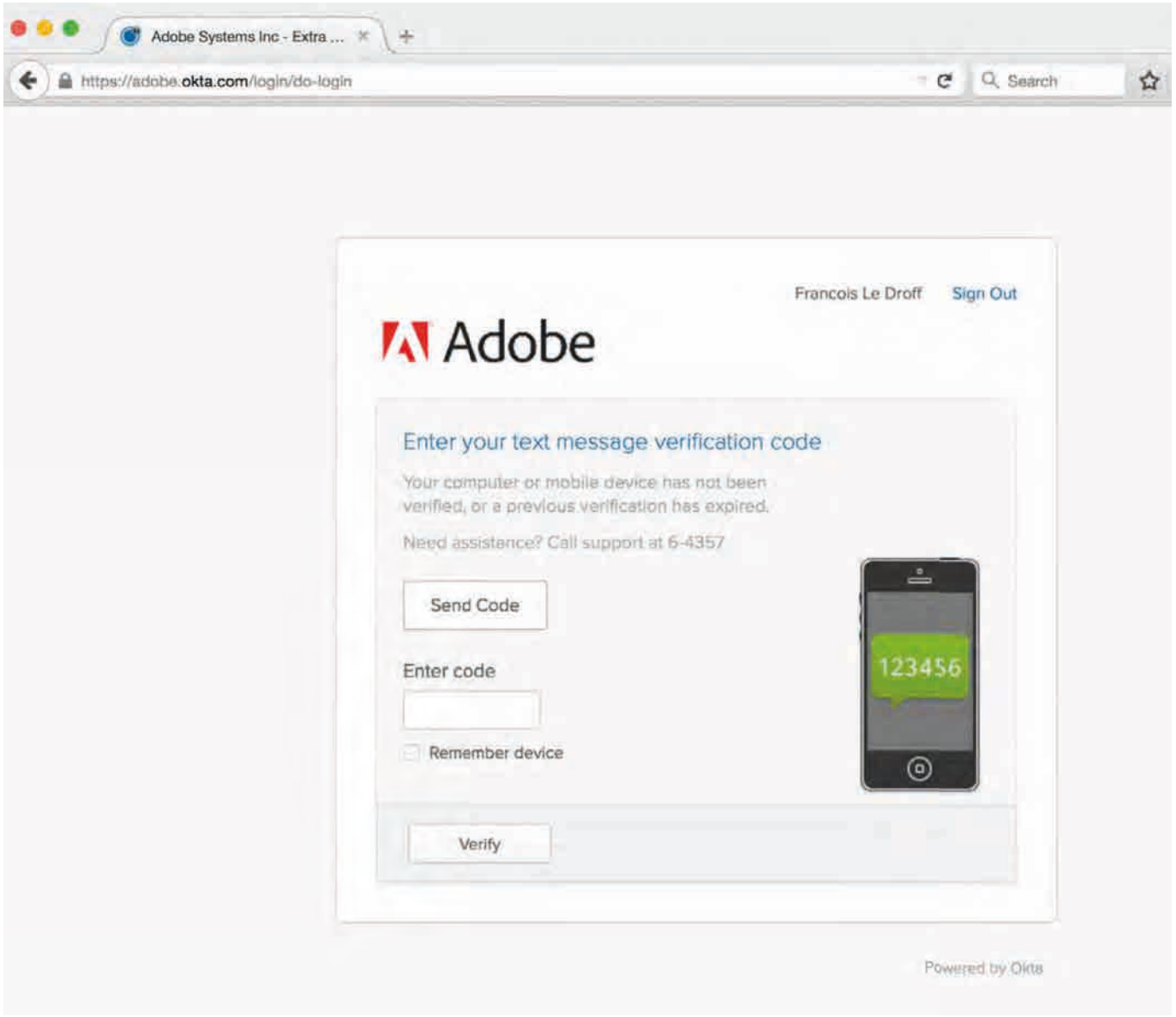
- Support dans Spring Security
- Pas de Support dans JHipster
  - #695
  - Francois à quand un PR ?

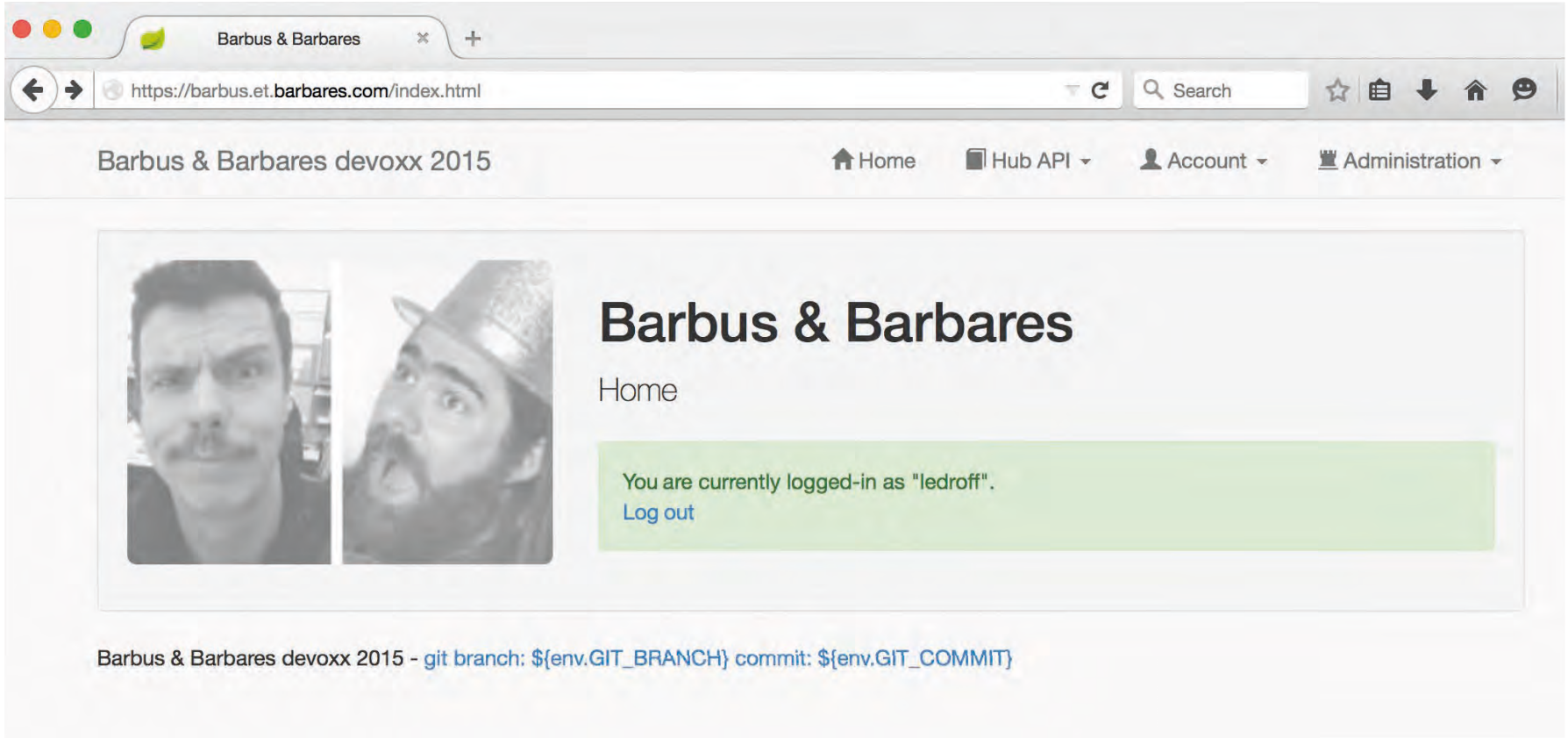
Click?



#barbusdevoxx


Adobe Stage Env - Sign In
https://adobe-stage.okta.com/app/template_saml_2_0/kzancf07QRTJSEYSKJGT/sso/saml
Search
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
Search
Francois 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
Send Code
Enter code
Remember device
123456
Verify
Powered by Okta


Barbus & Barbares
https://barbus.et.barbares.com/index.html
Search
Barbus & Barbares devoxx 2015
Home
Hub API
Account
Administration
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/

francojaledroff retweeted

Alain Buzzacaro @abuzzacaro · 24h

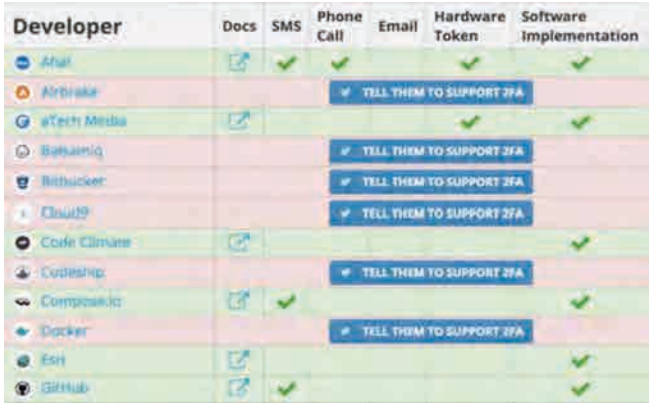
"Vous, développeurs, avez une grande responsabilité car les portes d'entrée de la surveillance sont des bugs!" Eric Filiol à #DevoxxFR

17 6

Henri Gomez ♻ @hgomez · 3h

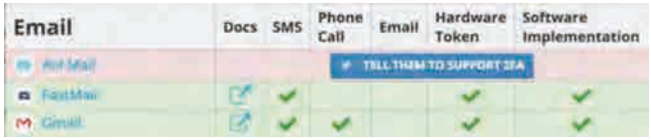
"@vinzniv: comment faire une attaque "élaborée" chez #tv5monde ? mots de passe affichés sur mur " cc @JJBourdin_RMC

2FA twofactorauth.org

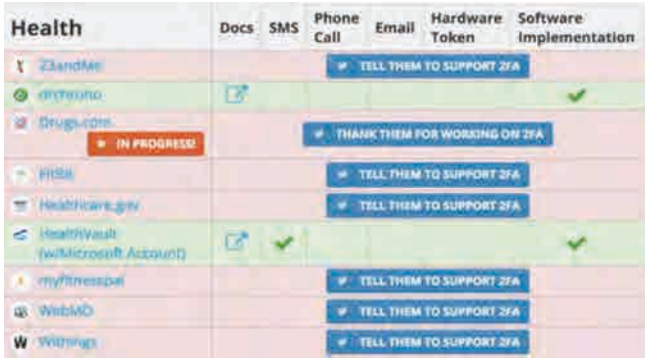


Developer	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
Abal	✓	✓	✓		✓	✓
Airbrake			TELL THEM TO SUPPORT 2FA			
aTech Media	✓				✓	✓
Balsamiq			TELL THEM TO SUPPORT 2FA			
Bitbucket			TELL THEM TO SUPPORT 2FA			
Cloud9			TELL THEM TO SUPPORT 2FA			
Code Climate	✓					✓
Codeship			TELL THEM TO SUPPORT 2FA			
Composer.io	✓	✓				✓
Docker			TELL THEM TO SUPPORT 2FA			
Esh	✓					✓
GitHub	✓	✓				✓

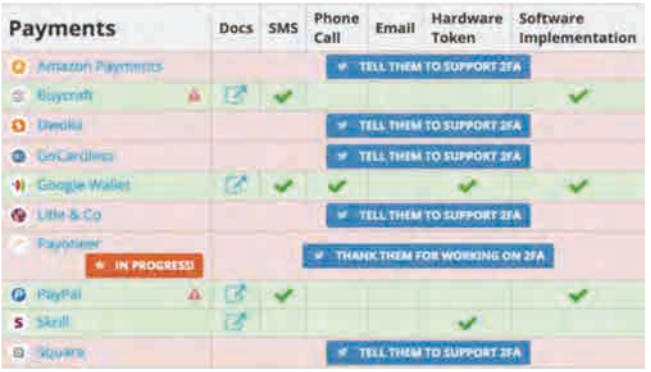
Finance	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
ADP			TELL THEM TO SUPPORT 2FA			
Check Inc			TELL THEM TO SUPPORT 2FA			
FreeAgent			TELL THEM TO SUPPORT 2FA			
HelloWallet			TELL THEM TO SUPPORT 2FA			
Intuit TurboTax			TELL THEM TO SUPPORT 2FA			
Kiva			TELL THEM TO SUPPORT 2FA			
LevelUp			TELL THEM TO SUPPORT 2FA			
Mint			TELL THEM TO SUPPORT 2FA			
Pocketsmith	✓					✓
Quickbooks Online			TELL THEM TO SUPPORT 2FA			



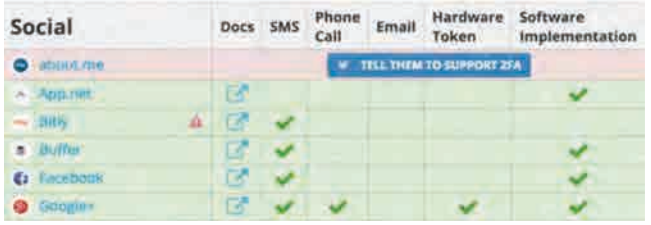
Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
Aol Mail			TELL THEM TO SUPPORT 2FA			
FastMail	✓	✓			✓	✓
Gmail	✓	✓	✓		✓	✓



Health	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
23andMe			TELL THEM TO SUPPORT 2FA			
Anthem	✓					✓
Drugs.com			THANK THEM FOR WORKING ON 2FA			
IN PROGRESS!						
Fitbit			TELL THEM TO SUPPORT 2FA			
Healthcare.gov			TELL THEM TO SUPPORT 2FA			
HealthVault (w/Microsoft Account)	✓	✓				✓
myfitnesspal			TELL THEM TO SUPPORT 2FA			
WebMD			TELL THEM TO SUPPORT 2FA			
Withings			TELL THEM TO SUPPORT 2FA			



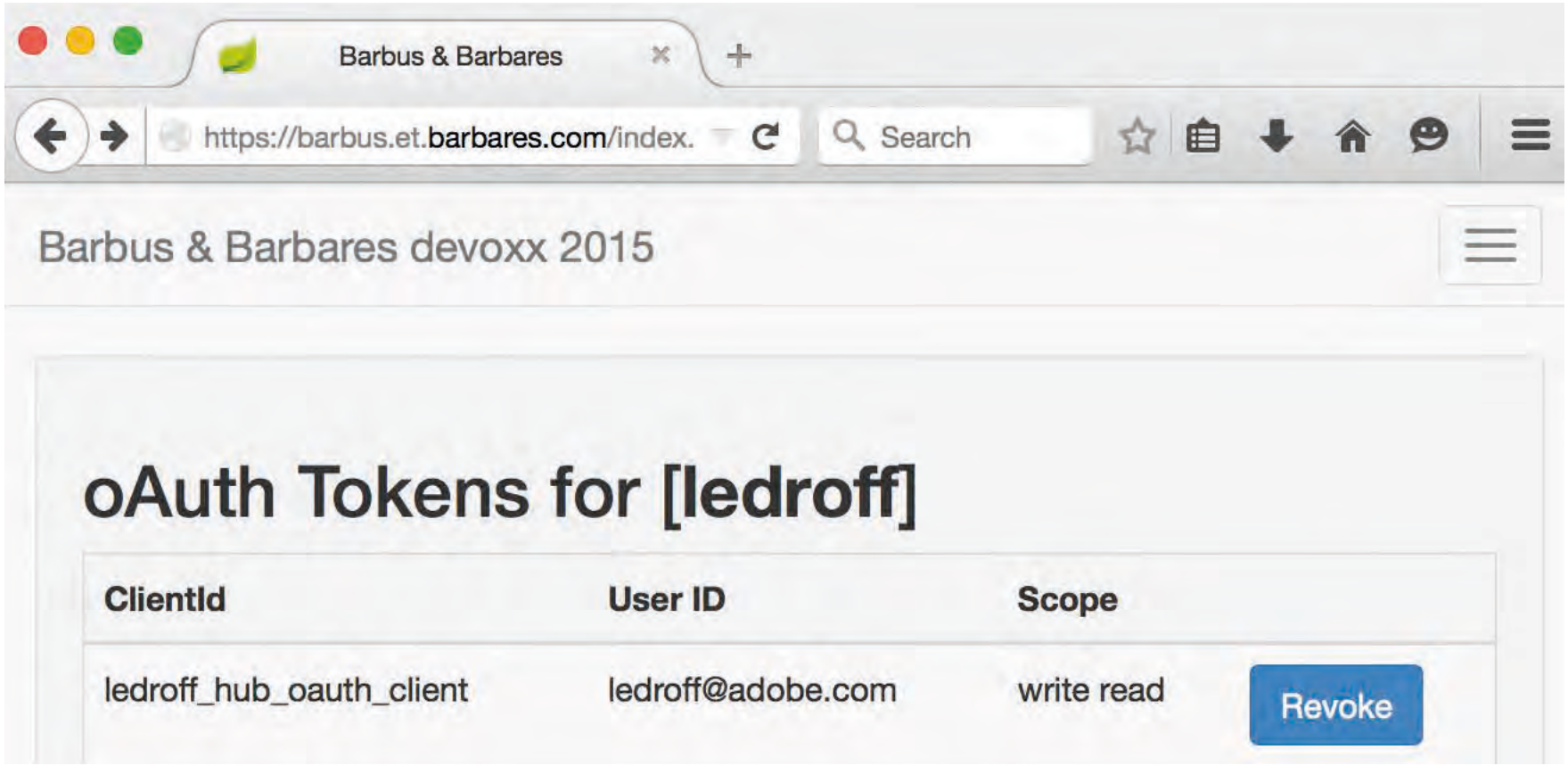
Payments	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
Amazon Payments			TELL THEM TO SUPPORT 2FA			
Buycraft	✓	✓				✓
Dwolla			TELL THEM TO SUPPORT 2FA			
GoCardless			TELL THEM TO SUPPORT 2FA			
Google Wallet	✓	✓	✓		✓	✓
Little & Co			TELL THEM TO SUPPORT 2FA			
Payoneer			THANK THEM FOR WORKING ON 2FA			
IN PROGRESS!						
PayPal	✓	✓				✓
Skrill	✓				✓	
Square			TELL THEM TO SUPPORT 2FA			



Social	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
about.me			TELL THEM TO SUPPORT 2FA			
App.net	✓					✓
Bitly	✓	✓				
Buffer	✓	✓				✓
Facebook	✓	✓				✓
Google+	✓	✓	✓		✓	✓

SAML2 + OAuth2

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

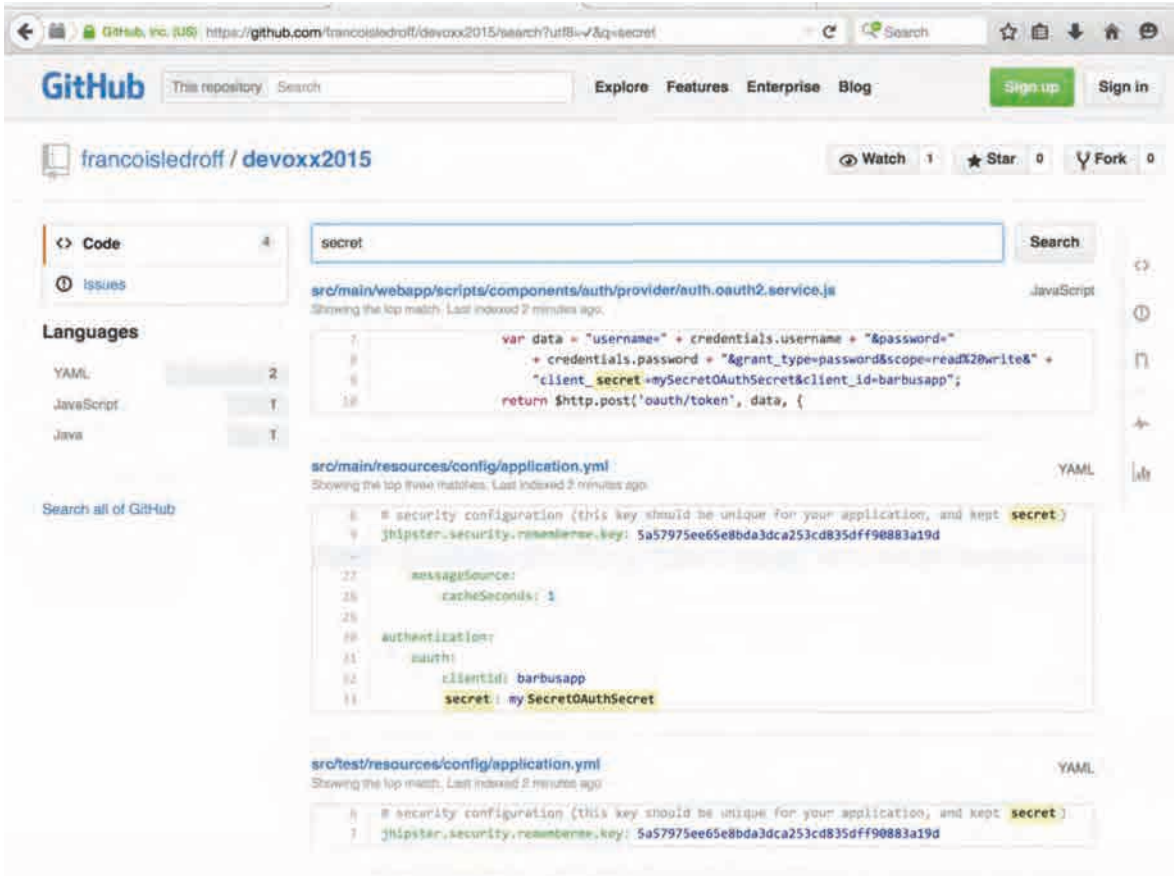

Barbus & Barbares
https://barbus.et.barbares.com/index.
Search
Barbus & Barbares devoxx 2015
oAuth Tokens for [ledroff]
ClientId
User ID
Scope
ledroff_hub_oauth_client
ledroff@adobe.com
write read
Revoke

Autres options

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

Intégration Continue
&
Gestion des Secrets

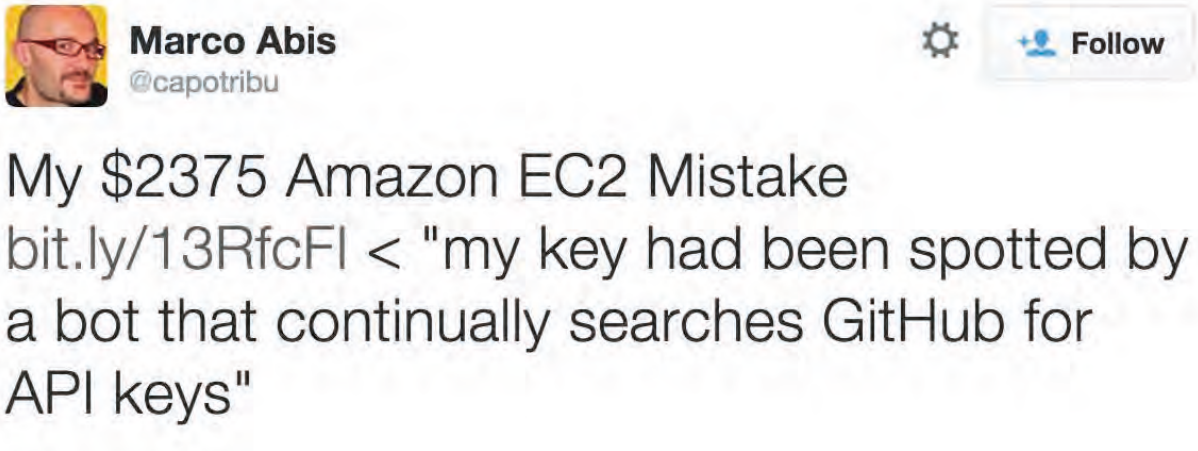
Ségrégation des secrets?



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

Ségrégation des secrets?



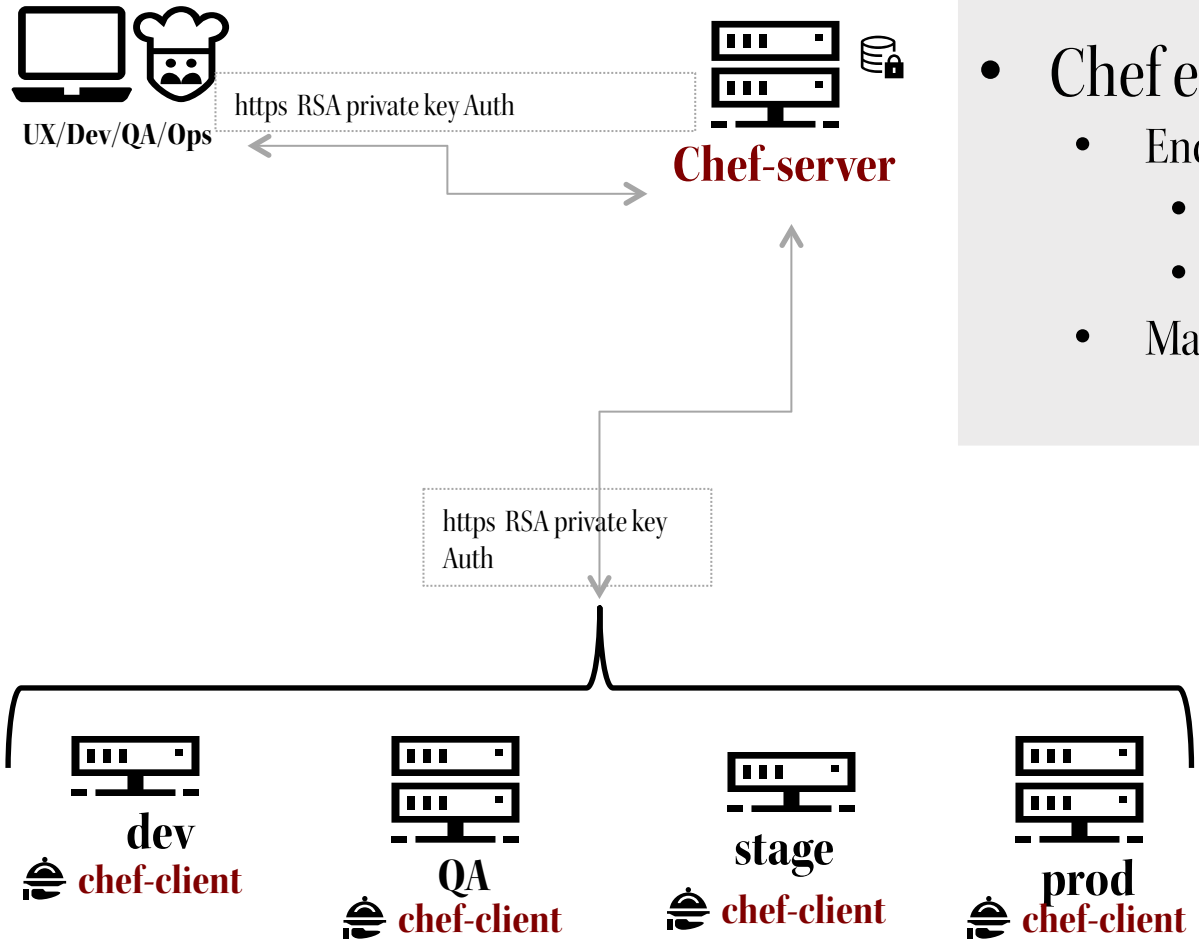
https://twitter.com/capotribu/status/550079317368381441
http://www.devfactor.net/2014/12/30/2375-amazon-mistake/

Gestion des Secrets

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

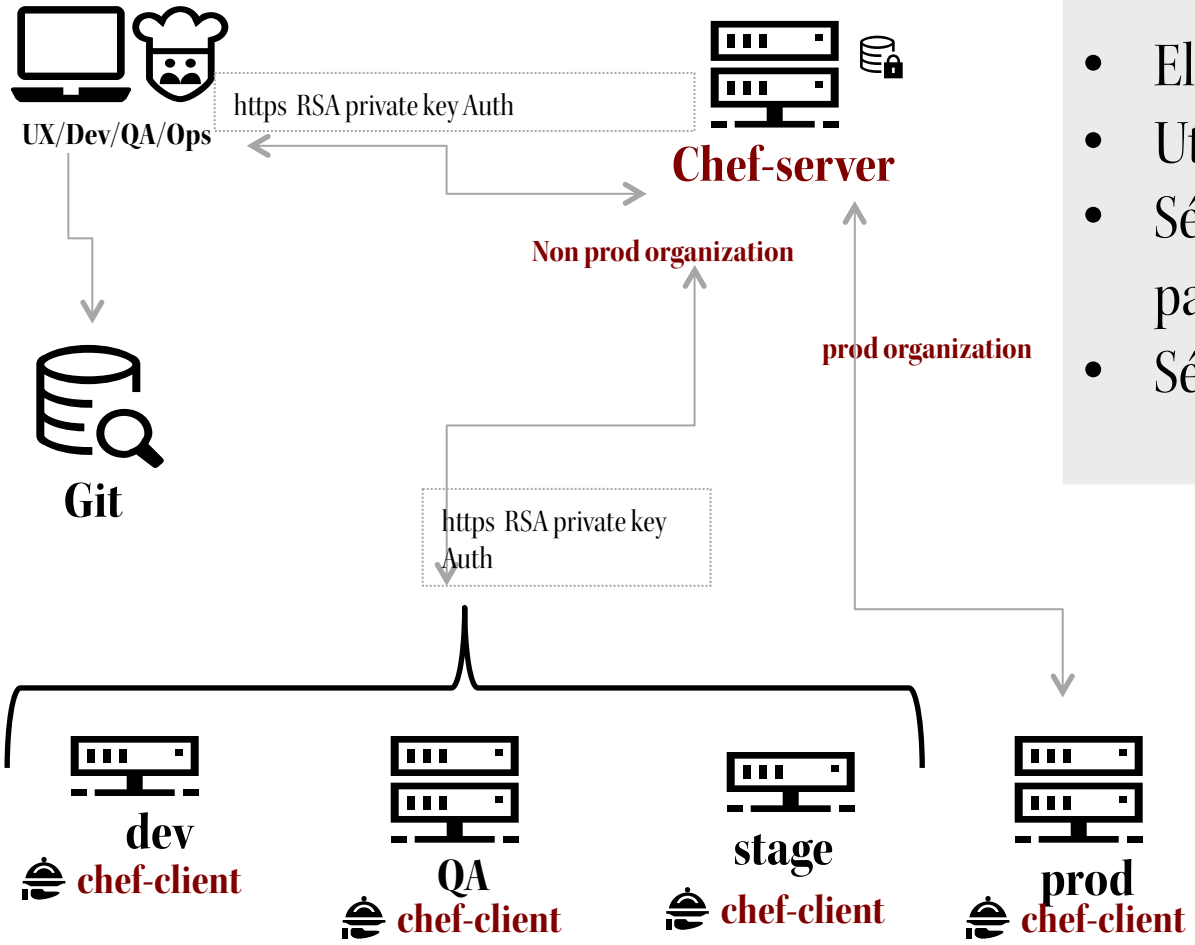
#barbusdevoxx

Chef-vault



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

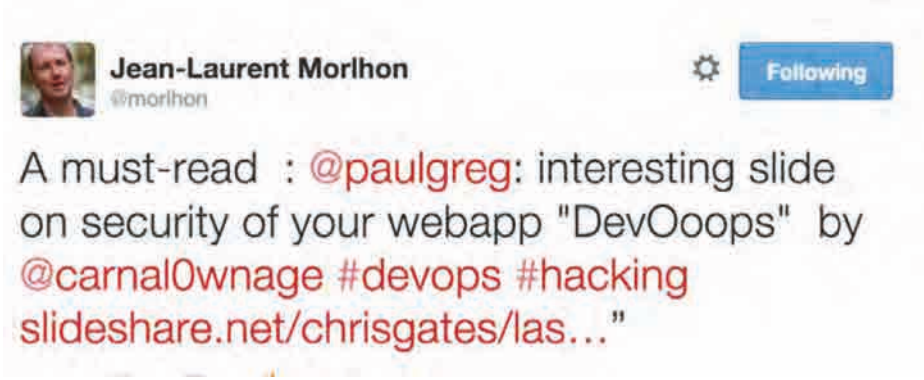
Chef-vault ?



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

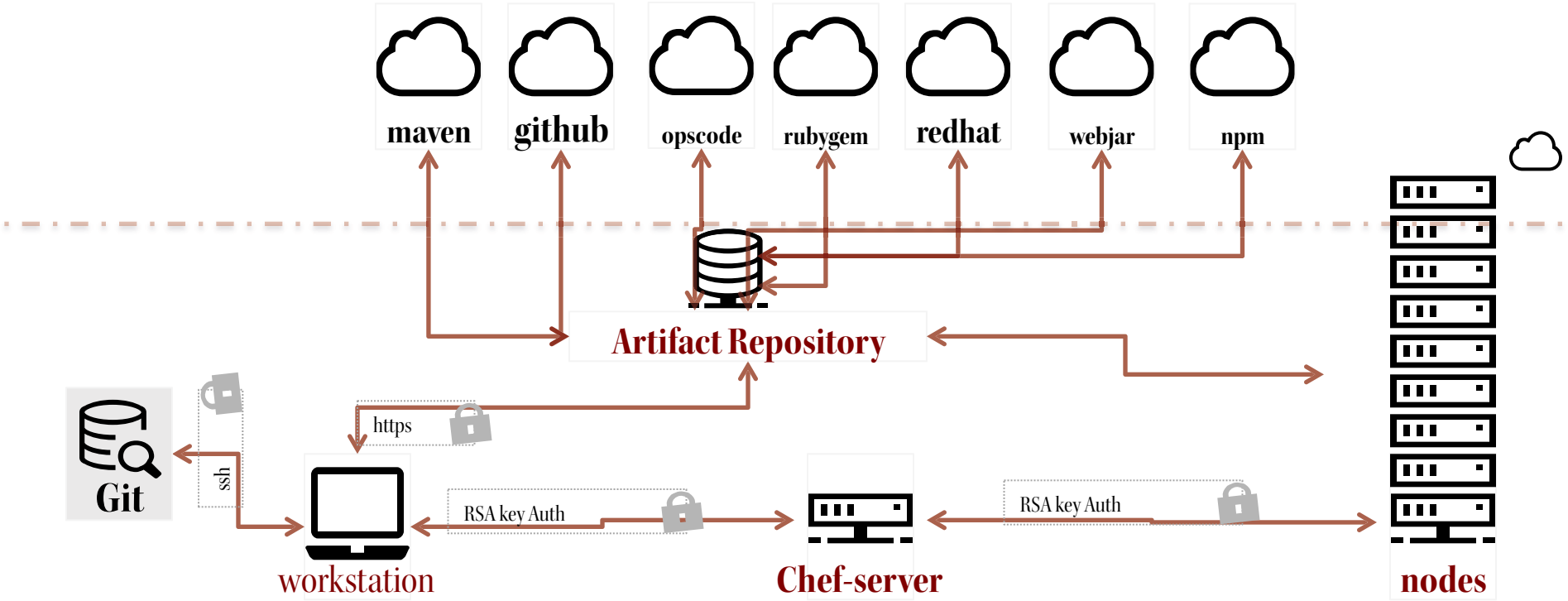
Jenkins sécurisé

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



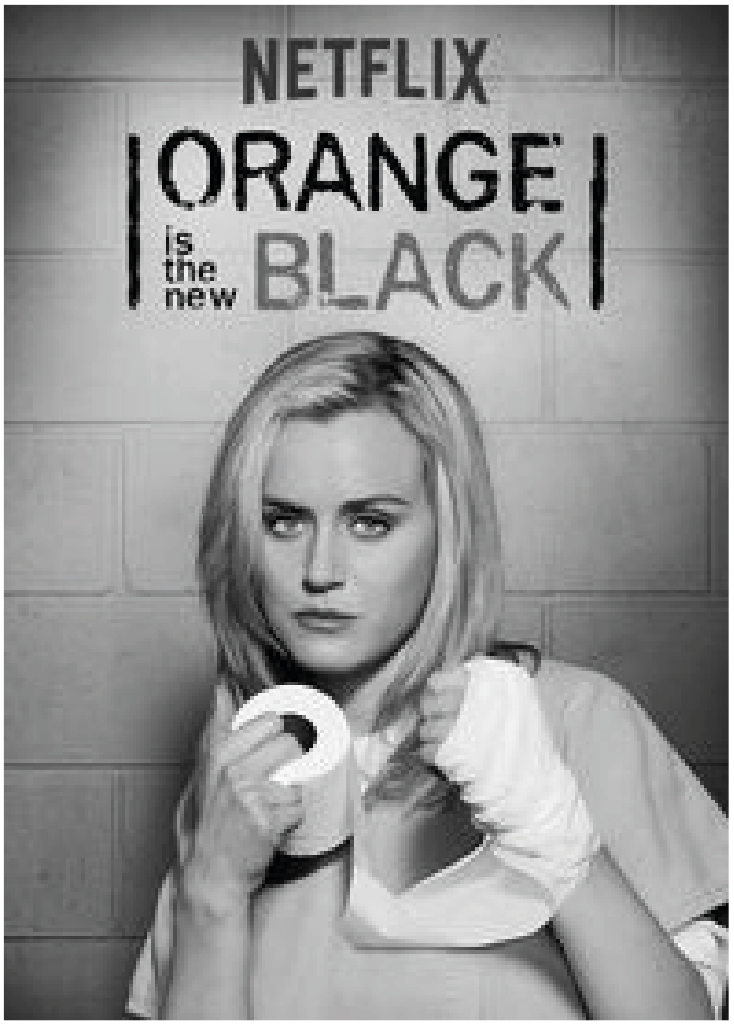
https://twitter.com/morlhon/status/554899543150850048

Gestion sécurisée des dépendances




Et le Cloud ?


3009
3009
DEVOX France


NETFLIX
ORANGE
is the new BLACK

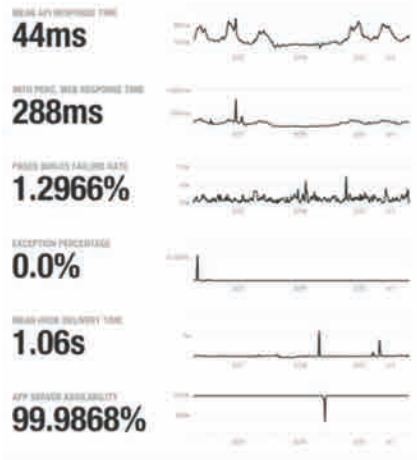
Prêt à te faire hacker?

Allo les pompiers ?

GitHub Status @githubstatus · Mar 26
We are currently experiencing some minor service outages.
17 5

Olivier Bazoud and 8 others follow
GitHub Status @githubstatus · Mar 27
We are investigating increased error rates as an incoming DDoS amplifies their attack.
19 6

Retweeted 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.
483 329



#barbusdevoxx

Y a la maison qui brûle

- Détecteur de fumée
  - HSM
  - IDS
- Porte coupe-feu
  - SELinux
  - SecurityManager

De DevOps à DevSec

Ce qu'il fallait retenir

Ce qu'il fallait retenir

- La securite 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 ?