Présentation finale projet de synthèse

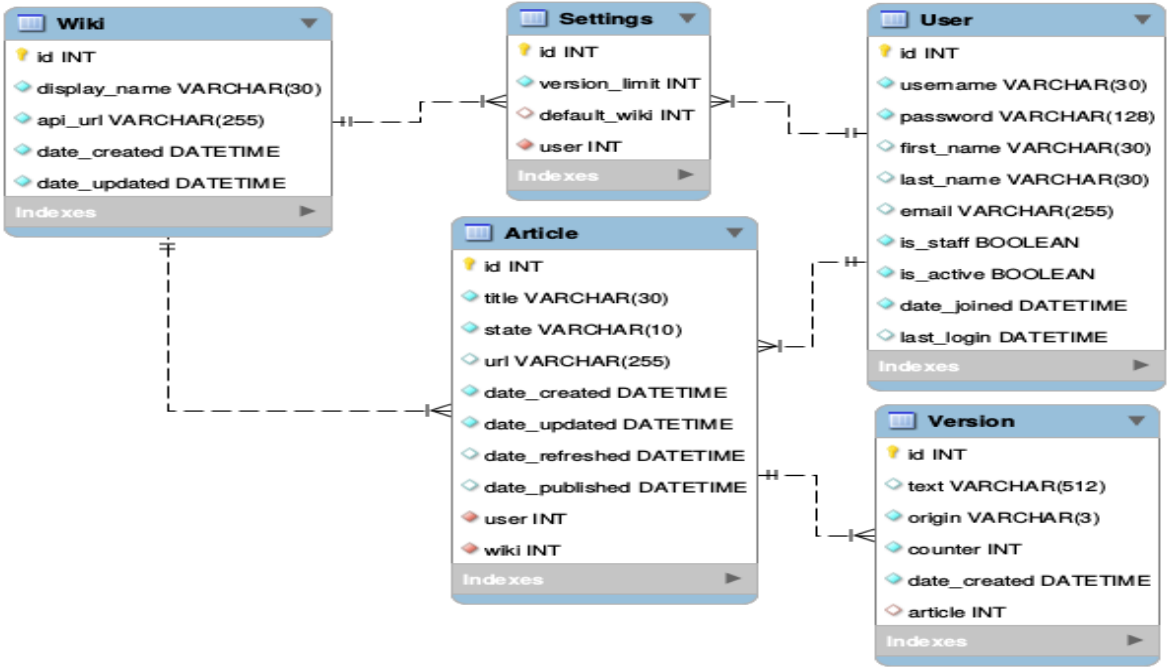
HURIER - LACAVE - GULDNER - SOILIHI

Plan

- Architecture générale
- Détails techniques
- Attaques
- Défenses
- Conclusion

Architecture Générale

Schéma de la BDD

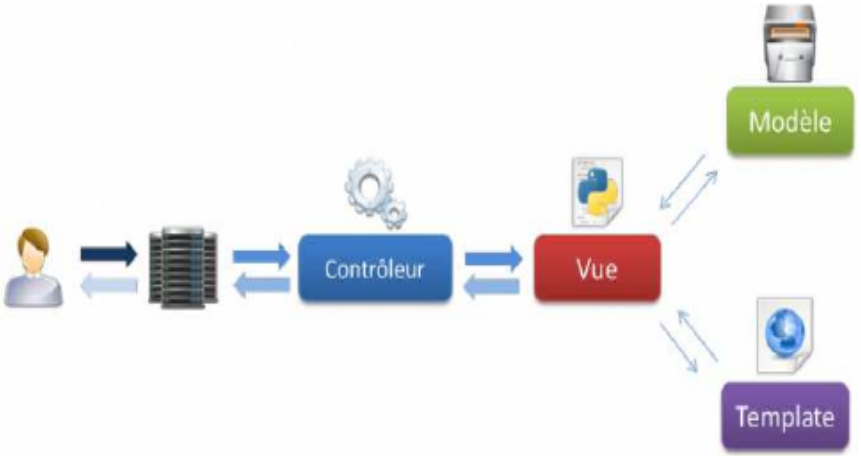


Contraintes d’intégrité

- Plus de 60 contraintes d’intégrité
  - unique, types (url, email …), reg. exp. …
- Permet d’assurer la cohérence de la BDD à bas niveau
  - meilleure sécurité (Fat Model / Skinny Controller)
- Génération et remplissage automatique (évite les erreurs)
  - avantage du cadriciel (DAL, fixtures, validators …)

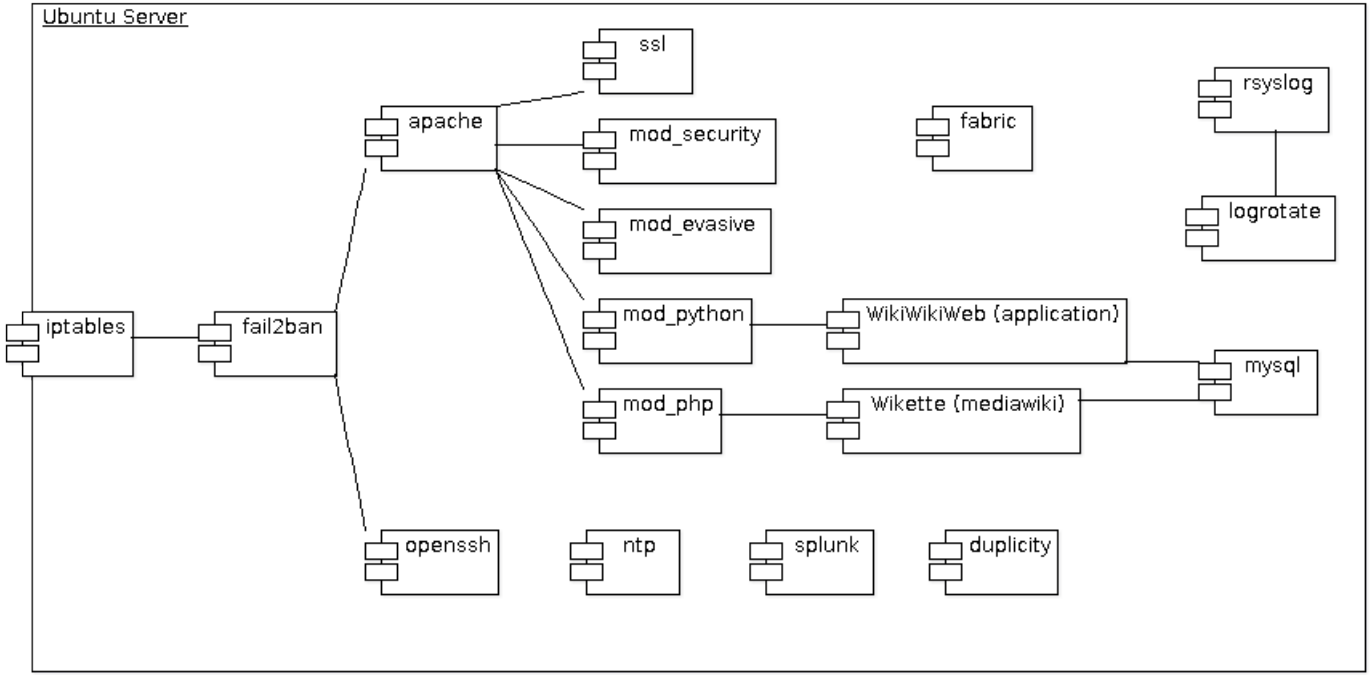
Traitements

- utilisation du patron MVC
- 18 traitements principaux
  - 24 cas nominaux
  - 35 cas d’erreurs
  - 3 cas liés au cadriciel



index, home, search, link, create, edit, review, refresh, publish, delete, profile, settings, subscribe, login, logout

Schéma de l'infrastructure



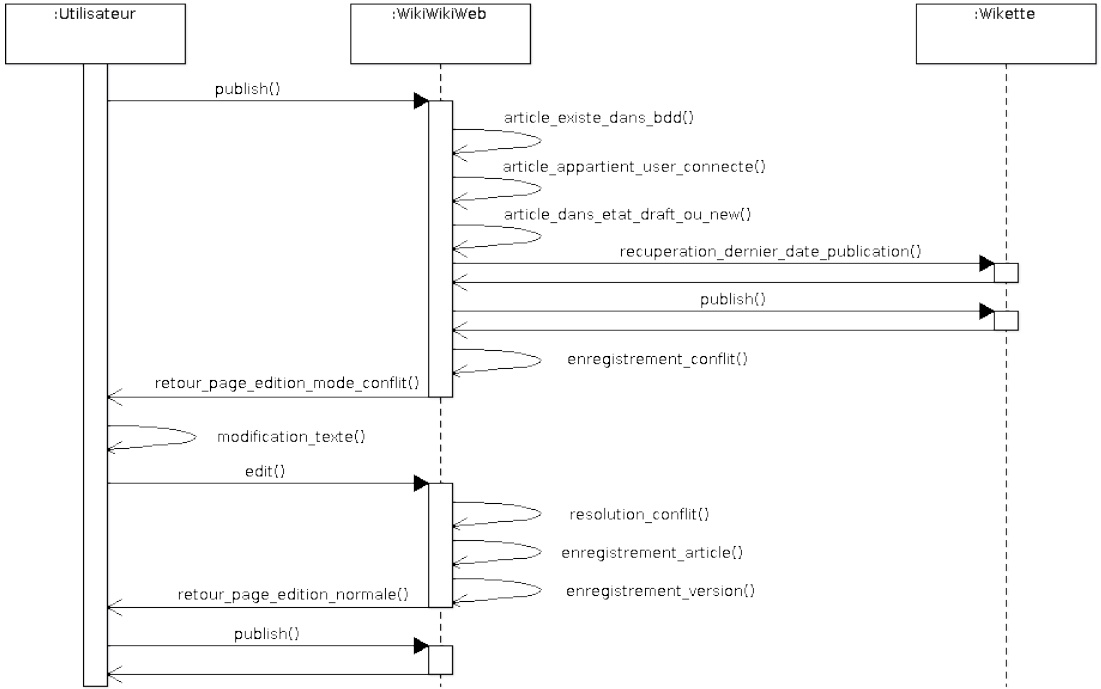
Détails techniques

4 instances applicatives

Chacune est isolée dans un hôte virtuel (VirtualHost)
SSL appliqué en suivant les consignes

- port 80: l'instance non sécurisée de Mediawiki (Wikette)
- port 443 : l'instance sécurisée de Mediawiki (Wikette-SSL)
- port 9667 : l'instance non sécurisée de l'application (WikiWikiWeb)
- port 10000 : l'instance sécurisée de l'application (WikiWikiWeb-SSL)

Résolution des conflits



Sécurité mediawiki

Fichier de configuration de mediawiki (LocalSettings.php)

->Limiter la taille des articles (512ko)
->Renforcer les règles basiques de sécurité
->Desactiver les mails
->Captcha pour les actions

Sécurité sys. (1/2)

- retrait de la bannière par défaut (/etc/issue)
- changement des points de montage (no-exec)
- configurations avancées (/etc/sysctl.conf)
- configuration du pare-feu (iptables et iptables-save)
- règles de gestion utilisateur (/etc/login.defs et PAM)

Sécurité sys. (2/2)

- changement du masque par défaut (umask 077)
- configuration de l’accès à disance (SSH avec clés)
- configuration attribution des hôtes (/etc/host)
- configuration de la journalisation (rsyslog et logrotate)
- configuration des sauvegardes (duplicity et Clonezilla)

Sécurité BDD (MySQL)

- script mysql_secure_installation
  - supprime utilisateur, BDD inutiles ...
- création de compte applicatif (1 par site)
- suppression des accès réseaux
- script mysqltuner.pl
  - améliore les performances de la BDD

Sécurité Web (Apache)

- modification de la configuration par défaut
  - /etc/apache2/conf-available/security.conf
- installation de module de sécurité
  - mod_security: I**P**S pour serveur web)
  - mod_evasive: Prévention des attaques DoS
- brouillage des scans

Sécurité applicative

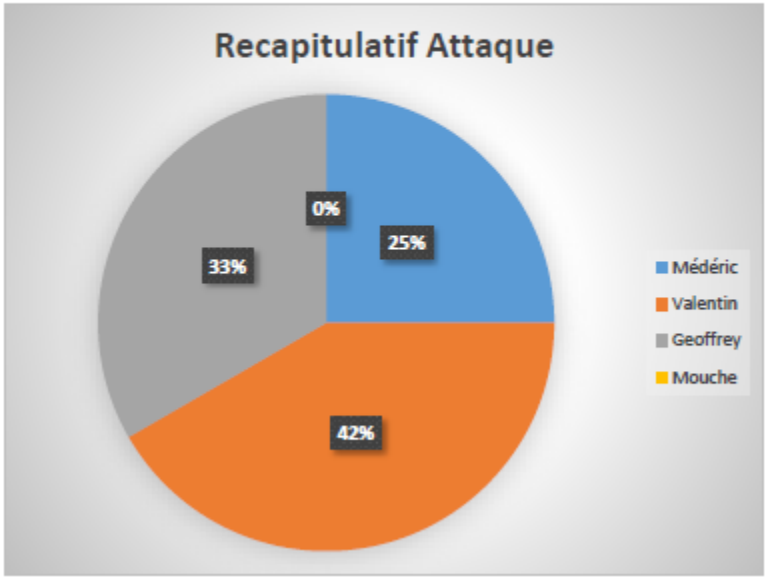
- Le cadriciel Django offre de nombreuses fonctions
  - dispatch, validateur, filtre de l'affichage …
  - protection contre SQLi, CSRF, XSS ...
- Mediawiki a été installé directement depuis les dépôts
  - facilite la mise à jours et la maintenance
- Tout est surveillé par des journaux
  - access, error, mod_security ...

Attaques

Résumé des attaques

N°Attaque	Attaquant	Envoyer le
A001	Médéric	22/01/2014
A002	Valentin	22/01/2014
A003	Valentin	22/01/2014
A004	Valentin	24/01/2014
A005	Valentin	29/01/2014
A006	Médéric	29/01/2014
A007	Médéric	29/01/2014
A008	Geoffrey	21/03/2014
A009	Geoffrey	21/03/2014
A010	Valentin	21/03/2014
A011	Geoffrey	27/03/2014
A012	Geoffrey	27/03/2014

Médéric	Valentin	Geoffrey	Mouche
3	5	4	0

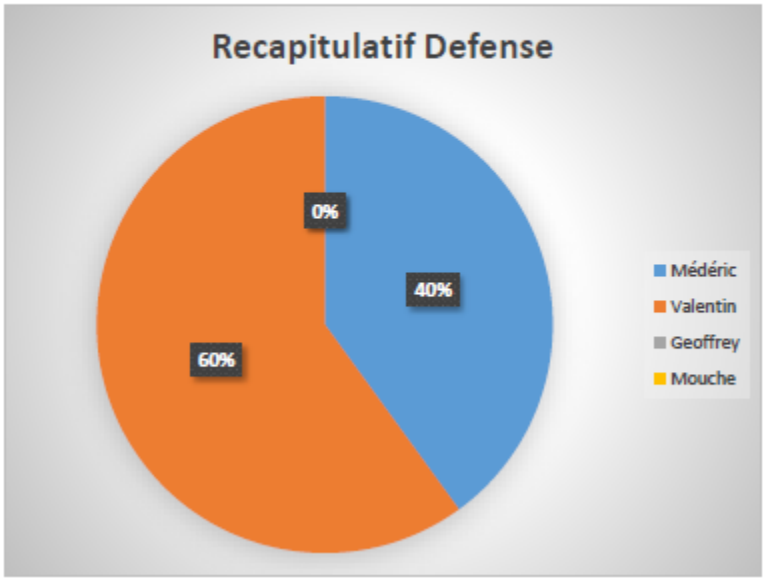


Défenses

Résumé des défenses

N° Defense	Attaquant	Envoyer le
D001	Médéric	23/01/2014
D002	Médéric	23/01/2014
D003	Valentin	30/01/2014
D004	Valentin	21/03/2014
D005	Valentin	26/03/2014

Médéric	Valentin	Geoffrey	Mouche
2	3	0	0

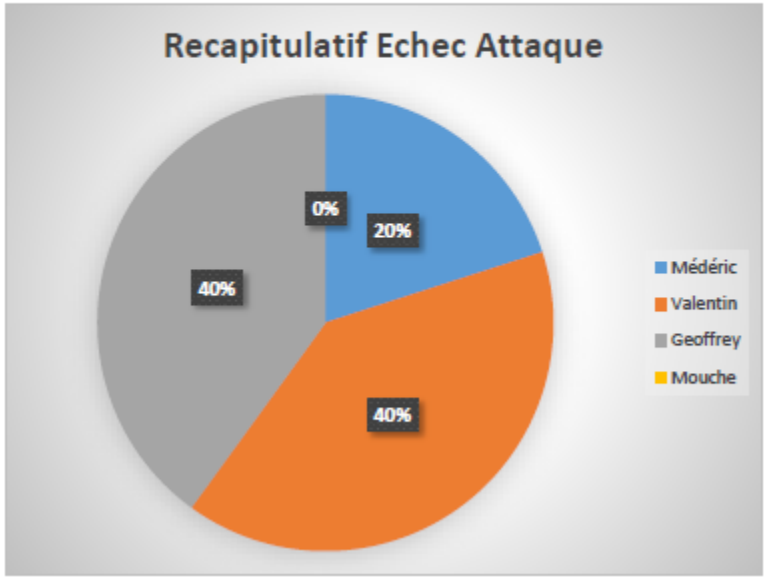


Attaques échouées

Résumé des attaques échouées

N° Echec	Attaquant	Effectué
EA001	Médéric	29/01/2014
EA002	Médéric	29/01/2014
EA003	Geoffrey	21/03/2014
EA004	Geoffrey	21/03/2014
EA005	Geoffrey	21/03/2014
EA006	Geoffrey	21/03/2014
EA007	Valentin	26/03/2014
EA008	Valentin	26/03/2014
EA009	Valentin	26/03/2014
EA010	Valentin	26/03/2014

Médéric	Valentin	Geoffrey	Mouche
2	4	4	0

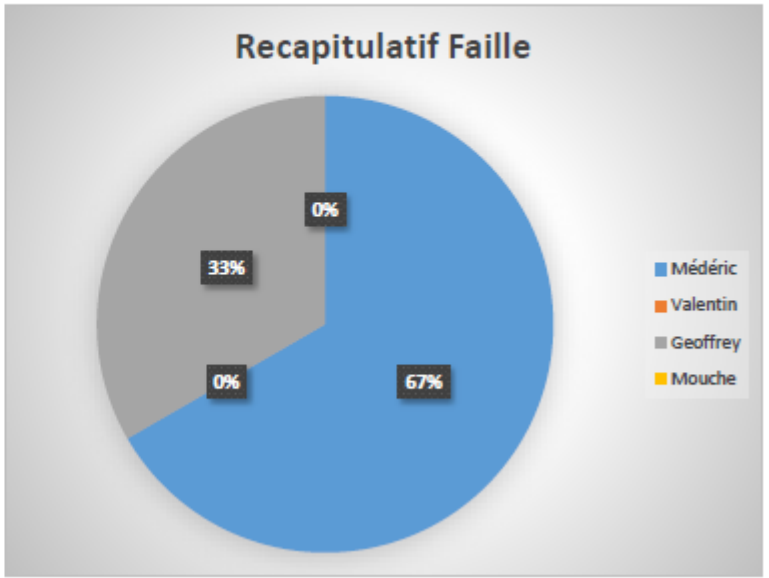


Faille corrigées

Résumé chez failles corrigées

N° Faille	Personne	Corrigé
F001	Geoffrey	29/01/2014
F002	Médéric	29/01/2014
F003	Médéric	30/01/2014

Médéric	Valentin	Geoffrey	Mouche
2	0	1	0



Notre faille de sécurité

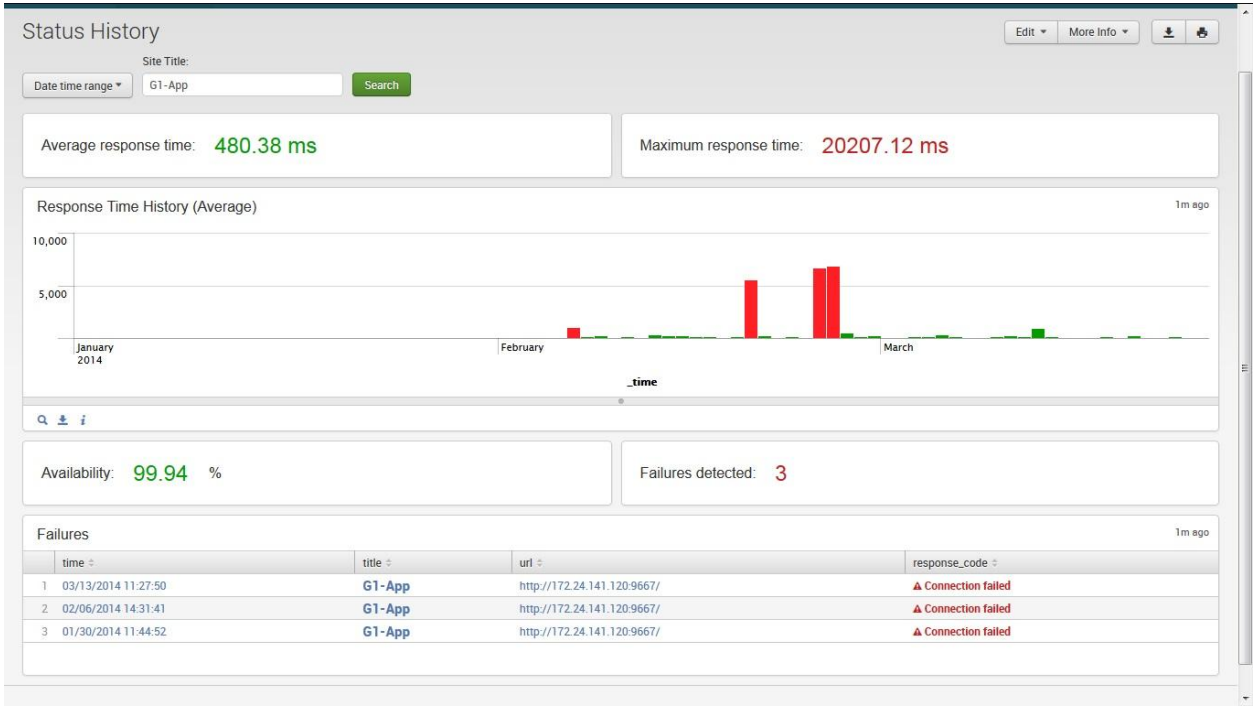
- Les échanges entre le site et le Wiki passent en clair !
  - contrainte imposée par le cahier des charges
  - des données peuvent être falsifiées (intégrité)
  - des infos. confidentielles peuvent être interceptées
- En interceptant de la boucle locale ou le trafic extérieur, il est possible de contrôler totalement l'API
- Pour corriger la faille, il suffit d'utiliser SSL sur le canal

Conclusion

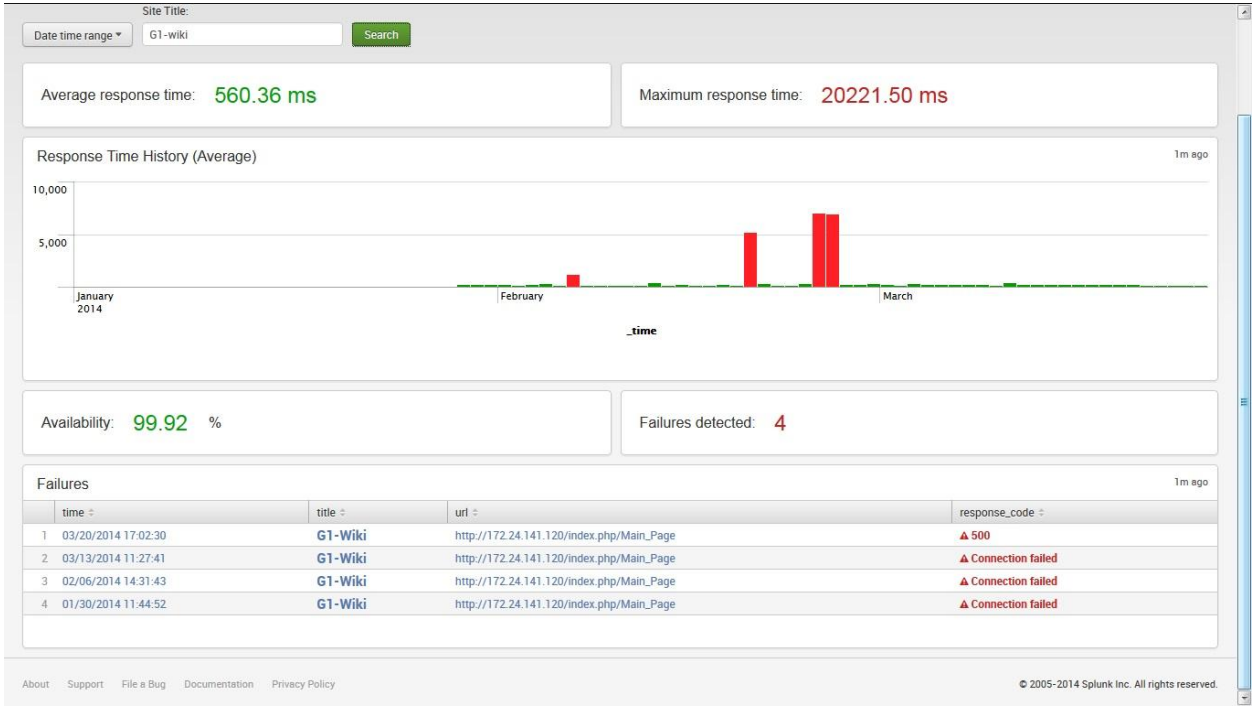
Bilan et rétrospective

- Difficile d’apprécier les résultats (secret des attaques)
  - mais bonnes statistiques (voir après)
- Bon rapport utilisabilité/sécurité du site
- **Avec le recul ...**
  - absence de la virtualisation
  - manque d’un outil de supervision
  - difficulté de préparation contre le DoS

Disponibilité application



Disponibilité du wiki



Faille

Bot entre notre application et le wiki.

Possibilité de faire un MITM pour capter le traffic et de voir le mot de passe, en ce connectant au wiki et en changeant le mot de passe, on fait un déni de service

Conclusion

- Expérience enrichissante (autonomie, créativité …)
  - manque de cours pour préparer les attaques
- Pas assez représentatif d'un cas réel
  - exigence d'utilisabilité, de disponibilité …
- Importance de la communication, de la collaboration, de l'automatisation et de la gestion de projet

The End
Questions ?