



# Sécurité des Applications Web

**Paris, 15 décembre 2011**

Événement organisé en partenariat avec :

**Orange Business Services**

**TelecityGroup**



## Actualités CLUSIF

### Nouveaux documents

- 👉 *Aider l'auditeur pour la revue de sécurité physique*
- 👉 *Défense en profondeur des applications web*

### Nouveaux GT :

- 👉 Panorama CyberCrime 2011, rdv le 11 janvier 2011
  - 👉 MIPS, édition 2012 (**phase d'enquête imminente**)
  - 👉 Bientôt...
    - Sécurité des *Web Services*
- et fiches pratiques de développement Web



## Pourquoi parler encore et encore de ce sujet ?

La technologie Web est omniprésente

- ☞ sites web ;-)
- ☞ applications mobiles
- ☞ applications dans les entreprises
- ☞ applications dans les nuages (offres SaaS)

Le « Web » devient le support de tous les échanges

- ☞ pour le grand public
- ☞ pour les usagers de l'e-administration
- ☞ pour les services
- ☞ pour les entreprises

## Véritables « pot de miel » pour les attaquants !

### Les cibles privilégiées des attaquants

- 👉 les informations sensibles à valeur « commerciale »
- 👉 l'atteinte à l'image d'institutions, grands groupes...
- 👉 l'atteinte à la disponibilité des services

### Plusieurs niveaux d'attaque

- 👉 l'hébergement
- 👉 le transport (HTTP ou HTTPS)
- 👉 le serveur et son système d'exploitation
- 👉 le serveur d'application
- 👉 l'application développée

## Les travaux du Clusif dans le domaine

### Sécurité des applications Web (2009)

- 👉 top 5 des mythes et réalités sur le sujet
- 👉 revue des principales failles de sécurité dans les applications web
- 👉 les bonnes pratiques
- 👉 les moyens de vérification de sa sécurité

### Défense en profondeur des applications Web (2011)

- 👉 la relation avec les besoins de sécurité
- 👉 la notion de « lignes de défense »
- 👉 le développement du principe dans les infrastructures et les applications

## Intervenants

☞ *Mise en place d'une politique de sécurité applicative : retour d'expérience d'un RSSI*

**Philippe LARUE**

✉ Responsable sécurité – **CBP**  
philippe.larue@cbp-prevoyance.fr

☞ Revue de code source, ou test sécurité applicatif, quel est le plus efficient pour évaluer un niveau de sécurité applicatif ?

**Sébastien GIORIA**

✉ Consultant Senior **Groupe Y** et leader du chapitre Français de l'**OWASP** - OWASP France  
seb@gioria.org

☞ Les enjeux réglementaires de la protection des informations en ligne

**Me Garance MATHIAS**

✉ Avocat – Cabinet d'Avocats  
garance@gmathias.ath.cx

☞ Table Ronde, Q&R avec la salle