L'insécurité des Applications Web

Paris le 24 Septembre 2009

Sébastien GIORIA (sebastien.gioria@owasp.org)
Ludovic PETIT (ludovic.petit@owasp.org)
Chapter Leaders, OWASP France

The OWASP Foundation
http://www.owasp.org

CONCLUSION

« Si vous pensez que l'éducation coûte cher,
essayez donc l'ignorance »

Abraham Lincoln

Agenda

- L'OWASP
- La sécurité Web - Mythes et réalités
- Le Cadre Légal
- Comment contrôler
- Et après ?

OWASP en France

Un Conseil d'Administration (Association loi 1901) :

- Président, évangéliste et relations publiques : Sébastien Gioria

Consultant indépendant en sécurité des systèmes d'informations. Président du CLUSIR Poitou-Charentes

- Vice-Président et responsable du projet de Traduction : Ludovic Petit. CISSP - Expert Sécurité chez SFR
- Secrétaire et Responsable des aspects Juridiques : Estelle Aimé. Avocate

Un Bureau :

- Le Conseil d'Administration
- Romain Gaucher : Ex-chercheur au NIST, consultant chez Cigital
- Mathieu Estrade : Développeur Apache.

Projets :

- Top 10 : traduit.
- Guides : en cours.
- Questionnaire a destination des RSSI : en cours.
- Groupe de travail de la sécurité applicative du CLUSIF

Sensibilisation / Formations :

- Assurance (Java/PHP)
- Société d'EDI (JAVA)
- Opérateur Téléphonie mobile (PHP/ WebServices)
- Ministère de l'intérieur / SGDN
- Conférences dans des écoles
- Ministère de la santé
- Banques / Assurances

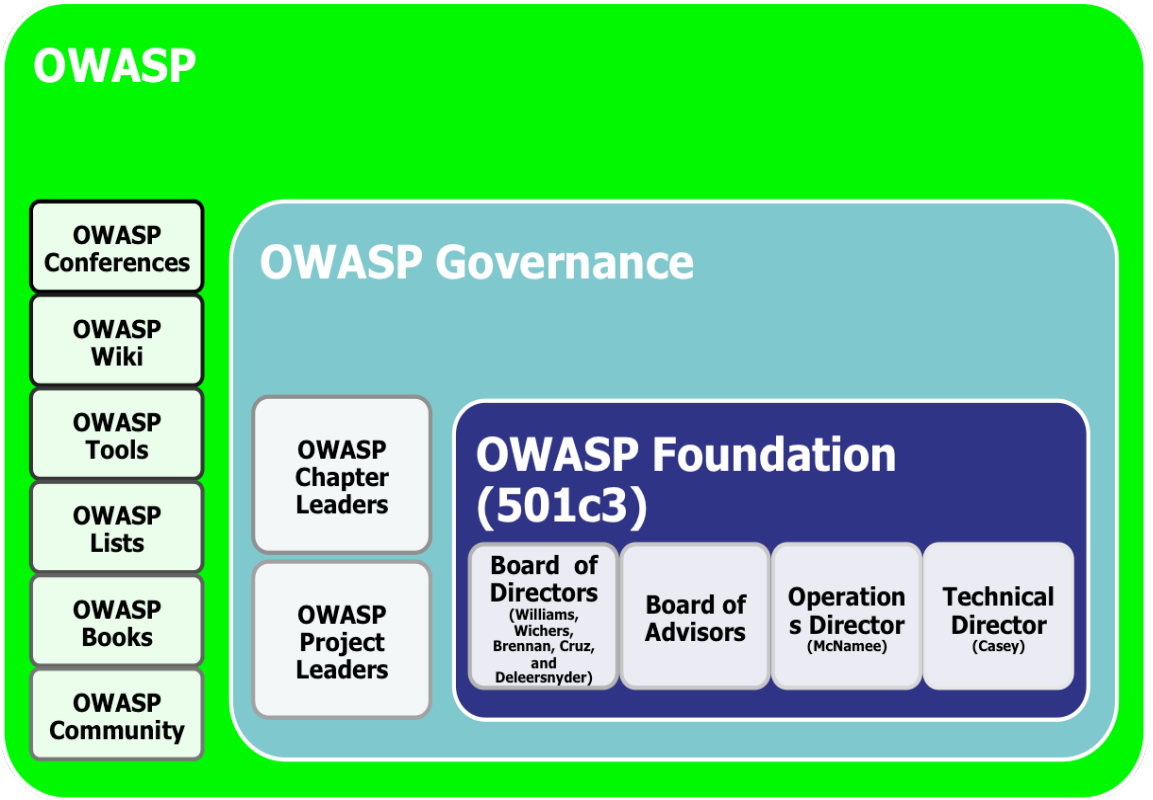
Interventions :

- Infosecurity
- OSSIR
- Microsoft TechDays
- PCI-Global
- CERT-IST

L'OWASP
(Open Web Application Security Project)

- Indépendant des fournisseurs et des gouvernements.
- Objectif principal : produire des outils, documents et standards dédiés à la sécurité applicative.
- Tous les documents, standards, outils sont fournis sur la base du modèle open-source.

- Organisation :
  - Réunion d'experts indépendants en sécurité informatique
  - Communauté mondiale (plus de 100 chapitres) réunie en une fondation américaine pour supporter son action. L'adhésion est gratuite et ouverte à tous
  - En France : une Association.
- Le point d'entrée est le wiki http://www.owasp.org



Les ressources de l'OWASP

- Vulnerability Scanners
- Static Analysis Tools
- Fuzzing

Automated Security Verification

- Penetration Testing Tools
- Code Review Tools

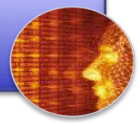
Manual Security Verification

- ESAPI

Security Architecture

- AppSec Libraries
- ESAPI Reference Implementation
- Guards and Filters

Secure Coding



- Reporting Tools

AppSec Management

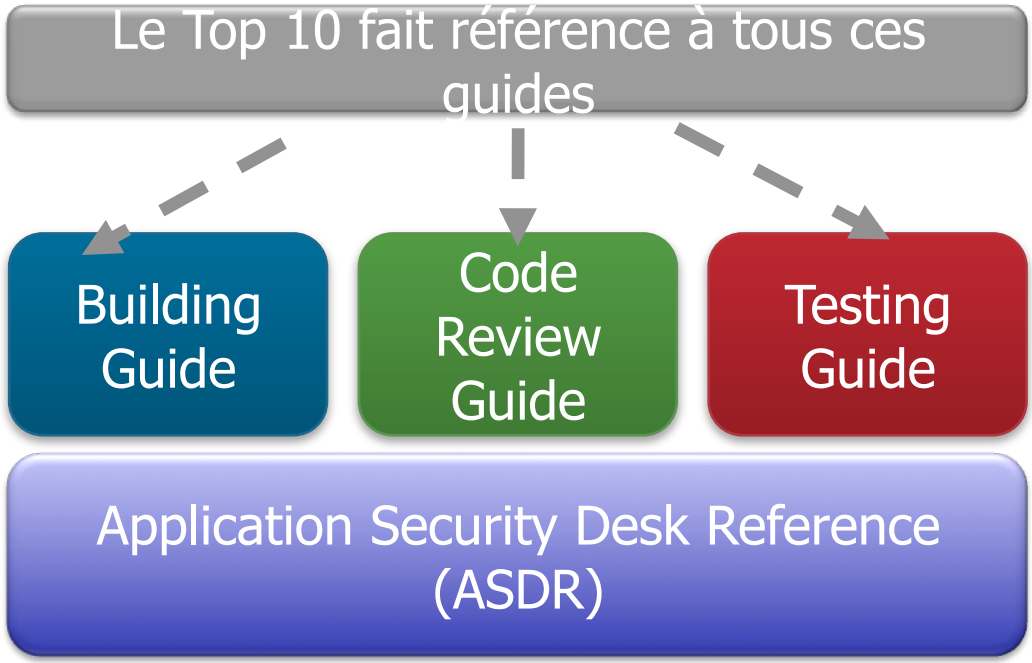
- Flawed Apps
- Learning Environments
- Live CD
- SiteGenerator

AppSec Education

Un Wiki, des Ouvrages, un Podcast, des Vidéos, des conférences, **une Communauté active**.

Les publications

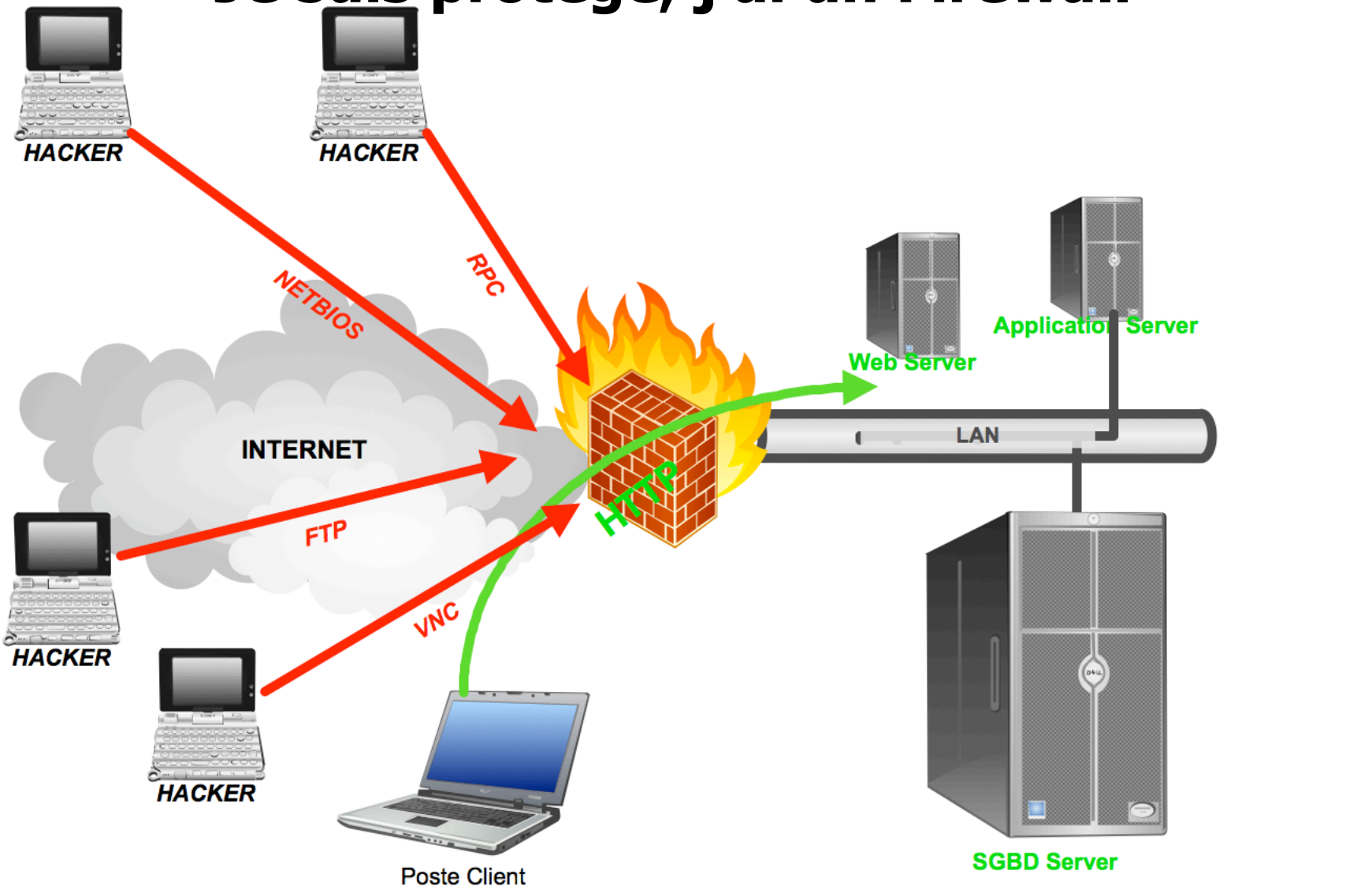
- Toutes les publications sont disponibles sur le site de l'OWASP: http://www.owasp.org
- L'ensemble des documents est régi par la licence GFDL (GNU Free Documentation License)
- Les publications majeures :
  - Le TOP 10 des vulnérabilités applicatives
  - Le Guide de l'auditeur/du testeur
  - Le *Code Review Guide*
  - Le guide de conception d'applications Web sécurisées
  - L'Application Security Verification Standard (ASVS)
  - La FAQ de l'insécurité des Applications Web



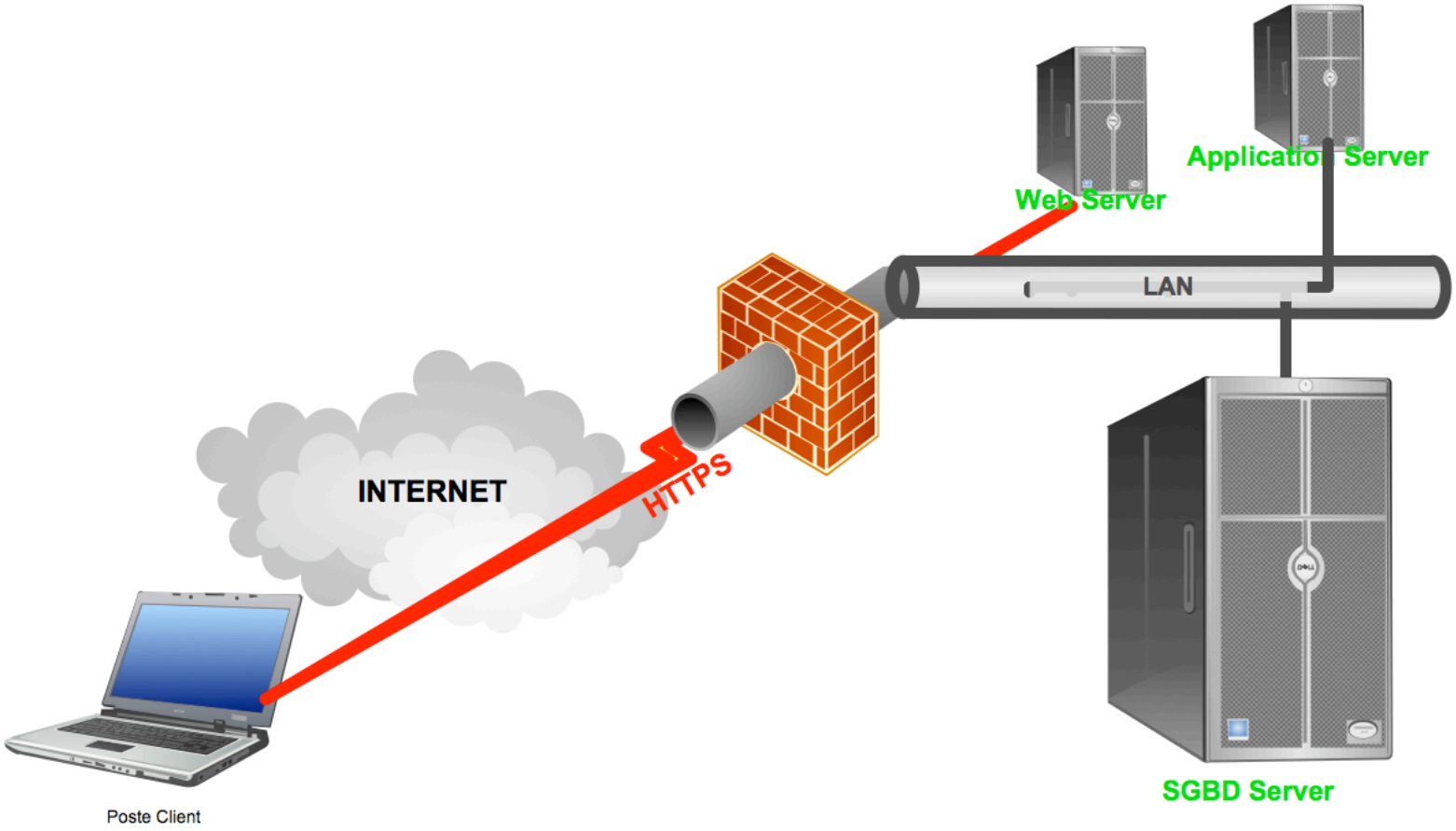
Agenda

- L'OWASP
- La sécurité Web - Mythes et réalités
- Le Cadre Légal
- Comment contrôler
- Et après ?

Je suis protégé, j'ai un Firewall

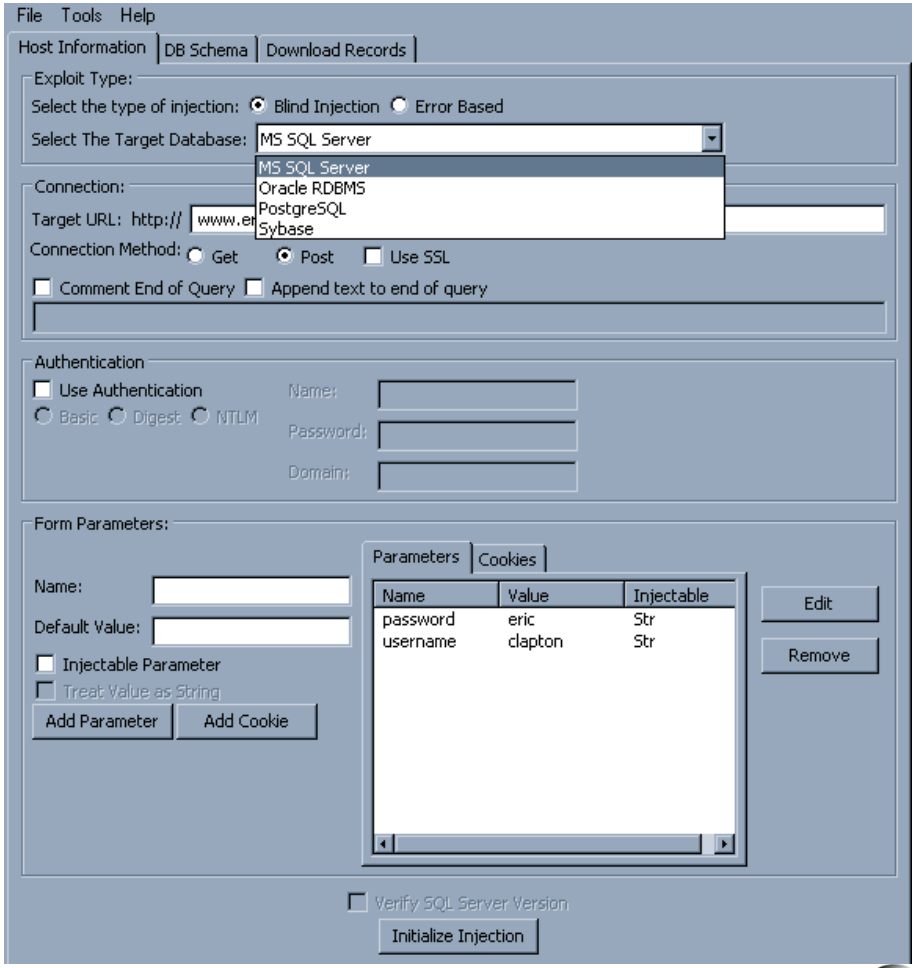


Mon site Web est sécurisé puisque il est protégé par SSL/TLS



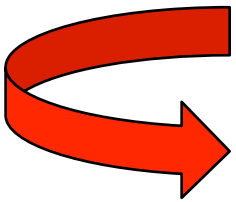
Seuls des génies de l'informatique savent exploiter les failles des applications Web

- Les outils sont de plus en plus simples d'emploi
- Une simple recherche sur Google permet de télécharger un logiciel permettant la récupération de bases de données.
- L'attaque d'un serveur web Français coute de 120$ à 1000$ dans le milieu « Underground »



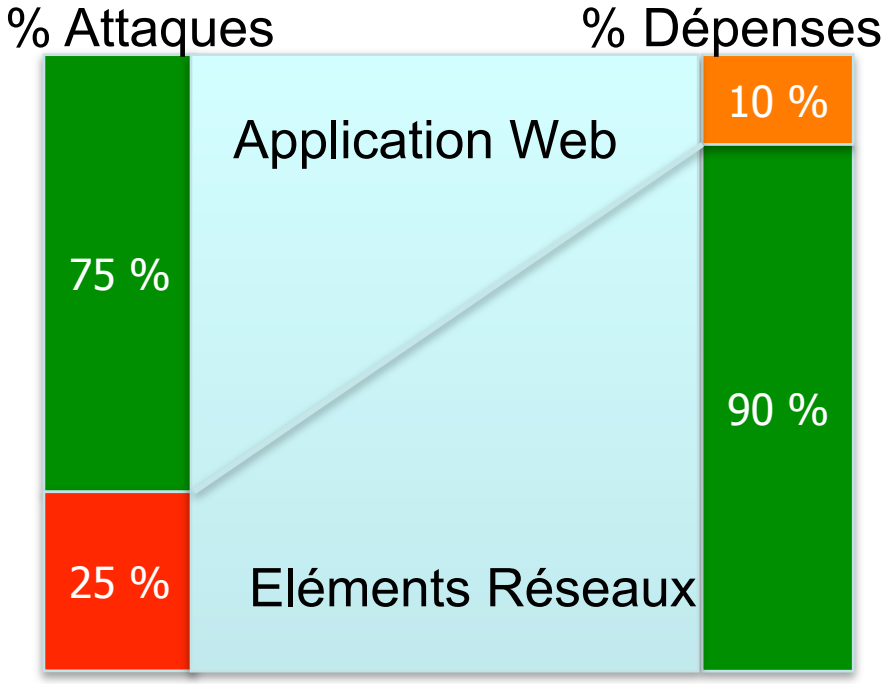
Une faille sur une application interne n'est pas importante

- De par l'importance du web actuellement, cela peut être catastrophique.
- Nombre de navigateurs permettent la création d'onglets :
  - Ils partagent tous la même politique de sécurité
  - Ils peuvent fonctionner indépendamment de l'utilisateur (utilisation d'AJAX)
  - La faille de clickjacking permet de générer des requêtes à l'insu de l'utilisateur

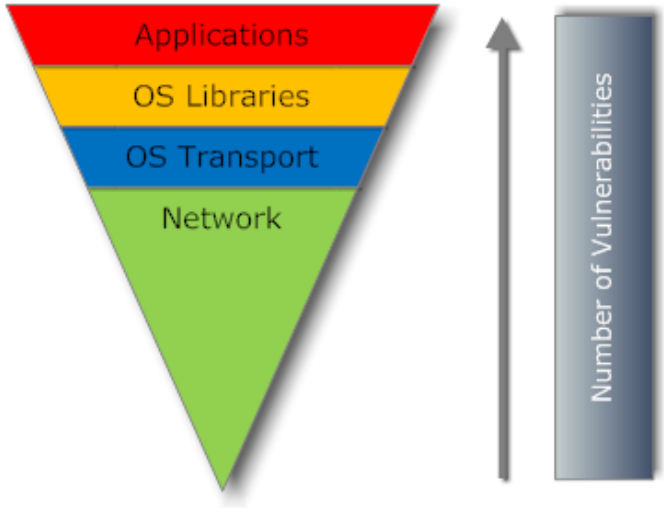


Le pirate se trouve alors dans le réseau local…

Faiblesse des Applications Web



Etude du GARTNER 2003
75% des attaques ciblent le niveau Applicatif
66% des applications web sont vulnérables



Etude du SANS (septembre 2009)
http://www.sans.org/top-cyber-security-risks/

"La veille d'un incident, le retour sur investissement d'un système de sécurité est nul. Le lendemain, il est infini." Dennis Hoffman, RSA

Agenda

- L'OWASP
- La sécurité Web - Mythes et réalités
- Le Cadre Légal
- Comment contrôler
- Et après ?

La CNIL

- **Disponibilité, Intégrité, Confidentialité**
- Obligation d'information des personnes concernées (salariés, clients, fournisseurs, etc.)
- Obligation de déclaration des applications relatives au traitement de données personnelles
- Principe de Proportionnalité
- Obligation de transparence des finalités poursuivies
- Durée de rétention des Journaux d'Evènements (Logs) et anonymisation
- le respect du droit à l'oubli (politique de conservation des données)

Ainsi, la « déclaration CNIL » n'est que l'une des obligations pesant sur l'entreprise.

La CNIL – Les sanctions

- **Sanctions CNIL :**
  - Avertissement, Mise en demeure
  - Sanctions pécuniaires (maximum 300 000 €)

- **Sanctions judiciaires diverses**

  Le défaut de respect de la loi Informatique et Liberté peut avoir des répercussions lors de l'exécution de contrats commerciaux ou des contrats de travail par exemple

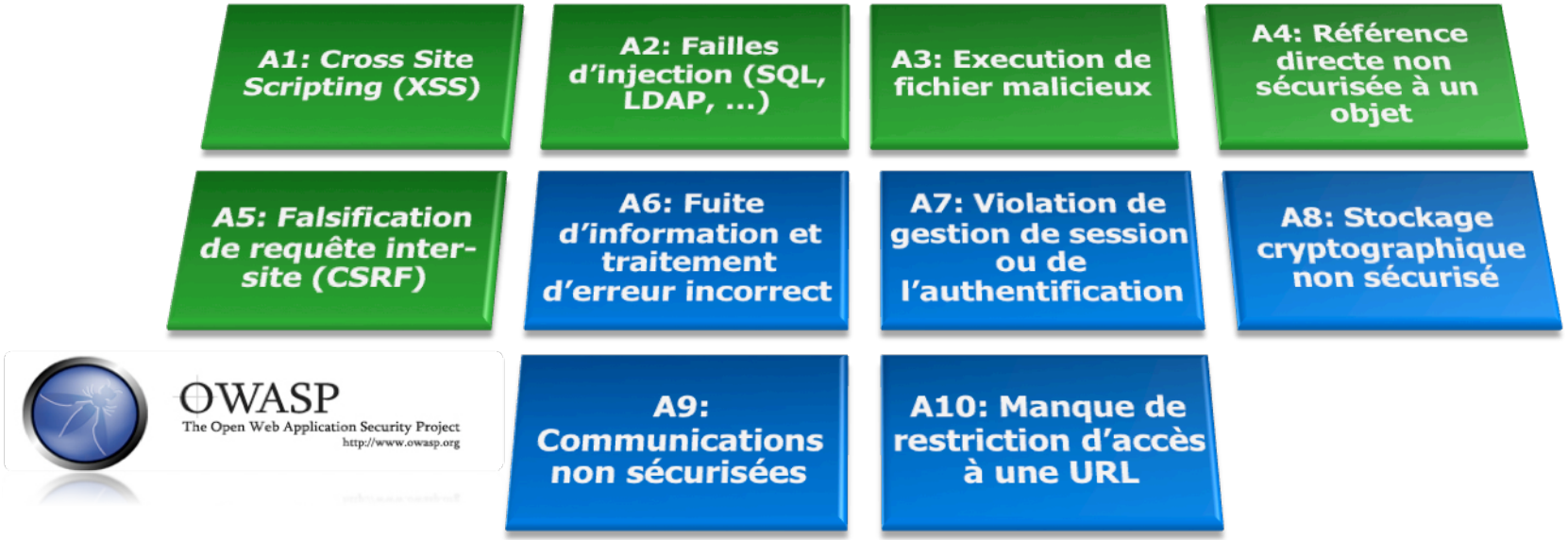
Responsable par négligence

- **Le dirigeant d'entreprise est pénalement responsable**
- **Sanctions pénales (**article 226-16 du Code pénal)
  - jusqu'à 5 ans d'emprisonnement
  - et 300 K€ d'amende

« *Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».*

PCI-DSS 6.5 – L'obligation *(trop souvent)* oubliée

Develop all web applications (internal and external, *and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following*



http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Les failles d'injection

6.5.1 : Cross Site Scripting

XSS permet à des attaquants d'exécuter du script dans le navigateur de la victime afin de détourner des sessions utilisateur, défigurer des sites web, potentiellement introduire des vers, etc

6.5.2 : Failles d'injections

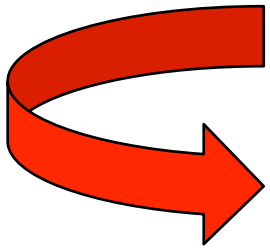
L'injection se produit quand des données écrites par l'utilisateur sont envoyées à un interpréteur en tant qu'élément faisant partie d'une commande ou d'une requête. Les données hostiles de l'attaquant dupent l'interpréteur afin de l'amener à exécuter des commandes fortuites ou changer des données

6.5.3 : Execution de fichier malicieux

Un code vulnérable à l'inclusion de fichier à distance permet à des attaquants d'inclure du code et des données hostiles, ayant pour résultat des attaques dévastatrices, telles la compromission totale d'un serveur.

6.5.5 : Falsification de requête inter-site (CSRF)

Une attaque CSRF force le navigateur d'une victime authentifiée à envoyer une demande pré-authentifiée à une application web vulnérable, qui force alors le navigateur de la victime d'exécuter une action hostile à l'avantage de l'attaquant.



Disponibilité
Intégrité
Confidentialité

La fuite d'information

6.5.6 : Fuite d'information et traitement d'erreur incorrect

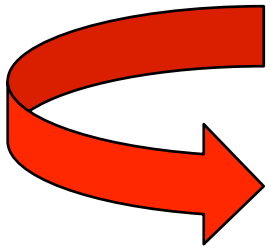
Les applications peuvent involontairement divulguer des informations sur leur configuration, fonctionnements internes, ou violer la vie privée à travers toute une variété de problèmes applicatifs. Les attaquants utilisent cette faiblesse pour subtiliser des données sensibles ou effectuer des attaques plus sérieuses.

6.5.9 : Communications non sécurisées

Les applications échouent fréquemment à chiffrer le trafic de réseau quand il est nécessaire de protéger des communications sensibles.

6.5.10 : Manque de restriction d'accès à une URL.

Fréquemment, une application protège seulement la fonctionnalité sensible en empêchant l'affichage des liens ou des URLs aux utilisateurs non autorisés. Les attaquants peuvent utiliser cette faiblesse pour accéder et effectuer des opérations non autorisées en accédant à ces URL directement.



Disponibilité
Intégrité
Confidentialité

La mauvaise gestion de l'authentification

6.5.4 :Référence directe non sécurisée à un objet

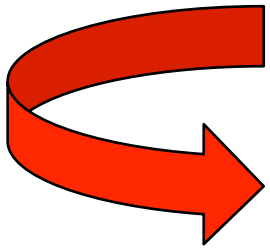
Une référence directe à un objet se produit quand un développeur expose une référence à un objet d'exécution interne, tel qu'un fichier, un dossier, un enregistrement de base de données, ou une clef, comme paramètre d'URL ou de formulaire. Les attaquants peuvent manipuler ces références pour avoir accès à d'autres objets sans autorisation.

6.5.7 : Violation de la gestion de l'authentification et des sessions

Les droits d'accès aux comptes et les jetons de session sont souvent incorrectement protégés. Les attaquants compromettent les mots de passe, les clefs, ou les jetons d'authentification identités pour s'approprier les identités d'autres utilisateurs.

6.5.8 :Stockage cryptographique non Sécurisé.

Les applications web utilisent rarement correctement les fonctions cryptographiques pour protéger les données et les droits d'accès. Les attaquants utilisent des données faiblement protégées pour perpétrer un vol d'identité et d'autres crimes, tels que la fraude à la carte de crédit.



Confidentialité
Intégrité

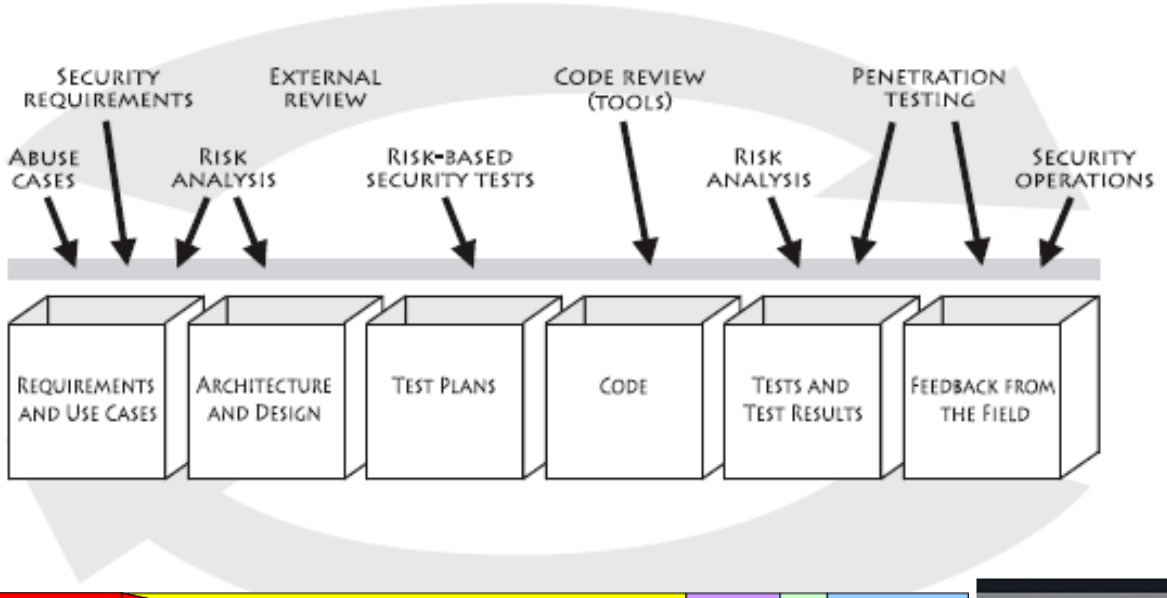
Coùt de la non-conformité

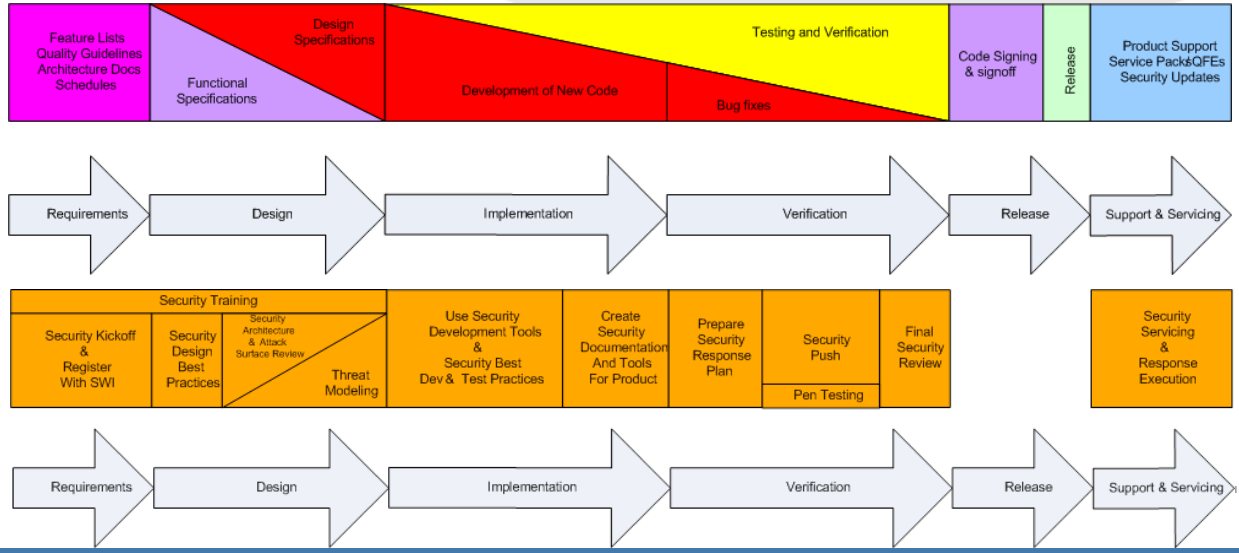
- Exemple: 50 000 cartes de crédits volées
  - Pénalité du PCI-SCC - $100,000 par incident, $500 000 s'il n'y a pas eu d'audit interne.
  - Remplacement des cartes - $500,000
  - Fraude aux transactions – $61,750,00 (moyenne 2004 des fraudes sur transactions $1,235 en 2004)
  - Très très mauvaise publicité !!!!

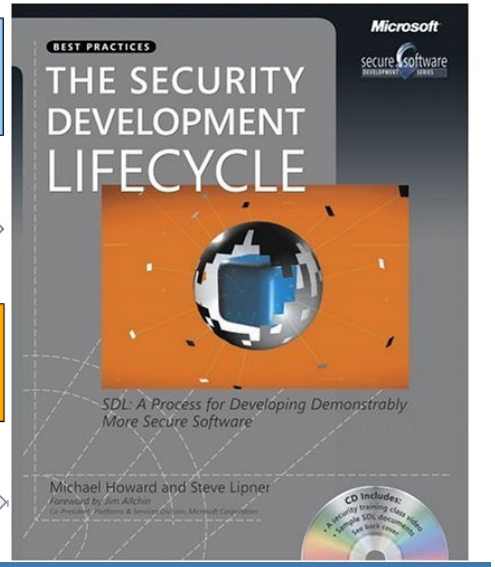
Agenda

- L'OWASP
- La sécurité Web - Mythes et réalités
- Le Cadre Légal
- Comment contrôler
- Et après ?

Le Saint Graal







Ajouter du contrôle dès les fondations

⇒**The OWASP Secure Software Development Contract Annex**

⇒http://www.owasp.org/index.php/Legal

- Un canevas contractuel pour les entreprises utilisant des MOA/MOE externes/externalisées.
- S'assurer qu'à toutes les étapes du cycle de développement une attention appropriée à la sécurité est apportée.
- « Compatible » avec le droit français.

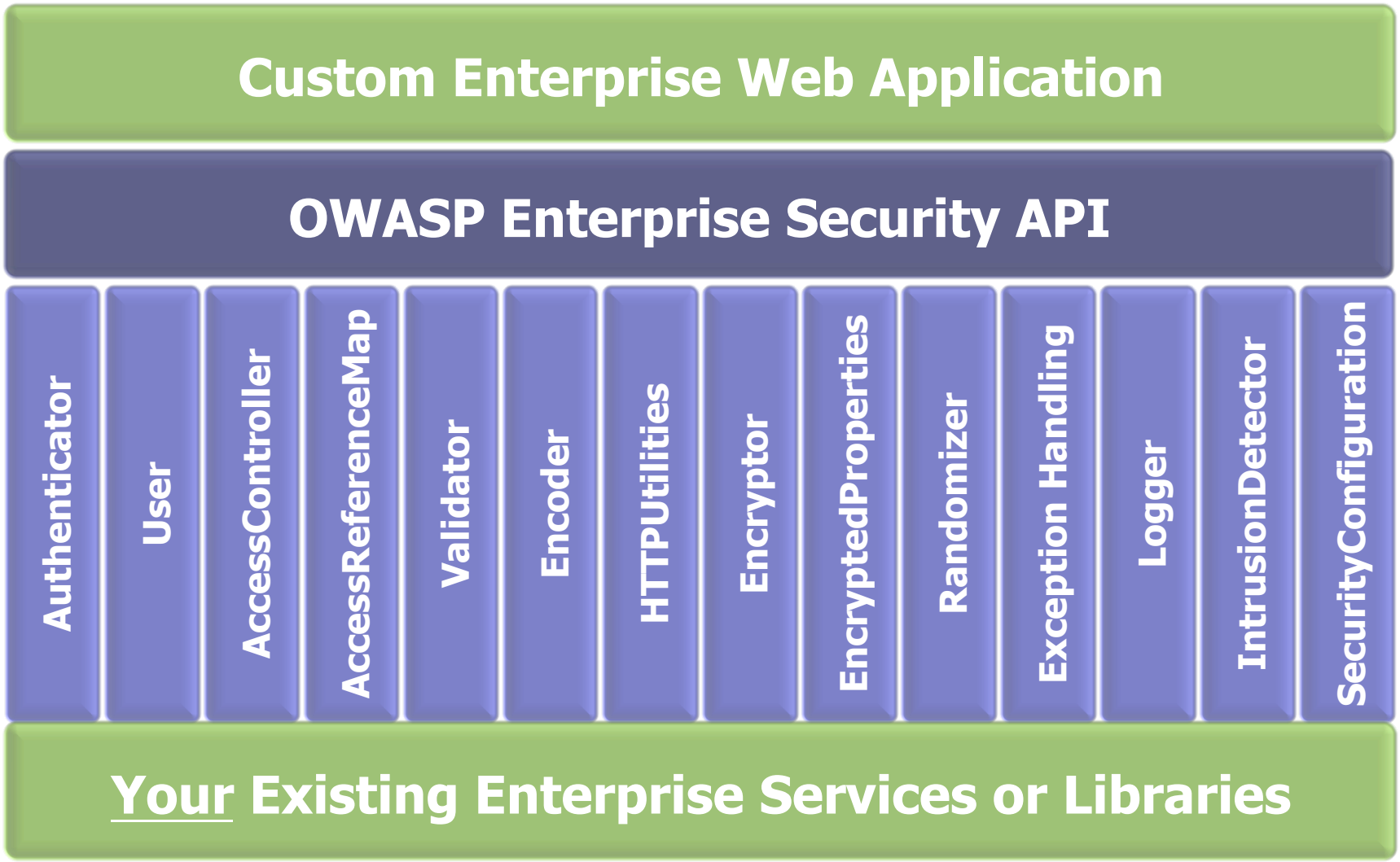
Ne pas réinventer la roue

⇒**Utilisez L'OWASP Enterprise Security API (ESAPI).**

⇒http://www.owasp.org/index.php/ESAPI

- Un framework de sécurité pour les développeurs.
- Permettre de créer une application Web Sécurisée.
- Classes Java et .NET (PHP en cours).
- 10 ans de Recherche et Développement.

Ne pas réinventer la roue



Apporter de la confiance

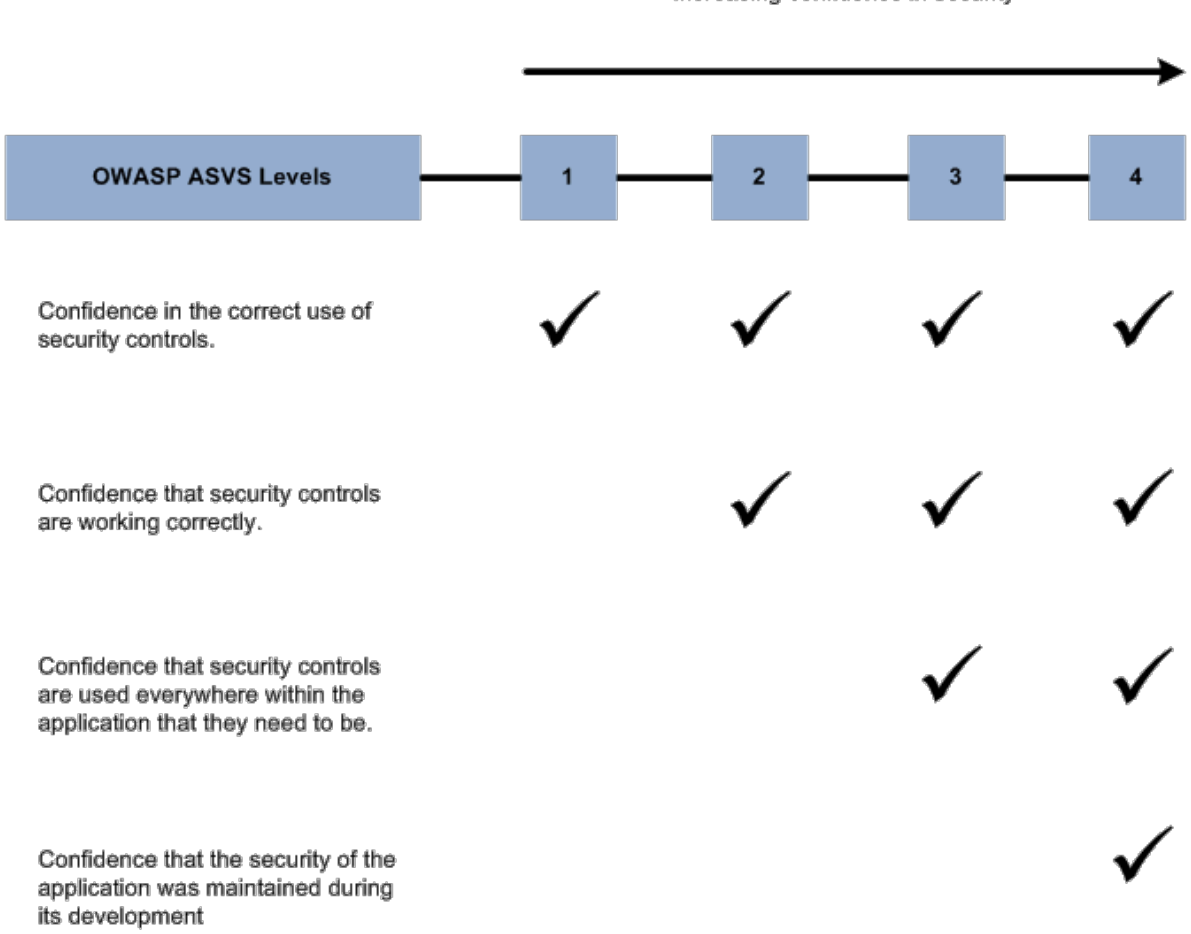
- L'Application Security Verification Standard (ASVS) vous aidera a répondre à ces questions :
  - Pouvez vous avoir confiance en votre application Web ?
  - Quel niveau de confiance avoir en l'application?
  - De quelles attaques est protégée votre application?

Quelle que soit votre maturité de SSI dans votre SDL :

- Etude/Scan de vulnérabilités
- Scan automatisé de code source
- Revue manuelle de code source
- Revue sécurité de l'architecture (fonctionnelle et technique)
- Tests sécurité spécifiques

Apporter de la confiance

⇒http://www.owasp.org/index.php/ASVS

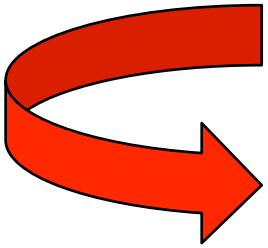


Agenda

- L'OWASP
- La sécurité Web - Mythes et réalités
- Les obligations
- Comment contrôler
- Et après ?

Pas de recette Miracle

- Sensibiliser ou… sensibiliser. Mais sensibiliser!
- Mettre en place un cycle de développement sécurisé !
- Auditer et Tester son code !
- Vérifier le fonctionnement de son Application !



La sécurité est d'abord et avant tout affaire de bon sens!

CONCLUSION

« Si vous pensez que l'éducation coûte cher,
essayez donc l'ignorance »

Abraham Lincoln

Rejoignez nous !

http://www.owasp.fr