



Sécurité du Développement Web

RSSIA
Bordeaux – France
27 Mai 2011

Sébastien Gioria (French Chapter Leader & OWASP Global Education Committee Member)
sebastien.gioria@owasp.org

Copyright © 2009 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License.

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

Qui suis-je ?

Consultant Sécurité au sein du cabinet d'audit

GROUPE Y

Président du CLUSIR Poitou-Charentes

OWASP France Leader - Evangéliste - OWASP Global
Education Committee Member
(sebastien.gioria@owasp.org)



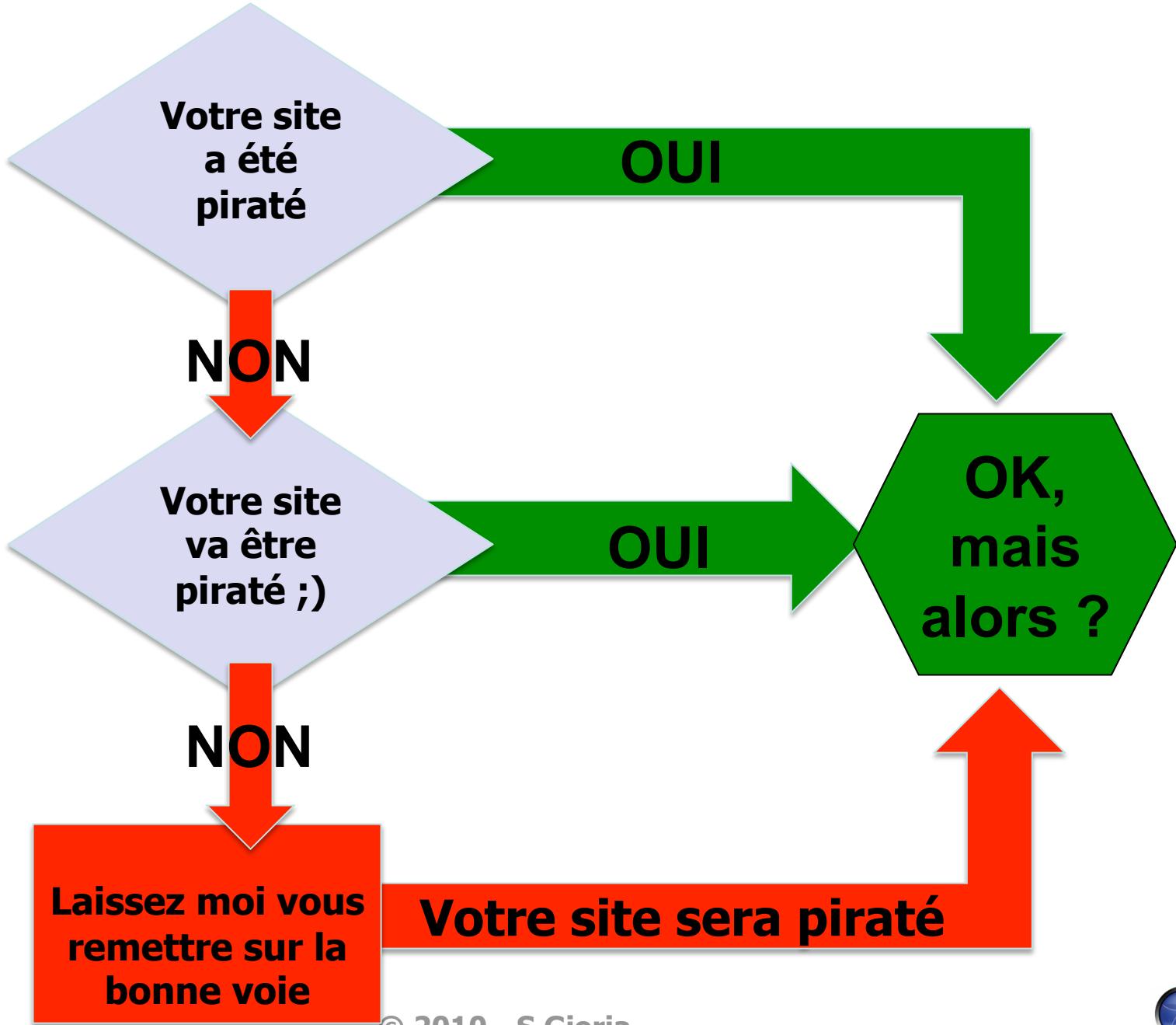
CISA & ISO 27005 Risk Manager

- +13 ans d'expérience en Sécurité des Systèmes d'Information
- Différents postes de manager SSI dans la banque, l'assurance et les télécoms

Twitter :@SPoint

- Expertise Technique
 - ✓ PenTesting, Digital Forensics
 - ✓ S-SDLC
 - ✓ Gestion du risque, Architectures fonctionnelles, Audits
 - ✓ Consulting et Formation en Réseaux et Sécurité
- Domaines de prédilection :
 - ✓ Web 4.2, WebServices, Insécurité du Web.





Agenda

- Pourquoi ?
- 4 préjugés
- La problématique
- Comment s'y prendre
- Et si ?
- Questions ?



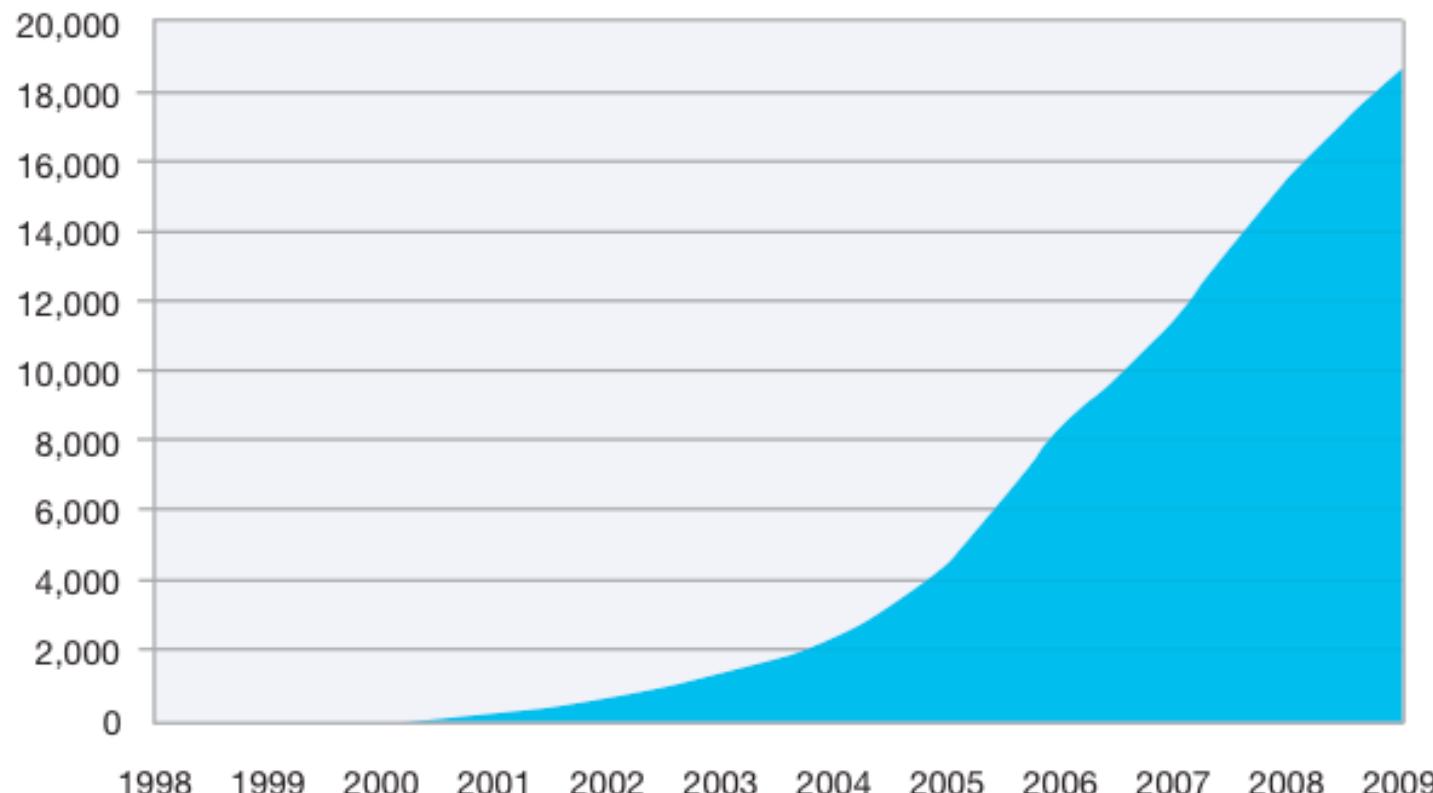
Pourquoi ?



Les hackers sont astucieux
© 2010 - S.Gioria



Cumulative Count of Web Application Vulnerability Disclosures 1998-2009

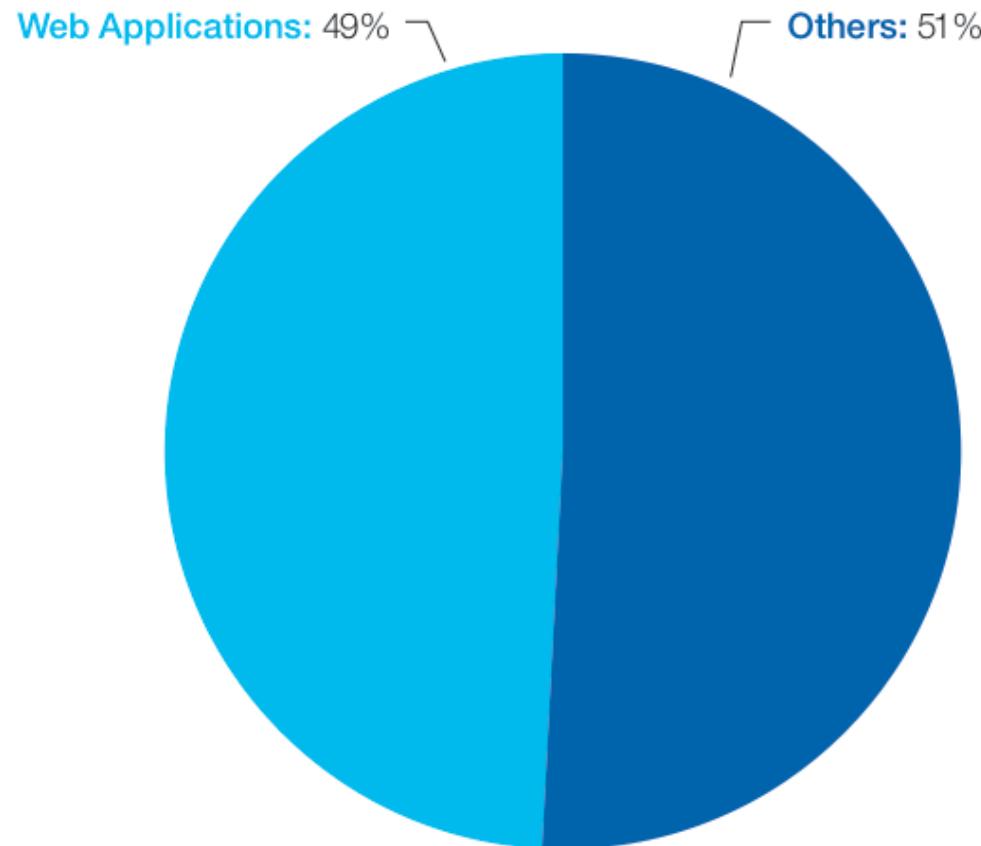


© IBM X-Force 2009 - Extrait du rapport 2009

© 2010 - S.Gioria



**Percentage of Vulnerability Disclosures
that Affect Web Applications
2009**

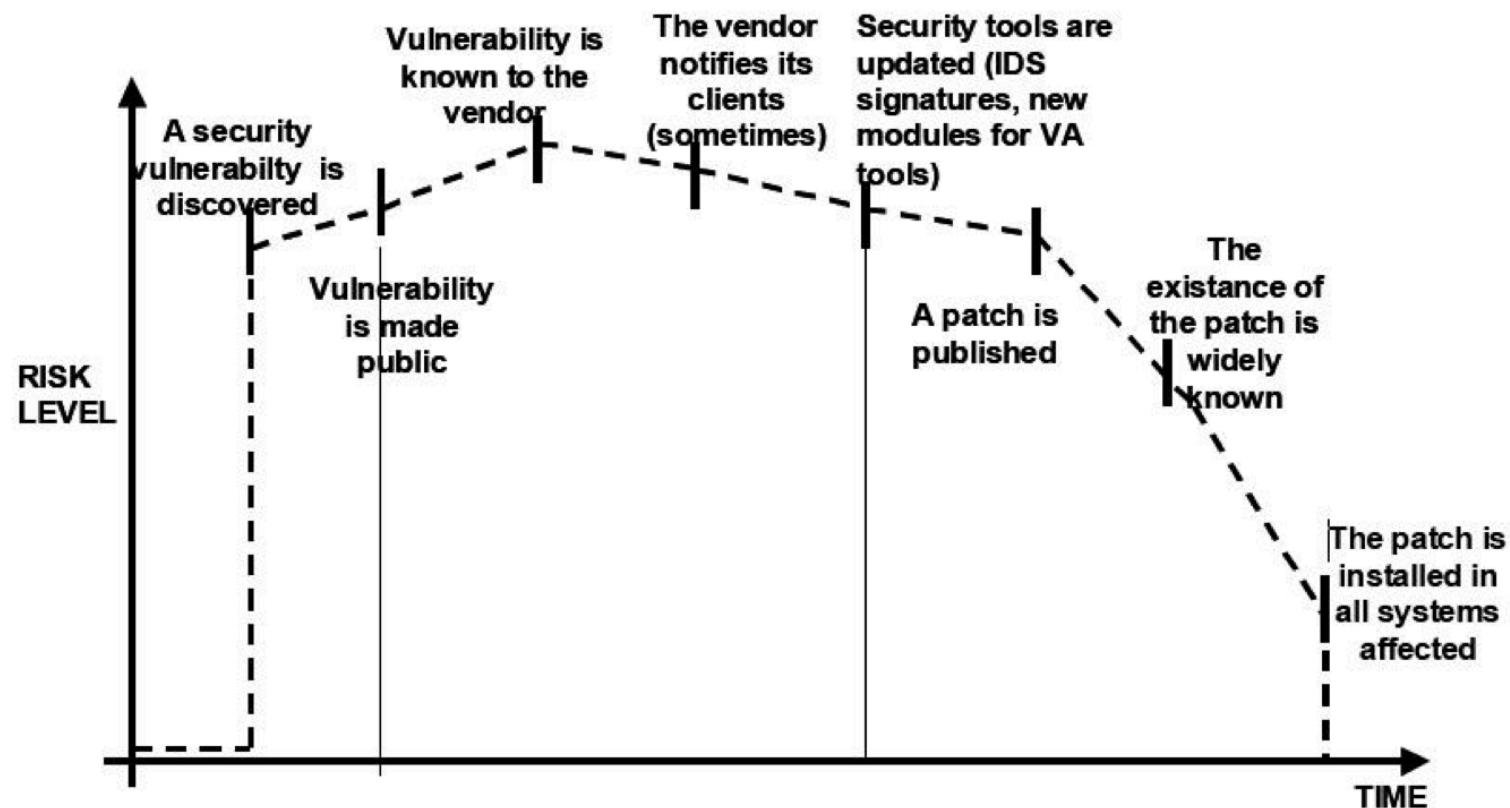


© IBM X-Force 2009 - Extrait du rapport 2009

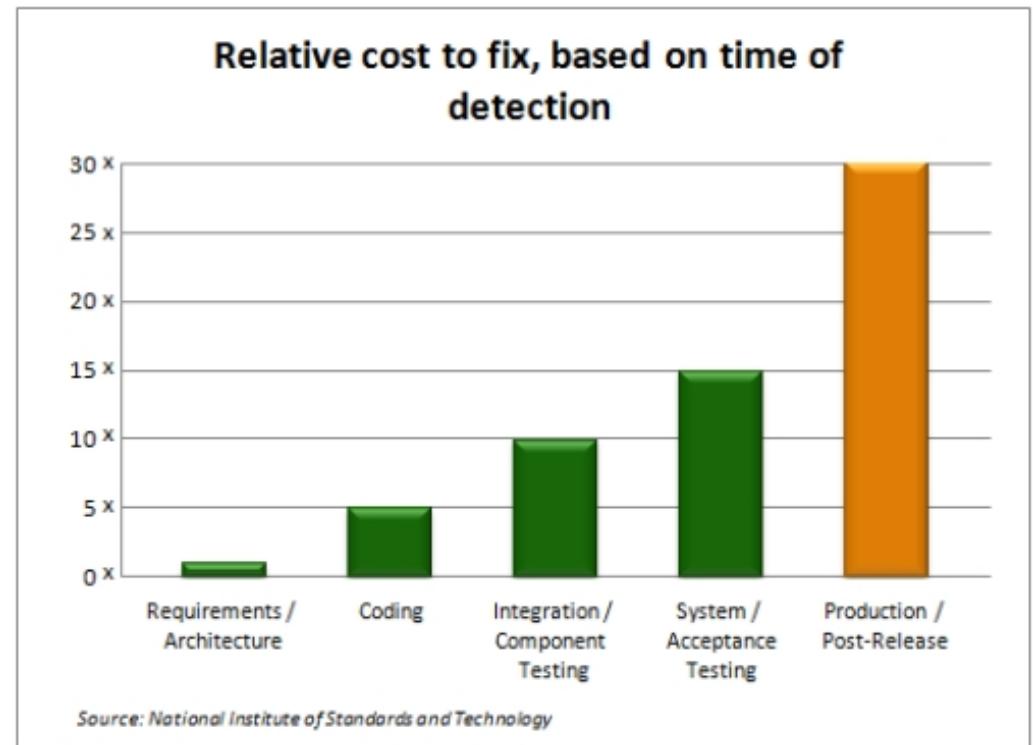
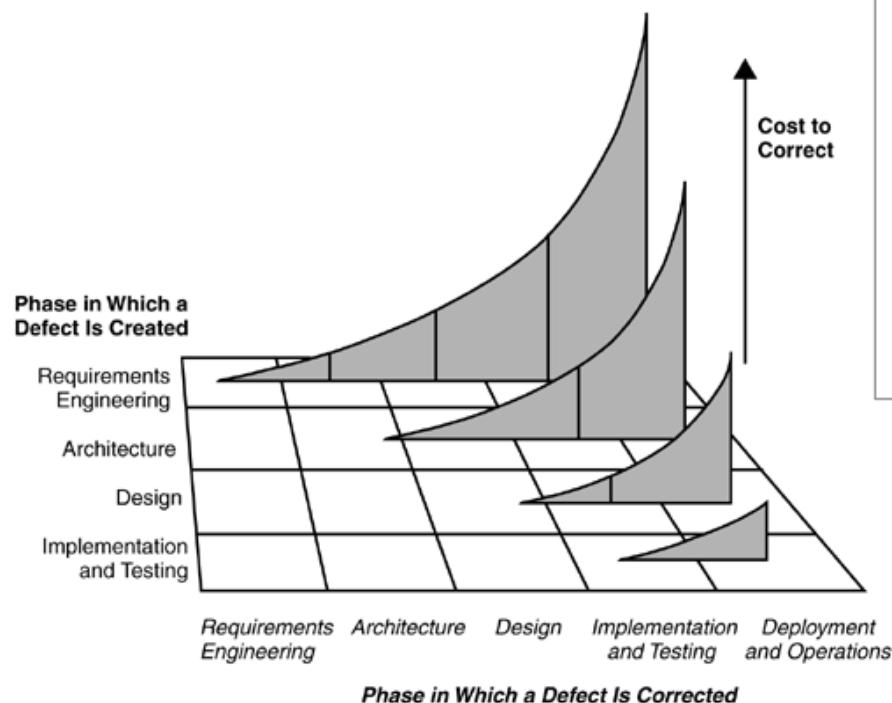
© 2010 - S.Gioria



L'exposition à une vulnérabilité



Cout de la correction d'une faille



Soyons donc précis !

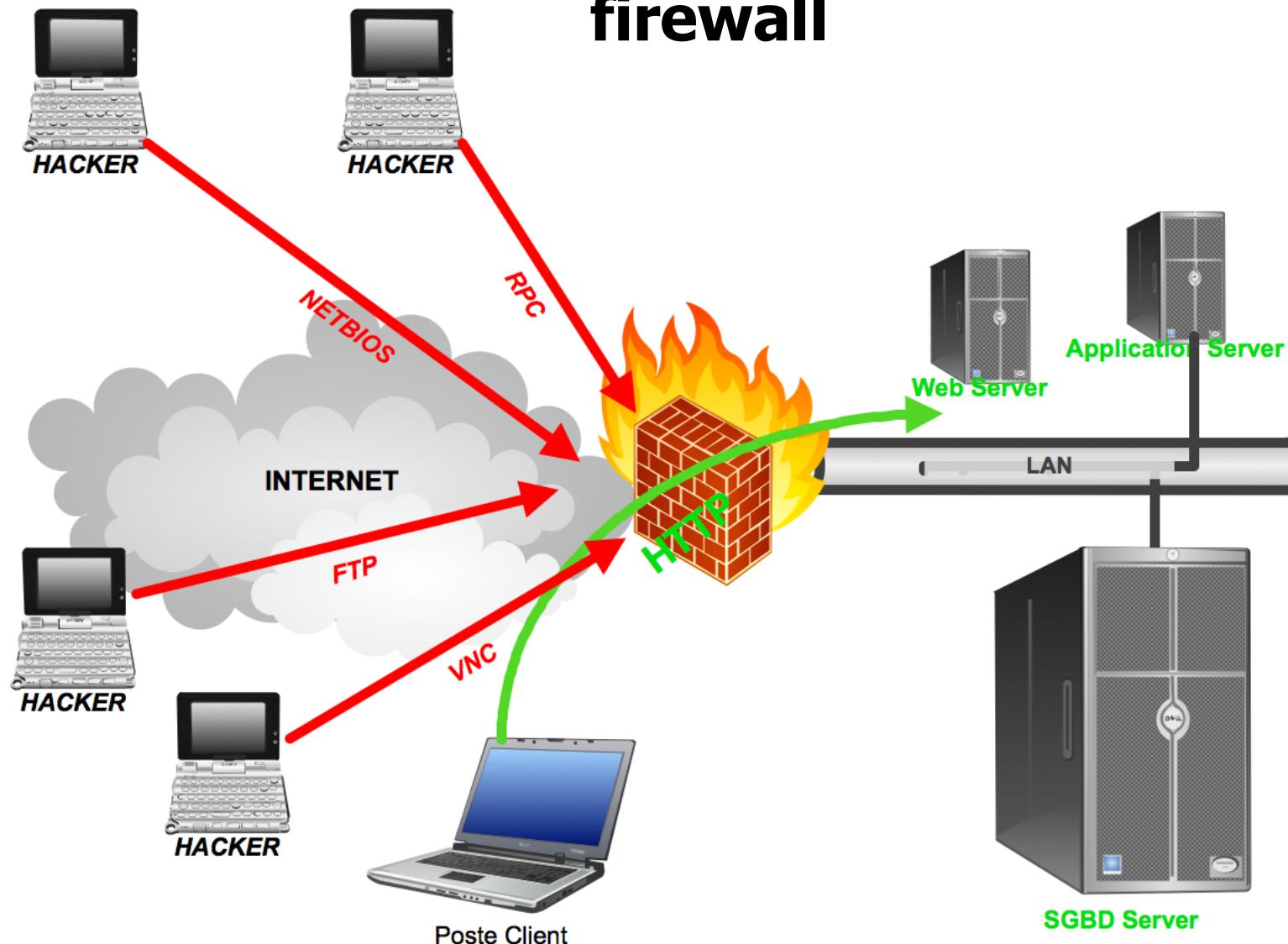


Agenda

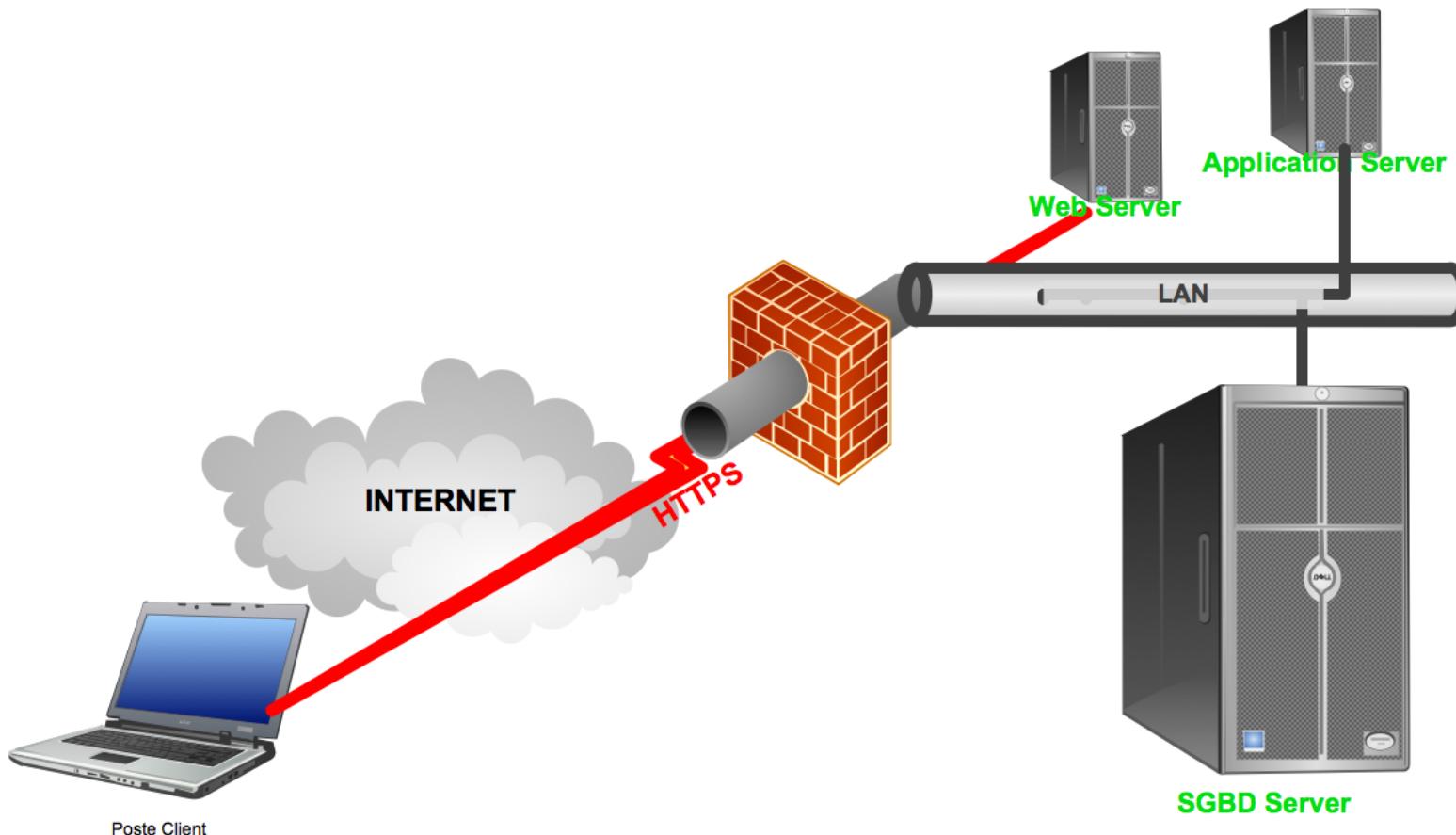
- Pourquoi ?
- 4 préjugés
- La problématique
- Comment s'y prendre
- Et si ?
- Questions ?



Je suis protégé contre les attaques, j'ai un firewall

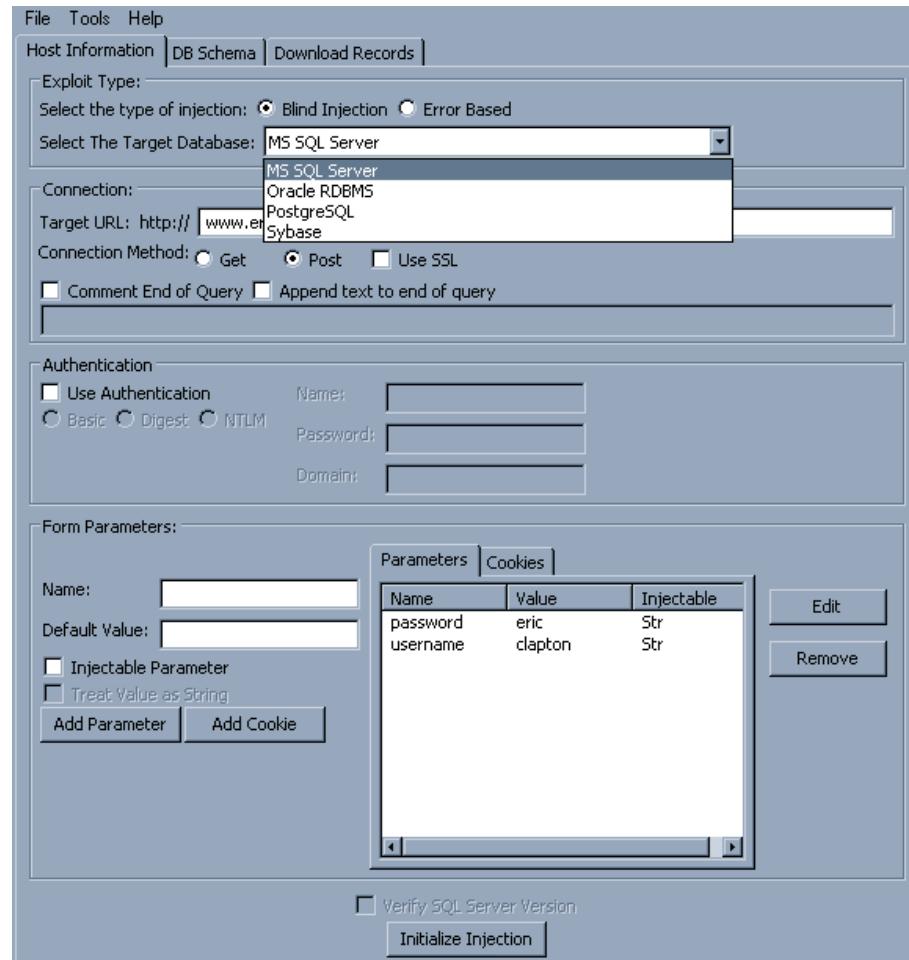


Mon site Web est sécurisé puisque il est protégé par SSL



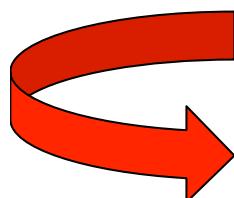
Seuls des génies de l'informatique savent exploiter les failles des applications Web

- 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 marché souterrain.



Une faille sur une application interne n'est pas importante

- De part l'importance du web actuellement, cela peut être catastrophique.
- Nombre de navigateurs permettant 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....



Agenda

- Pourquoi ?
- 4 préjugés
- La problématique
- Comment s'y prendre
- Et si ?
- Questions ?



Le problème

■ Confidentialité

- ▶ Protéger les données, les systèmes, les processus d'un accès non autorisé

■ Intégrité

- ▶ Assurer que les données, systèmes et processus sont valides et n'ont pas été modifiés de manière non intentionnelle.

■ Disponibilité

- ▶ Assurer que les données, systèmes et processus sont accessible au moment voulu



Le problème

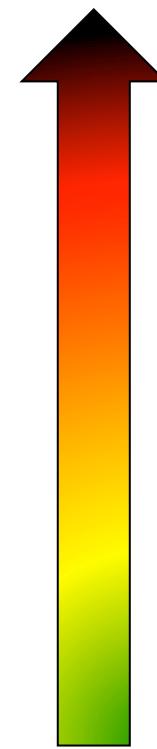
- Traçabilité
 - ▶ Assurer le caractère unique et la reconstru
- « Privacy »
 - ▶ Assurer que les données sont stockées et sous le contrôle de leur propriétaire
- Conformité
 - ▶ Adhérer aux lois et réglementations
- Image de marque
 - ▶ Ne pas se retrouver à la une du journal « Le Monde » suite à un incident

**Ce qui
intéresse
votre boss !**



La menace

- Les gouvernements ?
- Le concurrent
- La mafia
- Le chômeur...
- L'étudiant
- Le « script kiddies »
- Mon fils de 3 ans



Capacité
de
protection

Mais.....« Personne ne nous piratera »



The Web Application Hacker's Handbook
Discovering and Exploiting Security Flaws

Vulnerability Scanner (Enterprise edition)

OWASP Testing Guide v3.0

Audit Workbench - WebGoat

BURP Suite Professional v1.2

IBM Rational Application Developer

CODE OUNCE LABS



Agenda

- Pourquoi ?
- 4 préjugés
- La problématique
- Comment s'y prendre
- Et si ?
- Questions ?



Vainqueurs à la CVE 2010

Produit	1 ^{er}	2 ^{ème}	3 ^{ème}
Système d'exploitation	Linux Kernel (129)	Windows Server 2008 (93)	Apple IOS (35)
SGBD	Oracle (36)	Mysql (3)	MS-SQL Server (1)
Navigateur	Chrome (164)	Safari (130)	Firefox (115)
Clouds ? / Virtualisation	VmWare (125)	Xen (24)	Hyper-V(2) – Azure (1)

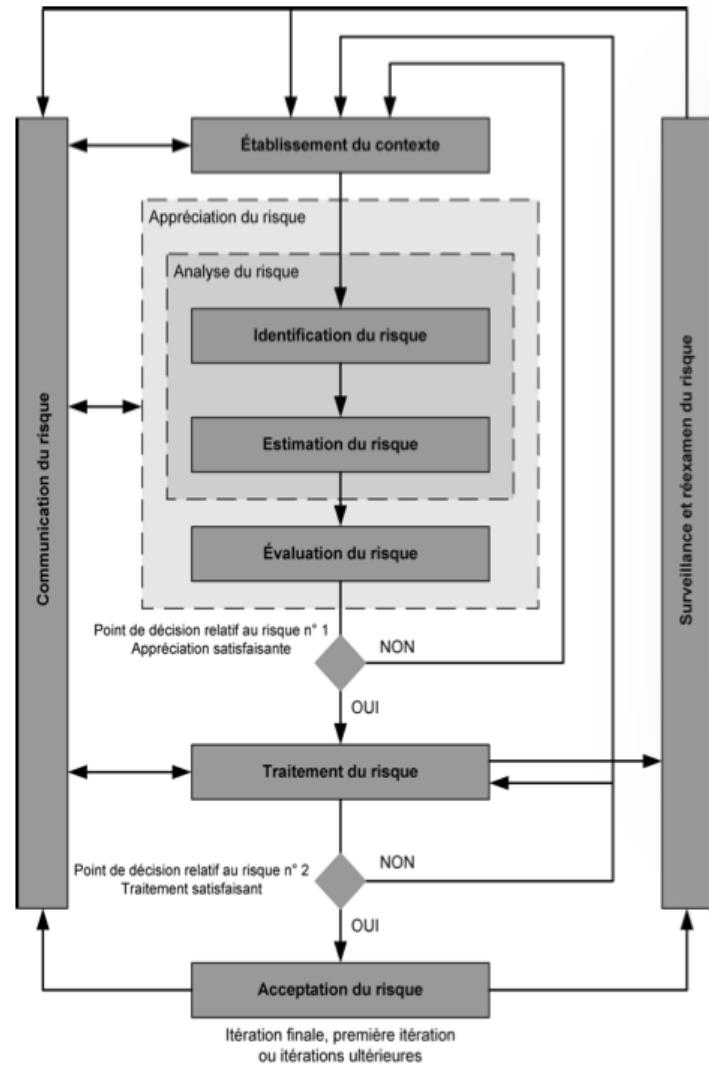
- Il n'y a pas un meilleur éditeur/constructeur.... Personne n'a la solution !
 - Sinon on ne serait pas aux aguets tous les 2èmes mardi du mois.
 - Sinon les bulletins du CERT seraient vides...
 - Et surtout Oracle ne mentirait pas sur son surnom*...
 - La plupart des méthodologies sont en version beta mais s'améliorent...
 - Le Web est compliqué.....

*:unbreakable => dernier Patch Update 10/10 à la CVSS (encore une fois)...

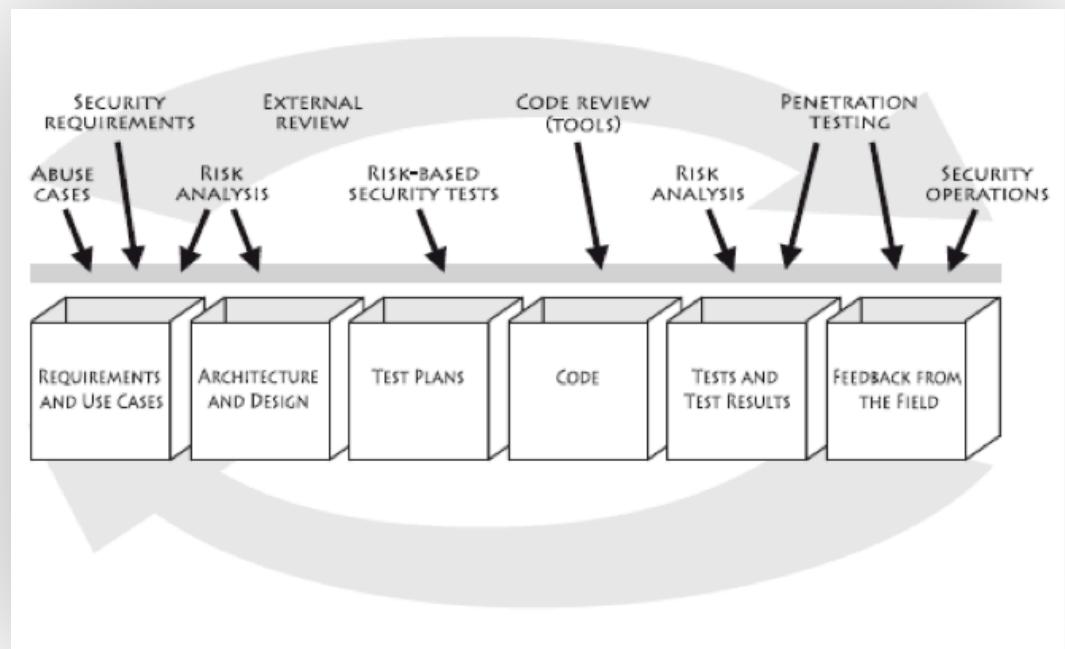


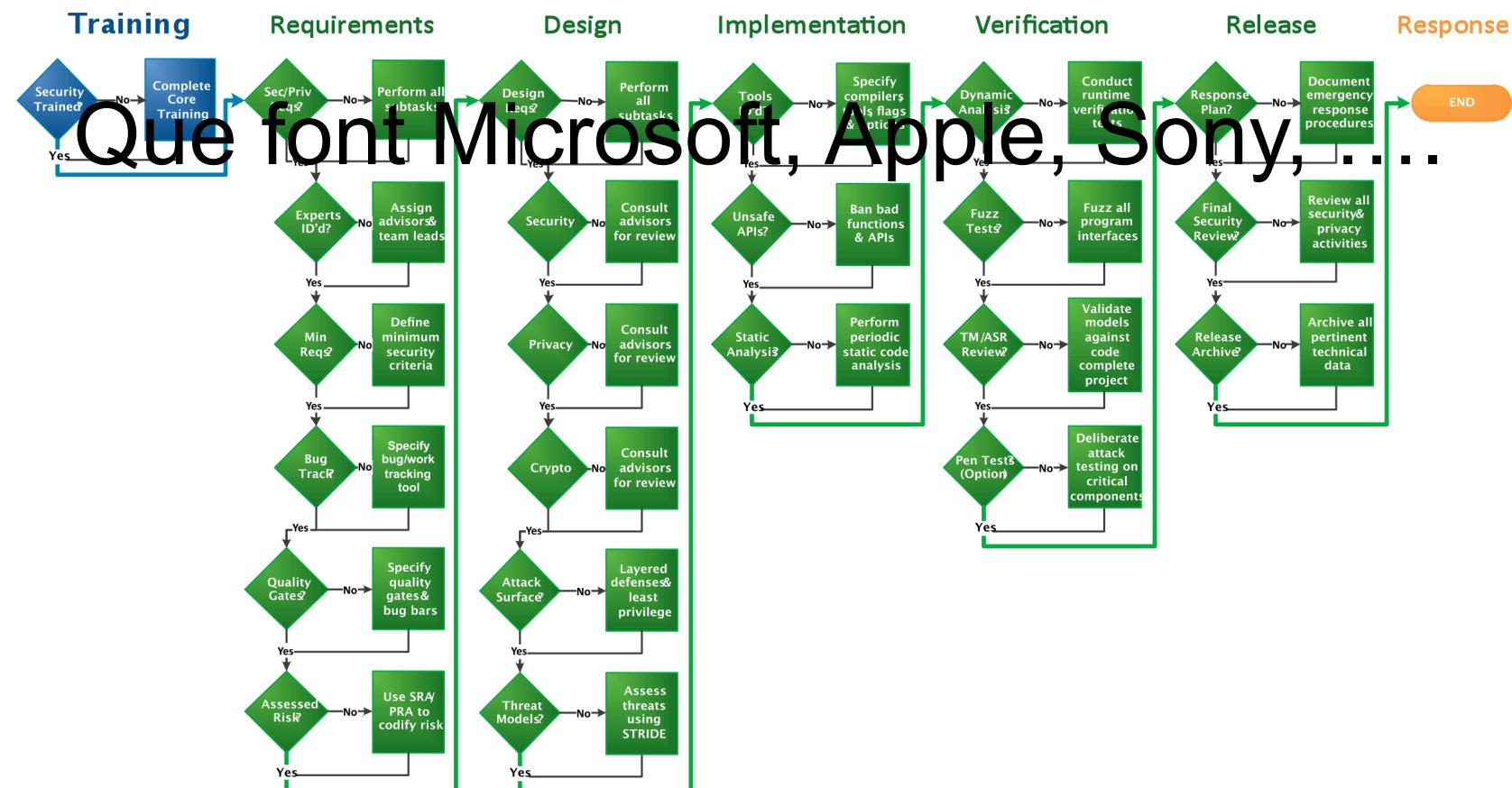
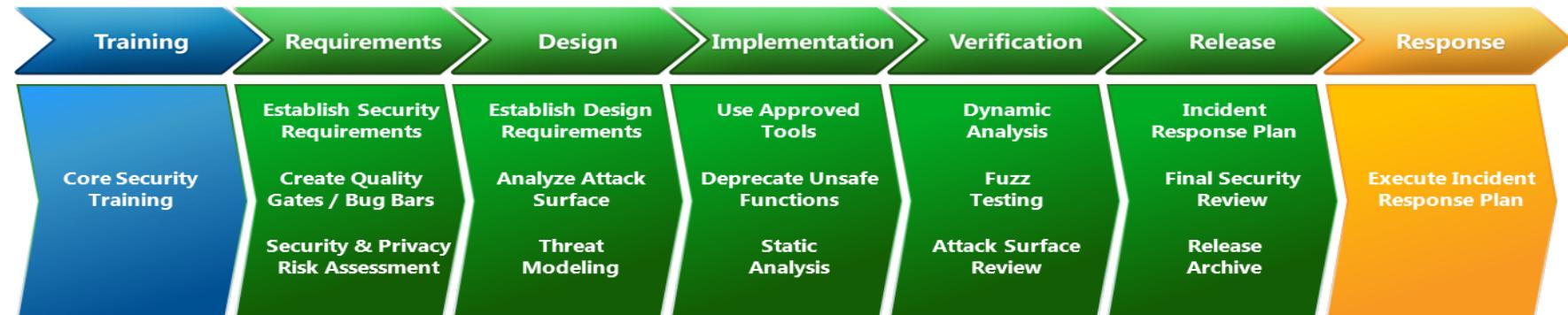
Que vous préconise-t-on ?

E BIOS 2010/ISO 27005 ?

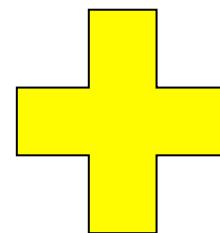


CERT Secure Coding ?









Défense en profondeur



© 2010 - S.Goria



Des politiques – OWASP ASVS



- Quelles sont les fonctionnalités à mettre en oeuvre dans les contrôles de sécurité nécessaires à mon application



Spécifications/Politique de sécurité des développements

- Quelle est la couverture et le niveau de rigueur à mettre en oeuvre lors de la vérification de sécurité d'une application.
- Comment comparer les différentes vérifications de sécurité effectuées



Aide à la revue de code

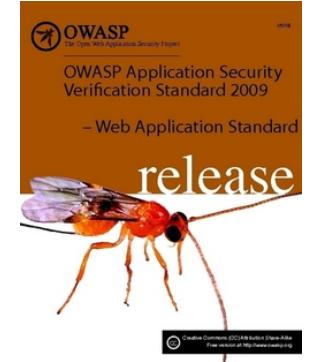
- Quel niveau de confiance puis-je avoir dans une application



Chapitre sécurité des contrats de développement ou des appels d'offres !

OWASP ASVS - 14 familles d'exigences

- V1. Architecture de sécurité
- V2. Authentification
- V3. Gestion de Sessions
- V4. Contrôle d'accès
- V5. Validations d'entrées
- V6. Encodage et échappement de sorties
- V7. Cryptographie
- V8. Gestion des erreurs et de la journalisation
- V9. Protection des données
- V10. Sécurité des communications
- V11. HTTP Sécurisé
- V12. Configuration de la sécurité
- V13. Recherche de codes malicieux
- V14. Sécurité interne



V5 - Input Validation Verification Requirements

The Input Validation Requirements define a set of requirements for validating input so that it is suitable for use within an application. The table below defines the corresponding verification requirements that apply for each of the four verification levels.

Table 5 - OWASP ASVS Input Validation Requirements (V5)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V5.1 Verify that the runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.	✓	✓	✓	✓	✓	✓
V5.2 Verify that a positive validation pattern is defined and applied to all input.	✓	✓	✓	✓	✓	✓
V5.3 Verify that all input validation failures result in input rejection or input sanitization.	✓		✓	✓	✓	✓
V5.4 Verify that a character set, such as UTF-8, is specified for all sources of input.			✓	✓	✓	✓
V5.5 Verify that all input validation is performed on the server side.			✓	✓	✓	✓
V5.6 Verify that a single input validation control is used by the application for				✓	✓	✓



Principes de développement

KISS : Keep it Short and Simple

■ 8 étapes clés :

- ▶ Validation des entrées
- ▶ Validation des sorties
- ▶ Gestion des erreurs
- ▶ Authentification ET Autorisation
- ▶ Gestion des Sessions
- ▶ Sécurisation des communications
- ▶ Sécurisation du stockage
- ▶ Accès Sécurisé aux ressources



OWASP
The Open Web Application Security Project
<http://www.owasp.org>

A Guide to Building
Secure Web
Applications and Web
Services

2.0 Black Hat Edition

July 27, 2005

Copyright © 2002-2005. The Open Web Application Security Project (OWASP). All Rights Reserved.
Permission is granted to copy, distribute, and/or modify this document provided this copyright notice and attribution
to OWASP is retained.



KISS : Keep it Short and Simple

- Suivre constamment les règles précédentes
- Ne pas « tenter » de mettre en place des parades aux attaques
- Développer sécurisé ne veut pas dire prévenir la nouvelle vulnérabilité du jour
- Construire sa sécurité dans le code au fur et à mesure et ne pas s'en remettre aux éléments d'infrastructures ni au dernier moment.

A Guide to Building
Secure Web
Applications and Web
Services

2.0 Black Hat Edition

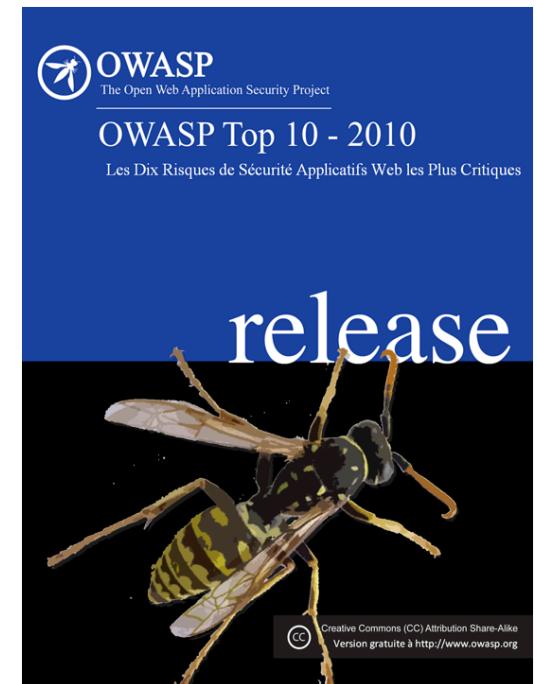
July 27, 2005

Copyright © 2002-2005, The Open Web Application Security Project (OWASP). All Rights Reserved.
Permission is granted to copy, distribute, and/or modify this document provided the copyright notice and attribution
to OWASP is retained.



Mettre en place les Tests Qualité

- Ne pas parler de tests sécurité !
- Définir des fiches tests simples, basées sur le Top10/TopX :
 - ▶ Tests d'attaques clients/image de marque (XSS)
 - ▶ Tests d'intégrité (SQL Injection, ...)
 - ▶ Tests de conformité (SQL/LDAP/XML Injection)
 - ▶ Tests de configuration (SSL, interfaces d'administration)
- Ajouter des revues de code basées sur des checklists
 - ▶ SANS/Top25
 - ▶ OWASP ASVS
 - ▶



Appliquez la règle du 80/20



http://www.owasp.org/index.php/Top_10



Agenda

- Pourquoi ?
- 4 préjugés
- La problématique
- Comment s'y prendre
- Et si ?
- Questions ?

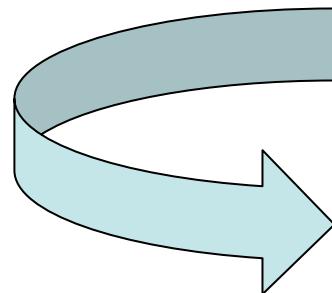


Et si vous commençiez ?

■ Il y a deux pas à franchir

1. Commencer

2. Utiliser les fameuses checklists



**Je commence à utiliser ces
fameuses checklists**



■ Je configure mon outil de suivi de bogue

- Ajout d'une catégorie "sécurité" et les éléments de suivi!

■ Je met en place des tests sécurité Web

- Automatisés si je n'ai pas le temps...
- L'OWASP Top10 et l'OWASP Testing Guide sont un bon début.
- L'OWASP ASVS est une avancée supplémentaire !

■ Je corrige tous les problèmes sécurité que je trouve !

➤ **Si vous n'êtes pas prêts à corriger, ne cherchez pas !**



■ Je forme et partage

► Développeurs, Architectes,

- Classification des Menaces (WASC)
<http://projects.webappsec.org/Threat-Classification>
- OWASP Top10 (OWASP)
http://www.owasp.org/index.php/Top_10

■ Je continue à améliorer mon cycle :

- Security Development Lifecycle (Microsoft)
<http://blogs.msdn.com/sdl/>
- Open Software Assurance Maturity Model (OWASP)
<http://www.opensamm.org/>
- Building Security in Maturity Model (Digital/Fortify)
<http://www.bsi-mm.com/>



J'externalise...

- J'ajoute les points de contrôles OWASP ASVS en amont...
 - ▶ Cahier des charges
 - ▶ Appels d'offres,
 - ▶
- Je sécurise ma relation avec un contrat de développement sécurisé
 - ▶ [http://www.owasp.org/index.php/
Category:OWASP_Legal_Project](http://www.owasp.org/index.php/Category:OWASP_Legal_Project)



Mon informatique « s'envole »...

■ Les menaces restent les mêmes :

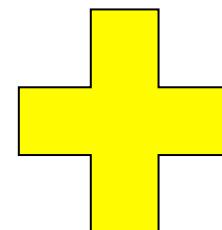
- ▶ Injections, XSS, CSRF,

■ Mais quelques unes s'ajoutent :

- ▶ abus de ressources
- ▶ code malveillant
- ▶ perte de données
- ▶ vol ou détournement du service
- ▶ partage de la technologie



Rappel !



Remerciements

■ Pascal Saulière (@psauliere)



■ AF (@starbuck3000)



■ Les deux Arthur(s)





- ◆ AppSec Europe – Dublin/Irlande
 - Training – 7 et 8 Juin
 - Conférences – 9 et 10 Juin

