



Sécurité du Développement Web

CRI'Ouest
Nantes– France
29 Novembre 2010

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)

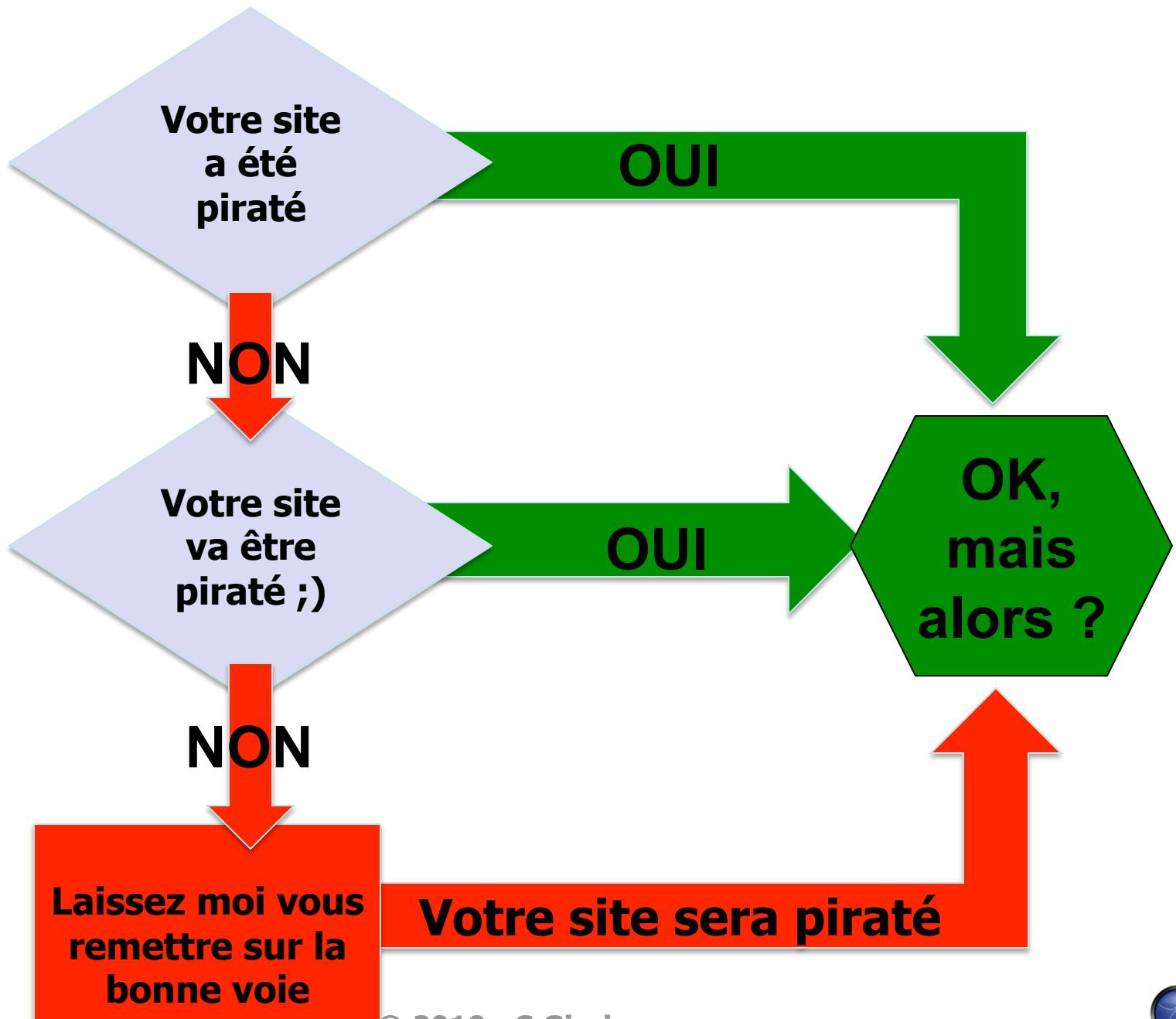


CISA & ISO 27005 Risk Manager

- +13 ans d'expérience en Sécurité des Systèmes d'Information
- Différents postes de manager SSI dans la banque, l'assurance et les télécoms
- Expertise Technique
 - ✓ PenTesting, Digital Forensics
 - ✓ S-SDLC
 - ✓ Gestion du risque, Architectures fonctionnelles, Audits
 - ✓ Consulting et Formation en Réseaux et Sécurité
- Domaines de préférence :
 - ✓ Web 4.2, WebServices, Insécurité du Web.

Twitter :@SPoint



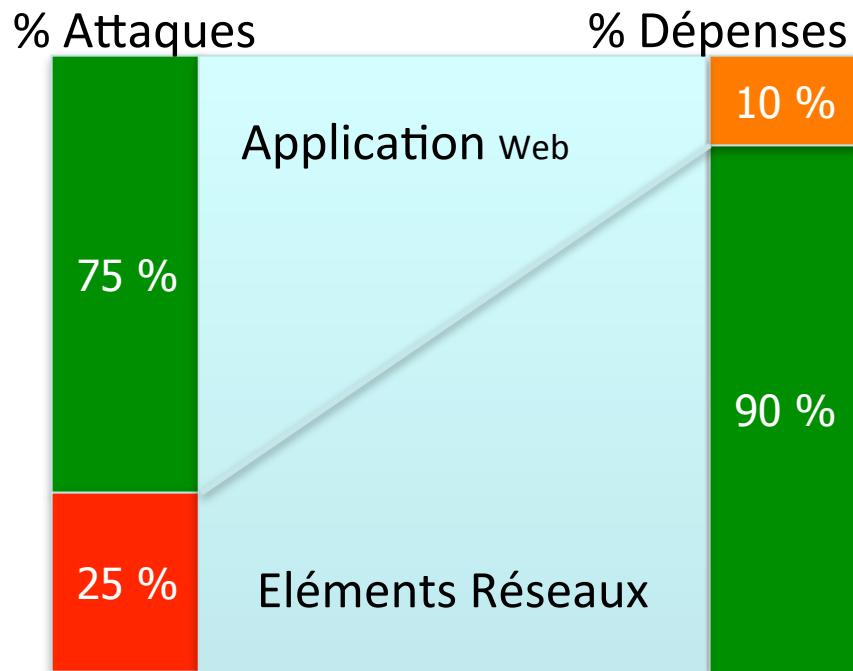


Agenda

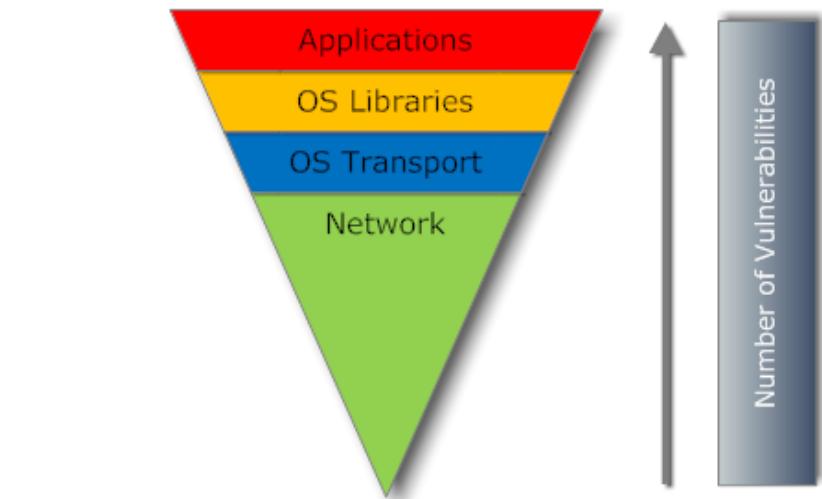
- Pourquoi ?
- 4 préjugés
- La problématique
- Comment s'y prendre
- Et si ?
- Retour d'expérience
- Questions ?



Faiblesse des Applications Web



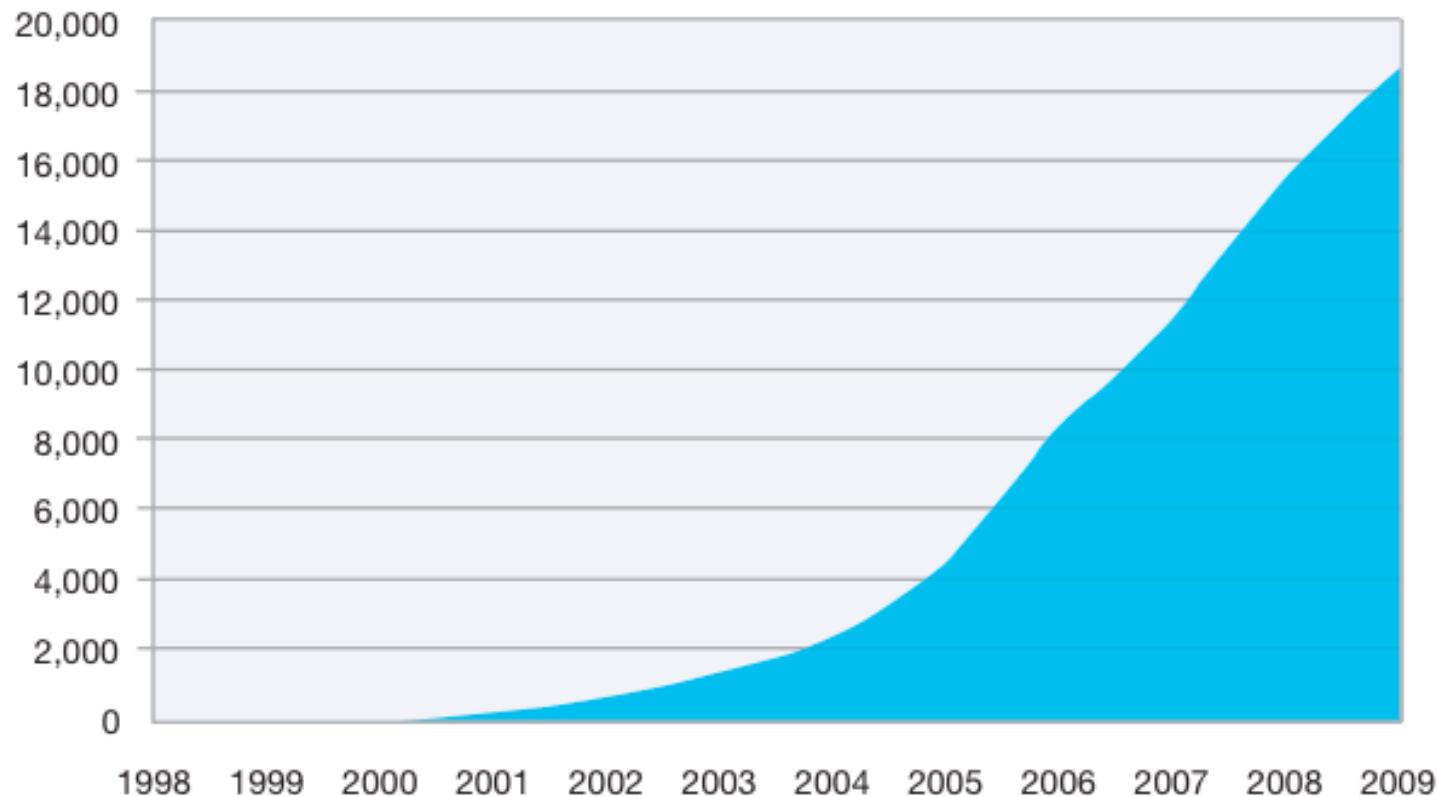
Etude du GARTNER 2003
75% des attaques ciblent le niveau Applicatif
66% des applications web sont vulnérables



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



Cumulative Count of Web Application Vulnerability Disclosures 1998-2009



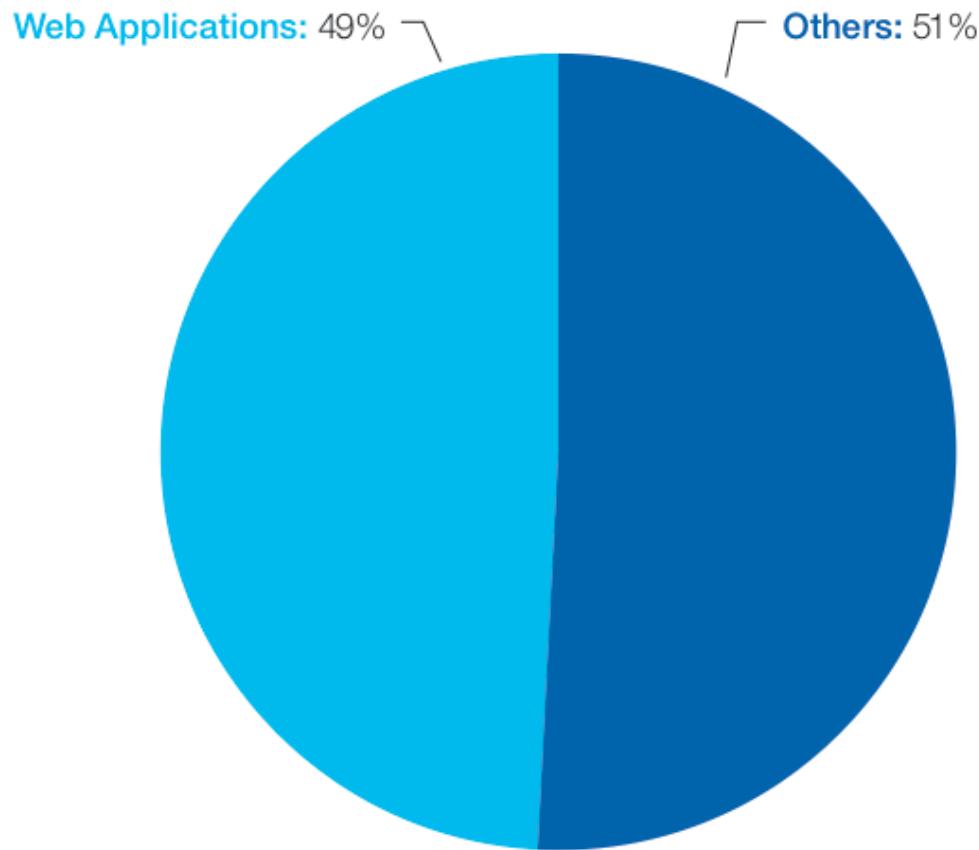
© IBM X-Force 2009 - Extrait du rapport 2009

29/11/2010

© 2010 - S.Gioria



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



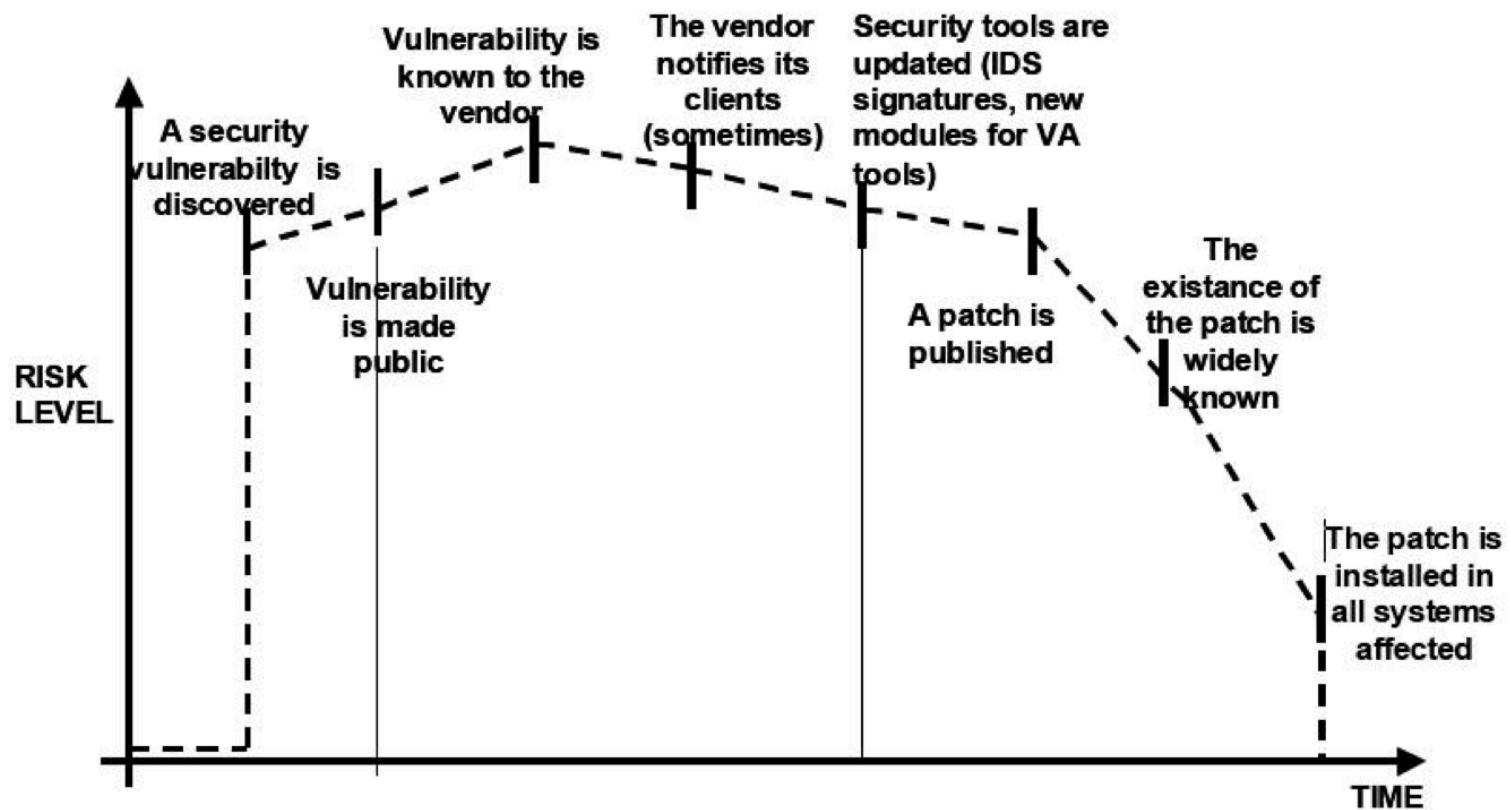
© IBM X-Force 2009 - Extrait du rapport 2009

29/11/2010

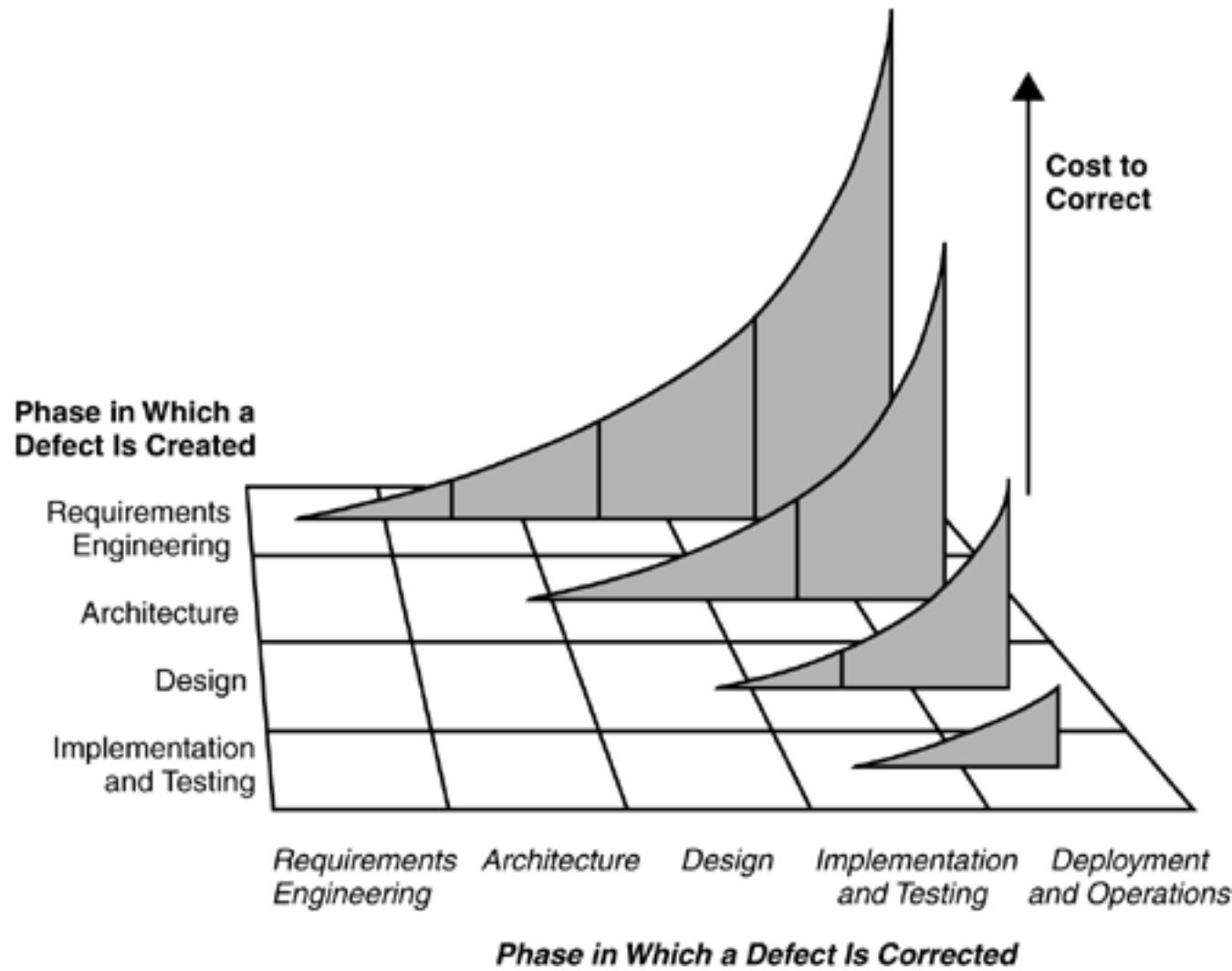
© 2010 - S.Gioria



L'exposition à une vulnérabilité



Cout de la correction d'une faille

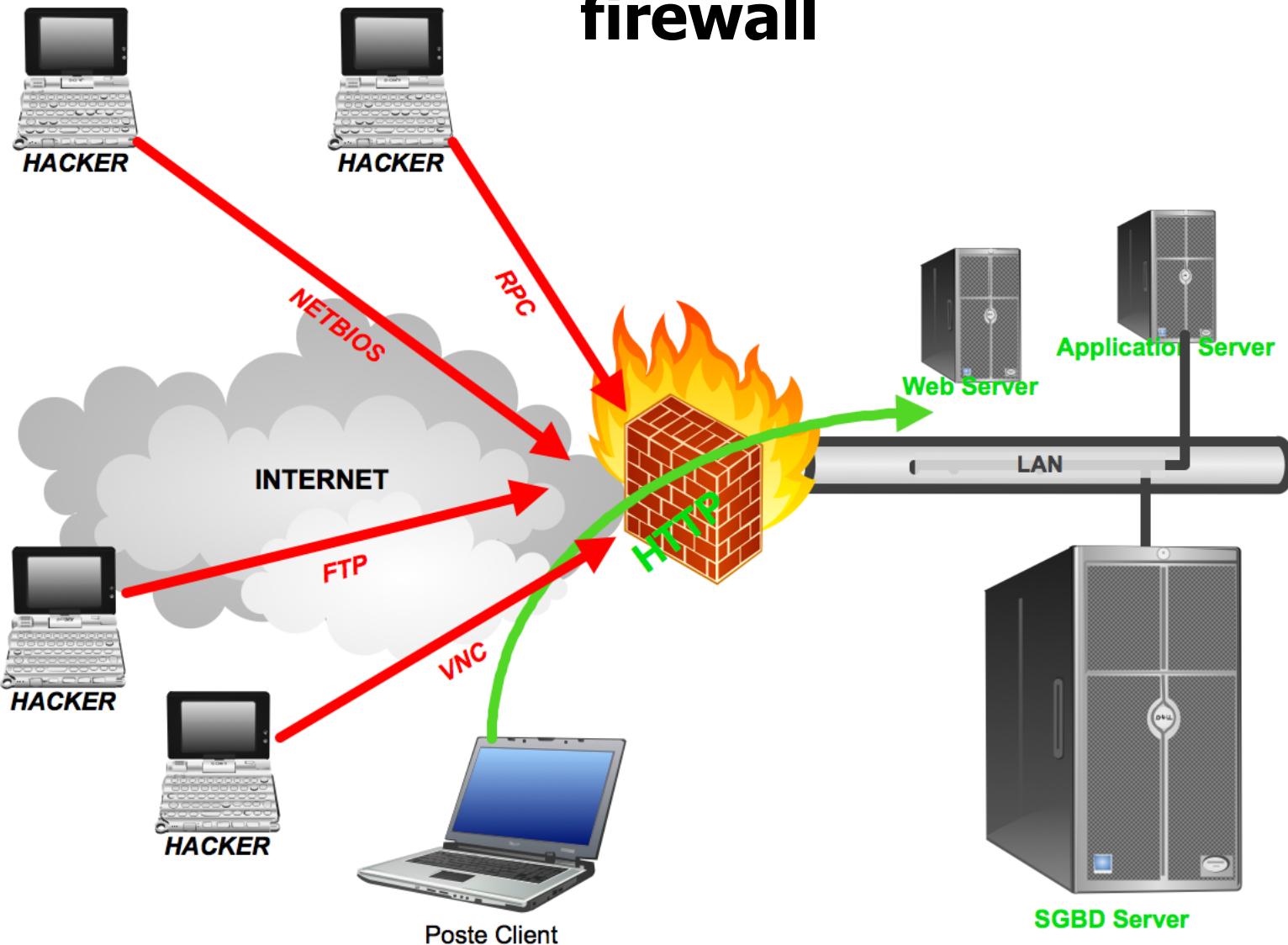


Agenda

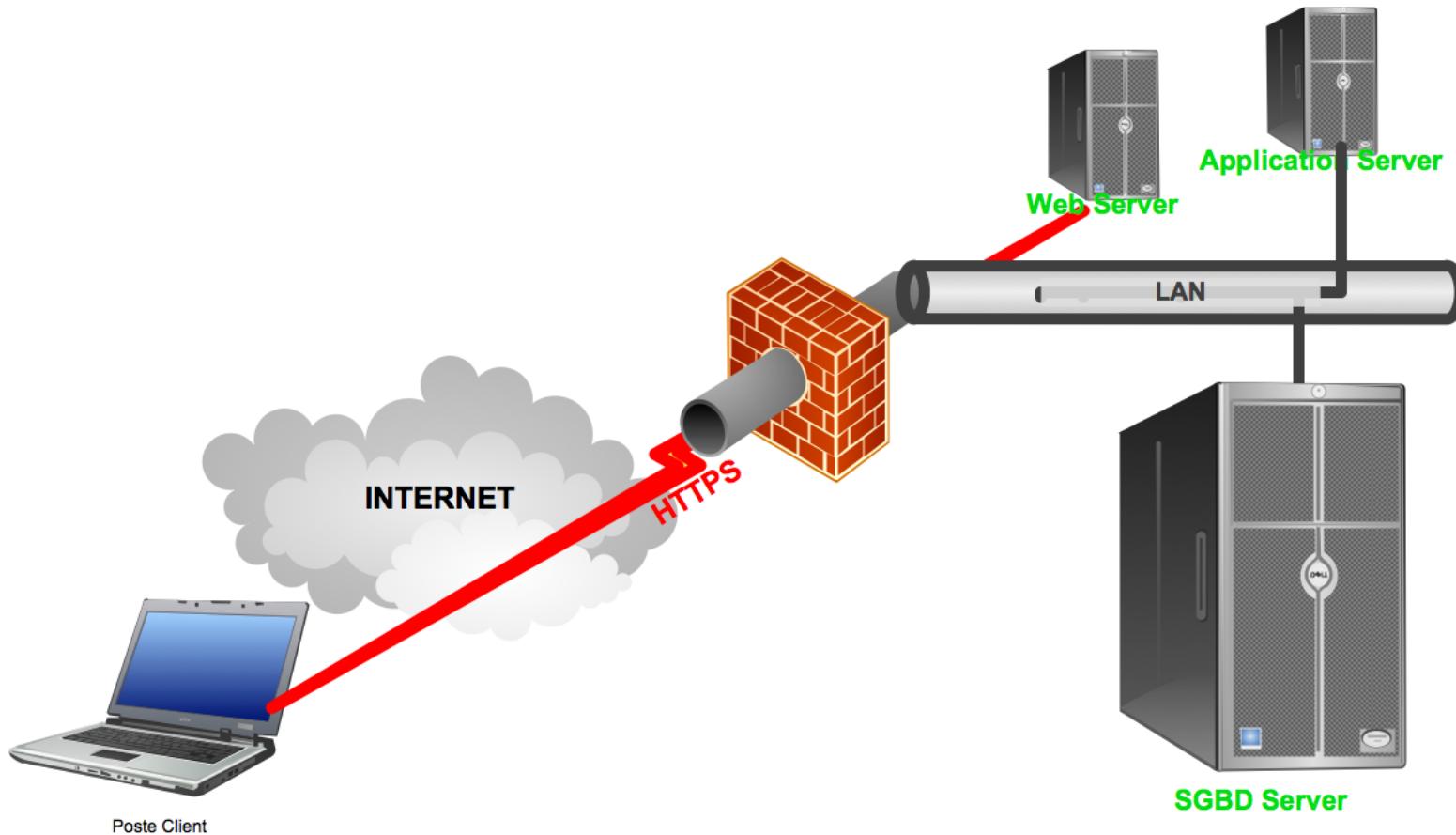
- Pourquoi ?
- 4 préjugés
- La problématique
- Comment s'y prendre
- Et si ?
- Retour d'expérience
- Questions ?



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

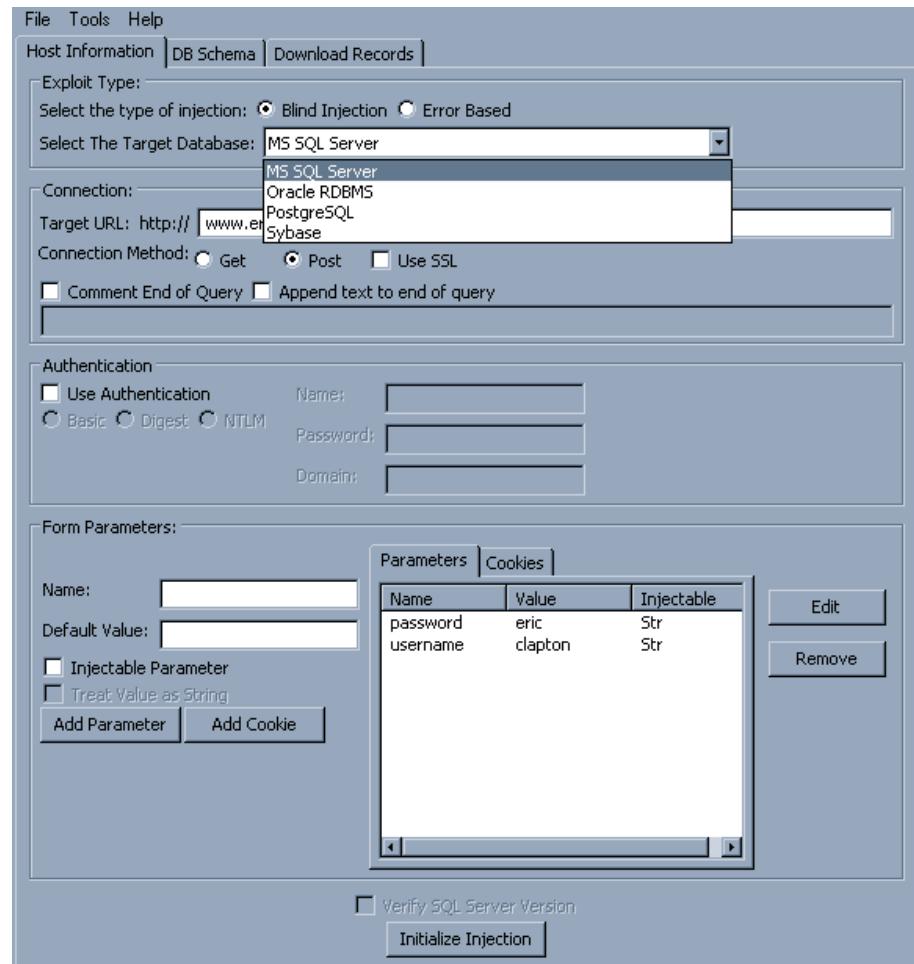


Mon site Web est sécurisé puisque il est protégé par SSL



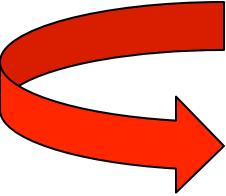
Seuls des génies de l'informatique savent exploiter les failles des applications Web

- 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 ?
- Retour d'expérience
- 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

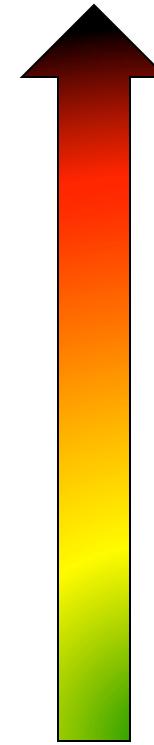
- Traçabilité
 - ▶ Assurer le suivi des données et la reconstruction de leur évolution
- « Privacy »
 - ▶ Assurer que les données sont stockées et traitées sous le contrôle de leur propriétaire
- Conformité
 - ▶ Adhérer aux lois et réglementations
- Image de marque
 - ▶ Ne pas se retrouver à la une du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

**Ce qui
intéresse
votre boss !**



La menace

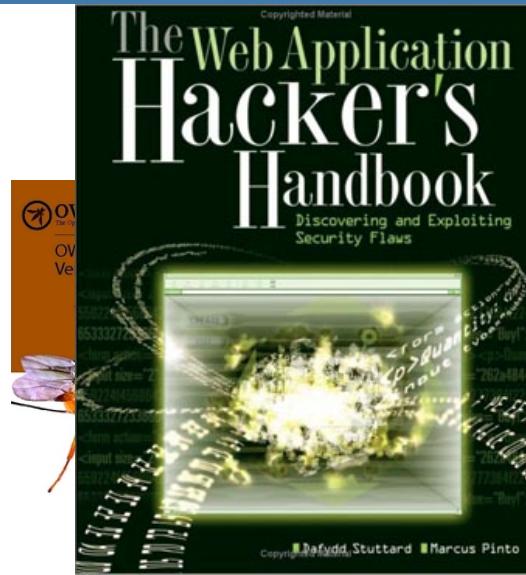
- Les gouvernements ?
- Le concurrent
- La mafia
- Le chômeur...
- L'étudiant
- Le « script kiddies »
- Mon fils de 3 ans



Capacité
de
protection

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





A screenshot of the Acunetix Web Vulnerability Scanner interface. It shows a tree view of scanned files under 'Scan Thread 1'. A 'Vulnerability information' panel displays a threat level of 'Level 3: High' (Acunetix threat). Below it, a chart shows 'Total alerts found': 341 (High), 9 (Medium), 25 (Low), and 55 (Informational).

A screenshot of the Fortify Audit Workbench. It shows a 'Project Summary' for 'Login.java' with a code snippet: 'boolean authenticated = false; try { String query = "SELECT * FROM employee WHERE userid = " + userId + " and password = " + password'; // System.out.println("Query:" + query);'. A 'Hot (184)' section highlights potential SQL injection vulnerabilities.

A screenshot of Burp Suite Professional. It shows a 'Project Summary' for 'Challenge2Screen.java:217 (SQL Injection)'. The proxy history pane lists several requests, including one from 'ad.doubleclick.net' to 'ad.amazon.us'. The 'Intercept' tab is selected, showing a modified request for 'Challenge2Screen.java:217 (SQL Injection)'.

A screenshot of IBM Rational AppScan. It shows a 'demoscan.scan' report with a 'Security Issues' list and a 'Remediation Tasks' section. A 'Blind SQL Injection' advisory is shown with a severity of 'High' and a type of 'Application-level test'.

A screenshot of Ounce Labs. It shows a 'CODE' logo and a 'Blind SQL Injection' section with a bar chart titled 'Total number of iss' showing counts for High (35), Medium (31), Low (32), and Info (11) severity levels. The 'OUNCE LABS' logo is at the bottom right.



29/11/2010



Agenda

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



Avant-propos...

■ Personne n'a la solution !

- ▶ Sinon on ne serait pas aux aguets tous les 2èmes mardi du mois.
- ▶ Sinon les bulletins du CERTA seraient vides...
- ▶ Et surtout Oracle ne mentirait pas sur son surnom*...

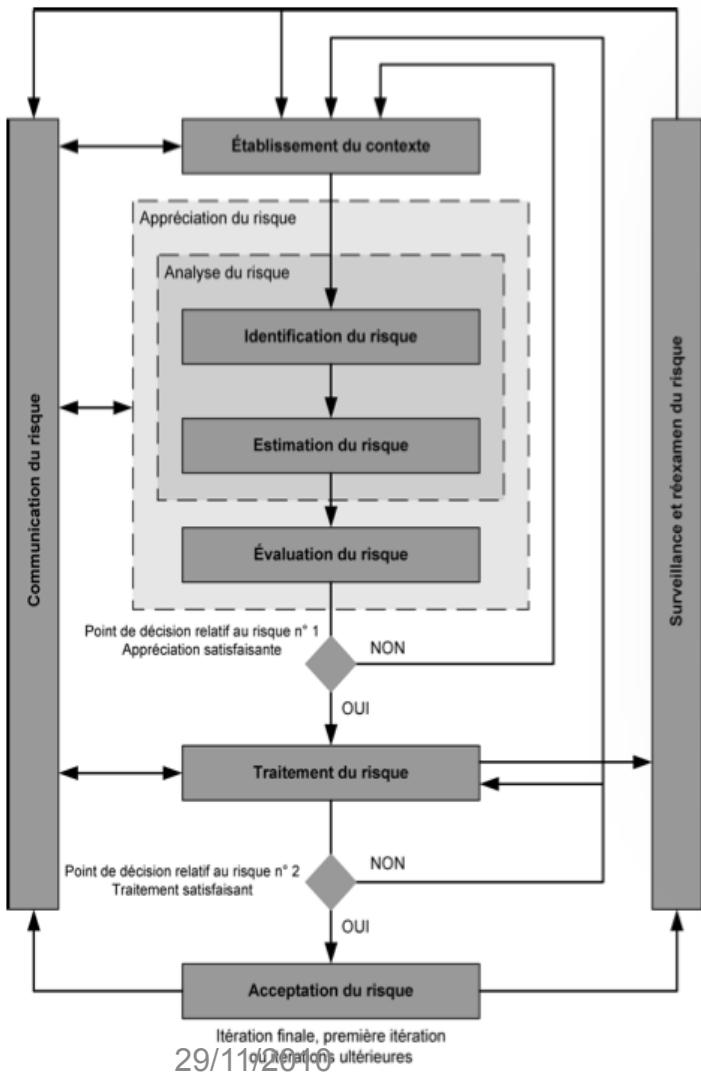
■ La plupart des méthodologies sont en version beta mais s'améliorent...

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

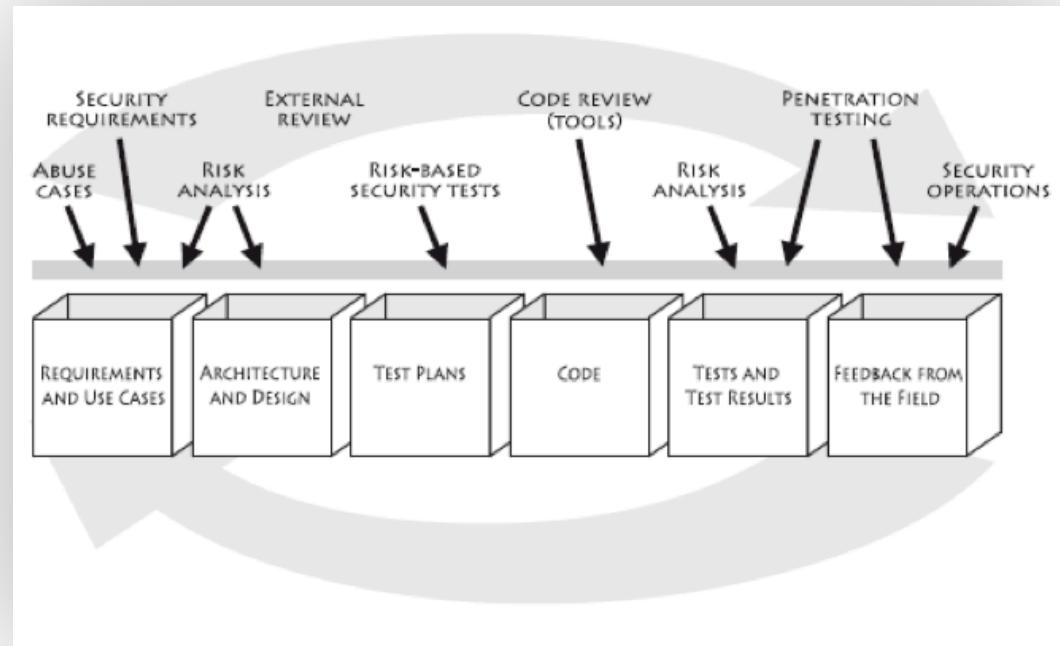


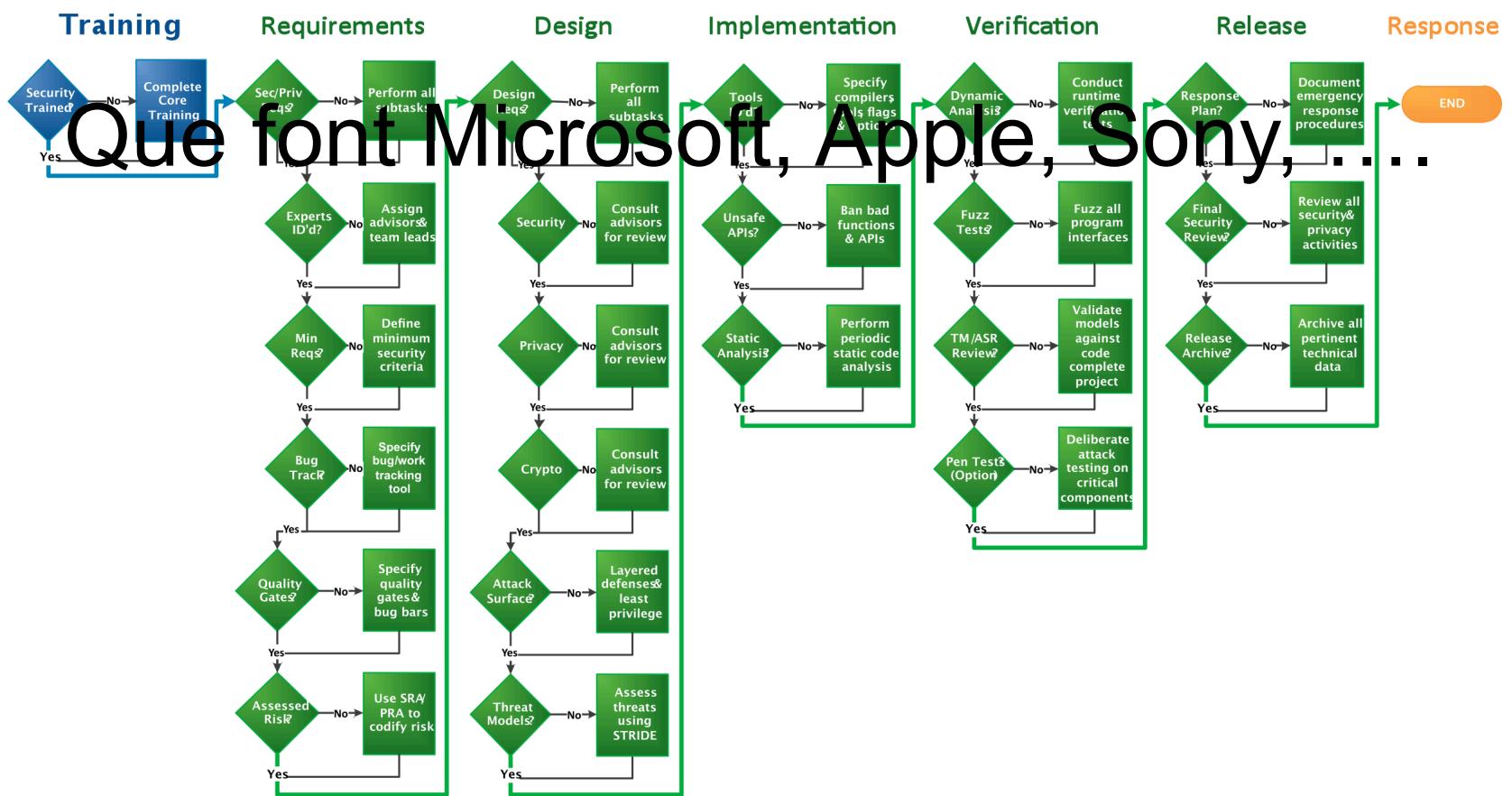
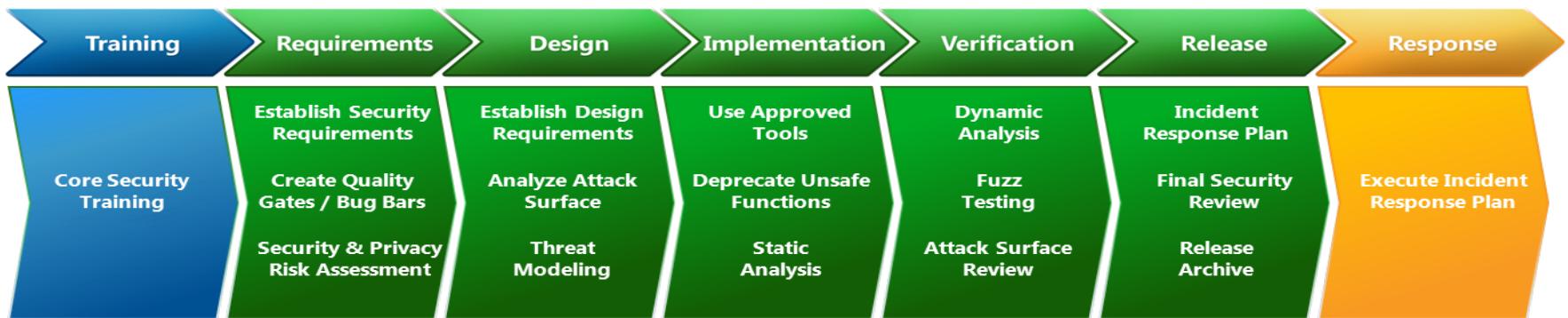
Que vous préconise-t-on ?

E BIOS 2010/ISO 27005 ?



CERT Secure Coding ?



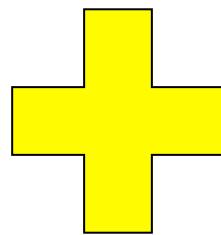




29/11/2010

© 2010 - S.Gioria





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

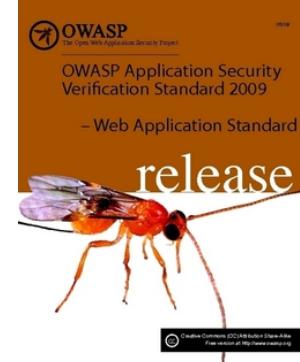


Chapitre sécurité des contrats de développement ou des appels d'offres !



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





Creative Commons CC BY-SA License Share Alike

From www.owasp.org/index.php

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



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.



KISS : Keep it Short and Simple

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.

- 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.



Mettre en place les Tests Qualité

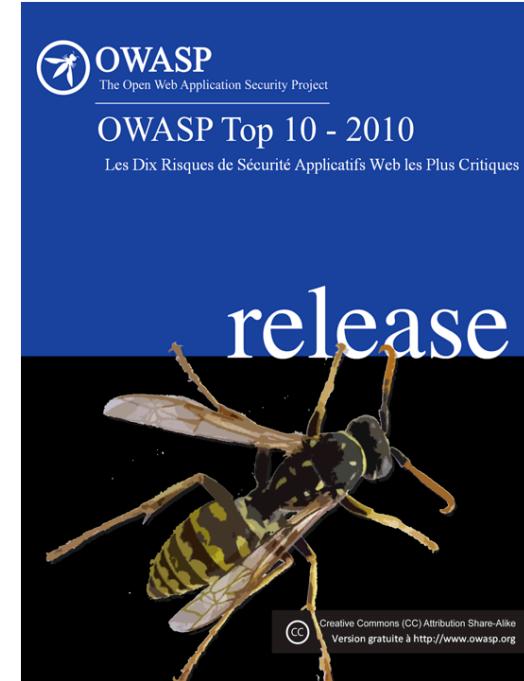
■ Ne pas parler de tests sécurité !

■ 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
- ▶ 29/11/2010



Appliquez la règle du 80/20

A1: *Injection*

A2: *Cross Site Scripting (XSS)*

A3: Mauvaise gestion des sessions et de l'authentification

A4: Référence directe non sécurisée à un objet

A5: *Cross Site Request Forgery (CSRF)*

A6: Mauvaise configuration sécurité

A7: Mauvais stockage cryptographique

A8: Mauvaise restriction d'accès à une URL

A9 : Protection insuffisante lors du transport des données

A10: Redirections et transferts non validés

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



Agenda

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

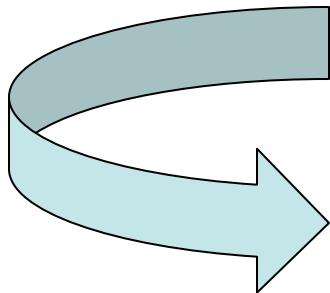


Et si vous commençiez ?

■ 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 (Cigital/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 :

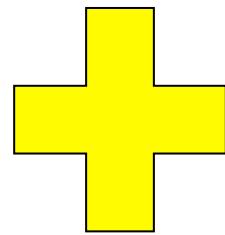
- ▶ Injections, XSS, CSRF,

- Mais quelques unes s'ajoutent :

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



Rappel !



Agenda

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



Le décor

- Société Française d'environ 400 personnes
- Forte dépendance à l'informatique
 - ▶ métier principal
- Beaucoup de compétences internes
 - ▶ Peu d'externalisation
- Créditation d'un poste de RSSI
 - ▶ Objectif de réduire le nombre de corrections sécurité
 - ▶ Améliorer la crédibilité vis à vis des clients
- Tests de sécurité réguliers après mise en production de modules/applications



Les étapes

■ Etat des lieux

- ▶ Relecture des différents audits passés pour établir le contexte et le niveau de maturité en sécurité :
 - En mode 'pifométrique' adapté de l'OpenSamm (<http://www.OpenSamm.ORG>)

■ Approche de gestion des projets

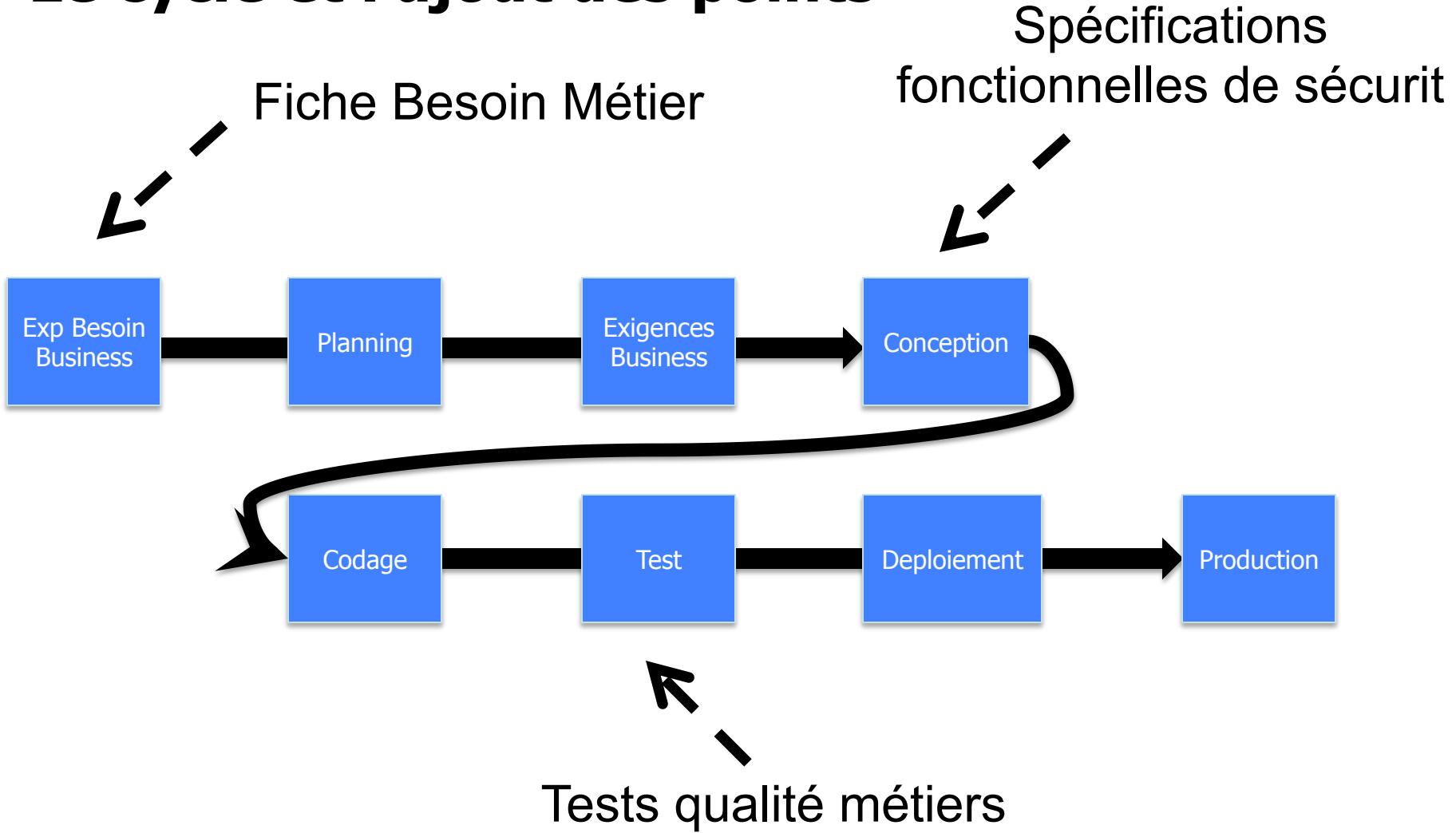
- ▶ Visualisez les endroits où il est possible d'entrer de la sécurité

■ Déploiement

- ▶ Education
- ▶ Ajout progressif d'activités



Le cycle et l'ajout des points



Les choix

- Projet nouveau et stratégique
 - ▶ Délais très courts
 - ▶ Exigences de sécurité élevée
- Définir des exigences fonctionnelles et politiques de sécurité associées
 - ▶ Utilisation des documents internes de code pour les développeurs



Les murs franchis

- L'ajout de la sécurité dès l'initiation du cycle projet
- La focalisation des tests intrusifs sur des tests complexes et utiles
- La mise en place d'un framework d'entreprise sécurisé
- La sensibilisation de tous les acteurs sur la sécurité



Les fausses routes

- Parler de tests sécurité en fin de cycle...
=> Rejet de la part des équipes de tests
- Vouloir présenter au top management rapidement le processus pour validation...
=> Incapacité à négocier un budget
- Imposer des outils/frameworks aux développeurs
=> Incapacité à les intégrer correctement



Le bilan final du projet



- Augmentation du cout unitaire du projet de plus de 30 % !
 - ▶ Mais centré sur le processus + framework
 - ▶ ROI attendu rapidement
- Meilleur intégration des équipes et des compétences.
 - ▶ Moins de ségrégation architectes/développeurs/MOA



Et aujourd'hui (9 mois plus tard...) ?

- Toujours des tests de sécurité en production, mais réduits de 50%.
- Une prise de conscience progressive des personnes en amont(commerciaux).
- Une bonne implication du management
- Des tests sécurité externes de meilleure qualité
- Une légère augmentation dans le cycle projet (5%)



Rejoignez nous !

Organization Supporters of OWASP's mission



Educational Supporters of OWASP's mission





Time	Module	Trainer	Presentation	Overview & Goal
09h00	Tour d'horizon des projets de l'OWASP	TBD	Tour d'horizon	See details and Trainer's notes
TBD	OWASP ASVS	Sébastien Goria	[OWASP ASVS]	See details and Trainer's notes
Coffee Break				
TBD	OWASP Guide	TBD	[OWASP Guide]	See details and Trainer's notes
TBD	OWASP ESAPI (English session)	Fabio Cerullo	[OWASP ESAPI]	See details and Trainer's notes
Repas				
TBD	OWASP Testing Guide		[]	See details and Trainer's notes
TBD	Revue de code	assigné	[Code review guide]	See details and Trainer's notes
Coffee break				
TBD	OWASP O2 Platform (English Session)	Dinis Cruz (project leader)	[]	See details and Trainer's notes

Cette formation, gratuite pour les membres de l'OWASP, payante (au prix d'une adhésion personnelle de la personne suivant le training) pour les autres, aura lieu dans Paris Intra-Muros sur une journée.

Au cours de cette formation, des experts vous présenteront les différents guides/outils disponibles et pourront échanger avec vous. Les présentations étant des présentations de l'ordre de 30mn à 1h par guide/outil....

