Web Application Firewalls (WAF)

OSSIR

Paris le 7 Juillet 2009

Sébastien GIORIA (sebastien.gioria@owasp.org)
French Chapter Leader

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

Qui suis-je ?

Président du CLUSIR Poitou-Charentes, OWASP France Leader & Evangeliste

sebastien.gioria@owasp.org

- 12 ans d'expérience en Sécurité des Systèmes d'Information
- Différents postes de manager SSI dans la banque, l'assurance et les télécoms
- Expertise Technique
  - ✓ Gestion du risque, Architectures fonctionnelles, Audits
  - ✓ Consulting et Formation en Réseaux et Sécurité
  - ✓ PenTesting, Digital Forensics

- Domaines de prédilection :
  - ✓ Web 4.2 : WebServices, Interfaces Riches (Flex, Air, Silverlight, …), Insécurité du Web.

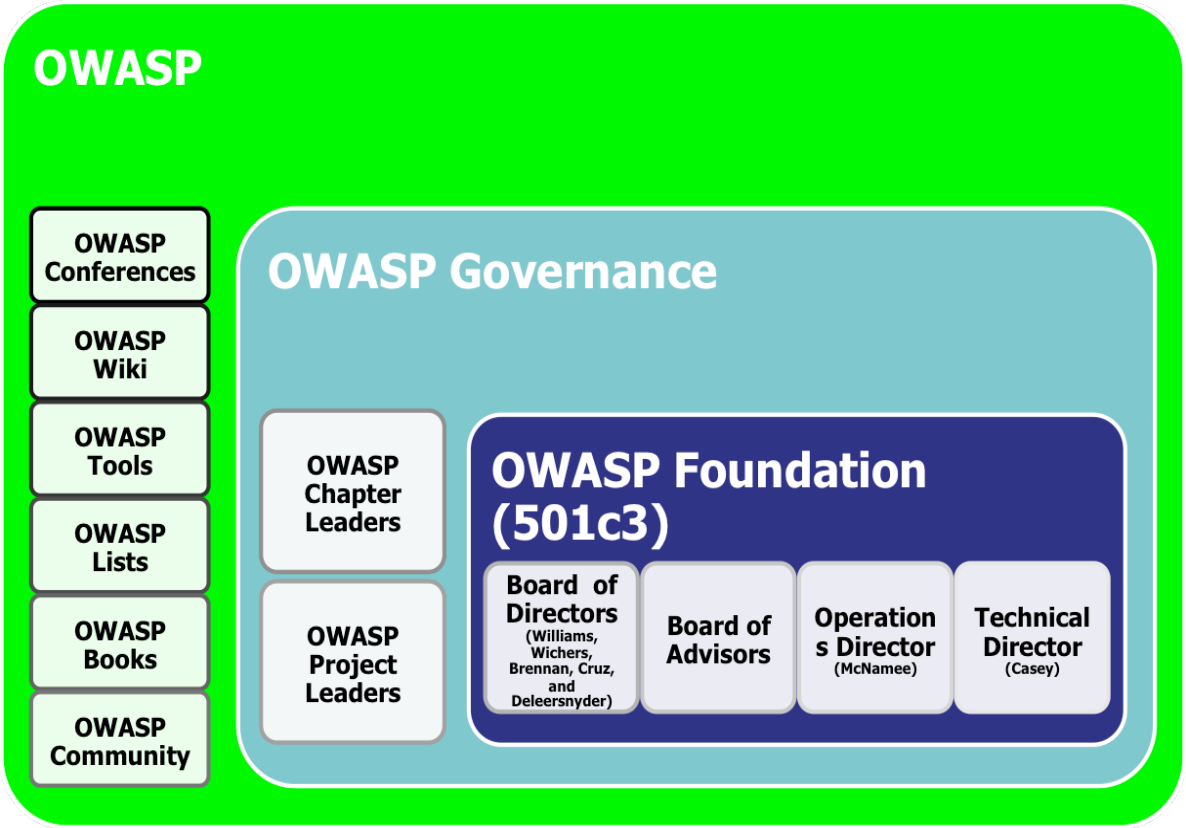
Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- Et après ?

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 des 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



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. 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

Interventions :

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

Les ressources de l'OWASP

- Vulnerability Scanners
- Static Analysis Tools
- Fuzzing

Automated Security Verification

- Penetration Testing Tools
- Code Review Tools

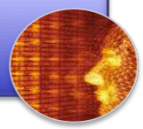
Manual Security Verification

- ESAPI

Security Architecture

- AppSec Libraries
- ESAPI Reference Implementation
- Guards and Filters

Secure Coding



- Reporting Tools

AppSec Management

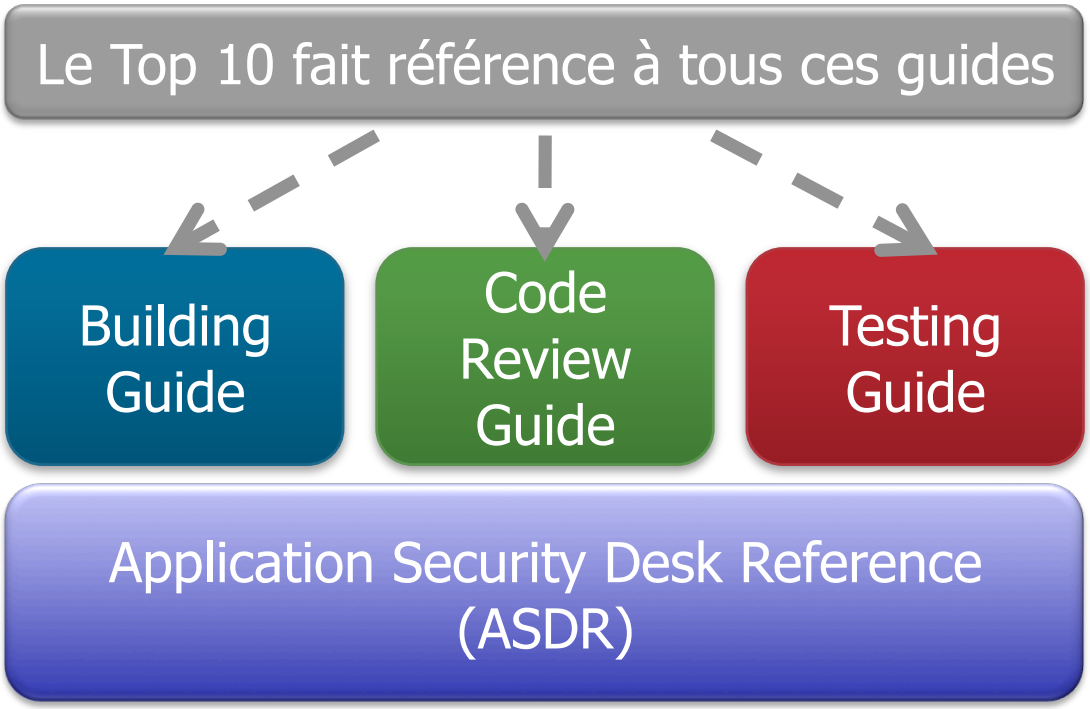
- Flawed Apps
- Learning Environments
- Live CD
- SiteGenerator

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



Le Top10 2007

- A1: Cross Site Scripting (XSS)
- A2: Failles d'injection (SQL, LDAP, ...)
- A3: Execution de fichier malicieux
- A4: Référence directe non sécurisée à un objet
- A5: Falsification de requête inter-site (CSRF)
- A6: Fuite d'information et traitement d'erreur incorrect
- A7: Violation de gestion de session ou de l'authentification
- A8: Stockage cryptographique non sécurisé
- A9: Communications non sécurisées
- A10: Manque de restriction d'accès à une URL

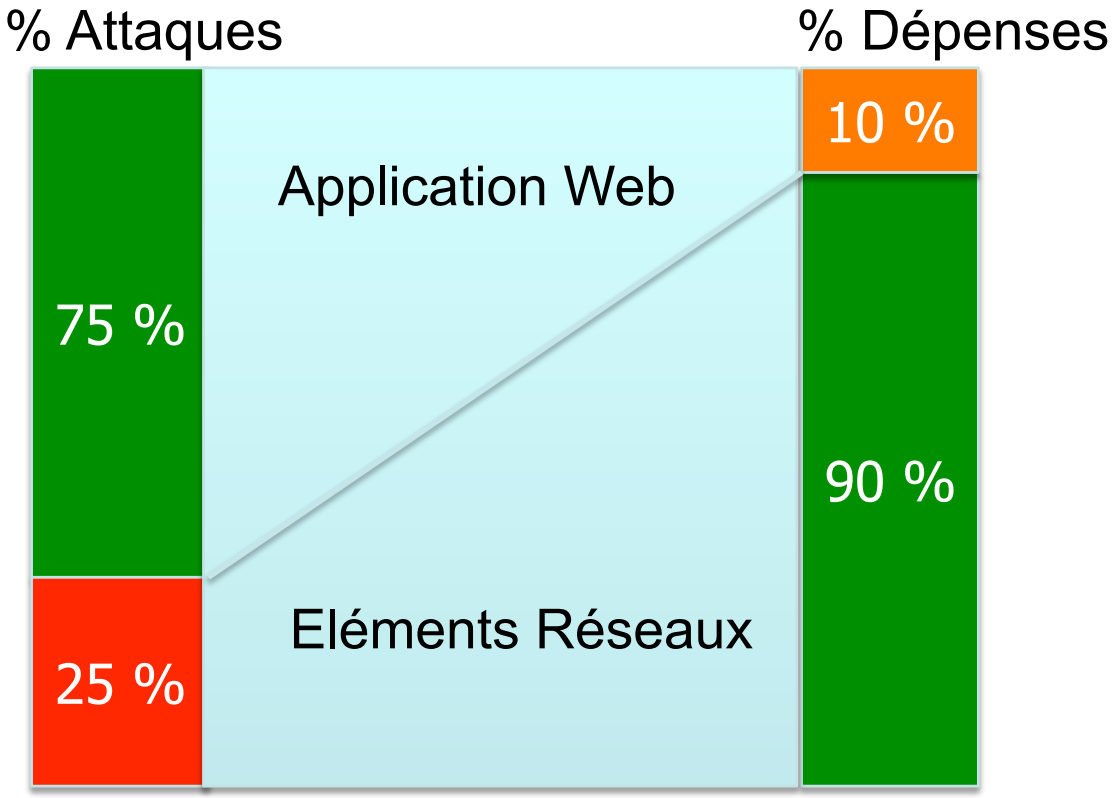
OWASP
The Open Web Application Security Project
http://www.owasp.org

www.owasp.org/index.php?title=Top_10_2007

Agenda

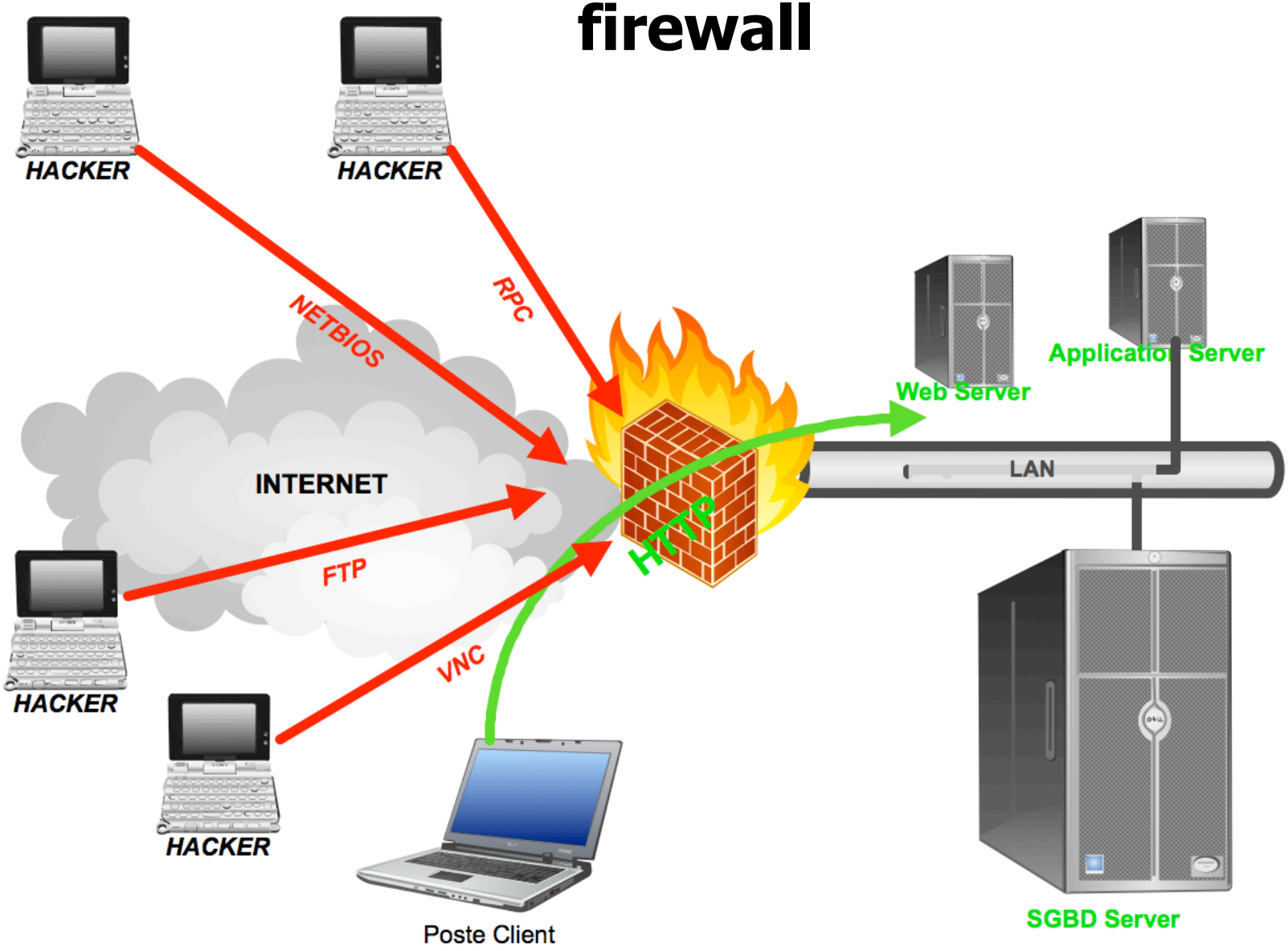
- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- Et après ?

Faiblesse des applications Web

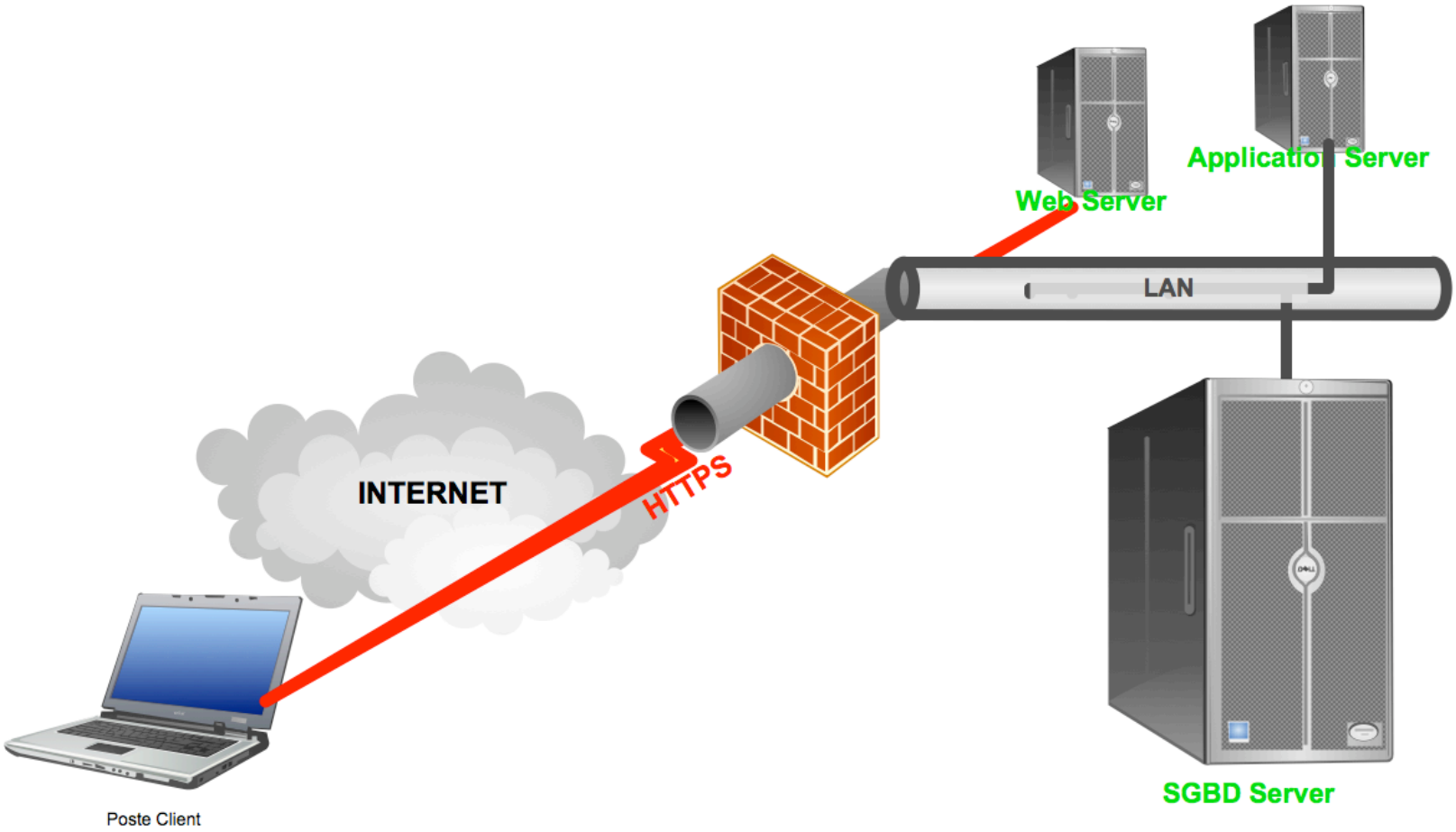


D'après une étude du GARTNER
75% des attaques ciblent le niveau Applicatif
33% des applications web sont vulnérables

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



Mon site Web est sécurisé puisque il est protégé par SSL



Et arriva le WAF…

- PCI-DSS (https://www.pcisecuritystandards.org/) 6.6 :

> In the context of Requirement 6.6, an “application firewall” is a web application firewall (WAF), which is **a security policy enforcement point positioned between a web application and the client end point**. This functionality can be implemented in software or hardware, running in an appliance device, or in a typical server running a common operating system. It may be a stand-alone device or integrated into other network components.

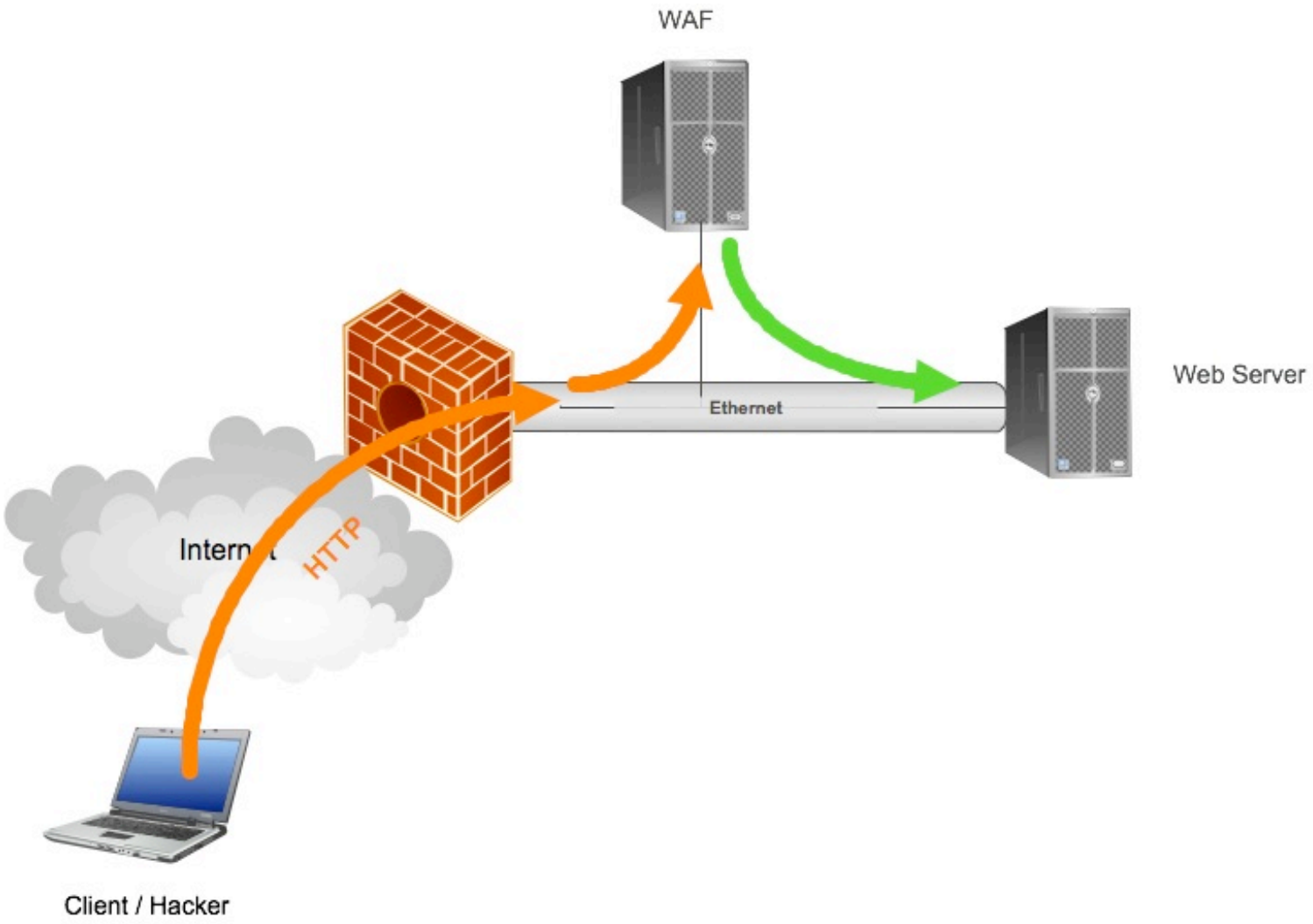
- http://www.owasp.org/index.php/Web_Application_Firewall
  - Le WAF est une **CONTRE MESURE**

> A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover **common attacks** such as Cross-site Scripting (XSS) and SQL Injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and **needs to be maintained as the application is modified.**

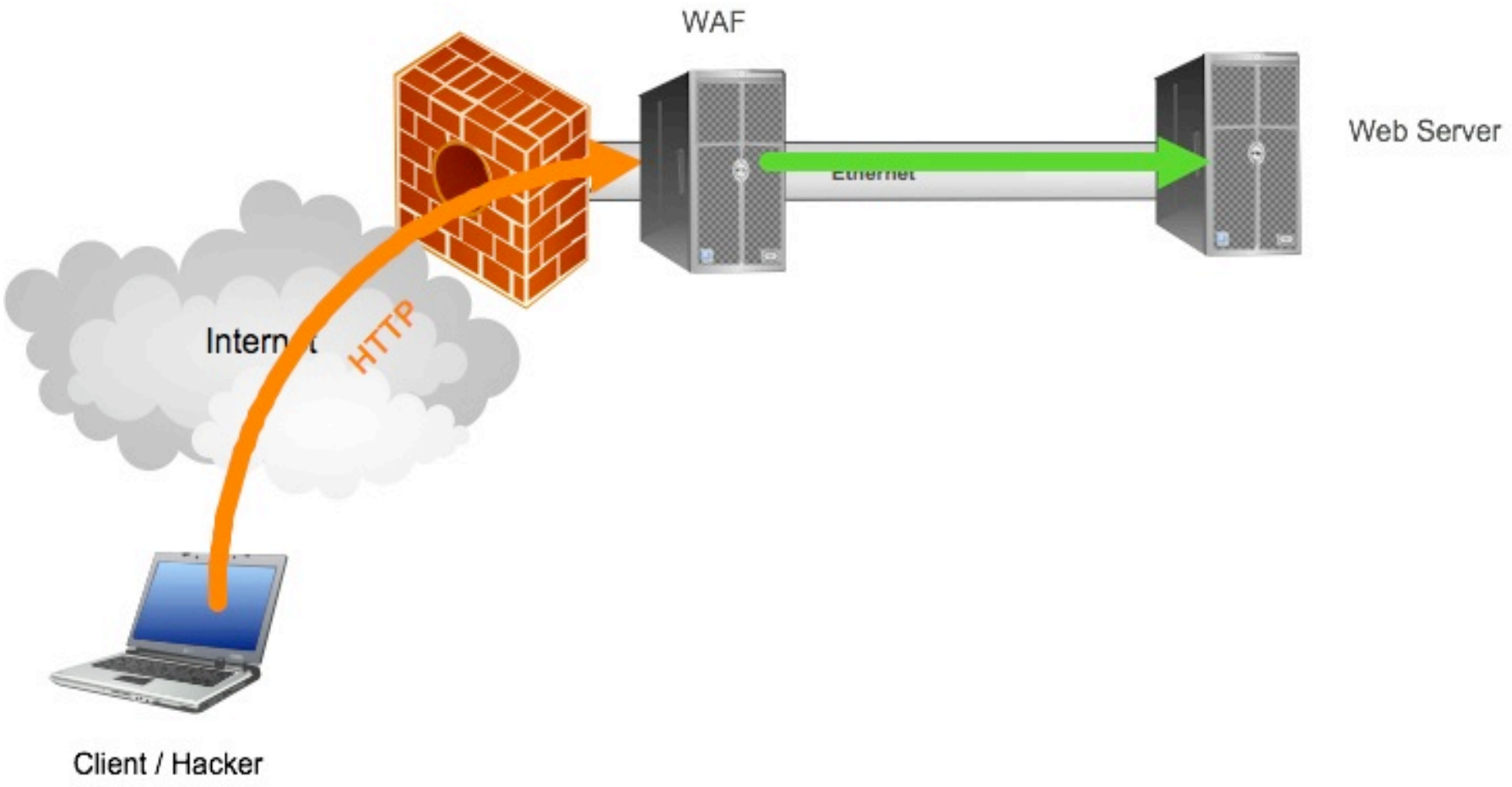
Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- Et après ?

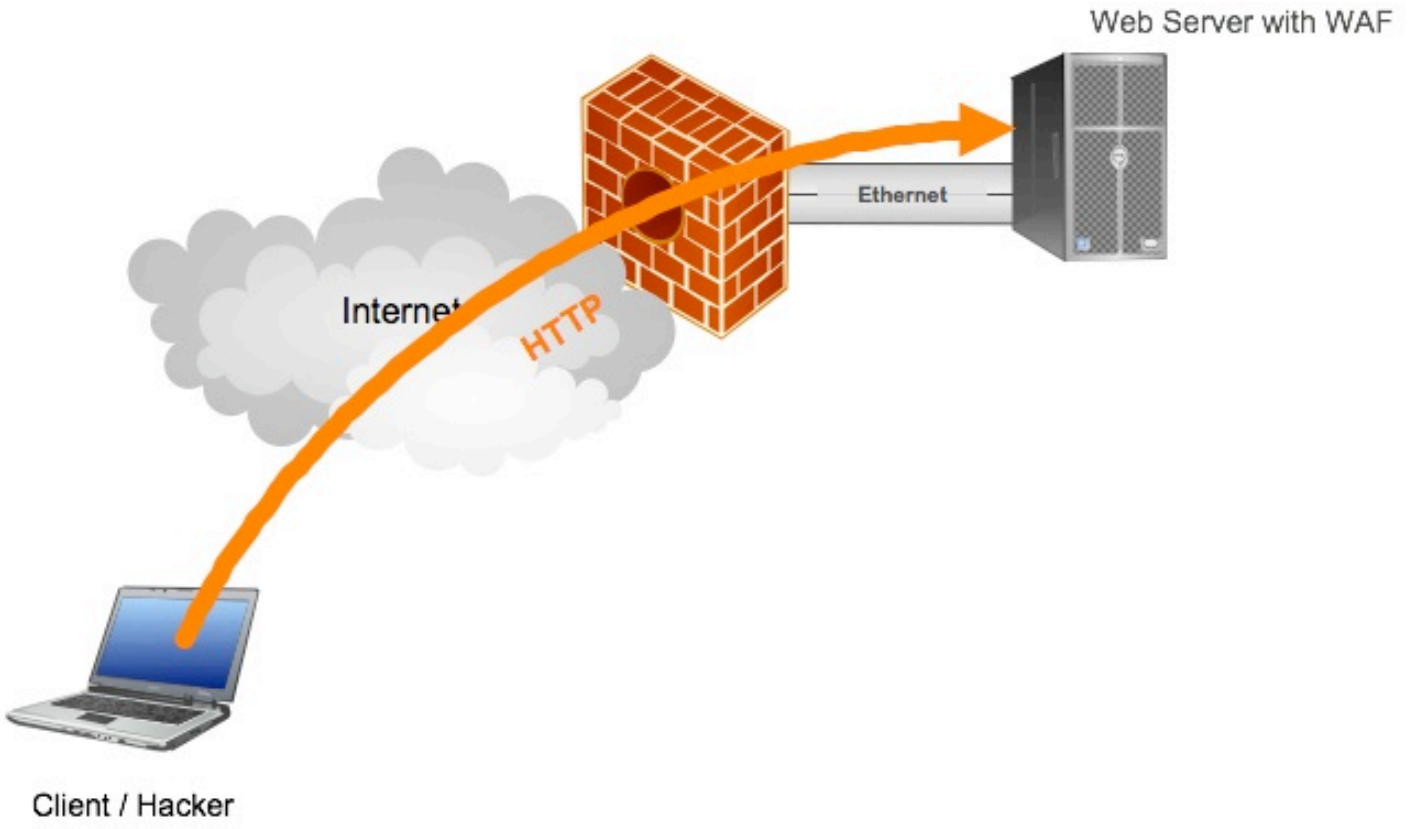
Mode Parallèle/Sonde



Mode Intrusif/Reverse Proxy



Intégré au serveur Web (mod_security d'Apache)



Choisir son WAF/son camp

	Négatif	Positif
Concept	Le WAF reconnait les attaques et les bloque, il autorise tous les accès.	Le WAF connait le trafic légitime et rejette tout le reste.
Avantages	• Aucun besoin de personnalisation • Protection standard • Simple a déployer	• Bloque les attaques inconnues • N'est pas dépendant d'une base de signature. • Détection précise
Inconvénients	• Extrèmement dépendant des signatures • Pas très précis	• Configuration complexe • Sensible aux faux positifs

Web Application Firewall Evaluation Criteria (WAFEC)

- Projet du Web Application Security Consortium
  - http://www.webappsec.org/projects/wafec/
- Liste les fonctionnalités possibles d'un WAF et non les fonctions minimum nécessaires d'un WAF
- Permet d'évaluer techniquement le meilleur WAF pour son environnement en fonction de 9 critères :
  1. Type d'architecture à déployer (pont, reverse-proxy, intégré, SSL, …)
  2. Support d'HTTP et d'HTML (Versions, encodages,…)
  3. Techniques de détection (signatures, techniques de normalisation du trafic, …)
  4. Techniques de protection (brute force, cookies, sessions, …)
  5. Journalisation (intégration NSM, type de logs, gestion des données sensibles, …)
  6. Rapports (types de rapports, distribution, format, …)
  7. Administration (politiques, logs, …)
  8. Performance (nb de connexions/s, latences, …)
  9. Support XML (WS-i intégration, validation XML/RPC, …)

Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- Et après ?

Réalités du WAF

- Patcher virtuellement les problèmes
  - Plus ou moins efficace suivant la méthode employée (positive, négative)
- Cacher tout ou partie de l'infrastructure
  - En mode reverse proxy
- Analyseur de trafic HTTP/HTTPS/XML puissant
  - Grace à ses fonctions de normalisation et son reporting

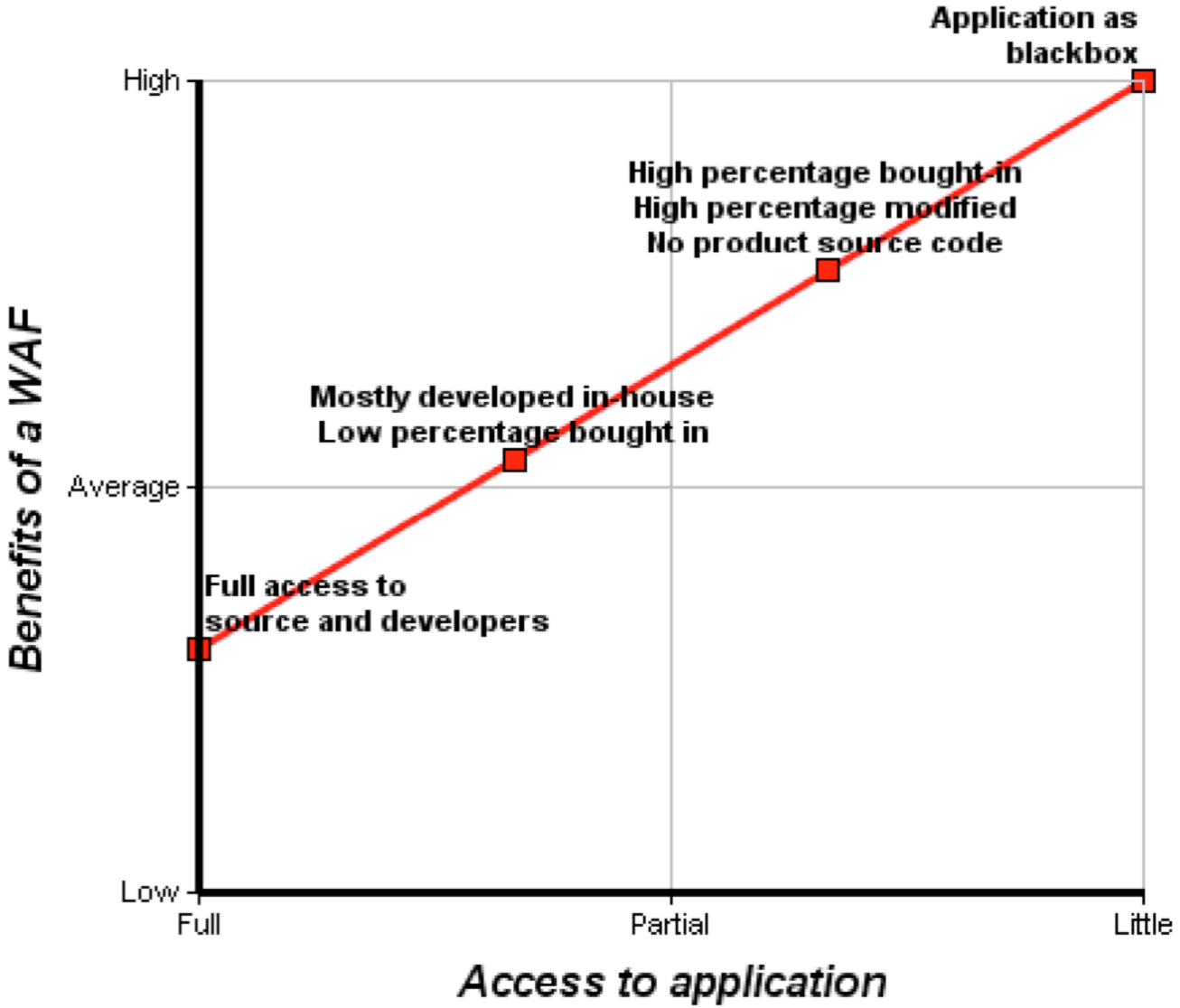
Mythes du WAF

- C'est un nouvel élément d'infrastructure
  - Couts supplémentaires, à intégrer en PCA, …
  - Compétence supplémentaire…
- Source de problèmes récurrents :
  - Modèle positif : à chaque modification de l'applicatif
  - Modèle négatif : dépendant des mises a jours.
  - Complexifie le debug
- Ce n'est pas la solution!
  - Il « laisse » passer des failles (Session Hijacking, élévation de privilèges, HTTP response splitting, …)
  - Il n'est pas (encore) obligatoire en PCI-DSS !

Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- Et après ?

WAF – En ai-je besoin ?



WAF – Mise en place

- Choisir le type (centralisé, décentralisé, performances, …) => Projet WAFEC
- Mettre en place l'organisation
  - Désigner (au minimum) un « WAF operation manager » en lien avec les équipes infrastructures et développement.
    - Rôle technico-MOA
- Mettre en place la protection minimale
  - XSS, Blind-SQLi, …
- Définir les priorités des applications à protéger
  - Itérer
    - depuis du traçage de toutes les requêtes à la protection optimale pour chacune des applications (peut se dérouler sur un très long terme….)

WAF – OWASP Top10 – Mise en Place

Top10	WAF Commentaire	Charge de mise en place
A1 (XSS)	Ne voit pas les XSS persistants (pas de filtres en sortie) Bloque la majorité des attaques en fonction du moteur de canonisation	Moyenne
A2 (Injections)	Bon sur les protocoles connus (SQL) grace au blacklistage de caractères.	Moyenne
A3 (RFI)	Peut se coupler avec un A/V via ICAP, permet de whitelister les paramètres autorisés	Faible a Moyenne
A4 (Insecure Objects)	Masquerade possible des ID internes.	Très Faible
A5 (CSRF)	Peut ajouter des ID à la volée	Faible

WAF – OWASP Top10 – Mise en Place

Top10	WAF Commentaire	Charge de mise en place
A6 (Info Leak/ Error)	Bloque facilement les accès aux URL non autorisées, mais détecte difficilement les erreurs coté serveur	Faible à Forte
A7 (Auth & Session)	Dépend du WAF et du Serveur Applicatif	Moyenne à Forte
A8 (Crypto)	Non Applicable	Non Applicable
A9 (SSL/VPN)	Totalement adapté	Faible
A10 (Restrict URL)	Blacklistage	Faible

Exemple vécu ~~de l'(in)utilité recyclage déploiement~~ d'un WAF

Société de type VPC sur un marché de niche en B2B.

1ere étape : le choix

- 2 options (via PCI-DSS 6.6, car il est bien connu que toute société qui vend sur internet se doit d'être conforme….) :
  1. Déployer un WAF + Scan automatisés
  2. Mettre en place un code review sécurité + SDLC

- Solution choisie : déployer un WAF(redondé) + Scans en mode ASP récurrent (1 par mois au minimum)

  => Magic quadrant + idée des conseils en régie + promo de Noël…

2ème étape : la vie du produit

- Résultats des scans réguliers :
  - Tout est vert (forcément il y a un WAF qui voit arriver avec ses gros sabots le robot….)
- Configuration du WAF :
  - Configuration faite par l'ingénieur en charge des Firewalls (normal, c'est un Web Application FIREWALL !)
  - Remontée des logs dans un fichier (non analysé, car trop d'alertes)
  - Règles parfois permissibles car des outils (type CMS propriétaires font des requêtes bloquées)

L'attaque

1. Un lutin malveillant lance une DOS (type slowloris) à destination du WAF en mode fail-open.
2. Pendant ce temps,
   - le lutin malveillant découvre une injection SQL basique (très très basique).
   - les bases sont téléchargées par le lutin malveillant.
3. Le lutin revend tout ou partie de la base au meilleur offreur.
4. Le lutin peut continuer à boire ses Guinness.

La détection

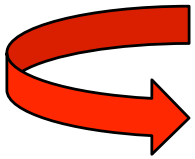
- Il n'a été vue que la DOS !!!

⇒**Dans les bases, des adresses e-mails spéciales permettent de découvrir une compromission post attaque.**

- L'investigation dans les logs HTTP a permis de découvrir l'injection SQL.

Le bénéfice

- +100% de bénéfice(financier) pour le vendeur du ~~*PC de la webcam de la machine a café*~~ WAF
- +100% de bénéfice(financier) pour le vendeur du scanner ~~*tout va bien quand je remets le rapport au DSI*~~ ASP



-424,2%(au minimum) pour l'entreprise :

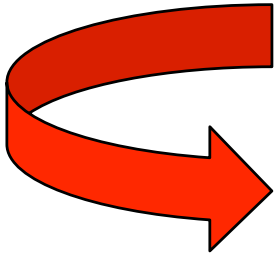
- **Perte d'image de marque**
- **Perte de l'agrément PCI-DSS (amendes ?)**
- **Pentests manuels en urgence**
- **Formation des développeurs en urgence**
- **Revue de code en urgence**
- **Achat de la WebCam**

Agenda

- L'OWASP
- Web Application Firewalls (WAF)
- Choisir son WAF
- WAF Mythes et réalités
- WAF mode d'emploi
- Et après ?

Pas de recette Miracle

- 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.

Rejoignez nous !

http://www.owasp.fr