
# JoomlaDay™

## FRANCE - 23 et 24 mai 2014

PARIS

Twitter Hastag
#jd14fr

Organisé par
AFUJ
Association Francophone
des Utilisateurs de Joomla!


# Améliorer la sécurité de son site web

# Introduction à aeSecure

v1.3 – 23/05/2014

# Qui suis-je ?

- Développeur d'aeSecure, logiciel de **sécurité** et **d'optimisation** de sites web Apache
- Développeur de l'extension AllEvents; gestionnaire d'évènements pour Joomla!®
- Modérateur Joomla! France (cavo789)
- Membre fondateur de la JUG! Wallonie

Christophe Avonture

http://aesecure.com/fr/accueil/contact.html


# Objectifs de cette présentation

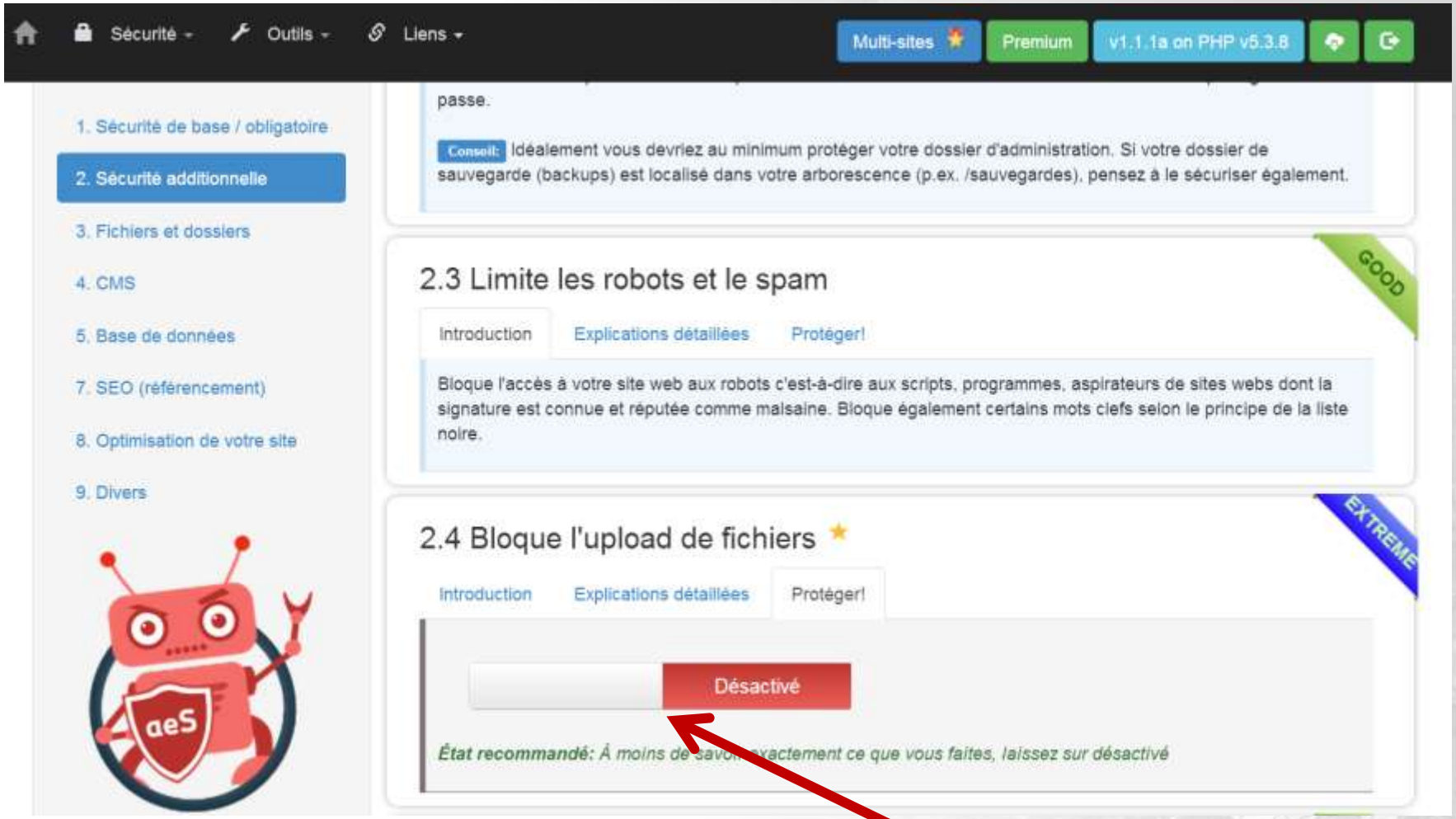
- Vous trouverez dans cette présentation quelques conseils que tout un chacun peut appliquer et ne requérant que peu de connaissances techniques.
- Cette documentation ne se veut nullement exhaustive mais être un recueil de trucs & astuces et de bonnes pratiques du web.
- Il s'agit de partager mon expérience personnelle et des outils que j'ai testés, le choix des outils proposés n'est donc pas exhaustif.
- N'hésitez pas à me suggérer vos propres trucs : http://aesecure.com/fr/forum/boite-a-idees.html


# Soyons d'accord

- La sécurité informatique devrait être à la base de l'écriture de tout code informatique. Un code défaillant le restera.
- La sécurité proposée ici part du postulat que l'on ne peut pas modifier le code du programme (CMS, extensions, …). Nous allons donc mettre en place différentes couches de protection afin de bloquer un maximum d'attaques (=fermer portes et fenêtres).
- Un logiciel non sécurisé installé sur votre site restera une porte grande ouverte.

# aeSecure

- aeSecure est un logiciel permettant de **sécuriser** et **optimiser** tout site web tournant sous **Apache** : Joomla!, Drupal, WordPress, Prestashop, SPIP, Typo3, Magento, Koken, …, php et même html : dès lors que le site est sous Apache, aeSecure le protégera et l'optimisera.
- Il s'agit d'un logiciel **Freemium** : gratuit avec des fonctionnalités additionnelles requérant un abonnement.
- Fonctions SEO également
- http://aesecure.com/fr/telechargement.html




Interface Bootstrap / jQuery - Interrupteur On / Off

Vous décidez de ce que vous activez; selon le site web

Options 1.1 & 2.1 / 2.2 / 4.3

# aeSecure

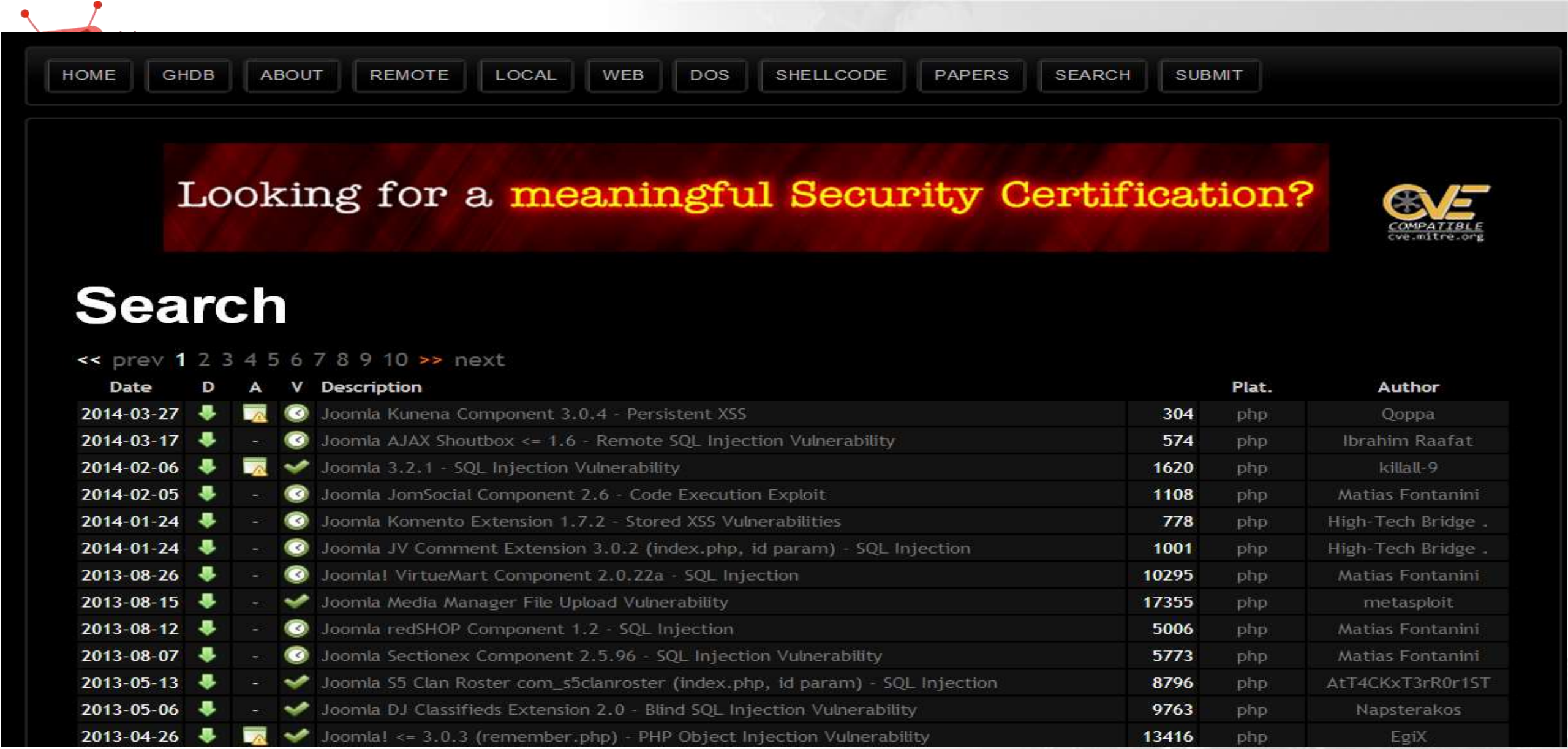
Au travers des pages de cette présentation, vous verrez parfois apparaître l'encadré ci-dessus.

Ce qui signifie que cette protection est apportée par aeSecure en activant une ou plusieurs options : le « / » voulant dire « ou ».

*Dans l'exemple ci-dessus, il faudrait activer l'option 1.1 et l'une des trois autres mentionnées (peu importe laquelle).*


# Quelles actions/que faire?

- Faites vos emplettes : ignorez ce qui vous semble superflu ou inutile.
- Exactement comme sur votre ordinateur où vous n'installez pas trois anti-virus, ne pensez pas qu'en multipliant les outils (aeSecure, CrawlProtect, Admin Tools, jHackGuard, …) vous allez être inattaquable; choisissez juste ceux avec lesquels vous êtes confortables.


HOME
GHDB
ABOUT
REMOTE
LOCAL
WEB
DOS
SHELLCODE
PAPERS
SEARCH
SUBMIT
Looking for a meaningful Security Certification?
CVE COMPATIBLE cve.mitre.org
Search
<< prev 1 2 3 4 5 6 7 8 9 10 >> next
Date D A V Description Plat. Author
2014-03-27 Joomla Kunena Component 3.0.4 - Persistent XSS 304 php Qoppa
2014-03-17 Joomla AJAX Shoutbox <= 1.6 - Remote SQL Injection Vulnerability 574 php Ibrahim Raafat
2014-02-06 Joomla 3.2.1 - SQL Injection Vulnerability 1620 php killall-9
2014-02-05 Joomla JomSocial Component 2.6 - Code Execution Exploit 1108 php Matias Fontanini
2014-01-24 Joomla Komento Extension 1.7.2 - Stored XSS Vulnerabilities 778 php High-Tech Bridge .
2014-01-24 Joomla JV Comment Extension 3.0.2 (index.php, id param) - SQL Injection 1001 php High-Tech Bridge .
2013-08-26 Joomla! VirtueMart Component 2.0.22a - SQL Injection 10295 php Matias Fontanini
2013-08-15 Joomla Media Manager File Upload Vulnerability 17355 php metasploit
2013-08-12 Joomla redSHOP Component 1.2 - SQL Injection 5006 php Matias Fontanini
2013-08-07 Joomla Sectionex Component 2.5.96 - SQL Injection Vulnerability 5773 php Matias Fontanini
2013-05-13 Joomla S5 Clan Roster com_s5clanroster (index.php, id param) - SQL Injection 8796 php AtT4CKxT3rR0r1ST
2013-05-06 Joomla DJ Classifieds Extension 2.0 - Blind SQL Injection Vulnerability 9763 php Napsterakos
2013-04-26 Joomla! <= 3.0.3 (remember.php) - PHP Object Injection Vulnerability 13416 php EgiX


# Obfuscation

- L'obfuscation n'est pas à proprement parler une technique de sécurité : il s'agit de ne pas montrer une information, de la rendre invisible, plus difficile à trouver.
- Cacher le meta generator de la page, le numéro de version de Joomla!, … ne change strictement rien à la sécurité intrinsèque du site; cela n'arrêtera pas les hackeurs qui font du « brute-force ».
- Faut-il laisser ces informations sur le net ? Je pense que non. Moins le pirate en saura sur le site, plus il devra en apprendre et plus on aura de chance de détecter son activité. Il y a fortes chances également qu'il se lasse et passe à un autre site.

# Prérequis

# Protéger votre ordinateur

« There is no point in following all the best Joomla! security advice you can find if you don't take the simple step of securing your own personal computer with up to date anti-virus software. »

Brian Teeman,

Co-founder Joomla!

# Installez un garde à l'entrée de votre site

« Ne publiez votre site qu'après y avoir installé un logiciel de protection tel qu'aeSecure. **Vous viendrait-il à l'esprit de laisser portes et fenêtres de votre maison ouvertes en votre absence ?** »

Christophe Avonture,

Développeur d'aeSecure ;-)

# Le B.A.BA

# Mots de passe 1/2

- **Planifiez d'oublier vos mots de passe** : utilisez SuperGenPass qui permet de générer à la volée un mot de passe unique par sites web.
- Configurez SuperGenPass pour générer un mot de 20 caractères ou plus.
- Modifiez tous vos mots de passes Web par ceux de SuperGenPass.
- Conservez une trace des mots de passe dans LastPass.
- Et vous, c'est quoi votre couple login-mot de passe ?



# Mots de passe 2/2

- Utilisez un mot de passe différent pour chaque site web mais aussi chaque utilisateurs, chaque outil (FTP, …) et chaque base de données.
- Si vous souhaitez contraindre vos utilisateurs à choisir des mots de passe selon certaines règles, il existe quelques plugins pour cela dans la JED : http://extensions.joomla.org/extensions/access-a-security/site-security/password-management

# Le CMS est-il à jour ?

- Quelque soit la version majeure de votre Joomla! que vous utilisez (1.5, 2.5, …), songez toujours à installer la dernière mise à jour.  Ainsi, ne restez pas avec un J1.5.22 alors que J1.5.26 est disponible.
- Si votre version majeure de Joomla! est ancienne, prévoyez dans votre agenda le temps nécessaire pour faire une mise à niveau.
- **Joomla 1.5 n'est plus maintenu depuis Septembre 2012.  Upgradez !!!**


# Extensions, modules, …

- Jamais, au grand jamais, de versions pirates vous installerez ! Hacking de votre site garanti.
- Limitez le nombre au maximum; désinstallez tout qui n'est pas utilisé.
- Mettez à jour vos extensions, plugins et modules. Consultez régulièrement les sites de leurs auteurs. Inscrivez-vous aux fils RSS ou fanpage.


# Extensions, modules, …

- Pouvez-vous avoir confiance en l'auteur de l'extension ? A-t-il bonne réputation ? Ne perdez jamais de vue qu'une extension (composant, module, …), c'est du code php que vous autorisez à s'exécuter sur votre site.
- Est-ce que ce code est sain ? Contient-il un « backdoor », va-t-il envoyer la configuration de votre site par email à un hackeur ? Ne devenez pas parano mais restez vigilant.


# Extensions, modules, …

- N’oubliez pas de mettre à jour votre template dès lors qu’une nouvelle version est disponible.
- Utilisez cUpdater; il s’agit d’un plugin qui vous envoie un email pour vous avertir qu’une mise à jour d’une extension, module, … est disponible.

# Configuration de votre site


# Hébergeur

- Analysez l'offre de votre hébergeur et comparez ce qu'il propose en matière de sécurité.  Tous ne se valent pas, loin de là. L'un des meilleurs étant SiteGround.com.  Faites la comparaison...
- Assurez-vous d'avoir la dernière version de PHP (Mai 2014 : 5.3.28, 5.4.26 ou 5.5.10)
- Il est parfois possible de choisir sa version depuis son panneau de contrôle.
- .htaccess – Activer PHP 5.4

Option 4.5

# Évitez le compte « admin »

- Veuillez à ne jamais utiliser un compte  nommé « admin ».
- Si vous en avez un, modifiez son statut de « super admin » à « public » puis désactivez-le (technique du « honeypot »). *Vous pourriez surveiller les tentatives de connexion avec ce compte.*
- Limitez au maximum le nombre de comptes de type admin / super admin.
- Apprenez à gérer les ACLs afin que les accès soient strictement ceux requis.

# Authentification à deux clefs

Depuis Joomla 3, il est possible d'activer un plugin nommé « Two factors authentication » et qui permet d'afficher une nouvelle zone; sous le mot de passe. Il faut alors introduire un code à six chiffres générés par, p.ex., Google Two Factors Authentification.


Infos : https://www.google.com/landing/2step/

Options 2.3 / 4.2

# Lutter contre le spam

- Si applicable, désactivez l'inscription frontend.
- Marre des inscriptions fantômes ?  Installez Community Builder et, dans les paramètres du gestionnaire des utilisateurs natifs de Joomla!, désactivez les inscriptions.
- Dans les paramètres de CB, activez les inscriptions indépendamment du paramètre global du site.
- Au besoin, achetez et installer le plugin CB Captcha.

Approfondir: http://aesecure.com/fr/blog/bloquer-les-robots-utilisateurs-fantomes.html


# Installation d'extensions

- Vérifier sur la Vulnerable Extensions List si l'extension n'est pas mentionnée.
- Jamais sans les avoir testées en local !
- Faites un backup de votre site auparavant.
- Limitez au maximum le nombre d'extensions installées sur votre site de production.

# Nettoyez, encore et toujours

- Supprimez régulièrement les extensions, modules et plugins que vous n'utilisez plus.
- Supprimez les templates que vous n'utilisez pas.
- Nettoyez régulièrement le dossier /tmp.  Une tâche dans le crontab de votre hébergeur peut le faire automatiquement.

# meta name="generator"

- Certains scripts tentent de repérer les sites Joomla!. Une des techniques est d'analyser le code de la page à la recherche du "generator". En supprimant ce code, vous rendez donc un (tout petit) peu plus difficile de cibler votre site.
- Pour cela, éditez le fichier index.php de votre template et ajoutez la ligne ci-dessous après la génération des metas de Joomla.

```
<?php  JFactory::getDocument()->setGenerator(''); ?>
```

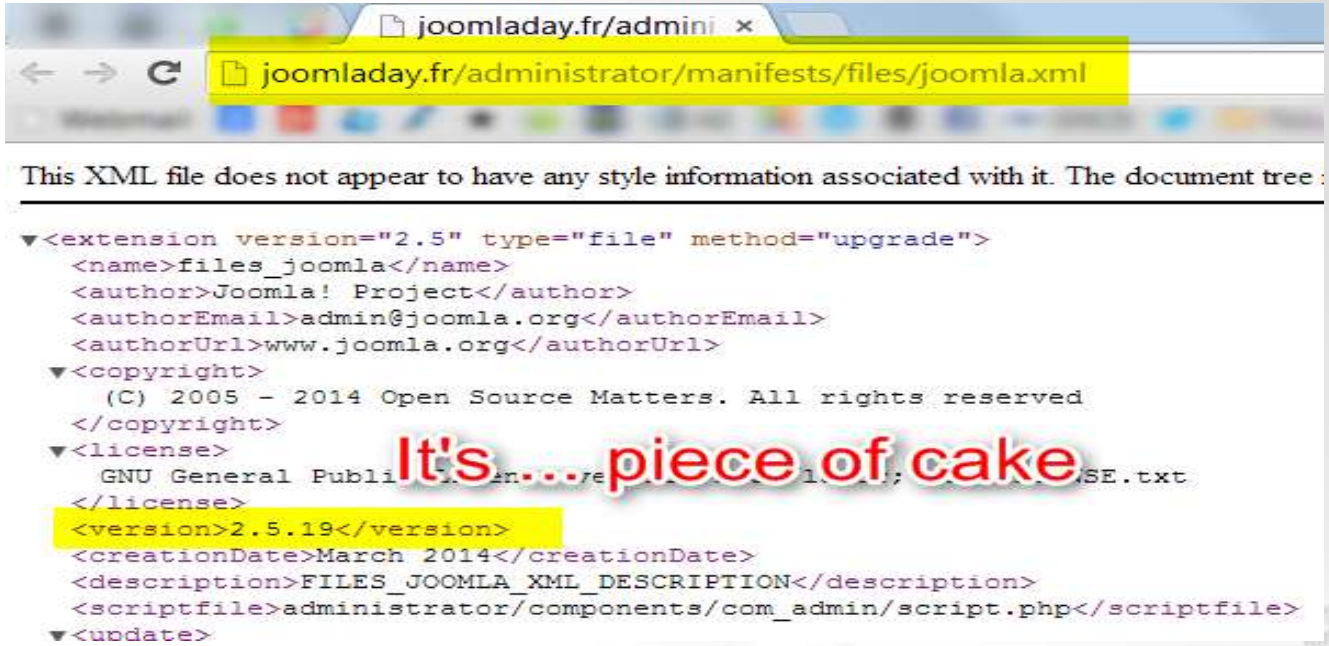
- Si vraiment, vous n'y arrivez pas, utilisez le plugin Generator Meta Tag for Joomla

# Firefox/Chrome - Addon


Installez le plugin « Joomla-version-check » pour Firefox ou Chrome : si votre numéro de version est dévoilé, votre site communique trop d'informations : Interdisez l'accès aux fichiers .xml de l'administration

Options 1.1 & 2.1 / 2.2 / 4.3

# Joomla.xml




Bloquez joomla.xml depuis le frontend et le backend.

Ajoutez dans le fichier /.htaccess ces deux lignes :

RewriteCond %{REQUEST_URI} ^/joomla.xml
RewriteRule .* - [F]

# Protégez /administrator

- Utilisez un fichier .htpasswd pour protéger l'accès au dossier /administrator.
- Exemple de fichier .htpasswd :

```
<IfModule mod_auth.c>
  AuthUserFile /home/path/.htpasswd
  AuthName "Ami ou ennemi ?   Veuillez montrer patte blanche et dire qui vous êtes"
  AuthType Basic
  <Limit GET POST>
     Require valid-user
  </Limit>
</IfModule>
```

http://perishablepress.com/htaccess-password-protection-tricks/

Remarque : la protection la plus efficace étant de spécifier les adresses IP (fixes) autorisées à faire une connexion sur /administrator.  Concept de liste blanche.

Option 7.1

# Activez le mode SEF

- Lorsque vous activez le mode SEF, votre site n'affiche plus des urls telles que index.php?option=com_user&view=login&... qui donnent trop d'informations et qui invitent à tenter de modifier "au petit bonheur la chance" les valeurs des paramètres.
- Effet collatéral : vous améliorez votre référencement.

Exemple de faille : accès aux factures chez showroomprive.com (zataz)


# Désactivez la couche FTP

- Il n'est, en général, pas nécessaire d'utiliser la couche FTP au niveau de la configuration générale de votre site, si vous l'utilisez, supprimez les données (login, mot de passe) et désactivez la couche FTP.
- **Problème majeur:** le login et le mot de passe est stocké en clair dans configuration.php
- Si votre hébergeur vous contraint à utiliser la couche FTP pour installer un composant, veillez à chaque fois supprimer le login/password.

Option 1.3

# Debug Mode / Rapport d'erreurs

- Sur un site de production, il ne faut jamais laisser activé le mode debug.
- Rendez-vous dans la configuration générale de votre site, onglet Système et veillez à ce que le débogage système et débogage de langue soient désactivés.
- Dans l'onglet Serveur, paramétrez le rapport d'erreurs sur Aucun.


# Masquez un maximum d'informations

- Moins l'attaquant en sait sur votre site, plus difficile sera pour lui de cibler une attaque fructueuse.
- Ne laissez donc pas des fichiers .php qui pourraient p.ex. afficher un phpinfo() (parfois de tels fichiers sont créés par l'hébergeur et sont placés à la racine de votre hébergement web).

Option 1.1

# Désactivez l'affichage des positions des modules

- Depuis Joomla! 1.6, vous pouvez désactiver l'utilisation du ?tp=1 depuis l'écran de gestion des paramètres des templates


- Pour Joomla! 1.5, veuillez bloquer cette utilisation depuis le fichier .htaccess


# INSTALL.txt, README.md, …

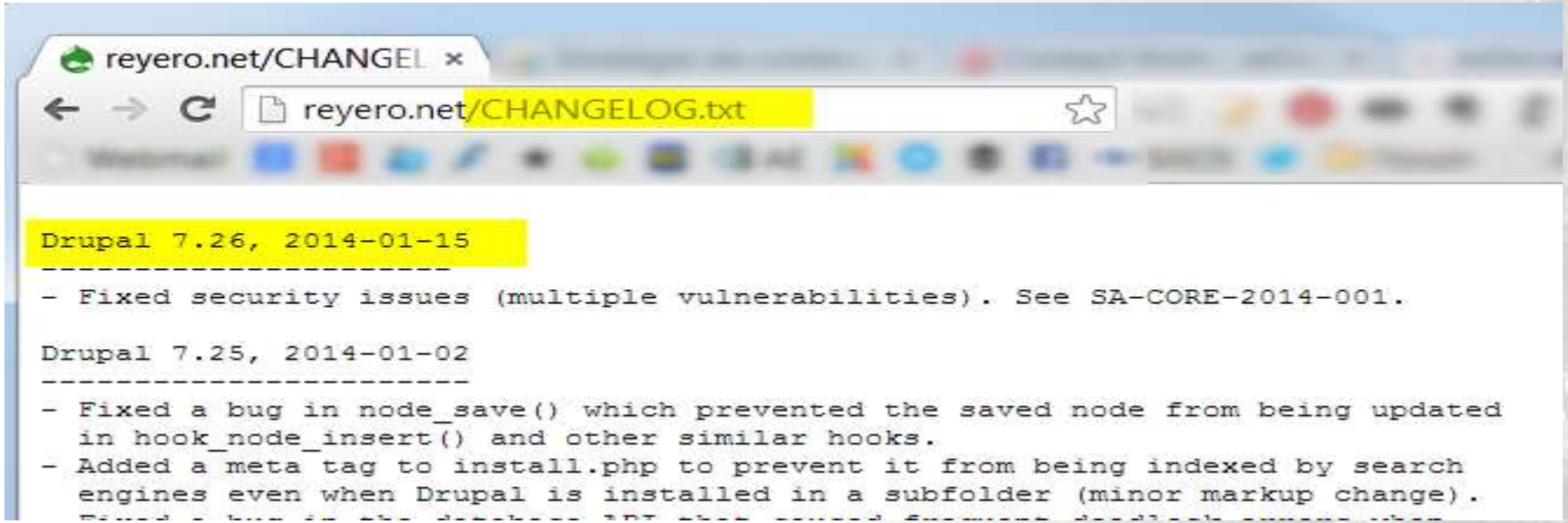
Jetez un œil à la racine de votre site web : vous avez quantité de fichiers tels que, peut-être CHANGELOG.txt, INSTALL.txt, README.md, etc.

Supprimez-les ces fichiers sans autre forme de procès.

Pourquoi ? http://votresite/INSTALL.txt, http://votresite/README.md, … vont dévoiler des informations sur votre configuration.

# INSTALL.txt, README.md, …

Un exemple : http://reyero.net/CHANGELOG.txt Et hop!, c'est donc du Drupal en version 7.26… *Cette version est-elle répertoriée comme contenant des trous de sécurité pourrait se demander un hacker?*



# Cron jobs

Si vous avez accès au cron de votre serveur, ajouter une tâche quotidienne telle que celle ci-dessous qui vous enverra un email si un fichier a été modifié dans les dernières 24 heures (excepté le dossier cache du site) :

find /home/account_name/public_html/ -path /home/account_name/public_html/cache -prune -o -type f -ctime -1 -exec ls -ls {} \;

http://forum.joomla.org/viewtopic.php?f=621&t=801614

Adaptez le chemin d'accès vers le vôtre.


# Base de données


# Quel est l'utilisateur qui accède à votre base de données?

- Au niveau de votre gestionnaire de base de données (voir votre panneau de contrôle), vérifiez que l'utilisateur qui accède à votre base de données n'est pas « root ». Si c'est le cas, changez-cela sans délai en créant un nouvel utilisateur.
- Un utilisateur = une base de données et un mot de passe unique (le plus long possible (20 caractères p.ex.))

# jos_

- Sous Joomla 1.5, le préfixe jos_ était proposé par défaut et peu de personnes prenaient le temps de le changer. Grosse erreur car, dans ce cas, le hackeur sait comment se nomme la table des utilisateurs : jos_users. Et il peut s'atteler à l'attaque (SQL injection).
- Si c'est votre cas, utilisez la fonctionnalité « Database table prefix editor » de Admin Tools pour changer ce préfixe sans délai.

Option 4.5

# Compte admin

- A l'installation de votre site Joomla, le premier utilisateur créé dans la base de données est un utilisateur de type super-admin.
- Idéalement, créez un utilisateur bidon qui sera donc le premier, puis seulement votre compte d'administration; désactivez le premier.
- Ne nommez jamais votre compte « admin » car vous réduisez de 50% la difficulté de casser votre login admin puisque le pirate ne devra deviner que le mot de passe; pas le login.


# ID 42 ou 62

- Sur les anciennes installations de Joomla!, le compte super-admin était toujours le compte ID 42 (ou 62). Vérifiez si c'est votre cas et si oui, créez-vous un nouveau compte super-admin et désactivez l'ancien.
- Admin Tools permet de changer le ID de votre compte admin mais **attention**, faites-le d'abord sur un site local et vérifiez tout car le ID n'est pas changé dans tous les composants (p.ex. pas dans AllEvents, Kunena, …) et cela va induire de gros problèmes si vous avez déjà du contenu.


# Outils

# Logiciels de protection, vous avez le choix

Il existe plusieurs outils pour protéger votre site :

- Admin Tools écrit par l'auteur d'Akeeba Backup; une référence incontestée dans le monde Joomla!
- RSFirewall! (payant)
- CrawlProtect, un des plus anciens, convient pour tout sites Apache

Et …

aeSecure, nouvel (janvier 2014) outil de protection et d'optimisation de sites Apache. Des dizaines de fonctionnalités activables (On/Off) depuis une interface simple. Inclus fonctions SEO.

# Outils de supervision

- Watchful.li (payant) propose un dashboard online qui reprend tous vos sites et permet, entre autre, de les mettre à jour ainsi que de planifier l'exécution de vos backups.
- Watchful.li propose plusieurs fonctionnalités avancées comme surveillance en temps réel de fichiers sensibles du site : en cas de modification, vous recevez un email dans les minutes qui suivent.
- **Offre spéciale Joomla!Day francophone : http://watchful.li/jd14fr (50% de rabais jusqu'au 25 Juin 2014)**

# FileZilla

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <FileZilla3>
  - <Servers>
    - <Server>
        <Host>example.com</Host>
        <Port>21</Port>
        <Protocol>0</Protocol>
        <Type>0</Type>
        <User>unmask</User>
        <Pass>parasites</Pass>
        <Logontype>1</Logontype>
        <TimezoneOffset>0</TimezoneOffset>
        <PasvMode>MODE_DEFAULT</PasvMode>
        <MaximumMultipleConnections>0</MaximumMultipleConnections>
        <EncodingType>Auto</EncodingType>
        <BypassProxy>0</BypassProxy>
        <Name>example.com</Name>
        <Comments />
        <LocalDir />
        <RemoteDir />
        <SyncBrowsing>0</SyncBrowsing>
        example.com
      </Server>
    </Servers>
  </FileZilla3>
```

Oups!

FileZilla sauve toutes les données en clair dans un fichier .xml

# FileZilla

- De préférence, paramétrez vos connexions en SFTP (ou SSH).
- Si vous utilisez FileZilla, il est **impératif** de protéger l'accès aux fichiers .xml.  Cet article propose une solution : http://aesecure.com/fr/blog/61-filezilla-stocke-les-donnees-login-mot-de-passe-non-cryptes-solution.html

# Akeeba Backup 1/2

- Si ce n'est pas encore fait, installez sans tarder Akeeba Backup et faites un backup de votre site.
- Copiez régulièrement les fichiers .jpa vers un autre endroit (votre disque dur p.ex.) et testez la sauvegarde afin de vous assurer qu'elle soit correcte.
- Sachez que la version Pro d'Akeeba Backup permet de sauvegarder dans le cloud (Dropbox p.ex.); intéressant en cas de crash de votre serveur.

# Akeeba Backup 2/2

Comme indiqué dans la documentation d'Akeeba, page 132 « Securing the output directory », ne stocker pas vos backup dans le dossier /administrator/components/com_akeeba/backup mais dans un dossier en dehors de votre site (au-dessus de « www » ou « public_html »)

"The best approach is to use a directory which is outside your web server's root. By definition, this is not directly exposed to the web and is usually unavailable to file administration utilities."

# EyeSite

- EyeSite est un composant backend qui va stocker dans la base de données de votre site le CRC de chaque fichier présent sur le site à un moment T.  Une seconde comparaison à un instant T2 permet alors de comparer la liste des fichiers ayant été modifiés.
- Outil pratique pour identifier si un fichier a été ajouté / supprimé / modifié.

# jHackGuard

jHackGuard est un plugin système gratuit développé par l'hébergeur SiteGroud.com et qui permet de bloquer certaines tentatives d'injection, des « remote URL/File inclusions », « remote code execution », … sans aucune action du webmaster qui en oublie jusqu'à son existence.

# Blocage des connexions par pays

cFBlockCountry est un plugin système de type Freemium permettant de bloquer les connexions provenant d'un pays sur base de son code ISO.


# Blocage des connexions par pays

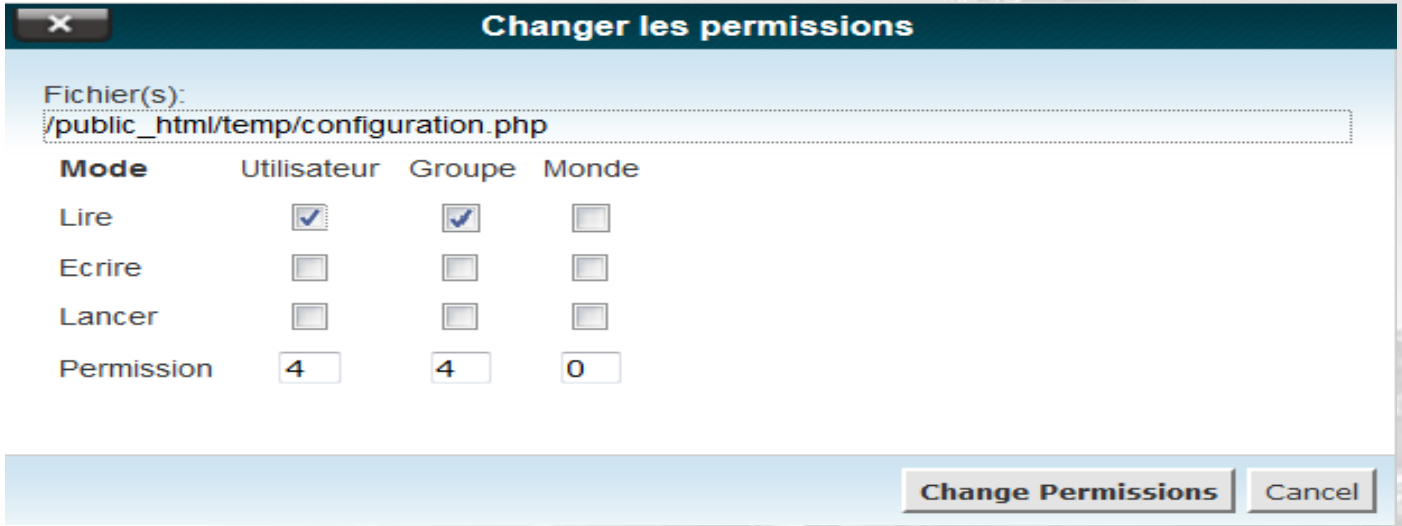
Outre l'aspect sécurité, bloquer les connexions provenant d'un pays permet d'économiser de la base passante et des ressources serveur (CPU).

Si, dans vos logs, vous voyez que la Chine est dans le haut du classement de vos visites alors que le contenu de votre site ne devrait, à priori, pas être intéressant pour ce public; bloquer la Chine vous fera économiser des ressources.


# Logiciels du type eXtplorer

- Des composants comme eXtplorer sont très pratiques lorsque vous n'avez pas un accès FTP à votre site de production mais présente une réelle menace car si un intrus parvient à se connecter sur votre administration, ce type de composant lui donne accès à l'entièreté de votre site; sécurité .htaccess en moins.
- Parfois, ces composants proposent une page d'accès en dehors de Joomla!, avec un login / password par défaut et donc connu.
- Si vous en avez besoin, installez le composant, faites ce que vous deviez faire puis désinstaller-le sans délai.

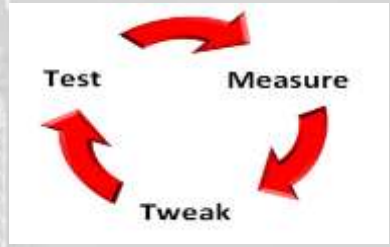
# chmod


Changer les permissions
Fichier(s):
/public_html/temp/configuration.php
Mode
Utilisateur
Groupe
Monde
Lire
Ecrire
Lancer
Permission
4
4
0
Change Permissions
Cancel

# chmod - Introduction

- Le chmod définit le niveau d'accès au fichier / au dossier.
- Un chmod **777 revient à ne rien sécuriser** : le monde entier peut lire, exécuter et modifier le fichier. Si votre but est d'être hacké, bingo, vous réussirez votre examen avec la plus haute distinction!
- Un chmod 400 ou 440 est idéal pour le fichier .htaccess qui est alors en lecture seule pour vous (propriétaire) et le groupe (si 440). (à tester toutefois au cas par cas)

# chmod




- Le chmod d'un dossier devrait être 750 (ou 755) et celui d'un fichier est généralement 640 (ou 644).
- Modifiez le chmod à 550 de votre dossier /templates/*yourtemplate* pour rendre impossible d'écrire et créer un fichier dans ce dossier très sensible.
- **Testez, testez et testez encore, sur un site de tests**. Ce qui fonctionne chez un hébergeur peut ne pas fonctionner chez un autre.

Option 3.1

# configuration.php

- Changer le chmod du fichier en 400 ou 440 afin que personne ne puisse écrire dedans.
- Si vous devez modifier la configuration générale de votre site, changez le chmod en 640 puis remettez le chmod d'origine après votre changement.

Option 3.1

# index.php

- Ce fichier devrait toujours être en chmod 440.
- Pensez que vous avez deux index.php : celui présent dans la racine de votre site et celui qui correspond à votre template utilisé (dans le dossier /templates/*votre-template*)
- Si vous devez modifier le fichier, changer le chmod en 640 puis remettez 440 après vos changements.

# Déplacer les dossiers /logs et /tmp - 1/3

- Ces dossiers ne doivent pas forcément être dans le dossier de votre site web mais peuvent « remonter » d'un niveau càd en dehors du dossier www (ou public_html).
- L'intérêt : ces dossiers n'étant plus dans le dossier www, ils ne sont plus accessibles depuis le navigateur; c'est donc une menace en moins.

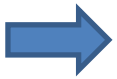

# Déplacer les dossiers /logs et /tmp - 2/3

- Connectez-vous avec votre client FTP sur votre site.
- A la racine de votre compte (pas de votre site), créez au besoin un dossier logs et un autre tmp (il est probable que ces dossiers existent déjà).

# Déplacer les dossiers /logs et /tmp - 3/3

- Rendez-vous dans votre dossier www/votre_site.
- Éditez votre fichier configuration.php.
- Modifiez les lignes public $log_path et $tmp_path et supprimez la partie /public_html/votre_site

public $log_path = '/home/xxxxx/public_html/votre_site/logs';



public $log_path = '/home/xxxxx/logs';

Option 1.1

# Interdire l'accès aux fichiers .htaccess et configuration.php

Soyez certain que vos fichiers .htaccess et configuration.php ne soient pas accessibles depuis un navigateur :

```
<Files .htaccess>
order allow, deny
deny from all
</Files>
```

```
<Files configuration.php >
order allow, deny
deny from all
</Files>
```

Option 4.3

# .htaccess – Interdire l'accès aux fichiers xml

- Ne révélez pas trop, interdisez donc que l'on puisse consulter les fichiers .xml de votre administration.
- Créez un fichier /administrator/.htaccess et ajoutez la règle suivante :

```
<Files ~ ".xml$">
order allow,deny
deny from all
satisfy all
</Files>
```

Option 1.1

# .htaccess – Interdire de lister le contenu d'un dossier

- Forcer l'utilisateur à introduire une url mentionnant un nom de fichier (p.ex. /index.php); les fichiers index.html ne sont dès lors plus nécessaires :

  IndexIgnore *
  Options All –Indexes

  *(à ne pas utiliser dans votre dossier / et /administrator sauf si vous souhaitez que l'utilisateur mentionne obligatoirement index.php dans l'URL)*

- Forcer index.php afin que le serveur n'exécute pas, p.ex., index.html, default.htm, …

  DirectoryIndex index.php

Option 1.2

# Interdire de lister le contenu d'un dossier

Soyez certain que chaque dossier sur votre site a son fichier index.html afin de garantir que lorsqu'on accède à une url telle que http://votresite/dossier1/sousdossier, il ne soit jamais affiché la liste des fichiers. Selon le paramétrage du serveur web, cela pourrait être le cas. La présence du fichier index.html va garantir que cela n'arrivera jamais.

Option 1.1

# .htaccess – Bloquer l'accès à certains dossiers

A priori, il n'y a aucune raison qu'un utilisateur accède à un fichier du, p.ex., cache de Joomla (/cache) ni à un fichier se trouvant dans le dossier temporaire (/tmp). Utilisez la règle ci-dessous pour bloquer ce type d'accès :

```
RewriteRule ^(cache|includes|language|libraries|logs|tmp)/ - [F]
```

Option 1.1

# .htaccess – Interdisez l'exécution de code php

Bloquez l'exécution de code .php depuis certains dossiers (particulièrement les dossiers /medias et /images) où ce type de code n'est pas supposé se trouver.  Cet article en parle :
http://aesecure.com/fr/blog/64-no-php-allowed.html

Testez, testez, testez.

**Cette mesure augmente fortement la sécurité de votre site!**

Option 2.3

# .htaccess – Refouler les robots malveillants

## Adoptez les règles .htaccess permettant d'interdire les robots malveillants sur votre site

#Liste fortement abrégée
RewriteCond %{HTTP_USER_AGENT} ^BadGuy [OR] RewriteCond %{HTTP_USER_AGENT} ^Zeus
RewriteRule .* - [F]

http://docs.joomla.org/Htaccess_examples_(security), Block bad user agents

Pour approfondir :http://aesecure.com/fr/blog/bloquer-les-robots-utilisateurs-fantomes.html

Option 2.3

# .htaccess – Refoulez les urls malveillantes

- Certaines attaques / spam se font en tentant de poster des formulaires par la méthode GET.
- Vous pouvez établir une parade sur base de certains mots clefs (à vous de compléter la liste):

```
RewriteCond %{QUERY_STRING} \b(ambien|blue\spill|cialis)\b [NC,OR]
RewriteCond %{QUERY_STRING} \b(erections|hoodia|viagra)\b [NC,OR]
RewriteCond %{QUERY_STRING} \b(vicodin|vuiton|xanax|ypxaieo)\b [NC]
RewriteRule .* - [F]
```

*(liste partielle)*

Option 1.1

# .htaccess – Ne pas afficher certains fichiers

- Interdisez l'affichage de certains fichiers; selon l'extension : si quelqu'un tente d'accéder à un tel fichier depuis le navigateur, l'affichage sera refusé.
- Ainsi, p.ex., bloquer l'accès aux fichiers de langues (.ini) de Joomla!

```
<Files ~ "\.(inc|class|sql|ini|conf|exe|dll|bin|tpl|bkp|dat|c|h|py|spd|theme|module)$">
deny from all
</Files>
```

Option 1.1

# .htaccess – Bloquer certaines requêtes (XSS, injection, …)

## Bloquer les urls reprenant certains mots / instructions, exemple :

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} (GET|POST) [NC]
RewriteCond %{QUERY_STRING} ^(.*)(%3C|<)/?script(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)(%3D|=)?javascript(%3A|:)(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)document\.location\.href(.*)$ [OR]
RewriteCond %{QUERY_STRING} ^(.*)(%3D|=)http(%3A|:)(/|%2F){2}(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)GLOBALS(=|[|%[0-9A-Z]{0,2})(.*)$ [OR]
RewriteCond %{QUERY_STRING} ^(.*)_REQUEST(=|[|%[0-9A-Z]{0,2})(.*)$ [OR]
RewriteCond %{QUERY_STRING}
^(.*)(SELECT(%20|\+)|UNION(%20|\+)ALL|INSERT(%20|\+)|DELETE(%20|\+)|CHAR\(|UPDATE(%20|\+)
|REPLACE(%20|\+)|LIMIT(%20|\+))(.*)$ [NC]
RewriteRule (.*) - [F]
```

Option 1.1

# .htaccess - Fingerprint

- Interdisez l'utilisation de ?tp=1, ?template=nom_template ou encore ?tmpl=offline
- Ajoutez dans votre .htaccess si nécessaire ces lignes :

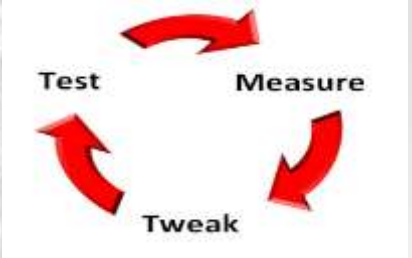
```
RewriteCond %{QUERY_STRING} (&|%3F){1,1}tp= [OR]
RewriteCond %{QUERY_STRING} (&|%3F){1,1}template= [OR]
RewriteCond %{QUERY_STRING} (&|%3F){1,1}tmpl= [NC]
RewriteRule ^(.*)$ - [R=404,L]
```

# .htaccess – Version de PHP

Une ancienne version de PHP est moins sécurisée qu'une plus récente.  Si cela vous est possible, upgradez votre version.

Pour les sites J2.5+, activez PHP 5.4 en ajoutant la ligne ci-dessous dans votre .htaccess

AddHandler application/x-httpd-php54 .php .php5 .php4 .php3
(Attention, cette instruction varie d'un hébergeur à un autre; parfois c'est **SetEnv PHP_VER 5_4**)




!!! Testez votre site pour être sûr qu'il fonctionne correctement avec cette version-là de PHP

http://aesecure.com/fr/documentation/faq/upgrade-php.html

Option 1.1

# .htaccess – Easter eggs & server infos

Préférablement à désactiver dans votre php.ini (voir ce slide), les « œufs de Pâques » sont utilisables depuis une url du type index.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42

Pour interdire les Easter eggs et la transmission d'informations sur votre serveur web, ajoutez ces lignes ci-dessous dans votre fichier .htaccess

```
RewriteCond %{QUERY_STRING} \=PHP[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12} [NC]
RewriteRule .* - [F]
```

# php.ini

Option 1.3

# Affichage des erreurs = off

Sur un site de production, il ne faut jamais afficher les messages d'erreurs qui donneraient alors des informations précieuses à l'attaquant.

1. Éditez votre fichier php.ini
2. Cherchez la variable display_errors
3. Au besoin, changez la valeur sur « off »

Si vous n'avez pas accès au fichier php.ini, vous pouvez obtenir le même résultat en ajoutant cette ligne dans votre fichier .htaccess :

php_flag display_errors off

Option 1.2

# Safe Mode

Contrairement à ce qu'on pourrait croire, activer le « safe mode » dans php.ini n'est pas une mesure de sécurité.  Safe Mode est d'ailleurs déprécié depuis PHP 5.3 et supprimé en 5.4.

Si votre site est configuré en Safe Mode ON, désactivez cette option.

Lire : http://us3.php.net/manual/en/features.safe-mode.php#ini.safe-mode

Option 1.1

# expose_php – Easter eggs 1/2

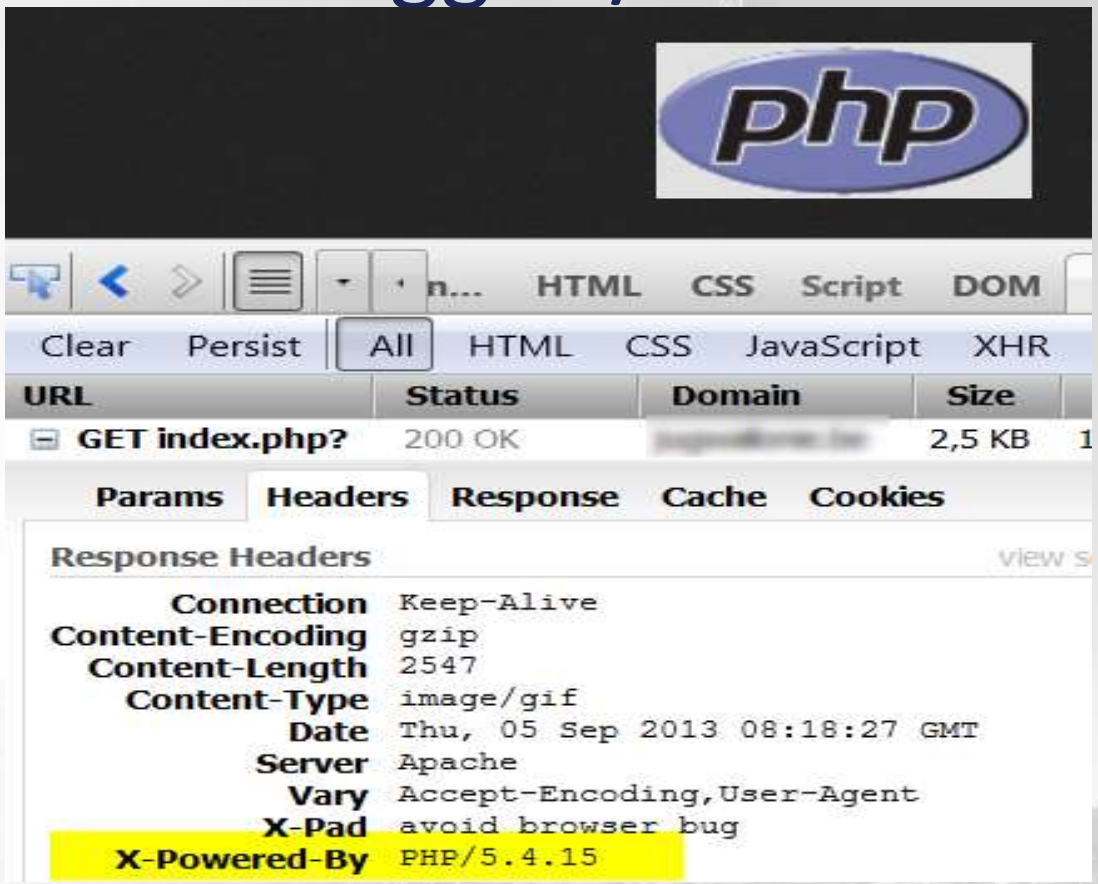
Tentez d'accéder à votre site web avec une url comme celle-ci :

index.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42

Voyez-vous le logo ?

Si oui, oups…

En affichant les en-têtes de la page; on découvre le numéro de version de PHP utilisée sur le site



Option 1.2

# expose_php – Easter eggs 2/2

1. Éditez votre fichier php.ini
2. Recherchez la variable expose_php
3. Modifiez sa valeur sur « Off »

Si vous n'avez pas accès au fichier php.ini, vous pouvez écrire une règle pour le fichier .htaccess : voir ce slide.

Lire : http://perishablepress.com/expose-php/

Option 2.4

# Interdisez l'upload

Votre site est « statique » dans le sens où il n'est pas nécessaire d'autoriser d'y uploader quelque chose; excepté à certains moments (mise à jour p.ex.); interdisez l'upload !

Ajouter la ligne ci-dessous dans votre fichier php.ini :

file_uploads=Off


# robots.txt

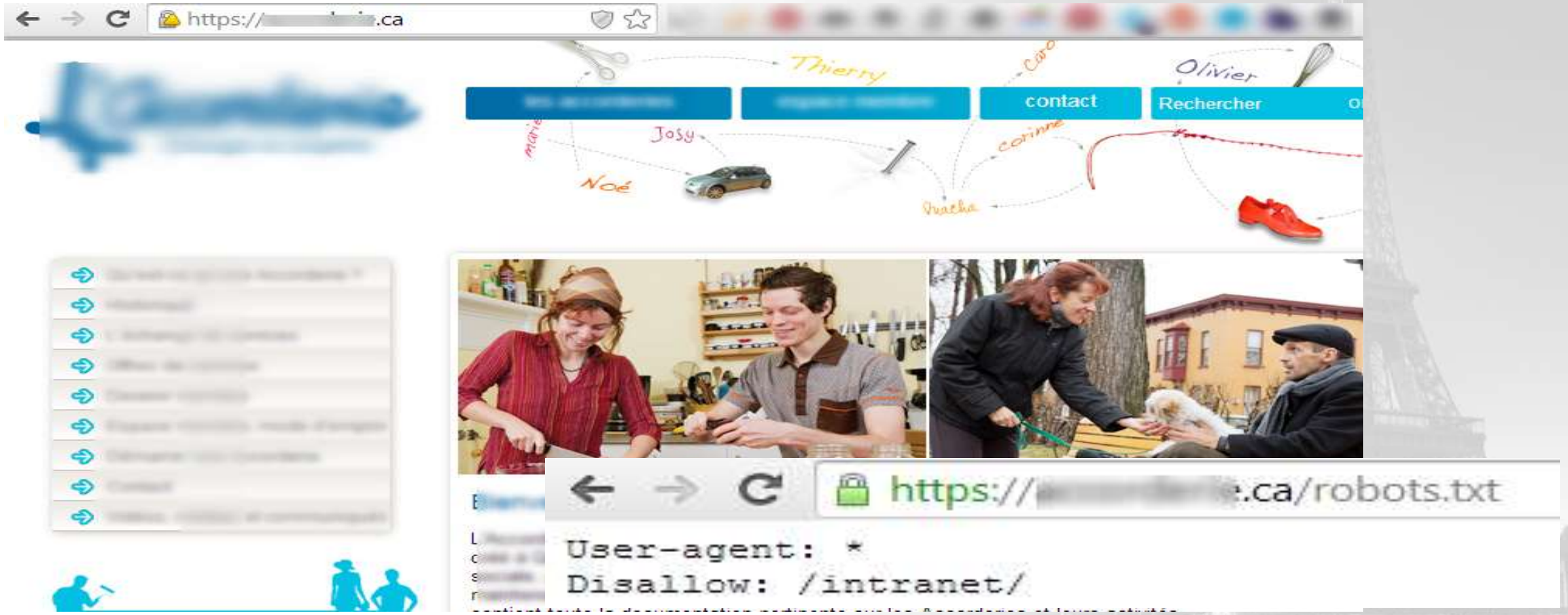

# robots.txt

Garder en mémoire que ce fichier est accessible par une simple url : http://votresite/robots.txt

Il doit être accessible car il indique aux « gentils » moteurs de recherche ce qu'ils peuvent ou pas faire.

Sachez que si vous mettez Disallow: secrets.txt la tentation sera ultra-forte pour un petit plaisantin de tenter d'accéder au fichier http://votresite/secrets.txt dont il a appris l'existence grâce à robots.txt.

# robots.txt



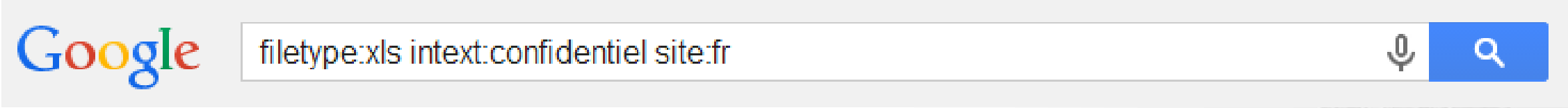

Humm, intéressant non ? Et si nous allions voir à quoi ressemble la partie « intranet »


GOOGLE
HACKING-DATABASE

Options 1.2 & 2.5

# Google indexe-t-il un peu trop ?

En principe, les moteurs de recherche suivent chaque lien qu'il rencontre. S'il voit une page avec un lien vers un fichier Excel, il va l'indexer. Ceci pourrait se révéler quelque peu ennuyeux…




Quelques exemples :

filetype:xls intext:confidentiel site:votresite.fr
filetype:txt intext:password site:votresite.fr
intitle:index.of intext:htaccess site:votresite.fr
Intitle: « Index of » administrator inurl:joomla

filetype:inc dbconn
filetype:jpa inurl:com_akeeba
inurl:robots.txt intext:security filetype:txt

Option 2.5

# Google indexe-t-il un peu trop ?

Afin d'interdire d'indexer certains fichiers, ajoutez les quelques lignes ci-dessous dans votre .htaccess.  Adaptez la liste des extensions selon votre besoin.

```
<FilesMatch "\.(doc|mdb|ppt|xls)$">
   <IfModule mod_headers.c>
      Header set X-Robots-Tag "noindex, noarchive"
    </IfModule>
</FilesMatch>
```


# Trop tard, votre site a été hacké

http://aesecure.com/fr/blog/site-hacke.html

# Trop tard 1/4 ?

- Sucuri SiteCheck permet de scanner online votre site web à la recherche de malware.
- myJoomla.com est une interface web payante (1er audit gratuit) permettant de lancer une batterie de tests et de vérifier la sécurité de votre site; avant et après un hack. Dans ce dernier cas, vous serez guidé dans la résolution du hack.
- Prenez connaissance de l'article « Your site has been hacked or defaced » sur doc.joomla.org

Option 1.9

# Trop tard 2/4 ?

- Désactivez l'accès à votre site; passez-le en mode maintenance : toutes personnes qui tentera d'accéder à votre site sera réorientée vers Google; sauf vous.  Ajoutez ces deux lignes dans votre .htaccess :

```
RewriteCond %{REMOTE_ADDR} !127.0.0.1
RewriteRule .* www.google.be [L,R=307]
```

(adapter 127.0.0.1 par votre adresse IP)


# Trop tard 3/4 ?

- Scannez votre site à la recherche d'une bestiole grâce au script JAMSS – Joomla! Anti-Malware Scan Script.
- Retrouver la liste complète des fichiers ayant été modifiés : http://ralph.davidovits.net/internet/se-proteger-des-pirates-et-hackers.html#fichmodif


# Trop tard 4/4 ?

- Nicholas K. Dionysopoulos, l'auteur de Akeeba, explique donne aussi quelques conseils « Unhacking your site »
- Réinitialisez le mot de passe de l'admin (kiwik.net) et/ou créez un nouveau compte (kiwik.net)
- Si n'avez pas accès à phpMyAdmin mais à votre FTP, utilisez « Reset Admin Password »


# Lectures additionnelles


# Lectures additionnelles

- Forum Sécurité Joomla France
- Sécurité Joomla – Aide-Joomla.com
- Votre site Joomla! est-il bien sécurisé ?
- Joomla Security Checklist
- Fortifying your Joomla! Website
- Joomla Security Feed
- Simple Security Guide, part 1 & part 2
- How to keep your Joomla-based website secure ?
- Top 10 Stupidest Administrator Tricks

Questions, suggestions, partage d'idées, contribution, …

Merci pour votre attention !


http://aesecure.com/fr/forum/boite-a-idees.html