

TYPO3 Security Cookbook

Traduction française

Copyright 2006, Ekkehard Guembel ; Michael Hirdes, <guembel@naw.de ; hirdes@elios.de>
This document is published under the Open Content License
available from <http://www.opencontent.org/opl.shtml>
The content of this document is related to TYPO3
a GNU/GPL CMS/Framework available from www.typo3.com

“A quoi sert ce document?”

Ce document contient une check-list pour les systèmes d'administration TYPO3. Vous pouvez l'employer pour vous assurer que vous avez fermé les portes de votre système.

Introduction

Etant le résultat d'une discussion au T3Board04 à Kitzbühel, ce document aura naturellement pour but de se développer à l'avenir. Si vous voulez contribuer en ajoutant de nouveaux chapitres, envoyer svp votre texte à l'auteur de ce document.

Conditions d'utilisation

La check-list est prévue pour un environnement TYPO3. On ne la prévoit pas pour être un autre manuel d'installation ! Ainsi, vous pouvez juste installer votre serveur comme d'habitude, et employez cette liste pour vérifier chaque chapitre.

Priorités et Structure

Bien qu'il soit recommandé lire les chapitres dans l'ordre du document, il y a naturellement des priorités. Pour faciliter la lecture, tous les sujets sont triés.

TYPO3

Sécurité le module d'Install

Priorité: Haute

Explication de fond : Le module d'Install TYPO3 est le centre névralgique de votre système TYPO3. Comme règle de base, il devrait ne jamais être accessible du Web à moins que vous n'ayez réellement besoin de lui.

Mesures:

neutraliser l'outil d'installation (enlever le commentaire devant la ligne de « die () » dans typo3/install/index.php) OU déplacer le dossier de typo3/install/ou le rendre inaccessible pour le web server OU limiter l'accès à typo3/install aux centres serveurs/aux réseaux/aux domaines spécifiques (employant .htaccess) - déprécié ! vous pourriez vouloir ajouter une authentification .htaccess (cependant également non considérée comme secure) veiller au moins à changer le mot de passe d'outil d'installation en valeur non triviale

Changer “admin” Password, Renommer “admin” User

Priorité: Haute

Explication de fond : les admins-password par défaut sont toujours le premier essai des hackers.

Mesures:

changer username et password de l'admin immédiatement après l'installation.
Remplacer l'admin user par d'autres administrateurs (de préférence avec des usernames personnalisés)

Ne pas utiliser “Quickstart“, “Testsite” et al. pour les sites en live

Priorité: Haute

Explication de fond: Le paquetage de « Quickstart » - comme d'autres packages de démo - est prévu pour fournir un système de démo immédiatement fonctionnel. Il contient beaucoup de code et de contenu que vous devriez nettoyer avant l'installation pour la production. Il vaut mieux commencer par « nettoyer » le système et installer (peut-être importer) seulement de ce que dont vous avez vraiment besoin.

Mesures:

Utiliser un package Dummy pour les sites en live.
S'assurer d'avoir modifié tous les be et fe users.

Droits d'accès au fichiers

Priorité: Haute

Explication de fond: les privilèges minimums devraient être donnés dans les dossiers TYPO3 et htdocs.

Mesures:

veiller à retirer tous les privilèges en écriture dans typo3_src pour le compte de l'utilisateur du web server. Paramétrer ownership et umask dans les htdocs par des valeurs appropriées (différentes pour les divers sous-répertoires !) parano-paramétrage: Placer localconf.php en dehors des htdocs en changeant typo3conf/localconf.php en ce qui suit :

```
<?php  
require("<nom du dossier>/localconf.php");  
?>
```

Oter le code inutile

Priorité: Haute

Explication de fond: Selon votre package de base (en particulier si vous employez le code CVS - déprécié de toute façon !), il peut contenir du code supplémentaire qui n'est pas nécessaire pour la production et ne devrait pas donc être accessible aux contrevenants potentiels.

Mesures:

Supprimer les dossiers ./misc, ./cvs et ./dev si présent, ou les rendre au moins inaccessibles pour l'utilisateur du web server . si vous avez le serveur live séparé du serveur de production de vos rédacteurs, enlevez le Backend des serveurs live Installer seulement les extensions requises.

Configurer les options de sécurité TYPO3

Priorité: Haute

Explication de fond: TYPO3 fournit de nombreuses options de configuration qui augmentent la sécurité du système. Les vérifier et employer ce qui a du sens dans votre situation !

Mesures dans l'outil d'Install (voir la section outil d'Install pour les dernières options et leurs descriptions):

```
[strictFormmail] – paramétrer à "1"  
[encryptionKey] – devrait être paramétrée ("Basic Configuration")  
[warning_email_addr]  
[lockIP]  
[lockRootPath]  
[fileCreateMask]  
[fileDenyPattern] – doit au moins contenir \.php$|\.php.$  
[folderCreateMask]  
[warning_mode]  
[IPmaskList]  
[lockBeUserToDBmounts]  
[lockSSL]  
[enabledBeUserIPlock]
```

[disable_exec_function]
[usePHPFileFunctions]
[noPHPscriptInclude] – considerer cette options si d'autres personnes ont accès à vos fichiers templates
[lockHashKeyWords]
[devIPmask]

Mesures / BE GUI

Ajouter un lockToDomain aux enregistrements be_users/be_groups .

Eviter config.baseURL=1

Priorité: Haute

Explication de fond: Dans des versions plus anciennes, votre cache peut être empoisonné, ceci résultant de pages externes affichées à la place de vos propres pages.

Mesures:

utiliser une URL absolue à la place OU s'assurer que le site Web peut seulement être accessible par une URL correcte (serveurs virtuels)

Penser à utiliser SSL pour l'accès Backend

Priorité: Moyenne

Explication de fond: Bien que le login BE soit chiffré, l'accès BE est non protégé à moins que vous n'employiez le SSL. Pour de l'information sensible, il vous est conseillé d'employer le SSL pour tout accès BE.

Mesures:

configurer HTTPS pour vos serveurs
redirection des accès HTTP /typo3 vers HTTPS sur vos serveurs web
utiliser lockSSL (voir "Configurer les options de sécurité TYPO3")

Sécurité FE User

Priorité: Moyenne

Explication de fond: Prendre svp les soucis de sécurité des users FE au sérieux, c.-à-d. protéger leurs données sensibles.

Mesures:

Utiliser SSL pour le login FE
Utiliser SSL pour les inscriptions et changement de mot de passé FE
Utiliser SSL pour les données sensibles telles que les formulaires (pas seulement les données de carte de crédit...) ou les informations personnelles
Ne stockez pas les mots de passe des user fe en clair, utilisez une extension comme kb_md5fepw, ou utilisez un stockage de mots de passe externe sécurisé comme le LDAP (de préférence via SSL) avec MD5.

Restriction de l'utilisation des éléments de contenus spéciaux

Priorité: Haute

Explication de fond: Quelques éléments de contenu de bas niveau peuvent laisser les utilisateurs principaux accéder au système au delà du niveau que vous aviez prévu, ou peuvent leur permettre de créer des failles de sécurité sans le savoir. Par conséquent, les restrictions suivantes sont recommandées pour tous les utilisateurs non avertis ou incapables de comprendre les implications de sécurité, ou auxquels vous ne faites pas entièrement confiance.

Mesures:

- Ne pas autoriser les contenus HTML
- Ne pas autoriser de contenu HTML dans les contenus de type texte
- Ne pas autoriser les plugins laissant insérer du code php

Choisissez des noms d'utilisateurs personnalisés pour l'accès Backend

Priorité: Haute

Explication de fond: « john.doe » est meilleurs que « bigboss » - éviter d'employer des comptes communs en général. Vous devriez toujours pouvoir garder la trace de qui fait quoi, et les utilisateurs principaux devraient être au courant de ce fait.

Mesures:

Donnez des noms d'utilisateurs personnalisés
Informez les users BE de leur login
Sensibilisez les au non partage des comptes utilisateurs

Logging / Auditing

Priorité: Haute

Explication de fond: Connaître vos fichiers de log, et être sûr qu'ils sont configurés pour auditer toute l'information dont vous avez besoin.

Mesures:

La table de sys_log est votre fichier de log des users BE par défaut (accessible par Outils->Log) vous pouvez activer des fichiers de log additionnels en utilisant les mots-clés [logfile_dir] et [logfile_write] [trackBeUser] prévu pour des debug [enable_DLOG] (en conjonction avec la constante TYPO3_DLOG)

Gestion des erreurs

Priorité: Moyenne

Explication de fond: Même si vous essayez de l'éviter - votre système peut avoir un jour une ou plusieurs erreurs - ainsi « soyez préparé ». Assurez vous que les erreurs sont dépestées, et les rendus des utilisateurs sont convenables et n'exposent pas n'importe quelle information interne.

Mesures:

Les erreurs PHP doivent être gérées, mais normalement par des méthodes PHP (voir ci-dessous). Ainsi [displayErrors] devrait être paramétré à 0. Une chose plus cosmétique : la page interne d'erreur TYPO3 "Page not Found" peut être configurée avec les réglages [pageNotFound_handling] et [pageNotFound_handling_statheader].

Utiliser les extensions révisées

Priorité: Moyenne

Explication de fond: Chaque extension peut potentiellement exposer votre système, par un bug de sécurité ou même intentionnellement.

Mesures:

Utiliser les extensions qui ont subi le processus de revue.
Si une extension n'est pas encore passée en revue, penser à commanditer sa revue.
Se rappeler d'assurer la qualité de vos propres extensions.

S'abonner à TYPO3-Announce

Priorité: Haute

Explication de fond: Au cas où un sujet concernant la sécurité avec TYPO3 ou une de ses extensions se produirait, « un bulletin de sécurité TYPO3 » sera communiqué par la liste de diffusion de « TYPO3-Announce ». Un « fix » ou un travail suivracette annonce.

Mesures:

S'abonner à TYPO3-Announce
Lire les bulletins et implémenter les mesures si vous êtes affecté.
S'assurer de faire les mêmes choses pour les installations futures

Tous les bulletins de sécurité peuvent être trouvés ici :
<http://news.typo3.org/news/teams/security/rss.xml>

Autres paramétrages (non TYPO3)

PHP

Ces paramétrages devraient être faits dans « php.ini ».
stocker les erreurs dans un fichier log d'erreur - nécessaire pour reproduire tous les problèmes.
Cacher l'affichage des erreurs - ne montrer aucune erreur par le web server - ' ne poussez pas des personnes aux fuites possibles.
employer le safemode, ou au moins open_basedir pour empêcher le Web d'accéder à d'autres dossiers ou pour exécuter des choses,
Employer un wrapper CGI/PHP (suPHP ?) ? ? ?
compiler votre PHP avec le minimum d'options de compilation, ou installer seulement les extensions nécessaires - ce qui n'est pas inclus, n'est pas vulnérable.
Register_globals = Off. Si ceci est vraiment exigé, il pourrait être paramétré à On pour certains webs dans le dossier .htaccess.
vérifier et utiliser .htaccess !

Apache

Dans httpd.conf ne loadez pas de modules dont vous n'avez pas besoin. Le mieux est de ne même pas les installer. Directory listing par exemple n'est pas nécessaire.
Ceci peut être fait par l'intermédiaire du manuscrit de php si nécessaire. Installer seulement les modules requis. neutraliser l'information de version en pages d'erreur, dites en le moins possible aux éventuels attaquants.

MySQL

Interdire les connexions réseau à MySQL, si besoin, utiliser un stunnel.
ne pas employer l'utilisateur root de mysql, utiliser un utilisateur par base de données.
Utilisez un mot de passe différent du mot de passe du serveur pour MySQL.

Général

Problèmes concernant l'hébergement mutualisé

conditions à l'ISP.
activer le su_exec.
ne pas stocker les mots de passe sur des serveurs ! Si vous avez besoin d'un dossier de password.txt : le stocker sur une feuille de papier, ou sur une boîte qui n'est pas reliée au Web. (je sais, celui-ci harcèle, mais...). souscrire aux listes de sécurité de votre fournisseur de distribution/logiciel d'exploitation. (OS, ssh, apache, php, mysql, openssl,...).
si possible, faire des mises à jour par un cron.
essayer d'employer des connexions sécurisées pour tous les protocoles (sftp, etc.).
limiter les accès des utilisateurs seulement aux dossiers nécessaires (c.-à-d. Proftpd : utilisateurs home = htdocs ; DefaultRoot =).
surveiller vos serveurs pour voir si quelque chose de peu commun se produit (c.-à-d. nagios, tripwire, tigre, logsurfer,...).
durcir le système (les services inutiles de désactivation, enlever des compilateurs,...).
protéger le phpMyAdmin avec .htaccess
ne pas faire les dumps ou backups sur fileadmin ou htdocs, si vous employez des extensions de backup, supprimez les backups après téléchargement.

Sujets non listés ici

renommer "/typo3" --> nous en avons discuté et décidé de ne pas le recommander.
Backups (devrait être clair)
sec.-extensions, sso, ... (nous avons mentionné de checker les resp. sites)
roles / permissions BE
règles des mots de passe – (il ne s'agit pas d'une checkliste pour débutant internet)