Рецепты безопасности TYPO3

Ключ расширения : **security**

Оглавление

"О чем это?"

Этот документ содержит контрольный перечень для системных администраторов TYPO3. Вы можете им воспользоваться чтобы быть уверенным, что обычно открытые двери вашей системы закрыты.

Введение

Являясь, в основном, результатом дискуссии на T3Board04 в Kitzbuhel, этот документ, конечно, будет в будущем расти. Если у вас есть желание поучаствовать, добавляя новые разделы, то высылайте текст автору этого документа.

Технические требования

Контрольный перечень связан с работой в окружении TYPO3. Не предполагается стать иным руководством по инсталляции!
Таким образом, вы можете просто установить сервер как обычно, и применять список для контроля пунктов по очереди.

Приоритеты и структура(Priorities & Structure)

Хотя предполагается, что вы изучите каждый пункт этого документа, существуют, конечно и приоритеты. Чтобы вам было легче, все рассмотрение отсортировано сверху вниз.

TYPO3

Защитите Install Tool

Важность: Высокая
Подоплека пояснения: В TYPO3 процедура Install Tool является важным центром вашей системы TYPO3. В качестве основного правила должно быть – процедура всегда недоступна через Web, разве только она вам действительно понадобилась.
Мероприятия:
отключите Install Tool (удалите комментарий в начале строки “die()” в файле typo3/install/index.php) ИЛИ
переместите каталог typo3/install/ или сделайте его недоступным для сервера web
ИЛИ
ограничьте доступ к typo3/install для определенных hosts / networks / domains (применяя .htaccess) – устаревшее !
возможно вы захотите добавить аутентификацию в .htaccess (хотя это не считается защитой)
НАКОНЕЦ убедитесь, что вы изменили пароль входа в Install Tool на что-то необычное.

Измените пароль “admin”, Переименуйте пользователя “admin”

Важность: Высокая
Подоплека пояснения: Пользователь admin и его пароль по-умолчанию, являются первой пробой для хакеров.
Мероприятия:
измените пароль для пользователя “admin” немедленно после установки
замените пользователя “admin” другими админами – желательно персонализированными (смотри “Выбор имен для пользователей(Choose Personal User Names)”).

Не используйте “Quickstart“, “Testsite” в рабочих системах

Важность: Высокая
Подоплека пояснения: Пакет “Quickstart”– также как и другие демонстрационные пакеты – планировался для обеспечения выполняемой демонстрационной системы. Он содержит порядочно кода и контента, который следует удалить перед рабочей установкой. Будет лучше начинать с «чистой» системы и установить (может быть импортировать) только то, что реально необходимо.
Мероприятия:
применяйте пакет “dummy” для рабочих сайтов
убедитесь НАКОНЕЦ, что вы удалили все пользователей, как внешних так и внутренних

Права доступа к файловой системе(File System Access Rights)

Важность: Высокая
Подоплека пояснения: Минимальные привилегии выделяются для каталогов TYPO3 и htdocs
Мероприятия:
убедитесь, что отменены все привилегии WRITE в typo3_src для пользовательской учетной записи на сервере web
задайте владельца и маску в htdocs соответствующими значениями (отличающимися для разных подкаталогов!)
установки paranoid: Поместите файл localconf.php вне htdocs изменив файл typo3conf/localconf.php следующим образом:

```
<?php
require("<directory outside htdocs>/localconf.php");
?>
```

Удалите ненужный код

Важность: Высокая
Подоплека пояснения: В зависимости от вашего базового пакета (особенно, если вы используете CVS код – устаревший в любом случае!), он может содержать часть кода не нужного для разработки и поэтому недоступного для потенциального применения.
Мероприятия:
Удалите каталоги ./misc, ./cvs и ./dev, если они присутствуют, или, по крайней мере, сделайте их недоступными для пользовательской учетной записи на сервере web
если ваш рабочий сервер отделен от системы редактирования, удалите внутренний интерфейс(BE) с рабочих серверов
Устанавливайте только необходимые расширения

Конфигурация опций безопасности TYPO3

Важность: Высокая
Подоплека пояснения: В TYPO3 обеспечивается многочисленное конфигурирования опций, которые улучшают безопасность системы. Проверьте их и подберите для своей ситуации!
Мероприятия / Install Tool (смотри главу Install Tool с новейшими опциями и подробными описаниями):
[strictFormmail] – установите в "1"
[encryptionKey] – следует установить (например в "Basic Configuration")
[warning_email_addr]
[lockIP]
[lockRootPath]
[fileCreateMask]
[fileDenyPattern] – должно содержать по крайней мере \.php$|\.php.$
[folderCreateMask]
[warning_mode]
[IPmaskList]
[lockBeUserToDBmounts]
[lockSSL]
[enabledBeUserIPLock]
[disable_exec_function]
[usePHPFileFunctions]
[noPHPscriptInclude] – обдумайте это, если у кого-то есть доступ к вашим файлам шаблонов
[lockHashKeyWords]
[devIPmask]
Мероприятия / BE GUI
Добавьте блокировку lockToDomain в записях be_users/be_groups

Избегайте config.baseURL=1

Важность: Высокая
Подоплека пояснения: В старых версиях ваш кеш может быть испорчен, что приводит к выводу чужих страниц вместо ваших.
Мероприятия:

используйте только абсолютный URL
OR
убедитесь, что доступ к сайту может быть получен только с правильного URL (то есть применяйте имена виртуальных хостов на вашем сервере web)

Рассмотрите применение SSL для внутреннего доступа (Backend Access)

Важность:Средняя
Подоплека пояснения: Хотя авторизация во внутреннем интерфейсе сама по себе зашифрована, последующий доступ к внутреннему интерфейсу не защищен, если не использовать SSL. Так как это может повредить важную информацию, вам предлагается применять SSL для всего доступа к внутреннему интерфейсу.
Мероприятия:
сконфигурируйте HTTPS для вашего сервера
пере направьте доступ к HTTP на /typo3 к HTTPS вашего сервера
применяйте опцию lockSSL в Install Tool (смотри “Конфигурирование опций безопасности TYPO3”)

Безопасность внешних пользователей(FE User)

Важность:Средняя
Подоплека пояснения: Пожалуйста отнеситесь к рассмотрению безопасности внешних пользователей серьезно, т.е. защитите их важные данные.
Мероприятия:
Применяйте SSL для авторизации внешних пользователей(FE logon)
Применяйте SSL для само регистрации внешних пользователей и изменению пароля
Применяйте SSL для всех важных данных, вроде форм (не только к данным кредитных карт…) или персонального вывода
не храните открыто пароли внешних пользователей – применяйте расширение вроде kb_md5fepw, или используйте безопасное внешнее хранение паролей вроде LDAP (предпочтительней чем SSL) с MD5

Ограничьте использование специальных элементов контента

Важность: Высокая
Подоплека пояснения: Некоторые низкоуровневые элементы контента могут позволить внутренним пользователям получить доступ вне пределов предполагаемого уровня, или могут позволить им создавать непреднамеренные нарушения безопасности.
Поэтому, следующие ограничения рекомендуются для всех беспечных пользователей или недооценивающих угрозы безопасности, или просто для тех, кому нет доверия.
Мероприятия:
- Запретите Content Element "HTML"
- Запретите плоский HMTL в Text Content Elements
- Запретите расширения, которые позволят пользователям внедрить код PHP

Выбор персонифицированных имен пользователей для внутреннего доступа(Backend Access)

Важность: Высокая
Подоплека пояснения: “john.doe” значительно лучше чем “bigboss” - избегайте применять общие учетные записи в принципе. Вы должны в любой момент знать кто и что делает, и внутренние пользователи должны быть об этом уведомлены.
Мероприятия:
назначайте персонифицированные имена пользователей
проинформируйте ваших внутренних пользователей(BE users) об авторизации
научите их не пользоваться общими учетными записями

Авторизация / Контроль(Logging / Auditing)

Важность: Высокая
Подоплека пояснения: Изучите свои log файлы и будьте уверены, что они сконфигурированы так, чтобы у вас

была вся информация для контроля.
Мероприятия:
Таблица sys_log является log по-умолчанию внутреннего пользователя (доступна из Tools->Log)
xxxxxxxxxxxxxxxxx вы можете дополнительно контролировать с помощью ключей [logfile_dir] и [logfile_write]
Установка [trackBeUser] предполагается для целей отладки
[enable_DLOG] (в сочетании с константой TYPO3_DLOG)

Обработка ошибок(Error Handling)

Важность:Средняя
Подоплека пояснения: Даже если вы захотите избежать этого – ваша система будет генерировать одну (или более) ошибку в день – итак «будьте готовы». Убедитесь, что ошибки отслеживаются и пользовательский вывод нормален и не содержит никакой важной информации.
Мероприятия:
Ошибки PHP должны управляться, но лучше самим PHP (смотри ниже). Для этого нужно установить [displayErrors] в 0.
Еще немного косметики: внутренние ошибки TYPO3 "Страница не найдена(Page not Found)" можно конфигурировать с помощью [pageNotFound_handling] и установкой
[pageNotFound_handling_statheader].

Используйте проверенные / Пересмотренные расширения

Важность:Средняя
Подоплека пояснения: Каждое расширение потенциально вскрыть всю вашу систему, либо из-за ошибок в безопасности либо преднамеренно.
Мероприятия:
Используйте только те расширения, которые уже проверены.
Если расширение еще не проверено, подумайте о стимулировании такой проверки.
Помните, что ваши собственные расширения должны быть также качественными.

Подпишитесь на анонсы TYPO3, применяйте исправления

Важность: Высокая
Подоплека пояснения: В случае возникновения проблемы с безопасностью в TYPO3 или одним из расширений, нужно подписаться на "TYPO3 Security Bulletin" в списке рассылки "TYPO3-Announce". Решение или алгоритм решения будут найдены.
Мероприятия:
Подпишитесь на анонс TYPO3 (goto xxxxxxxxxxxxx)
Читайте Bulletins, и применяйте необходимые меры.
Не забывайте делать это при будущих инсталляциях!
Все TYPO3 Security Bulletins можно найти в xxxxxxxxxxxxxxx

Установки не TYPO3

PHP

Эти установки следует сделать в php.ini
log errors – в файл ошибок – необходимо для воспроизведения любой проблемы
Display errors off – не выводите любые ошибки в webserver – не провоцируйте утечки информации
Применяйте safemode, или наконец откройте basedir, во избежание доступа из web к другим каталогам или для выполнения того, что они не должны –повторим : чем меньше, тем - лучше.
Применяйте CGI/PHP wrapper (suPHP?) ???
компилируйте PHP с минимумом опций компиляции, или установите только необходимые расширения – что не включено, то – не опасно.
Register_globals = Off . Если это действительно нужно, то может быть переключено для единичных web в файле .htaccess.
Проверьте и примените в .htaccess !

Apache

В файле httpd.conf не загружайте модули, которые не нужны. А лучше всего их и не устанавливать. Список каталогов(Directory listing), к примеру, не нужен.
Это можно сделать с помощью программы на php при необходимости
Установите только требуемые модули
Отключите информацию о версии при выводе ошибок, сообщайте возможным атакующим как можно меньше

MySQL

Запретите сетевые подключения к mysql, при необходимости, туннелируют их безопасным соединением (stunnel)
не пользуйтесь пользователем mysql root, только одного на базу данных
создайте собственный пароль для mysql root, не применяйте пароль root сервера

Основное

проблемы связанные с разделяемым хостингом

требования к isp
активируйте su_exec
не сохраняйте пароли на сервере ! Если вам требуется файл password.txt: храните его на клочке бумаги, или на коробке не имеющей соединений с интернет. (я знаю, что ворчу, но ...)
подпишитесь на рассылки по безопасности нашей дистрибуции / Разработчика ОС. (OS, ssh, apache, php, mysql, openssl, …)
если возможно, запускайте обновления ежедневно с помощью cron
старайтесь использовать безопасные соединения для все протоколов (sftp, etc)
ограничьте доступ пользователей только к необходимым каталогам (например Proftpd: users home = htdocs ; DefaultRoot = ~)
следите за серверами чтобы увидеть любое отклонение (например nagios, tripwire, tiger, logsurfer, ...)
затвердите(harden) систему (отключите ненужные службы, удалите компиляторы, ...)
защитите phpMyAdmin с помощью .htaccess
не делайте dump или backup в каталоги fileadmin или htdocs, если вы применяете расширение backup, то удаляйте backup после сохранения.

Чего здесь НЕ достает

переименуйте "/typo3" --> мы обсуждали это и пришли к выводу – не делайте этого.
Backups (должны быть чистыми)
sec.-extensions, sso, … (мы рекомендуем просматривать соответствующие сайты)
BE роли / разрешения
правила для паролей – (это же не книга “безопасность интернет сервера для болванов(dummies)”)