

TYPOLightのセキュリティホール

2010年第2回K*BUG研究会



TYPOLight

2010年3月5日

神戸 隆博

taca at back-street.net / @_taca_

話題

- TYPOlight webCMSについて
- 2009年末のセキュリティ・ホール
- その後

自己紹介

- 神戸 隆博(かんべ たかひろ)
 - 京都在住13年目: 二人暮らし
 - 京都生まれ、横浜東京育ち
 - 本業: ケイアイエスユー株式会社
 - <http://www.kisu.co.jp/>
 - NetBSD(pkgsrc)開発者
 - 2000年8月頃より
 - 本業でも使用中
 - その他
 - K*BUG: <http://www.kbug.gr.jp/>
 - Geeklog日本語版お手伝い

TYPOLight webCMS

- コンテンツ管理システム
 - <http://www.typolight.org/>
- 最新リリース: 2.8.1
- ライセンス: LGPL2.1
 - 2.8からLGPL3
 - 商用ライセンスあり
 - 生成するHTMLソースから著作権表示を削除できる。
- Made in Germany

動作環境

- UNIX系OSやWindows
- Webサーバ
 - Apache, IIS
- データベース
 - MySQL 4.1以降
 - MSSQL, Oracle, PostgreSQL, Sybase等
- スクリプト言語
 - PHP 5.2以降
 - mcrypt, mbstring (or iconv), soap

特徴(1)

- 多言語対応: UTF-8、36の言語ファイル
- XHTML strict
 - W3C/WAI要求
- ライブアップデート・サービス
 - 有償(8.32ユーロ)
- バックエンドとフロントエンド
 - 管理ページと公開ページ
- 複数ドメインと複数言語

特徴(2)

- テンプレート・ベース
- 強力な権限システム
- 様々なコンテンツ
 - アーティクル、ニュース、イベント、
ニュースレター、コメント、フォームジェネレータ
- 完全なブログ機能なし(track back)
- エクステンション
 - エクステンション・レポジトリ: 264個が登録
 - ダウンロード、インストール、アップデート

バックエンド

TYPOlight Open Source CMS 2.8



TYPOlight Open Source CMS へのログイン

ユーザ名

パスワード

バックエンドの言語


日本語



ログイン

TYPOlight Open Source CMS :: Copyright ©2005-2010 by Leo Feyer :: Extensions are copyright of their respective owners :: Visit www.typolight.org for more information :: Obstructing the appearance of this notice is prohibited by law!

TYPOlight is distributed in the hope that it will be useful but WITHOUT ANY WARRANTY :: Without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE :: See the GNU Lesser General Public License for more details :: TYPOlight is free software :: You can redistribute it and/or modify it under the terms of the GNU Lesser General Public License (LGPL) as published by the Free Software Foundation.

 [フロントエンドへ行く](#)

ログイン後

TYPOlight Open Source CMS 2.8.RC2

ユーザ webmaster :: フロントエンドのプレビュー :: ホーム :: ログアウト

バックエンドモジュール

コンテンツ

- ✓ アーティクル
- 🕒 ニュース
- 📅 カレンダー/イベント
- 🗉 FAQ
- ✉ ニュースレター
- 📄 フォームジェネレーター
- 💬 コメント

レイアウト

- 📁 モジュール
- 📄 スタイルシート
- 📄 ページレイアウト
- 🌐 サイト構造
- 📄 テンプレート

アカウントマネージャー

- 👤 メンバー
- 👤 メンバークラウド
- 👤 ユーザ
- 👤 ユーザグループ

システム

- 📁 ファイルマネージャー
- 📄 システムログ

TYPOlight Open Source CMS

➔ TYPOlight Open Source CMS バックエンド

システムメッセージ

- 🚫 期限切れタスク (2)
- 🕒 最後のログイン: 2010-02-10 13:11

バックエンドのアクセスキー

- [ALT] + s 保存 (Save)
- [ALT] + c 保存して閉じる (Save and close)
- [ALT] + e 保存して編集 (Save and edit)
- [ALT] + n 作成 (Create new)
- [ALT] + b 戻る (Go back)
- [ALT] + t トップへ戻る (Back to top)
- [ALT] + f フロントエンドのプレビュー (Frontend preview)
- [ALT] + q 終了 (Quit (logout))

コンテンツ

✓ アーティクル

アーティクルは、テキストやイメージ、ハイパーリンクのような、コンテンツ要素のコンテナ（容器）として使われます。各アーティクルは、特定のページに掲載されます。このモジュールは、記事を管理することができます。

🕒 ニュース

歴史とセキュリティ

- 2.0.RC1: 2006年
- 2.2.5(開発版): 2007年3月19日
 - CVE-2007-1632:
 - <http://www.securityfocus.com/bid/23048>
- 2.4.7: 2007年10月11日
 - バックエンドのプレビュー
 - <http://www.securityfocus.com/bid/25975>
- 2.5.3: 2008年1月28日
 - Cross-Site Request Forgeries

今回のセキュリティ問題

- 2009年12月19日
 - インストーラのパスワード回避
 - データベースのパスワード奪取
 - Safe Mode Hackが有効: FTPのログイン情報も奪取
 - 通常のバックエンドやフロントエンドには問題なし
- 2.7.6のリリース
 - 2.4, 2.5, 2.6, 2.7へのパッチ提供
 - 本来はサポートの終わった古いバージョンも対象
 - 2.4.0のリリースは2007年6月

CMSのインストーラ

- あるもの、ないもの
 - Webインターフェイスのもの、そうでないもの
- 初期パスワード
 - 有効にするためのおまじない
 - TYPO3: ある名前のファイルを作成
 - インストーラ使用後に削除を推奨
 - Geeklogなど

TYPOLightのインストーラ

- バックエンドのURL + install.php
- 初期パスワードが設定
- インストーラの最初の処理
 - 新パスワードの設定
- その後、様々な設定
 - セキュリティー・キー
 - データベース接続の設定
 - データベースのテーブルの作成
 - 管理者ユーザの作成

インストーラの起動

TYPOlight Open Source CMS 2.8




インストール・ツール ログイン

インストール・ツールのパスワードを入力してください。インストール・ツールのパスワードは TYPOlight のバックエンドのパスワードとは別のものです。

パスワード

ログイン

 TYPOlight のバックエンドにログイン

パスワード設定

TYPOlight Open Source CMS 2.8



インストール・ツールのパスワード

✓ デフォルトのパスワードから変更しました。

このスクリプトをさらに安全に保つには、**exit;** 命令文を **typolight/install.php** に加えるか、完全にサーバから削除してください。この場合、ローカル設定ファイルにあるシステム設定を直接編集しなければなりません。

パスワード

パスワードの確認

パスワードを保存

暗号鍵の生成

✓ 暗号鍵を生成しました。

この鍵は暗号化されたデータを保存するときに使用します。暗号化されたデータは、この鍵だけで復号できることに注意してください。従って、どこかに保存した上で、既に暗号化されたデータがある場合は決して変更してはいけません。空のままにするとランダムなキーを生成します。

暗号鍵を生成

鍵を生成または保存

何が問題だったか

- 2.7.5と2.7.6の違い
 - 修正されたファイルは3つだけ
 - system/constants.php
 - バージョン情報の修正だけ
 - typolight/ftp.php
 - 14行程度
 - typolight/install.php
 - 12行程度
 - いわゆるセッション管理の問題

修正前

- TL_INSTALL_AUTHセッション変数
 - パスワード認証に成功後
 - md5(“クライアントのIP”)
 - またはmd5(session_id())
 - 5分の有効期限でcookieを設定
 - 名前は TL_INSTALL_AUTH
 - ログイン後
 - cookie名TL_INSTALL_AUTHの存在を確認
 - パスワードそのもののチェックは行わない。
 - 存在の確認だけなので、同名のcookieを偽装されるとアウト
 - パスワード認証に成功後と同様に値を設定
 - 5分の有効期限を再設定

修正後: ログイン前

- 明示的にセッション変数を初期化
 - TL_INSTALL_AUTH
 - 空文字列に初期化
 - 以前はしていなかった。
 - TL_INSTALL_EXPIRE
 - 新設で、セッションの有効期限を保持
 - 0に初期化

修正後: パスワード認証の後

- セッション変数に値設定
 - TL_INSTALL_AUTH
 - md5(uniqid('', true) . “クライアントのIP”)
 - または md5(uniqid('', true) . session_id())
 - より推測しにくい値
 - TL_INSTALL_EXPIRE
 - time() + 300
 - 現在から5分後に設定
- cookieを設定
 - TL_INSTALL_AUTHの名前と値
 - TL_INSTALL_EXPIREの有効期限

修正後: 認証処理完了後

- セッションの確認
 - TL_INSTALL_AUTH
 - 同名のcookieの存在
 - 同名のcookieの値とセッションに中の値が等しいこと
 - セッションの値が初期値(空文字でないこと)
 - TL_INSTALL_EXPIRE
 - 現在時刻がセッション中の値より小さいこと
- パスワードそのものの確認は行わない。

修正後: セッション確認後

- セッション確認の成功後
 - セッション変数の値を更新
 - TL_INSTALL_AUTH
 - md5(uniqid('', true), "クライアントのIP")
 - または md5(uniqid('', true), session_id())
 - より推測しにくい値
 - TL_INSTALL_EXPIRE
 - time() + 300
 - 現在から5分後に設定
 - cookieの設定
 - TL_INSTALL_AUTHの名前と値
 - TL_INSTALL_EXPIREの有効期限

Safe Mode

TYPOlight webCMS 2.6

 **TYPOlight install tool**

Check local configuration file

 The local configuration file is not writeable!

TYPOlight is not allowed to edit the local configuration file. Please activate FTP to modify files (*Safe Mode Hack*) by adding the following lines to your local configuration file **system/config/localconfig.php**:

```
$GLOBALS['TL_CONFIG']['useFTP'] = true;
$GLOBALS['TL_CONFIG']['ftpHost'] = ''; // FTP host
$GLOBALS['TL_CONFIG']['ftpPath'] = ''; // FTP path (e.g. html/)
$GLOBALS['TL_CONFIG']['ftpUser'] = ''; // FTP username
$GLOBALS['TL_CONFIG']['ftpPass'] = ''; // FTP password
```

[Check FTP connection](#)

 [TYPOlight back end login](#)

Safe Mode: PHPでのファイル操作が制限

Safe Mode Hack

- ファイル操作をFTP経由
 - FTPのログイン情報を設定に保存
 - それ以外はインストーラと同じ
- 修正内容も同じ

影響

- インストーラへの勝手なアクセス
 - データベースのパスワードを取得
 - データベースに外部から接続できることが前提
 - 同じユーザで管理されたデータベース
 - データの勝手な取得や破壊
- Safe Mode Hack有効の場合
 - FTPアクセスの情報も取得
 - FTPでアクセスできる範囲のデータの取得や破壊

対処方法

- TYPOlightの更新
 - バージョン2.7.6に更新
 - 提供されたパッチの適用
 - 2.8.RC1には提供されず。
 - ベータ版でパッケージ作るな言われました。
- バックエンドの保護
 - URLパスを保護: /typo|ight
 - IPアドレスの制限
 - Basic認証の設定

他に取られた対策

- TYPOLightコミュニケーションサイト
 - ユーザ用のフォーラム
 - Showroomの一時閉鎖

まとめ

- TYPOlight webCMSの紹介
- TYPOlightのセキュリティーホール
 - 詳細
 - 対処方法
 - 取られた対応

参考

- 関係URL
 - <http://www.typolight.org/>
 - <http://dev.typolight.org/>
 - <http://sourceforge.net/projects/typolight/>
- 国内サイト
 - RsStudio
 - <http://web.r-studio.jp/index.html>
 - 有限会社GMJコンサルティングサービス
 - http://gmjcs.jp/index.php/communication_design/CMS/TYPOLight.html
 - TYPOLight研究
 - <http://www.tyli.jp/>