WORDPRESSの

セキュリティ状況

2011-6-25 池田 百合子

自己紹介

* WordPress プラグイン作者
  - Ktai Style
  - Ktai Entry
* 2010年OSS奨励賞受賞
* 旅行が好き
* http://www.yuriko.net/
* @lilyfanjp

パスワード強制リセット

* WordPress.orgの全アカウントをパスワード強制変更

  http://ja.wordpress.org/2011/06/22/passwords-reset/

  - AddThis, WPtouch, W3 Total Cacheプラグインに不正コード混入

* Contact Form 7も偽プラグイン作成事件があった

  http://wordpress.org/support/topic/contact-form-7-version-732-plugin-is-malicious

WordPress 動作環境

＊近日リリース予定の WordPress 3.2 からレガシーフリー

- PHP 5.2+
- MySQL 5.0.15+

文字コード

* UTF-8 を前提

* マルチサイトでは UTF-8 に決め打ち

文字コード設定

* mbstring があれば mb_internal_encoding() を実行

  (wp-inclues/load.php:511)

* mb_check_encoding() は未使用

DB 文字コード設定

* mysql_set_charset() があれば使う

  (wp-includes/wp-db.php:541)

* なければ SET NAMES utf8 COLLATE utf_general_ci

DB 呼び出し

* プリペアード構文 $wpdb->prepare()

  (wp-inclues/wp-load.php:876)

  - 文字列は %s
  - 数値は %d

* 実体は vsprintf()

  - $mysqli->prepare() を使ってない

SQLインジェクション対策

* WordPress 起動時、以下に addslashes()

  (wp-includes/load.php:524 function wp_magic_quotes())

  - $_GET
  - $_POST
  - $_COOKIE
  - $_SERVER

* $_POST 等を使うときは stripslashes() が必要

XSS 対策

* テンプレートタグ esc_html(), esc_attr(), esc_js() など
* テーマやプラグインが適切に使う必要あり
* 詳細は Codex の「Data Validation」参照

  http://wpdocs.sourceforge.jp/Data_Validation

CSRF 対策

* wp_nonce というトークンで対策
  - 24時間だけ有効
  - ログアウトにもトークン要求
  - 管理パネルを増やすテーマ・プラグインが使ってないケースあり
* 詳細は Codex「WordPress Nonce」

  http://codex.wordpress.org/WordPress_Nonces

ログイン管理

＊クッキーで管理

＊PHPのセッション機構・セッション変数は使わない

WordPressのクッキー

非SSL	ログインクッキー	認証クッキー
SSL		セキュア認証クッキー
パス	サイト閲覧 画像表示	管理URL プラグインURL

WordPressサイト構成

* /site/example/public_html/blog/ にインストール

ウェブURL	http://example.com/blog/
管理URL	http://example.com/blog/wp-admin/
プラグインURL	http://example.com/blog/wp-content/plugins/

クッキー内容

* クッキー自体に有効期限を埋め込む

lily%7C1287759937%7C68d78e88a2b54ec6c3c365e7dbb3249e

ログイン名 | 有効期限 | ハッシュ

* ハッシュは以下から生成
- wp-config.php のランダム文字列
- ログイン名
- パスワードのSALT
- 有効期限

クッキーの検査

* wp_validate_auth_cookie() で検査

(wp-includes/pluggable.php:577)

1. wp_parse_auth_cookie() で分解

2. 有効期限を確認

3. ハッシュを照合

自動ログイン

* 自動ログインは有効期限を延長する実装

(wp-includes/pluggable.php:709: function wp_set_auth_cookie())

✦通常

- ブラウザを閉じるまで

- または172800 秒 (48時間)

✦「ログイン情報を記憶」を設定時

wp_set_auth_cookie()

```
if ( $remember ) {
  $expiration = $expire = time() +
    apply_filters('auth_cookie_expiration', 1209600, $user_id, $remember);
} else {
  $expiration = time() +
    apply_filters('auth_cookie_expiration', 172800, $user_id, $remember);
  $expire = 0;
}
```

* $expiration: クッキーに書き込む有効期限
* $exipre: setcookie() に設定する expire

WordPress 2.3.3 以前

* クッキーは2種類
  - ログイン名
  - パスワードを2回 md5 したもの
* ……とても脆弱

まとめ

対象	評価
認証クッキー	△
文字コード	△
SQL インジェクション	$wpdb->prepare() を使えば大丈夫?
CSRF	OK
XSS	テーマ・プラグインによって脆弱

* 出来の悪いテーマ・プラグインがネック

利用者がとれる対策

* 常に最新版を使う
* 強いパスワードを設定する
* あやしいテーマやプラグインを入れない
  - ブロガーがおすすめするものが特にやばい

やった方がいい対策

* wp-config.php のアクセス禁止
  - DocumentRoot より上位に移動
  - http.conf や .htaccess の Files ディレクティブで Deny
* /wp-admin/ の IP アドレス制限
* ログイン失敗時の一定時間ロックアウト

効果がない・低い対策

＊バージョン隠し

➡WordPress の挙動でバージョンはバレる

＊admin ユーザーの名前変更

➡/author/ アーカイブで admin ユーザーの推測可能

＊テーブル接頭辞を wp_ 以外に変更

スライド配付

* http://www.yuriko.net/tag/slides/

  で配付予定