はじめに

WordPressを使ってWebサイトを運営していても、運用後のセキュリティまで考慮してない方が多いかと思います。しかし、近年、Webサイトの改ざんや、不正アクセスによる顧客情報の流出は後を絶ちません。攻撃の多くは、SQLインジェクションと、クロスサイト・スクリプティングと言われる手法によるもので、適切な対策さえ行なわれていれば、被害を未然に防ぐことが可能な場合が多くあります。実際に、2011年上半期に脆弱性関連情報で届出のあったWebサイトのうち、約70％がクロスサイト・スクリプティング、約10％がSQLインジェクションによる攻撃でした（IPA調べ）。

被害が起こる前に、必要最低限の防御策を行っていれば、Webサイト復旧に伴う作業コストも抑えられます。また、顧客情報流出のような被害を受けてしまうと、顧客への信頼回復にはかなりの時間を要し、多大な損害を被ることでしょう。そのため、事前の防御策をことをお薦めします。

尚、事前に対策を行なっても攻撃を一切受けないという保障はありませんのでご注意ください。100％有効な手法は存在しません。被害を最小限に留めるために、基本的なセキュリティ対策を施しておきましょう。 また、セキュリティ対策を行なう際は、必ずファイルとデータベースのバックアップを行ってください。

*注意点

- 本来、ハッキングとクラッキングは使い分けられます。ハッキングは高い技術力でシステムを操作することが本来の意味ですが、一般には悪い意味合いでとられることが浸透しているため、本書でも便宜上、悪意をもって他人のPCに侵入し不正を行う行為を「ハッキング」という言葉で説明させて頂きます。

※クラッキングとは、コンピュータネットワークに繋がれたシステムへ不正に侵入したり、コンピュータシステムを破壊・改ざんするなど、悪意をもって他人のコンピュータを不正に利用すること。

本書のサポートサイトについて

ご不明な点や、その他本書に関するご質問等ございましたら、下記Webサイトにてユーザーアカウント作成の上、お気軽にお問合せください。

サポートサイト
http://www.lotusws.com/wordpress

目次

はじめに

第1章 ハッキングの被害例

第2章 ハッキングの主な攻撃手法

第3章 Webサイトのセキュリティ対策

第4章 Webサイトの復旧

目次

第3章 Webサイトのセキュリティ対策

赤色の星印（★）はサーバー管理者からみたセキュリティの重要度を意味しています。 星の数が少ない場合は、重要度が低くなります。
橙色の星印（★）はWebサイト開発者からみた作業の難易度を意味しています。 星の数が少ない場合は、難易度が低くなります。

3-1. 本体、プラグイン、データベース

★★★|★★☆ 3-1-1. WordPress本体やプラグインのアップデート
★★☆|★☆☆ 3-1-2. WordPressのバージョン情報削除
★★☆|★★★ 3-1-3. データベースのテーブル名の接頭辞変更

3-1-1. WordPress本体やプラグインのアップデート

概要

重要度 ★★★ 難易度 ★★☆

WordPressのソフトウェア本体やインストールしたプラグインを常に最新版にアップデートして、セキュリティレベルを向上し、悪意のあるユーザーからの攻撃に備えます。 最新版へのアップデート作業は、最新バージョンとテーマやプラグインの相性に依存しています。アップデートして何も問題がなければ、簡易的に完了できる作業ですが、動作上不具合が起きて解決が図れない場合は、元のバージョンのものに切り戻す作業を考慮する必要があります。

影響

ソフトウェア本体やプラグインを最新版にしてない場合、悪意のあるユーザーが行なう不正アクセスによってWebサイトを乗っ取られてしまう危険性があります。特にWordPress2.8.4未満のバージョンをまだ使用している環境であれば、危険な状況で公開している事になります。このバージョン未満のソフトウェアに、緊急度の高い脆弱性が発見されており、この脆弱性を突かれるとWebサイト自体が乗っ取られる恐れがあります。

*注意点

- WordPressを最新版にアップデートすると、テーマやプラグインによっては動作しない可能性があるため、必要に応じて、試験環境でインスール試験及び動作確認を行なってください。
- 作業前には必ず有事の際の切り戻し用のファイルとデータベースのバックアップを行なってください。「3-6-1.バックアップの実施」参照。

前提

試験環境にて事前にインストール試験及び動作検証作業を行いたい場合は、前提として下記の作業を行ってください。

Step-1. 既存サイトのデータバックアップ
アップデートして不具合が発生し、解決できない場合があります。その際に、事前にバックアップを行っていれば、アップデートする前の状態にすぐに戻すことができるため、バックアップは必ず行っておきましょう。具体的なバックアップ方法に関しては、「3-6-1. バックアップの実施」をご確認ください。

Step-2. 本番サイトのクローンサイトを作成
この項目はWebサイトの規模に応じて対応を行うかどうか切り分けてください。 クローンサイトを立ち上げず、最初から本番サイトに対してアップデートを行った際に、もし不具合が発生して解決できない事態が起きた場合、これがあなたのお客様のWebサイトであれば、お客様からの信用を失ってしまうでしょう。そういった事態を防ぐためにも、不具合の影響範囲を考慮してアップデート用のクローンサイトを予め立ち上げておきます。まず、クローンサイトでアップデートを試みて、動作や機能面で問題ないことを確かめた後、本番サイトに反映します。

a. 新規ディレクトリの作成
クローンサイト用に新規ディレクトリを作成します。そちらには、バックアップしたファイルをすべて展開しておきます。

b. 新規データベースの作成
クローンサイト用に新規データベースを作成します。そちらには、バックアップしたデータベースを展開しておきます。

c. 設定ファイルの変更
「a. 新規ディレクトリの作成」で作成したディレクトリ内の wp-config.php ファイルを開いて、データベースの接続先を変更します。バックアップファイルを展開した段階では、設定ファイルは本番サイトのデータベースを接続する記述がされているため、その接続先を変更する必要があります。

d. 動作確認
本番環境と同様の動作で動くかを細部まで確認してください。問題なければ、本番環境のクローンとしてテスト用に使用できます。

Step-3. アップデートを行なう前に
クローンサイトを用意した場合は、まずは試験環境にてアップデートを行います。もし試験環境を用意してない場合は、本番環境で実施してください。

WordPressのバージョンをアップデートする際は、テーマをデフォルトのものに変更します。バージョンによっては不具合が発生する可能性があるためです。また、有効化しているプラグインがあれば、すべて停止にしてください。

方法

アップデートするには次の２つの方法があります。

1. ダッシュボード画面から自動アップデート
WordPressのダッシュボード画面より簡易的に行います。

2. FTP接続による手動アップデート
FTPクライアントソフトウェアを利用し行います。

詳細**1**

ダッシュボード画面から自動アップデート

a. WordPressのダッシュボード画面へアクセスします。新しいバージョンのWordPressがリリースされると、画面上部に「更新してください」の記載がありますのでクリックします。

`WordPress 3.3.2` が利用可能です ！ 更新してください。

b. 更新の実施 「**WordPress** の更新」というページに移動します。表示の内容に従って進めてください。

詳細**2**

FTP接続による手動アップデート

a. 手動アップデートの場合、WordPress本体のバージョンを対象としています。**2.8.4**未満のバージョンをアップデートする際は、致命的な不具合が報告されてます。その為、ダッシュボード画面の自動アップデートではなく、手動によるアップデートを行なってください。WordPressの公式サイトから最新版をダウンロードし、FTP経由による手動でのアップデートを行ってください。（Version 2.8/FAQ・トラブルシューティング）

動作確認

アップデート作業を実施する前にデフォルトに変更したテーマの設定を、本番環境で利用しているテーマに変更し、プラグインを有効化します。Webコンテンツのページ表示の正常性確認とプラグインの動作確認を行います。

切り戻し

1. WordPress本体のダウングレード
アップデート作業前に事前にバックアップしておいたファイルを利用してリストア作業を行います。データベースの復元作業に関しては以下の2つの方法があります。
a. 該当のデータベースとバックアップしたものを入れ替える。
b. 新規にデータベースを追加して、そこにバックアップしたものを展開する。設定ファイル「wp-congif.php」にてデータベースの設定情報を変更する。

2. プラグイン
プラグインによって対処方法が異なるため、参考までに幾つか方法を紹介します。但しこれが全てではありません。

- ダッシュボード画面からプラグインを削除します。
- インストール時にデータベースにテーブルが追加されている場合はダッシュボード画面からのプラグイン削除で、テーブルも削除されているか確認します。 削除されていなければ、データベースにアクセスして直接削除します。
- サーバーにアクセスして、該当のディレクトリごと削除します。
- バックアップしておいた該当ディレクトリをアップロードしてダッシュボード画面から有効化してみます。
- 前述の「前提b. 新規データベースの作成」で作成したデータベース（アップデート前のデータ）に繋ぎ直してみます。「wp-config.php」ファイルのデータベースの設定情報を変更します。