Защита сайта на базе WordPress

Сайт, работающий на платформе WordPress, требует обеспечения безопасности, поскольку является одной из наиболее популярных и широко используемых систем управления контентом.

Ряд уязвимостей WordPress включает:

- Уязвимости плагинов и тем: Неправильно разработанные или устаревшие плагины и темы могут содержать уязвимости.
- Слабые пароли и учетные записи: Использование слабых паролей или повторение паролей для различных учетных записей делает сайт уязвимым для атак перебора паролей или подбора.
- Необновленный WordPress: Необновленная версия WordPress может содержать известные уязвимости, которые могут быть использованы злоумышленниками.
- SQL-инъекции и межсайтовые сценарии (XSS): Уязвимости, которые позволяют злоумышленникам внедрять и выполнять вредоносный код на сайте.
- Вредоносные программы: Злоумышленники могут использовать вредоносные программы для внедрения вредоносного кода на веб-сайт.

Наиболее распространенные причины взлома WordPress:

- Получение нежелательного доступа к административной панели или учетным записям.
- Внедрение вредоносного кода на сайт.
- Перехват данных пользователей, таких как логины и пароли.
- Загрузка вредоносных файлов на сервер.
- Выполнение атаки отказа в обслуживании (DDoS) для отключения сайта.

> Обеспечение безопасности WordPress-сайта включает регулярные обновления, использование надежных плагинов и тем, сложные пароли, использование защитных плагинов и мониторинг безопасности.

Для обеспечения безопасности и защиты от уязвимостей следует принять базовые меры:

1. Уязвимости плагинов и тем:

- Поддерживайте все плагины и темы в актуальном состоянии, регулярно обновляя их до последних версий.
- Устанавливайте плагины и темы только из надежных и проверенных источников, чтобы уменьшить риск внедрения вредоносного кода.

2. Слабые пароли и учетные записи:
   - Используйте сильные и уникальные пароли для всех учетных записей, включая административные.
   - Регулярно меняйте пароли и избегайте повторного использования паролей.
   - Рассмотрите возможность использования плагинов для управления паролями и реализации двухфакторной аутентификации.

3. Необновленный WordPress:
   - Регулярно проверяйте наличие обновлений для WordPress и его компонентов (плагины, темы).
   - Включите автоматические обновления, чтобы гарантировать, что ваш сайт будет иметь последние исправления уязвимостей.

4. SQL-инъекции и межсайтовые сценарии (XSS):
   - Используйте фильтры данных и экранируйте пользовательский ввод для предотвращения внедрения вредоносного кода.
   - Используйте параметризованные запросы и подготавливайте данные перед внесением их в базу данных.

5. Вредоносные программы:
   - Установите надежный антивирус и анти-вредоносное программное обеспечение на сервере.
   - Регулярно сканируйте веб-сайт на наличие вредоносного кода.
   - Ограничьте загрузку файлов на сервер и проверяйте загружаемые файлы на предмет вирусов или вредоносного кода.

Рекомендуемые настройки прав доступа для файлов и папок в WordPress:

1. Права доступа для файлов: 644
   - Владелец (Owner): Чтение и запись
   - Группа (Group): Чтение
   - Остальные пользователи (Others): Чтение
2. Права доступа для папок: 755
   - Владелец (Owner): Чтение, запись и выполнение
   - Группа (Group): Чтение и выполнение
   - Остальные пользователи (Others): Чтение и выполнение

Команды для массового изменения прав на папки и файлы:

```
find ./ -type d -exec chmod 755 {} \;
find ./ -type f -exec chmod 644 {} \;
```

Дополнительные рекомендации:

- Права доступа к файлам конфигурации (например, wp-config.php) должны быть установлены на 400 или 440, чтобы ограничить доступ к конфиденциальным данным, таким как данные базы данных.
- Если ваш хостинг поддерживает это, рекомендуется использовать suPHP или FastCGI, что позволит вам установить права доступа для файлов и папок 644 и 755 соответственно, и при этом сохранить безопасность.
- Избегайте установки прав доступа 777 для файлов и папок, так как это дает полные права на запись для всех пользователей, что может создать риск безопасности.

Отключение возможности выполнить PHP файлы в определенных каталогах:

Используя файл .htaccess:

Создайте файл .htaccess в каталоге, где вы хотите отключить выполнение PHP файлов, например в `./wp-content/uploads/`.

В файл .htaccess добавьте следующий код:

```
emoveHandler .php .phtml .php3
emoveType .php .phtml .php3
```

можно использовать этот код:

```
Files *.php>
eny from all
/Files>
```

от код отключит обработку файлов с расширением .php, .phtml и .php3 как исполняемых скриптов в выбранном каталоге.

Отключение индексирования и просмотр каталогов:

пользуя файл .htaccess:

утри файла .htaccess добавьте следующий код:

```
ptions -Indexes
```

Этот код запрещает серверу отображать список файлов и папок, если в URL указан каталог без конкретного файла.

Revision #2
Created 8 May 2023 11:40:41 by Maru
Updated 8 May 2023 20:34:47 by Maru