УДК 338

ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННОЙ ДОСКИ ОБЪЯВЛЕНИЙ

Малейко С.В.,
магистрант, 2 курс, экономический факультет
Кубанский государственный университет
Краснодар, Россия

Аннотация:
Раскрыта сущность электронной доски объявлений. Рассмотрены инструменты обеспечения информационной безопасности. Сформулированы рекомендации по совершенствованию внутреннего кода системы управления контентом.

Ключевые слова: электронная доска объявлений, CMS, аутентификация, плагин, ХЭШ-функция, PHP, MySQL, логин, спам, TrueCrypt, SSL

TOOLS TO ENSURE THE SAFETY OF THE ELECTRONIC ANNOUNCEMENT BOARD

Maleiko S.V.,
Magistrant, 2-nd year, faculty of economics
Kuban State University
Krasnodar, Russia

Annotaion:
The essence of the electronic bulletin board. Considered tools to ensure information security. The recommendations for improving the internal code of the content management system are formulated.

Keywords: bulletin board, CMS, authentication, plugin, HASH function, PHP, MySQL, login, spam, TrueCrypt, SSL

По мере распространения Интернета появилось множество сайтов, вполне аналогичных обычным бытовым доскам объявлений или же рекламным газетам. Их содержимое представляет собой набор объявлений коммерческого и/или некоммерческого характера. Электронная доска объявлений функционально подобна обыкновенной: это сайт, где каждый желающий может вывесить своё объявление, а все посетители сайта — прочитать его.

Но перед тем, как создать подобный сайт, стоит позаботиться о безопасности будущего ресурса и защиту данных, ведь с каждым днем злоумышленники осваивают новые методы взлома сайта - возникают новые вирусы, СПАМ-атаки, вредоносные скрипты, программы подбора паролей, которым под силу не только похитить данные, но и полностью исключить работу сайта. Поэтому если вы являетесь владельцем сайта на популярной CMS или планируете его разработку, вам стоит ознакомиться со следующими советами для защиты сайта на:

1. Безопасность хостинга. При выборе хостинга, на котором будут храниться данные вашего ресурса, обращайте внимание не только на выделенную память и стоимость тарифа обслуживания, но и на следующие параметры: поддержка последних версий PHP и MySQL; регулярные и частые автоматические бэкапы сайта; сканирования на наличие вирусов и угроз; обновление версий программного обеспечения.

2. Скрытая версия системы управления контентом. По определенным причинам не всегда удается вовремя обновить версию CMS, поэтому стоит запретить передачу действующей версии с кода файлов и страниц - такая информация может упростить работу для злоумышленников. Скрыть информацию можно добавив следующий код в файл functions.php:

remove_action ('wp_head ',' wp_generator'). Также следует удалить файлы, которые могут содержать информацию о CMS - readme.html и license.txt. Как свидетельствует статистика, 8-10% взломов сайта состоялись из-за слабого вход в систему. Для защиты личного кабинета следует принять следующие меры.

3. Нестандартный логин. Самый популярный логин - admin, именно его по умолчанию предлагает система. При попытке взлома боты сразу "разоблачат" стандартный логин, поэтому им останется только подобрать пароль. Для того, чтобы изменить стандартный логин на более надежный, выполните следующие действия: Добавьте в админ-панели нового пользователя - его имя и будет новым надежным именем. Предоставьте ему все права на сайт с ролью "Администратор". После создания нового пользователя войдите в кабинет под новым аккаунтом и удалите пользователя admin. Эти действия лучше выполнить еще перед созданием любого контента на сайте - записи, которые ранее опубликованные от имени admin, останутся под его авторством. Чтобы это исправить, нужно запросить к базам данных: update wp_posts set post_author = 'ваш новый логин' where post_author = 'admin'[1].

4. Ограничение попыток входа в CMS. Как правило, при попытке подбора паролей осуществляется большое количество попыток входа. Для блокировки возможности входу таких действиях на несколько часов можно воспользоваться специальными плагинами, например, Login Lockdown. При этом, у вас будет возможность самостоятельно определить после стольких попыток блокировать вход.

5. Двойная аутентификация. Для надежного входа на сайт можно воспользоваться плагином для двойной аутентификации Google Authenticator. Он работает таким образом, что при входе вам дополнительно нужно будет ввести код, который поступит на ваш смартфон[3].

6. Защита сайта спама в комментариях. Если на ресурсе есть множество информационных материалов с возможностью оставлять комментарии, стоит защитить сайт от спам-ботов, которые размещают в комментариях ссылки на сторонние ресурсы. Для этого можно воспользоваться плагинами, например, Akismet.

7. Использование надежных плагинов. Устанавливайте только надежные и проверенные темы и плагины, которые часто обновляются. Для проверки можно воспользоваться плагинами Theme Check и Plugin Detective plugin соответственно. Если информация о плагин отсутствует или ее мало, лучше его не устанавливать. Также не забывайте удалять ненужные плагины и те, которые не обновляются в течение длительного периода[2].

8. SSL сертификат. Используйте сертификат SSL для шифрования данных между браузером и сервером, особенно это необходимо для сайтов с использованием платежных систем. Кроме того, сегодня наличие сертификата безопасности является одним из весомых факторов для продвижения сайтов в Google.

9. TrueCrypt – это программа, которая имеет открытый код (open source), она позволяет осуществлять шифровку данных. Процесс шифровки происходит следующим образом: происходит создание зашифрованного виртуального логического диска, где каждый элемент подвергается шифровке, включая даже каждую папку и файл. Виртуальный диск, который в последующем монтируется, схож с винчестером, таким образом, над ним можно оперировать какими утилитами, как проверка диска на ошибки (scandisk) и дефрагментация[4]. Для доступа к зашифрованной информации применяется ключевое слово (пароль), файлы (возможно несколько) либо сочетание первого и последнего вариантов. Ключами выступают любые файлы на съемных носителях, в локальной сети, что дает возможность сгенерить личные ключи. TrueCrypt может поддерживать такие алгоритмические схемы шифрования данных: Тройной DES, Twofish,

Blowfish, Serpent, AES и пр. К тому же имеется возможность проводить каскадное шифрование, к примеру, Blowfish + Serpent + AES. Применяемые алгоритмические схемы производят шифрование «на лету» в защищенном режиме, который именуется как LRW, нежели CBC. Приложение выдает одну из трех hash-функций для того, чтобы сгенерировать заголовок ключа и ключей шифрования: HMAC-Whirlpool, HMAC-SHA-1, HMAC-RIPEMD-160. Примечательная особенность TrueCrypt заключается в том, что софт выдает несколько возможностей правдоподобной отказоспособности, необходимой при принудительном открытии пользовательского пароля. Созданные тома TrueCrypt не идентифицируются. При образовании невидимого тома можно прибавить еще и второй пароль плюс комплект ключевых файлов для того, чтобы получить доступ к данным обычного тома. Но даже, если у вас будет основной пароль, то вы все равно не получите доступ к данным в скрытом разделе; нужно заметить, что скрытый раздел может располагаться на свободном пространстве и в любой системе файлов в основном томе.

10. ХЭШ-функция. Данная алгоритмическая схема разработана профессором Рональдом Ривестом в 1991 году. Она предназначается для образования сообщений произвольной длинны, чтобы в последующем провести проверку их достоверности. За вводные данные принимается поток произвольной длинны, и вычисляет 128-битный хэш. Алгоритмическая схема применяется для того, чтобы быстро сгенерировать ключи шифрования и электронно-цифровые подписи. Не требует больших размеров памяти, и скорость его работы на 32-битных системах впечатляет. В то же время, алгоритмическая схема MD4 работает еще быстрее, но обладает низкой сопротивляемостью к криптографическим атакам, чем MD5. MD5 позволяет быстро получить надежный идентификатор блока данных, что позволяет ему быть использованным во многих областях. Например, для поиска дублирующихся данных. Гораздо быстрее сравнить MD5 двух файлов, нежели производить проверку их сходства по битам. Так же используется для

хранения паролей в системе FreeBSD. Хеширование, как принцип защиты данных, очень распространено среди систем, которые используют базу данных для хранения информации о своих пользователях. Самым распространенным из них, конечно, является обычный метод получения хэша из строки и занесение этой информации в базу данных. При авторизации, пользователь вносит свою кодовую фразу, которая преобразуется с хэш, сравнивается со значением, которое сохраняется в базе, и, если, они идентичны – пользователь проходит аутентификацию. Более надежный способ – хранение идентификатора пароля с применением двойного хеширования и нескольких случайных символов, которые будут известны только системе. Это дает возможность уменьшить вероятность вычисления пароля при помощи словарей или радужных таблиц.

В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Бондарев, В. Введение в информационную безопасность автоматизированных систем [Текст] / В. Бондарев – М.: «МГТУ им. Н. Э. Баумана», 2018. – 61 с.

2 Внуков, А. Основы информационной безопасности. Защита информации [Текст] / А. Внуков – М.: «Юрайт», 2019. – 135 с.

3 Гребенников, В. Управление информационной безопасностью. Стандарты СУИБ [Текст] / В. Гребенников – Спб.: «Издательские решения», 2018. – 100 с.

4 Казарин, О. Основы информационной безопасности. Надежность и безопасность программного обеспечения [Текст] / О. Казарин, И. Шубинский – М.: «Юрайт», 2018. – 230 с.

Оригинальность 90%