ПРОБЛЕМЫ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ CMS

м. т. н. ***Бакунова О. М.,***
студент ***Высоких В. А.,***
студент ***Кузнецов В. А.,***
студент ***Матусевич А. В.,***
студент ***Иваньков А. Ю.***

Республика Беларусь, г. Минск, Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники

ARTICLE INFO
Received 30 November 2017
Accepted 18 December 2017
Published 10 January 2018

KEYWORDS
modern CMS systems,
developing technologies,
cms security systems

ABSTRACT
In today's world, more and more developing technologies that use the Internet. Therefore, all the more urgent problems of modern security cms. Great demand began to recruit CMS systems, allowing the user to create a site based on the example of an existing template or individual needed parts. With the advent and development of CMS systems and this crackers hackers emerged same direction, so the subject of the protection problems of the leading CMS systems is very important.

В современном мире всё больше развиваются технологии, использующие всемирную сеть интернет. Причина такой востребованности данным направлением является развитие малого бизнеса, который не может существовать без web поддержки и рекламы.

Для большинства развивающихся компаний нанять программиста для разработки своего интернет ресурса с «нуля» с «административной панели» достаточно дорого. По этой причине всю большую востребованность стали набирать CMS системы, позволяющие пользователю самому создать сайт на примере существующего шаблона или отдельные необходимые части. С появлением и развитием CMS систем появились хакеры и взломщики этого же направления, поэтому тема проблемы защиты ведущих CMS систем очень актуальна.

Joomla – одна из самых популярных CMS, к ней приковано внимание большого числа злоумышленников. С начала 2015 года, в Joomla было найдено 37 уязвимостей. Большинство из них были достаточно серьезными и приводили к утечке данных неавторизованных пользователей, возможности выполнения SQL-инъекций, а также возможности получений комбинаций имени пользователя и пароля, сброс в начальное состояние, а также способность повышения своих привилегий. Большинство этих уязвимостей были исправлены в последующих версиях Joomla. Однако рассмотрим некоторые из них, представляющие интерес:

– Уязвимость в компоненте EQ Event Calendar, позволявшая злоумышленнику удаленно выполнить SQL-инъекцию. Проблема заключается в том, что в обработчике поля ID не была выполнена фильтрация данных. На данным момент не известно, принимались ли какие-то изменения в Joomla для исправления данной проблемы. Общая рекомендация – заменить этот компонент на другой аналогичный.

– Единственная уязвимость за последние 3 года, позволявшая модифицировать данные существующего пользователя. Также использовалась для сброса имени пользователя, пароля и группы. Проблема была исправлена в версии 3.6.4, однако до сих пор активно используется против сайтов, не обновивших версию Joomla.

– Уязвимость, затрагивающая Joomla, начиная с версии 1.7.3, выпущенной еще в 2011 году. Заключалась в некорректной инвалидации кэша, приводившей к утечке содержимого форм. Исправлена в версии 3.7.2.

– Уязвимость в инсталляторе Joomla, которая не проверяла принадлежность webspace пользователю, что позволяло удаленному пользователю получить контроль над приложением оценивая файлы, содержащие информацию о ходе работы программы, накопленные во время его работы. Исправлено в версии 3.7.4.

– Уязвимость, позволявшая пользователю обойти двухфакторную авторизацию. Проблема, показывающая, что двухфакторная авторизация не является

гарантией полной защищенности пользовательских данных.

Большинство уязвимостей исправляются своевременно после их обнаружения. Главная рекомендация пользователю – обновлять свою CMS своевременно.

Далее рассмотрим программные продукты компании 1С, которые являются неким стандартом для работы бухгалтерского, управленческого и других видов учета в малом и среднем бизнесе. Многие работодатели требуют от своих сотрудников обязательных знаний и навыков работы именно с этим программным продуктом. В современном мире любой процесс автоматизации малого и среднего бизнеса начинается с продуктов 1С и продолжается доработкой необходимых блоков. Для каждой компании и или фирмы они могут быть абсолютно разными от простых отчетов в несколько строк, до целых отдельных блоков в зависимости от отрасли, где используется программный комплекс. В CMS Bitrix, используемых на данный момент можно выделить следующие проблемы безопасности:

1) Большое количество XSS

Административный раздел «Дополнительные поля» - стал самым уязвимым местом для XSS атак непостоянного характера. Данный раздел позволяет создавать различные поля для пользователей. При создании указанных полей самыми уязвимыми стали конструкции для создания типов данных «Список» и «Видео».

2) CSRF атака

Допустимость принятия CSRF токенов, как при настройке пользователей, так и при настройке аккаунта администратора системы. Например, при смене пароля, или иных учетных данных администратора, данные отправляются на обработчик следующим образом:

```
POST /bitrix/admin/user_edit.php?ID=1&lang=ru HTTP/1.1
Host: 1071lab.bitrixlabs.ru
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://1071lab.bitrixlabs.ru/bitrix/admin/user_edit.php?lang=ru&ID=1
Cookie: PHPSESSID=fdtc1nha7vd6fsgq9spuih3na0; BITRIX_SM_SOUND_LOGIN_PLAYED=Y; BITRIX_SM_GUEST_ID=1; BITRIX_SM_LAST_VISIT=13.01.2017+08%3A14%3A53;
BITRIX_SM_SALE_UID=a44218257184b130c660695f7132ea02;
BITRIX_CONVERSION_CONTEXT_s1=%7B%22ID%22%3Anull%2C%22EXPIRE%22%3A1484351940%2C%22UNIQUE%22%3A%5B%22sale_payment_add_day%22%5D%7D
Connection: keep-alive
Content-Type: multipart/form-data; boundary=---------------------------81949277201
Content-Length: 9588
```

Рис. 1. Пример кода

Для взлома сайта на CMS 1С-Битрикс, пользуясь XSS+CSRF, достаточно сделать направлением атаки запрос, который, например, поменяет учетные данные доступа администратора сайта, или добавит нового, созданного атакующим.

Использование XSS атаки, когда её исполнение чётко проработано, гарантирует взлом практически любого сайта, работающего под управлением CMS 1С-Битрикс последних версий. Использование XSS атаки вместе с CSRF позволяет:

– менять учётные данные пользователей;

– создавать новый пользователей сайта, с возможностью приобретение различных привилегий;

– замена привилегий пользователям сайта.

В некоторых частных ситуациях, особенно для ресурсов с недостаточным уровнем защиты на уровне сервера, возможна использование CSRF без XSS. К тому же, упомянутая атака делает обычную XSS максимальной угрозой безопасности сайта.

Wordpress – одна из самых распространённых CMS систем в сети и составляет более четверти всех существующих веб-сайтов. Именно поэтому данная система является причиной большой заинтересованности среди хакеров и взломщиков. Проблема безопасности в Wordpress с каждым годом принимает всё большую актуальность. Данная CMS система имеет свои уязвимости. Большинство из них идентичны с другими схожими системами, но всё же осветим самые ключевые из них:

1) SQLI – данная уязвимость заключается в выполнении SQL-запроса на URL-адресе атакуемого сайта;

2) XSS – возможность хакера вводить необходимый код в сайт через поля ввода и другие подобные поля;

3) Brute Force – подбор взломщиком информации об имени и пароле администратора сайта;

4) DOS – атака сайта постоянным потоком трафика с вредоносного адреса и в результате потеря его работоспособности;

5) DDOS – похож на DOS, отличается только тем, что вредоносный поток исходит из множества источников;

6) Open Redirect – внедрение вредоносного кода на сайт, который осуществляет множественный переход по различным нежелательным URL адресам;

7) Фининг – кража личных данных у пользователей по средствам создания копии сайта;

8) LFI – контроль злоумышленником выполнения частей кода.

Нужно учитывать, что данные проблемы составляют только часть в вопросах безопасности Wordpress. Немаловажным фактором до сих пор остаётся человеческие ошибки при создании сайта на данной системе, т.е. недостаточная проработка вопросов организации функционирования системы в виду наличия уязвимых мест. Так же проблемы с безопасностью зачастую связаны с несвоевременным обновлением компонентов на актуальные версии.

В платформе Magento существуют две значимые проблемы безопасности:

– Даёт возможность отобразить произвольный JavaScript код, добавленный через форму регистрации путём задания в поле с email (например, можно указать '><script>alert(7);</script>'@yandex.by). Выполнение кода в контексте интерфейса администратора атакующий может перехватить куки сеанса и получить доступ к сайту.

– Позволяет подставить JavaScript код в комментарий к заказу при использовании модуля PayFlow Pro, в дальнейшем данный код будет выполнен при просмотре администратором списка заказов.

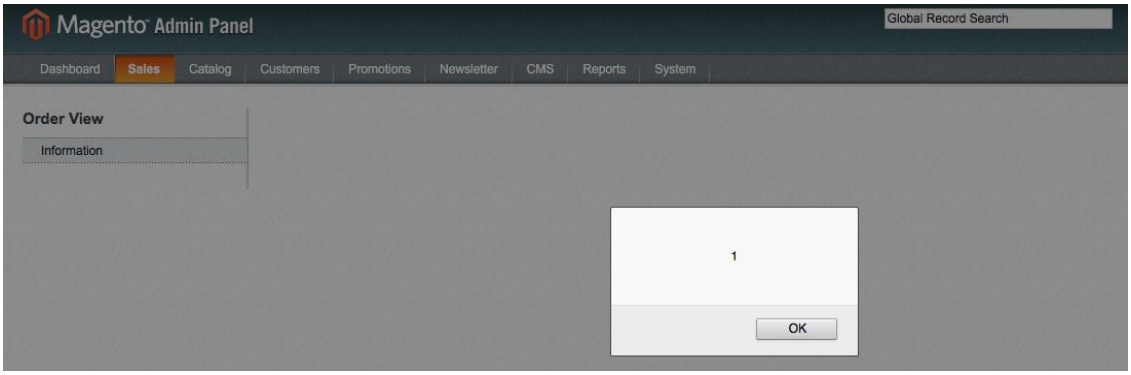

Рис. 2. Пример уязвимости Magento

Для устранения подобных уязвимостей разработчики Magento выпускают патчи, чтобы повысить безопасность и устранить всякую уязвимость.

Проанализировав крупные указанные CMS системы можно сделать вывод, что все они имеют достаточное количество недостатков. Из вышеуказанного видно, что в основном все веб системы данного назначения имеют схожие проблемы. Причём разработчики каждой из ведущих CMS систем проводят сбор статистики уязвимых мест и решают данные проблемы с выпуском обновлений. Что в очередной раз доказывает необходимость своевременного обновления.

Что касается выбора той или иной CMS системы для работы, то с уверенностью рекомендовать определённую невозможно. У каждой есть какие то плюсы и минусы, которые нужно учитывать при выборе.

ЛИТЕРАТУРА

1. Петренко С. А., Курбатов В. А. Политики безопасности компании при работе в Интернет. Изд-во ДМК Пресс, 2011. 396 с.

2. Моор, П. К. Информационные системы в экономике: учебное пособие. / П. К. Моор, С. М. Моор, А. П. Моор. – Тюмень: Издательство Тюменского государственного университета, 2011. – 192 с. 2. ЗАО «Интеллектуальные системы» [Электронный ресурс]. – 2012. – Режим доступа: http://www.is.by/. – Дата доступа: 11.04.2012