

## ПРОБЛЕМЫ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ CMS

Институт информационных технологий БГУИР,  
г. Минск, Республика Беларусь

Кузнецов В.А., Иваньков А.Ю., Матусевич А.В., Высоких В.А.

Бакунова О.М. - ст. преподаватель каф. ИСиТ, м.т.н.

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 собственной «админкой» и т.д. очень накладно с финансовой стороны. По этой причине всю большую востребованность стали набирать CMS системы, позволяющие пользователю самому создать сайт на примере существующего шаблона или по крайней мере платить не за всю разработку сайта, а лишь отдельных его частей. Данные системы упростили процесс создания простых сайтов, без каких-либо необычностей. С появлением и развитием CMS систем пропорционально началась востребованность данным направлением и хакеров, взломщиков, недоброжелателей. В данной статье рассмотрим основные проблемы ведущих CMS систем в пространстве интернет.

### Joomla

Joomla – одна из самых популярных CMS, и соответственно, 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 данным неавторизованным пользователям, возможности выполнения SQL-инъекций, а также возможности получения комбинаций имени пользователя и пароля, либо же их сброс в начальное состояние, а также способность повышения своих привилегий. Большинство этих уязвимостей были исправлены в последующих версиях Joomla. Однако мы 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 данный 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 логи, 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.

### 1С-Битрикс

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».*

### 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:*



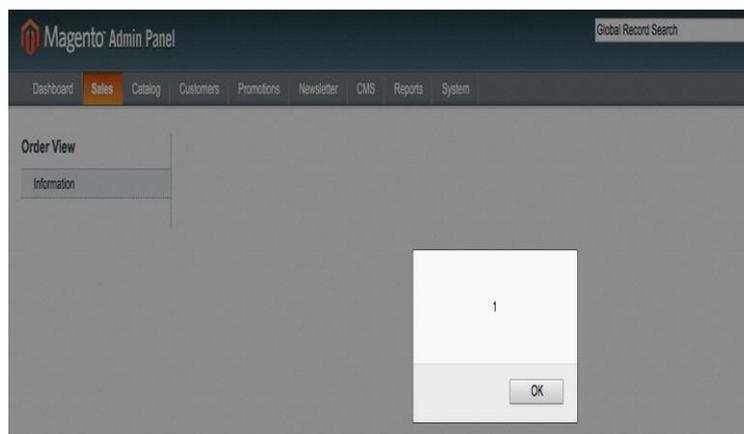


Рисунок 1 – Пример уязвимости Magento

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.

Список использованных источников:

1. Петренко, С.А. Политики безопасности компании при работе в Интернет./ С.А. Петренко, В.А. Курбатов. – Изд-во ДМК Пресс, 2011, 396 с.
2. Моор, П.К. Информационные системы в экономике: учебные пособие./ П.К. Моор, С.М.Моор, А.П. Моор, – Тюмень: Издательство Тюменского государственного университета, 2011, 192 с.
3. ЗАО «Интеллектуальные системы» [Электронный ресурс]. – 2012. – Режим доступа: <http://www.is.by/>. – Дата доступа: 25.12.2017

## **ДИАГНОСТИЧЕСКАЯ СИСТЕМА ЭЛЕКТРОНИКИ АВТОМОБИЛЯ НА ПРЕДМЕТ ОШИБОК. ИЗМЕНЕНИЕ ПАРАМЕТРОВ ВПРЫСКА И ЗАЖИГАНИЯ ТОПЛИВА**

*Институт информационных технологий БГУИР,  
г. Минск, Республика Беларусь*

*Кузьмицкий В.И., Биркос В.А.*

*Бакунова О.М. – ст. преподаватель каф. ИСиТ, м.т.н.*

В докладе представлен сравнительный анализ диагностическая система электроники автомобиля.

С развитием технологий, в автомобиле строении начали применяться различного рода электронные системы. Очень значимым шагом стал переход на электронные блоки управления двигателем (ЭБУ). Первые моторы с таким типом управления появились в конце 1970х начале 1980х годов. В самом начале это были примитивные микросхемы, считывающие данные с нескольких значимых датчиков, таких как датчик массового расхода воздуха, датчик положения дроссельной заслонки, датчик температуры поступающей смеси и т.д.. Такие моторы выгодно отличались от старых, производство смеси и впрыск топлива которых осуществлялись механическим карбюратором. Более рациональное распределение топлива, стабильная работа не зависимо от температуры воздуха, существенно увеличили производительность, понизили расход топлива и как следствие снизили загрязнение окружающей среды.

Новый тип управления двигателем позволил добиться от моторов колоссального прироста производительности, при тех же параметрах механических составляющих. Но кроме плюсов появились и минусы. Самый главный, это цена. Новые системы были очень дорогими в производстве и ремонте, и для эффективности определения проблем понадобилось средство диагностики. Информация, поступающая от датчиков, преобразуется специально установленным преобразователем в цифровой сигнал. В состав ЭБУ входят информационный и контрольно-вычислительный модули, с помощью которых и происходит оптимизация и отладка всей системы. Если на ЭБУ приходит сигнал от датчика, который выходит за диапазон допустимого значения, система сигнализирует об ошибке и записывает её код. В этом случае, необходимо лишь считать код ошибки, чтобы найти неисправный датчик.