УДК 004.056

**А.Ю. Оладько, В.С. Аткина**

## МОДЕЛЬ ЗАЩИТЫ ИНТЕРНЕТ-МАГАЗИНА

*Цель исследования: разработка модели защиты web-приложения на примере интернет-магазина. Рассмотрена проблема обеспечения безопасности web-приложений, относящихся к различным отраслям. Проанализированы данные статистических исследований безопасности web-приложений, относящихся к различным отраслям. По результатам анализа выделены основные уязвимости web-приложений и наиболее распространенные атаки злоумышленника на web-приложения, реализация которых может привести к утечке информации, НСД к конфиденциальным данным, финансовым и репутационным потерям организаций собственников web-приложений. Определены методы и этапы защиты web-приложений. Предложен подход к защите web-приложения на примере интернет-магазина, представлена и описана архитектура защищенного магазина, приведены результаты экспериментальных исследований направленных на оценку предложенных методов защиты. Сделан вывод о том, что разработанные модули защиты интернет-магазина позволяют защититься от ряда атак злоумышленника, что свидетельствует о возможности применения предложенного подхода к защите на практике при разработке и сопровождении web-приложений.*

*Web-приложение; защита; электронная коммерция; уязвимости.*

**A.Yu. Oladko, V.S. Atkina**

## MODEL OF ONLINE STORE PROTECTION

*Objective: to develop security model web pplications on the example of an online store. The problem of security of web-applications pertaining to various industries. Analyzed data from statistical studies of the safety web - applications pertaining to various industries. According to the analysis highlights the major vulnerabilities of web-applications and the most common malicious attacks on web-application that may lead to information disclosure, unauthorized access to confidential data, financial and reputational losses to owners of web-applications. Defined methods and stages of protection web-applications. An approach to the protection of web-applications on the example of an online store, presented and described architecture secure store, the results of experimental studies aimed at evaluating the proposed methods of protection. Concluded that the developed protection modules online store can protect against a number of attacks. And the proposed approach to protection can be used in practice to develop and maintain web-applications.*

*Web- application; protection; e-commerce; vulnerabilities.*

**Проблема безопасности web-приложений.** В связи с постоянным развитием технологий высокоскоростного доступа в Интернет важные компоненты бизнеса перемещаются в среду Web. Системы типа Банк-Клиент, публичные сайты организаций, интернет-магазины, новостные, развлекательные и торговые площадки, блоги, государственные порталы являются обязательной составляющей всемирной сети (рис. 1). Из-за своей доступности они часто становятся привлекательной целью для злоумышленников, поэтому решения по эффективной защите web-приложений сейчас являются все более актуальными и востребованными.

При этом обеспечение безопасности подразумевает защиту ценностей, где ценность определяется как нечто, имеющее стоимость. Некоторые активы являются материальными и имеют денежное выражение, другие – нематериальны, но тем не менее имеют стоимость. Необходимость защиты «почти материальных» активов, таких как реестр имущества компании, персональные данные пользователей, клиентов и сотрудников, электронные деньги сомнений не вызывает. Но важно понимать и то, что такая, безусловно, нематериальная ценность, как репутация компании, тоже имеет стоимость и нуждается в защите.

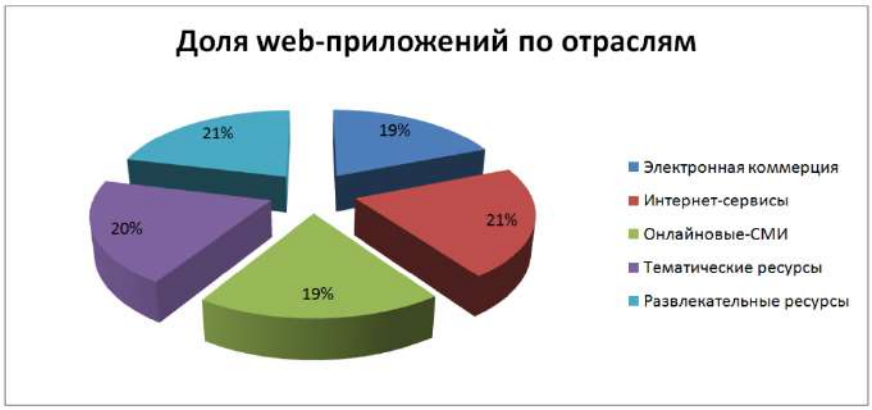


*Рис. 1. Статистика распределения web-приложений*

Анализ данных исследований проводимых аналитическим центром PT Research, а также компанией PositiveTechnologies [1, 2] осуществляющих проведение тестов на проникновение и аудит информационной безопасности показывают, что ошибки в защите web-приложений по-прежнему остаются одним из наиболее распространенных недостатков обеспечения защиты информации. Более того, уязвимости web-приложений являются одним из наиболее распространенных путей реализации злоумышленниками атак на web-приложения с целью кражи информации и последующим проникновением в корпоративные информационные системы. Согласно данным статистики (см. табл. 1 и рис. 2) наиболее распространенными угрозами безопасности web-приложений являются: межсайтовый скриптинг (XSS–атаки), SQL-инъекции, вызов исключительных ситуаций, подделка межсайтовых запросов(CSRF), угрозы заражения вредоносным программным обеспечением.

Таблица 1

**Статистика угроз и их распределение по web-приложениям**

| № п/п | Угроза информационной безопасности | Доля угроз, % | Доля уязвимых сайтов, % |
|---|---|---|---|
| 1 | Межсайтовое кодирование (XSS –атаки) | 19,23 | 27,27 |
| 2 | SQL-инъекция | 17,65 | 49,35 |
| 3 | Неправильная конфигурация web-сервера | 11,09 | 37,36 |
| 4 | Вредоносное программное обеспечение | 12,44 | 37,66 |
| 5 | Подделка межсайтовых запросов(CSRF) | 2 | 7,79 |
| 6 | Вызов исключительных ситуаций | 11,54 | 20,78 |
| 7 | Прочие | 26,05 | 50 |

Результатом успешной реализации угроз безопасности web-приложений и атак злоумышленника может стать утечка или уничтожение конфиденциальных данных, заражение компьютеров пользователей вредоносным ПО, недоступность сервисов, финансовые и репутационные потери. Следовательно, возникает необходимость в использовании специализированных средств и методов защиты web-приложений.

**Методы защиты web-приложений.** Анализ литературных источников [3–7] показывает, что при обеспечении защиты web-приложений необходимо учитывать ряд особенностей связанных непосредственно с процессом их функционирования:

- корпоративные web-сайты и соответствующие web-приложения должны быть доступны для пользователей, заказчиков и партнеров 24 часа 7 дней в неделю;

- межсетевые экраны и применение SSL не обеспечивают защиту от взлома web-приложений просто потому, что доступ к сайту из внешних сетей должен быть всегда открыт;
- web-приложения часто имеют прямой доступ к корпоративным данным, таким как базы данных пользователей или платежных данных, ERP системам и другой важной информации;
- узконаправленные пользовательские приложения более восприимчивы к атакам, так как они не подвергаются такому длительному тестированию и эксплуатации, как общедоступные известные приложения;
- традиционные сетевые средства защиты не предназначены для отражения специализированных атак на web-приложения, поэтому злоумышленники при помощи браузеров легко проходят через периметр корпоративной сети и получают доступ к внутренним системам и серверам;
- ручное обнаружение и устранение уязвимостей в самом приложении, сайте или web-портале также часто не дает положительных результатов – разработчики могут находить и исправлять тысячи уязвимостей, но злоумышленнику для проведения результативной атаки достаточно обнаружить всего одну.


*Рис. 2. Статистика угроз web-приложениям*

Проведенный анализ позволяет сделать вывод о том, что обеспечение защиты web-приложений должно осуществляться как на этапе проектирования и разработке самого web-приложения, так и в процессе его эксплуатации с внесением в случае необходимости своевременных корректировок [3–5]. При этом защита должна строиться по двум основным направлениям:

- недопущение ошибок в скриптах при разработке web-приложения;

- применение специализированных межсетевых экранов уровня приложений (например, решения типа ApplicationFirewall), которые обладают встроенным функционалом предотвращения вторжений и обеспечивают защиту от целенаправленных web-атак, таких как переполнение буфера, SQL инъекции, Cross-Site-Scripting, изменение параметров запросов и других. Решения этого класса фильтруют запросы на доступ к приложению и блокируют все действия, которые не относятся к разрешенной активности пользователей.

**Модель защищенного интернет-магазина.** Таким образом, на основе проведенного анализа процесса функционирования web-приложения, уязвимостей, основных угроз, требуется, авторами предлагается подход к защите web-приложения, реализованный на примере модели интернет-магазина. Поскольку любой интернет-магазин представляет собой web-приложение относящееся к системе электронной коммерции, то разработанная модель защищенного интернет-магазина должна обеспечивать решение следующих задач:

- регистрация клиентов;
- отображения каталога товаров;
- оформление заказа;
- администрирование;
- защита от угроз.

Для решения задач защиты от угроз мошенничества, несанкционированного доступа к платежным данным пользователей, защиты от уязвимостей web-приложений, в модели должны быть реализованы следующие методы:

- метод защиты от мошенничества;
- метод защиты платежных данных;
- метод защиты от web-уязвимостей.

Разработанная архитектура модели защищенного интернет-магазина представлена в виде взаимосвязанных между собой модулей (рис. 3). Каждый модуль предназначен для решения определенного круга задач и связан с другими модулями двунаправленными связями.

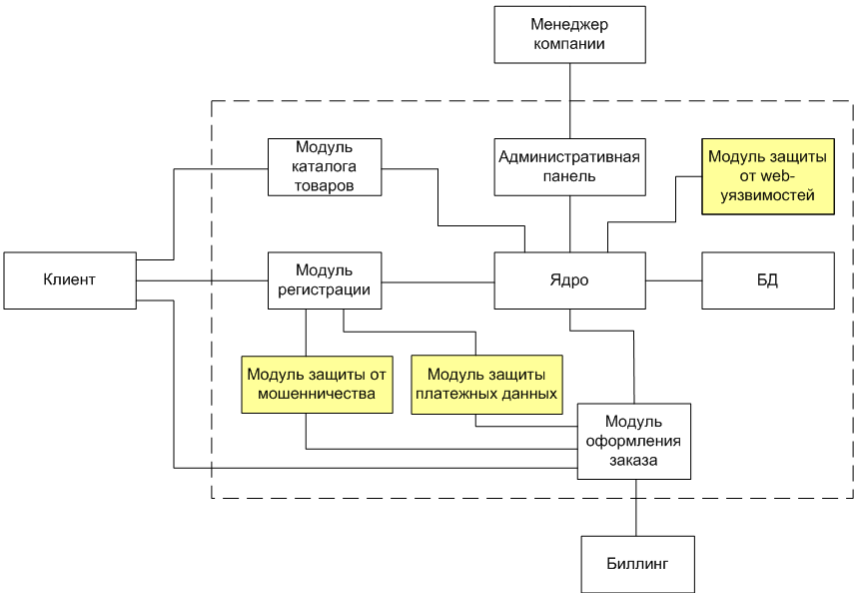


*Рис. 3. Архитектура модели защищенного интернет-магазина*

Блок «менеджер компании» является внешним по отношению к разработанной архитектуре модели защищенного интернет-магазина. Осуществляет контроль за выполнением заказов.

Блок «клиент» является внешним по отношению к разработанной архитектуре модели защищенного интернет-магазина. Осуществляет покупку товаров и оплату за них.

Блок «биллинг» является внешним по отношению к разработанной архитектуре модели защищенного интернет-магазина. Осуществляет перевод денежных средств со счета клиента, согласно предоставленным им платежным данным, на счет интернет-магазина.

Блок «модуль регистрации» предназначен для регистрации клиентов интернет-магазина. При этом клиент должен вводить контактные данные (электронную почту, номер телефона), адрес доставки товара, платежные данные (включая биллинг-адрес для тех платежных систем, в которых он предусмотрен, например кредитных карт).

Блок «модуль каталога товаров» предназначен для отображения товаров, доступных для покупок в данном интернет-магазине. Используя данный модуль, клиент выбирает необходимый ему товар и переходит к оформлению заказа и оплате выбранного товара.

Блок «модуль оформления заказа» предназначен для составления счета и передачи платежных данных и суммы заказа биллингу.

Блок «административная панель» предназначен для вывода менеджеру компании информации о зарегистрированных пользователях, совершенных заказах.

Блок «ядро» предназначен для осуществления работы с базой данных, HTML-кодом. Может включать в себя интерфейс работы с различными стандартными модулями.

Блок «БД» представляет собой базу данных, в которой хранятся данные о товарах, клиентах, заказах.

Блок «модуль защиты от web-уязвимостей» осуществляет защиту от web-уязвимостей.

Блок «модуль защиты от мошенничества» осуществляет защиту от мошенничества.

Блок «модуль защиты платежных данных» осуществляет защиту платежных данных клиента.

**Экспериментальные исследования модели защиты интернет-магазина.** Для экспериментального исследования модели защищенного интернет-магазина на виртуальной машине VMware была установлена и настроена операционная система Linux Red Hat 10, в которой было установлено программное обеспечение, необходимое для функционирования разработанной модели защищенного интернет-магазина, включая:

- web-сервер Apache версия 2.0.40;
- СУБД MySQL версия 3.23.54;
- криптографический пакет OpenSSL версия 0.9.7a;
- интерпретатор Perl версия 5.8.9.

С моделью защищенного Интернет-магазина проводились два эксперимента:

1. Оценка воздействия на Интернет-магазин злоумышленника при попытке внедрить вредоносный javascript код через проведение XSS-атаки с целью получения cookie администратора/менеджера интернет-магазина (эксперимент 1).

2. Оценка эффективности модуля защиты платежных данных путем моделирования регистрации пользователей и указания платежных данных (эксперимент 2).

Каждый эксперимент проводится сначала при выключенных модулях защиты, затем данные эксперименты повторяются при включенных модулях защиты.

В эксперименте, направленном на оценку воздействия на Интернет-магазин злоумышленника, при попытке внедрить вредоносный javascript код через проведение XSS-атаки с целью получения cookie администратора магазина моделировалась попытка злоумышленника внедрить вредоносный javascript код, путем проведения XSS-атаки на форму регистрации интернет-магазина. При этом вредоносный javascript код внедрялся в поле ввода данных и региона клиента Интернет-магазина.

При отключенном модуле защиты от уязвимостей web-приложений опасные символы не были отфильтрованы, и вредоносный javascript код выполнился в браузере менеджера компании. Таким образом, злоумышленник достиг своей цели.

При включенном модуле защиты от уязвимостей web-приложений опасные HTML-символы, с использование которых осуществлялась XSS-атака, были заменены на безопасные. Символ ‘<’ был заменен на ‘<’, символ ‘>’ был заменен на ‘>’. В результате этого вредоносный javascript код не был выполнен, а отобразился в браузере менеджера компании (рис. 4).

При проведении второго эксперимента, направленного на оценку эффективности модуля защиты платежных данных была смоделирована регистрация в интернет-магазине трех пользователей и ввод ими своих платежных данных, которые сохранялись в базе данных интернет-магазина.

При отключенном модуле защиты платежных данных платежные данные клиента интернет-магазина были сохранены в базе данных в открытом виде. Таким образом, если злоумышленник сможет получить несанкционированный доступ к базе данных, то сможет завладеть платежными данными клиентов интернет-магазина.

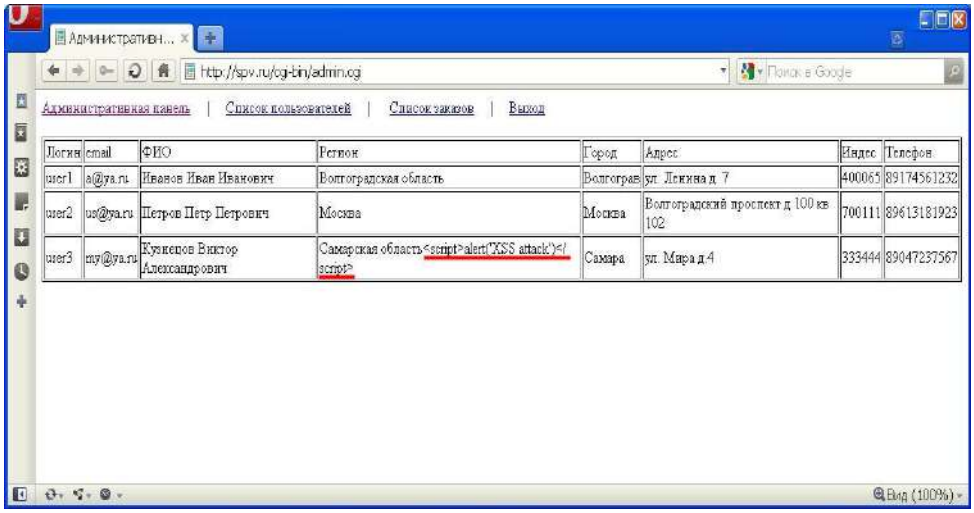


*Рис. 4. Результат проведения злоумышленником XSS-атаки, при включенном модуле защиты от уязвимостей web-приложений*

При включенном модуле «защита платежных данных платежные данные клиентов интернет-магазина были сохранены в базе данных в зашифрованном виде. Таким образом, если злоумышленник сможет получить несанкционированный доступ к базе данных интернет-магазина (например, используя уязвимости сервера), то в его распоряжении окажутся платежные данные пользователей в зашифрованном виде и он без применения средств криптоанализа и больших временных затрат не сможет ими воспользоваться в свих целях.

**Выводы.** Результаты проведенных исследований показывают, что разработанные модули защиты интернет-магазина позволяют защититься от таких атак злоумышленника как несанкционированный доступ и кража платежных данных из БД, XSS-атаки, SQL-инъекции, а следовательно могут использоваться при разработке и сопровождения реальных систем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. January 2013 WebServerSurvey.[Электронный ресурс] – Официальный сайт компании Netcraft. – Режим доступа:http://news.netcraft.com/ (дата обращения 23.02.2014).
2. Статистика web-уязвимостей за 2013 год. [Электронный ресурс] – Режим доступа: http://netnsk.ru/publica/security/sec_10.php (дата обращения 23.02.2014).
3. *Леонтьев В.С.* Безопасность в сети интернет. – М.: ОЛМА Медиа Групп, 2008. – 256 с.
4. *Рэйнолдс М.* Сделай сам Интернет-магазин. – М.: Изд-во “Лори”, 2009. – 538 с.
5. Защита Web приложений//ООО «СОВИТ». [электронный ресурс]: URL –http://www.sovit.net/services/endpoint_security/web_application_protection (дата обращения 23.02.2014).
6. Статистика национального домена в рунете//Координационный центр национального домена сети интернет: URL - http://www.cctld.ru/ru/statistics (дата обращения 23.02.2014).
7. Статистика и аналитика // Домена России: URL – http://statdom.ru/researchs (дата обращения 23.02.2014).

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Бабенко.

**Оладько Алексей Юрьевич** – Волгоградский государственный университет; e-mail: bop-x@yandex.ru; 400062, г. Волгоград, пр-т Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; старший преподаватель.

**Аткина Владлена Сергеевна** – e-mail: atkina.vlaldlena@yandex.ru; кафедра информационной безопасности; к.т.н.; старший преподаватель.

**Oladko Alexey Yuryevich** – Volgograd State University; e-mail: bop-x@yandex.ru; 100, Ave University, Volgograd, 400062, Russia; phone: +78442460368; the department of information security; lecture.

**Atkina Vladlena Sergeevna** – e-mail: atkina.vlaldlena @ yandex.ru; the department of information security; cand. of eng. sc.; lecture.

УДК 004.056

**А.В. Никишова, Р.Ф. Рудиков, Е.А. Калинина**

## НЕЙРОСЕТЕВОЙ АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

*Статистика за 2013 год и предсказания на 2014 год относительно атакующих воздействий на информационную систему показывает как рост возникающих атакующих воздействий из числа известных, так и рост новых образцов и направлений реализации атак. В связи с этим актуальной является задача сбора сведений о событиях, происходящих в информационной системе и относящихся к основным объектам информационной системы, и проведение их эффективного анализа. Основными требованиями к средствам анализа являются: скорость и возможность приспособления к новым обстоятельствам – адаптивность. Средствами, удовлетворяющими этим требованиям, являются системы искусственного интеллекта. В частности существует ряд исследований, применяющих нейронные сети в качестве средства анализа. Выделяют различные типы нейронных сетей, различающиеся в зависимости от решаемых задач и более подходящие для различных входных данных. Построена многоагентная система обнаружения атак, осуществляющая сбор и анализ собранных сведений о событиях информационной системы с помощью двух типов нейронных сетей. Для анализа различных журналов*