Гайдамака А. В., Евдокименко М. Н.

Моженкова Е. В. – м - р. техн. наук, ассистент

Рассматриваются основные угрозы безопасности веб-приложений и способы борьбы с ними. Работа представляет собой краткий обзор зарубежных исследований.

Интернет прочно вошел в жизнь любого жителя на Земле. Поскольку основным инструментом для взаимодействия пользователя и бизнеса в сети Интернет является веб-приложение или веб-сервис, в данном докладе рассмотрены самые распространенные способы защиты веб-приложений от посягательств со стороны недобросовестных пользователей и других категорий злоумышленников.

Все угрозы информационной безопасности веб-приложений можно разделить на несколько категорий [1-6]:

1. Инъекция вредоносного пользовательского кода в веб-приложение. Включает подкатегории:
   - Межсайтовый скриптинг – XSS (атака на пользователя, направленная на выполнение в его браузере произвольного сценария) – внедрение вредоносного JavaScript-кода на страницу атакуемой веб-системы [1]. При загрузке страницы браузер автоматически исполняет JavaScript-код, собирая данные аутентификации и отправляя их на сайт злоумышленника. Способы предотвращения XSS-атак: запрет на вложение HTML-страниц, экранирование спецсимволов “<“, “>”, передача всех куки с флагом HttpOnly.
   - SQL-инъекция – внедрение вредоносного SQL-кода в тело HTTP-запроса к веб-приложению [5]. Способы предотвращения SQL-инъекций: повсеместное использование ORM в веб-приложении, клиентская и серверная валидация данных, тестирование веб-приложения, экранирование «очищенных» параметров, поступающих в сырые SQL-запросы, тестирование приложения инструментами на нахождение потенциальных SQL-инъекций.
2. CRLF-атака – техника модификации HTTP-заголовков запроса [2]. Можно выделить 2 её вида:
   - CRLF-инъекция – использование ASCII-представления комбинации CR + LF (перенос каретки + новая строка) для формирования «вредных» URL.
   - Расслоение HTTP-запроса. С его помощью злоумышленник может сформировать URL, который подменит собой ответ сервера, а также, инициировав внутреннюю ошибку веб-приложения, увидеть как информацию о сервере веб-приложений, так и служебную информацию.

   Способы предотвращения CRLF-атак: обязательное кодирование CRLF-последовательности до передачи в HTTP-заголовки, а также полное кодирование передаваемых данных.

   2. XXE (XML eXternal Entity) -атака [3]. При валидации XML-документа парсером (объектно-ориентированным скриптовым языком программирования, созданным для генерации HTML-страниц на веб-сервере с поддержкой CGI) с помощью схемы DTD, все ее директивы обязательно должны быть выполнены. Если правилами определено, что во входном документе допускаются спецсимволы XML, – риск быть атакованным очень велик. Способы предотвращения XXE: тщательная настройка XML-парсеров, использование XML Schema вместо DTD для валидирующего парсера.

   3. CSRF (Cross Site Request Forgery) – межсайтовая подделка запросов [5]. Дает возможность злоумышленнику воспользоваться аутентификационными данными жертвы (cookies) и провести от ее имени какую-либо зловредную операцию. Способы предотвращения CSRF: установка HttpOnly-флага передачи cookie, использование одноразовых сессионных token и отправка скрытой формы, чтобы token нельзя было подделать, проверка рефереров при HTTP-запросах к веб-приложению.

   4. Атаки со стороны пользовательского интерфейса. Используя клиентские JavaScript-библиотеки веб-приложения, злоумышленник может «разблокировать» его элементы управления, таким образом скомпрометировав функциональность сайта. Предотвращение атак через пользовательский интерфейс осуществляется путем сверки данных, отправляемых от пользователя, с теми, что хранит веб-приложение.

В докладе подробно рассматриваются все вышеперечисленные угрозы информационной безопасности и методы их парирования.

Список использованных источников:

1.Cross-Site Scripting – Wikipedia [Электронный ресурс] – Режим доступа: http://en.wikipedia.org/wiki/Cross-site_scripting. – Дата доступа: 15.03.2015.

2.CRLF Injection – Open Web Application Security Project [Электронный ресурс] – Режим доступа: https://www.owasp.org/index.php/CRLF_Injection. – Дата доступа: 15.03.2015.

3.Testing for XML Injection – Open Web Application Security Project [Электронный ресурс] – Режим доступа: https://www.owasp.org/index.php/Testing_for_XML_Injection_(OTG-INPVAL-008). – Дата доступа: 15.03.2015.

4.XML Validation – Wikipedia [Электронный ресурс] – Режим доступа: http://en.wikipedia.org/wiki/XML_validation. – Дата доступа: 15.03.2015.

5.Paco Hope, Paco, Walter, Ben. Web Security Testing Cookbook. – Sebastopol (USA): O'Reilly Media, 2008. – 314 p.

6.Types of Attacks for Web Applications – University Of California, San Francisco [Электронный ресурс] – Режим доступа: https://it.ucsf.edu/services/application-and-website-security/types-attacks-web-applications. – Дата доступа: 15.03.2015.

АВТОМАТИЧЕСКАЯ СИСТЕМА УПРАВЛЕНИЯ БИЗНЕС-ПРОЦЕССАМИ

Институт информационных технологий БГУИР, Минск, Республика Беларусь

Ганчарук М А.

Шпак И.И. – зав.кафедрой ПЭ, канд. техн. наук, доцент

В настоящее время необходимость автоматизации различных процессов становиться уже привычным для нас явлением. На сегодняшний день сложно представить себе бухгалтерский или складской учёт без использования специального программного обеспечения. Покупки в интернет-магазинах приходят продавцу в виде готовых к обработке документов или заявок, приложения для смартфонов позволяют заказать доставку еды на дом. Производственные процессы так же нуждаются в автоматизации. Для решения таких задач и служит данная CRM-система.

Разрабатываемая система предназначена для управления бизнес-процессами компании, взаимодействий с заказчиками (клиентами), в частности, для повышения уровня продаж, оптимизации маркетинга и улучшения обслуживания клиентов путём сохранения информации о клиентах и истории взаимоотношений с ними [1-3]/

В предлагаемой системе использованы современные средства веб-разработки, которые не привязывают пользователя к конкретной платформе и месту, для полноценной работы необходима только актуальная и поддерживаемая версия браузера. Схематическое отображение процесса функционирования системы показано на рисунке 1.

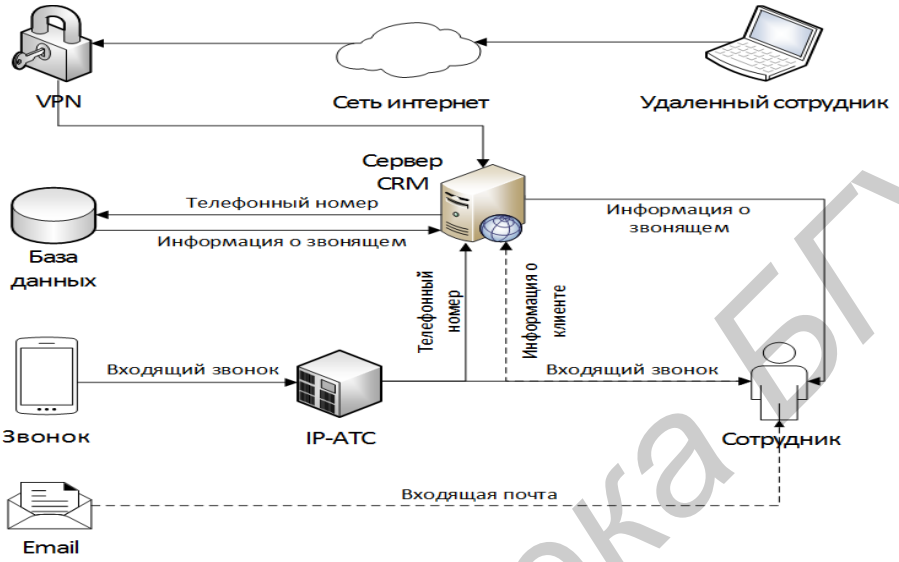

Рисунок 1 – Обобщенная структурная схема системы

На представленной выше схеме изображено следующее: входящий звонок, поступивший на цифровую IP-АТС распределяется на одного из сотрудников, в то же время, АТС отдаёт номер звонящего серверу CRM, который в свою очередь проводит поиск по номеру в базе данных, и по результатам поиска открывает в браузере карточку клиента. Если соответствующей записи в базе данных нет, будет открыта новая карточка с уже внесённым номером звонящего. Так же, найти нужного клиента можно задав в строке поиска адрес электронной почты отправителя. Удалённые сотрудники имеют возможность взаимодействия с системой через сеть Интернет посредством VPN подключения, получая тем сам весь функционал системы не находясь в офисе.

Таким образом, разработанная система позволит более эффективно осуществлять:
- контроль качества работы отдела продаж,
- вести стандартизированную базу контактов,
- коллективную работу сотрудников,
- статистику и аналитику эффективности работы с входящими звонками, запросами.

Список использованных источников:

1.Шуремов, Е.Л. Информационные технологии управления взаимоотношениями с клиентами./ Е.Л. Шуремов - М.: 1С-Паблишинг, 2005. - 98 с.
2.Резникова, Н.П. Менеджмент в телекоммуникациях./ Н.П. Резникова. - М.: Эко-Трендз, 2005. - 392 с.
3.Трофимов, С.А. CRM для практиков. / С.А. Трофимов. – М.: ООО АвтоКод, 2006. - 308 с.
4.Молино П. Технологии CRM: Экспресс-курс./ П. Молино – М.: ФАИР-ПРЕСС, 2004. - 272 с.

ИССЛЕДОВАНИЕ НАДЁЖНОСТИ ТЕХНОЛОГИЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гивойно А.А.

Шахлевич Г.М. − канд. техн. наук, доцент