ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ (НА ПРИМЕРЕ ИНТЕРНЕТ-АУКЦИОНА)

Солодков Денис Сергеевич
Тимохов Сергей Дмитриевич
Российский университет дружбы народов, Москва, студенты

Кравченко Николай Юрьевич
Финансовый университет при Правительстве РФ, Москва,
ст. преподаватель
d.solodkov@yandex.ru, greytim95@rambler.ru

Введение

Темп роста аудитории пользователей Интернета во всем мире, стимулирует развитие экономической деятельности, активные участники которой стремятся увеличить свой доход, используя всемирную глобальную сеть как торговую площадку. Такая экономическая активность, получившая название «электронная коммерция», призвана упростить процедуру купли-продажи товаров и услуг, как для продавцов, так и для покупателей. Примерами «электронной коммерции» можно назвать продажу рекламного места на популярных веб-ресурсах, создание интернет-магазинов, интернет-аукционов и других информационных систем.

В настоящее время интернет-аукционы (далее ИА) – это динамично развивающаяся область электронной коммерции, в которой теоретическая база и сама технология разработки таких информационных систем слабо систематизированы и формализованы.

1. Основные положения проектирования информационной системы интернет-аукциона

Целью данной статьи является изложение основных принципов построения информационных систем ИА и выработка практических советов.

ИА – это сфера электронной коммерции, в основе которой лежат принципы традиционных аукционных торгов.

Самым известным и посещаемым (свыше 88 миллионов активных пользователей) ИА в мире является eBay (www.ebay.com), позиционирующий себя как интернет-аукцион общего профиля, построенный по принципу C2C (consumer to consumer), что означает, что в роли продавцов и покупателей выступают частные лица.

2. Обеспечение безопасности информационной системы интернет-аукционов и ее участников

При разработке любого веб-приложения в сфере электронной коммерции, в том числе интернет-аукциона, необходимо предусмотреть механизмы защиты как самого веб-приложения, так и его участников. Статистика уязвимостей по типу приложений показывает, что наиболее проблемными в этом плане являются web-приложения, доля обнаруженных уязвимостей в которых превышает 40% от общего числа.

Межсайтовое выполнение сценариев (Cross-site Scripting, XSS) - наличие уязвимости Cross-site Scripting позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя.

Утечка информации (Information Leakage) – эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например, комментарии разработчиков или сообщения об ошибках.

Внедрение операторов SQL (SQL Injection) - эти атаки направлены на Web-серверы, создающие SQL запросы на основе данных, вводимых пользователем.

Недостаточная защита данных при их передаче на транспортном уровне (Insufficient Transport Layer Protection) – эта уязвимость позволяет перехватывать данные, передаваемые, например, по HTTP вместо HTTPS.

Идентификация приложений (Web Server/Application Fingerprinting) – определение версий приложений, которое используется злоумышленниками для получения информации об используемых сервером и клиентом операционных системах, Web-северах и браузерах.

Расщепление HTTP-запроса (HTTP Response Splitting) – данная уязвимость позволяет злоумышленнику посылать серверу специальным образом сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа.

Необходимо оснастить веб-приложение продуманной и эффективной системой защиты от взлома, которая поддерживалась бы в актуальном состоянии. Тем самым обеспечивается безопасность не только самой системы от возможности ее копирования, изменения и уничтожения, но и личных данных ее участников и финансовых операций между ними.

Также информационная система должна иметь свои собственные механизмы по защите участников системы от мошенников. Эти механизмы должны проверять надежность другой стороны и тем самым снижать риски, основанные на недобросовестности участников системы.

Возможными механизмами могут быть:

- система рейтинговой оценки, суть которой сводится к выставлению участниками системы друг другу оценок после совершения сделки купли-продажи;
- проверка продавцов и покупателей на реальность телефонных номеров, почтовых адресов, и т.д. вплоть до проверки паспортных данных;
- проверка участников системы на наличие средств на банковском счете при регистрации и/или вводе ставки для обеспечения финансовых гарантий;
- система штрафов (может быть привязана к системе рейтинговой оценки), которая позволит наказывать участников, которые не выполнили свои обязательства по продаже или покупке;
- система возмещения убытков, которая будет предусматривать выплату оговоренной суммы пострадавшей стороне.

Для обеспечения гарантий оплаты товара\услуги покупателем владелец интернет-аукциона может взять на себя обязательство посредничества при проведении операции с денежными средствами через банковский счет или кошелек электронных денег интернет-аукциона.

Заключение

Обеспечение безопасности своего веб-ресурса – необходимое условие разработки информационной системы ИА. Кроме того, защищенность системы повышает доверие со стороны целевой аудитории, следовательно, способствует получению дополнительных конкурентных преимуществ.

Список источников

1. Данные официального сайта eBay (www.ebayinc.com).

2. Данные сайта www.alexa.com, занимающимся составлением рейтингов веб-ресурсов.

3. Источник описаний уязвимостей - проект по защите информации www.protectme.ru.