Емельянова Елена Сергеевна
студентка
Калуцкий Игорь Владимирович
канд. техн. наук, преподаватель
ФГБОУ ВО «Юго-Западный
государственный университет»
г. Курск, Курская область

АНАЛИЗ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

Аннотация*: в работе рассматриваются возможные уязвимости интернет-приложений и способы их устранения. С каждым днем интернет-торговля становится популярнее, в связи с этим увеличивается количество возможных угроз безопасности. Для обеспечения бесперебойной работы веб-приложений необходимо внимательно подойти к вопросу информационной безопасности.*

Ключевые слова*: интернет-магазин, безопасность, информация, данные.*

В связи с постоянным развитием технологий и возможностей, создание интернет-магазинов стало общедоступно для всех пользователей сети Интернет. На сегодняшний день интернет-торговля является достаточно популярным способом совершения покупок, которому отдает предпочтение множество покупателей. Многие компании перемещают все важные компоненты бизнеса в Web, т. к. покупки в данном случае могут совершаться в любой момент времени и из любой точки мира. Из-за своей доступности и в связи с активным ростом и развитием данных площадок, интернет-магазины все чаще становятся целью для киберпреступников, поэтому решения по эффективной защите web-приложений сейчас являются все более актуальными и востребованными. Также многие компании особое внимание обращают на вопрос безопасности и обеспокоены сохранностью данных своей компании и своих клиентов. Организации заинтересованы в надежной и бесперебойной работе своего сайта, т. к. если сайт не будет работать, то компания понесет убытки и недополучит прибыль [3, с. 175].

Угрозы информационной безопасности интернет-магазина могут быть самыми разными: DDOS-атаки, взлом, заражение вирусным ПО, межсайтовый скриптинг (XSS-атаки), SQL-инъекции, вызов исключительных ситуаций [4]. Необходимо иметь представление о том, какие действия могут предпринять киберпреступники, чтобы была возможность предотвратить или сократить до минимума возможные потери.

Угрозы могут быть внешними и внутренними. Источником внешней угрозы может выступать человек, у которого нет санкционированного доступа к системе, а источником внутренней угрозы – люди, у которых есть санкционированный доступ к информационной системе (администраторы, конечные пользователи, разработчики приложений).

К внешним воздействующим факторам, которые создают угрозы безопасности работе информационной системы, относятся:

1) целенаправленные, деструктивные действия лиц, целью которых является хищение, уничтожение или искажение данных и документов системы;

2) целенаправленное воздействие на каналы передачи информации, поступающей от внешних источников, с целью вызвать отказ в обслуживании;

3) неправильная работа аппаратуры вычислительных средств;

4) вирусы и иные деструктивные программные элементы, распространяемые с использованием систем телекоммуникаций, обеспечивающих связь с внешней средой [8].

Среди внутренних угроз можно выделить следующие атаки:

1) атаки со стороны авторизованных пользователей с целью увеличения уровня привилегий в информационной системе;

2) непреднамеренные ошибки сотрудников, нарушающих по разным причинам установленную политику безопасности, или некорректно построенная политика безопасности;

3) умышленное изменение или искажение хранимых данных;

4) угрозы, возникающие из-за ошибок в программном обеспечении и неверной конфигурации системы;

5) угрозы, возникающие из-за ошибок в аппаратном обеспечении и неверной его настройки [1, с. 367].

В результате успешно осуществленной атаки на web-приложение могут быть перехвачены персональные данные, большой объем которых передают пользователи при совершении покупок в интернет-магазинах; уничтожена или похищена конфиденциальная информация, представляющая интерес для злоумышленников; заражена система вредоносным программным обеспечением [2, с. 77].

Для завладения данными пользователей, как правило несущими экономический характер (номер карты, счета и т. д.), может быть использовано заражение вирусным кодом интернет-магазина, в результате чего замедляется работа приложения, появляются ошибки или посторонний текст, всплывает реклама, призывающая перейти по указанной ссылке, в результате чего на компьютер пользователя устанавливается вредоносное ПО. Также внедрение вредоносного кода отражается на рейтинге сайта в поисковых системах. Для того, чтобы заполучить персональные данные, может осуществляться перенаправление пользователей, заходящих в интернет-магазин, на сайты конкурентов или фишинговые сайты.

Вредоносное ПО, распространяемое через сеть Интернет, также представляет опасность, т. к. данные программы применяются для завладения данными и денежными средствами пользователей. С помощью данных программ злоумышленники могут управлять компьютером пользователя, вымогать денежные средства. В соответствии с ст. 273 УК РФ, создание, применение и распространение вредоносных компьютерных программ уголовно наказуемо [7]. Но злоумышленники действуют анонимно, поэтому довольно сложно их поймать и привлечь к ответственности.

Одними из наиболее распространённых угроз безопасности web-приложений является межсайтовый скриптинг: XSS-атака (Cross-Site

Scripting) – внедрение вредоносного кода на страницу сайта, выполняемого на компьютере пользователя при открытии данной страницы. Основной целью данной угрозы является кража cookies пользователей, служащих для сохранения учетных данных сайта на компьютере посетителя. XSS-атаки – это атаки на пользователей сайта, а не на сам сайт. Атаки XSS могут быть активными и пассивными. Пассивные не очень ценятся, т. к. требуют дополнительных действий для того, чтобы заставить жертву перейти по необходимой ссылке. В случае активной атаки не требуется никаких дополнительных действий, достаточно того, чтобы пользователь открыл страницу с вредоносным кодом, который выполнится автоматически [6].

Следующей угрозой является проведение DDOS атаки (Distributed Denial of Service), направленной на отказ в обслуживании. Так как веб-серверы имеют ограничения по количеству запросов, которые могут обслуживаться одновременно, а также существуют ограничения пропускной способности канала, который выполняет соединение сервера с Интернетом, то в том случае, когда ресурс не может справиться с большим потоком обращений, происходит существенное замедление времени ответа на запрос или же отказ в обслуживании запросов, что ведет к простоям в бизнесе. Так же стоит отметить SQL-инъекции, при помощи которых можно внедрить SQL-код, который сервер обработает и выдаст ответ. Если сайт уязвим и выполняет такие инъекции, то у злоумышленника есть возможность делать с БД практически что угодно.

Таким образом, можно сделать вывод, что обеспечение информационной безопасности интернет-магазина является одним из важнейших требований для успешного и прибыльного бизнеса. Осуществление сделок посредством сети Интернет предполагает обмен большим объемом информации через сеть общего доступа. Поэтому, для повышения надежности работы интернет-магазина, подход к обеспечению информационной безопасности должен быть комплексным и включать в себя такие задачи, как доступ к приложениям, авторизация пользователей, обеспечение конфиденциальности персональных данных и применение прочих мер обеспечения информационной безопасности.

На сегодняшний день большинство атак на web-приложения осуществляются в автоматическом режиме, при помощи сканирования, позволяющем обнаружить уязвимости в обеспечении безопасности сайта.

Для обеспечения должной безопасности интернет-магазина прежде всего необходимо регулярно делать резервные копии. Также резервные копии должны периодически проверяться на возможность восстановления из них.

Чтобы обеспечить конфиденциальность информации, передаваемой в электронном формате, обычно применяются различные виды шифрования. Данный способ дает возможность защитить информацию при ее хранении на открытых носителях, подтвердить подлинность передаваемой информации, защитить другие информационные ресурсы организации от несанкционированного использования.

Необходимо использовать антивирусные средства, регулярно обновлять их, следить за настройкой web-сервера с открытием прав доступа только в необходимом объеме. В связке с гибким межсетевым экраном, антивирусное программное обеспечение является одним из самых действенных способов защитить сайт от угроз безопасности.

Используя сетевые экраны, можно повысить устойчивость интернет-магазина к хакерским атакам за счет фильтрации и проверки интернет-трафика, а также уведомлений в случае попытки эксплуатации. Для того, чтобы избежать эксплуатации существующих в web-приложении уязвимостей, межсетевой экран должен быстро обрабатывать трафик, блокировать противоправные запросы, уметь работать с любым протоколом http/https, не зависеть от платформы веб-приложения, содержать актуальную и пополняемую базу признаков атак.

В случае, когда web-сервер стал мишенью атаки, злоумышленником сразу же будет предпринята попытка загрузки инструментов взлома или вредоносного программного обеспечения, чтобы успеть воспользоваться уязвимостью системы безопасности до ее закрытия. Если качественное антивирусное про-

граммное обеспечение не установлено, уязвимость системы безопасности может продолжительное время оставаться необнаруженной [5, с. 420].

Стоит отметить, что наиболее эффективным способом защиты является применение многоуровневого подхода. Переднюю линию защиты составляют межсетевой экран и операционная система, за ними находится антивирус, который должен заполнять возникающие бреши в защите.

Таким образом, основными принципами, позволяющие повысить безопасность WEB-сайта (в части атак на операционную систему) являются:

– установка ненужных компонентов является нежелательной. Любой компонент может быть объектом атаки, следовательно, увеличение количества компонентов повышает суммарный риск;

– своевременная установка обновлений системы безопасности для операционной системы и приложений;

– использование антивирусного программного обеспечения с включением установки автоматических обновлений (при этом должна постоянно производиться проверка их установки).

Конечно, применение всех вышеперечисленных принципов может быть затруднительным, но это необходимо, так как для того, чтобы атака злоумышленника была успешна, вполне хватит и одной бреши в системе безопасности. При этом могут наступить такие негативные последствия, как кража данных и трафика, занесение IP-адреса сервера в черные списки, причинение ущерба организации и нестабильность работы web-сайта.

Для предотвращения подбора пользовательских паролей можно установить блокировку учетной записи на определенное время в том случае, если обнаружено несколько неудачных попыток ввода пароля подряд. Вдобавок к данному способу необходимо обязать пользователей применять сложные пароли и регулярно их менять. Также своевременное обновление программной платформы сайта помогает закрывать уже обнаруженные «дыры» в безопасности.

Вдобавок многими сайтами используется протокол SSL для защиты данных в сети Интернет, который гарантирует безопасное зашифрованное соеди-

нение между сервером и браузером пользователя. Данное соединение может гарантировать, что передаваемая информация остается защищенной от злоумышленников. Примером использования может служить безопасное совершение платежей при покупке товара, оплате на сайте.

В тех случаях, когда необходимо предотвратить и отразить DDOS атаку при попытке ее проведения, необходимо использовать специализированные программно-аппаратные решения или онлайн сервисы, направленные на обнаружение и защиту от данного вида атак. Работа данных фильтров основана на анализе входящего трафика и обнаружении подозрительной активности.

Таким образом, можно сделать вывод, что защита web-приложений состоит из комплекса непрекращающихся действующих и развивающихся мер. Необходимо обращать повышенное внимание к безопасности, чтобы защитить интернет-магазин от внешних угроз и предотвратить возможные потери и убытки.

Список литературы

1. Горбулин А.А. Аспекты разработки метода оценки угроз безопасности информационным системам на основе численных показателей / А.А. Горбулин, И.В. Калуцкий, В.А. Шумайлова // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения. – 2019. – С. 366–369.

2. Калуцкий И.В. Модель интерактивного справочного ресурса сведений и рекомендаций в области безопасности субъектов персональных данных / И.В. Калуцкий, А.Г. Спеваков, С.В. Остроцкая // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. – 2018. – С. 73–81.

3. Калуцкий И.В. Роль человеческого фактора в обеспечении безопасности бизнеса / И.В. Калуцкий, А.А. Агафонов // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. – 2012. – С. 173–178.

4. Киреенко А.Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения [Элек-

тронный ресурс]. – Режим доступа: https://moluch.ru/archive/38/4365/ (дата обращения: 20.12.2019).

5. Конорева Е.Е. Уязвимости межсетевых экранов и способы их устранения. / Е.Е. Конорева, И.В. Калуцкий // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения. – 2019. – С. 418–423.

6. Полное пособие по межсайтовому скриптингу [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/analytics/432835.php (дата обращения: 19.11.2019).

7. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 27.12.2019).

8. Щеглов А.Ю. Компьютерная безопасность. Вопросы комплексирования. Системный подход к построению системы защиты информации от несанкционированного доступа [Электронный ресурс] – Режим доступа: http://www.itsec.ru/articles2/Inf_security/voprosy-kompleksirovaniya (дата обращения: 20.12.2019).