УДК 004.056.53 **Информационные технологии**

Камбулов Данил Александрович, *студент I курса, магистратура*
Федеральное государственное бюджетное образовательное учреждение высшего образования "Донской государственный технический университет"

АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОБЗОР СУЩЕСТВУЮЩИХ МЕТОДОВ ЗАЩИТЫ

Аннотация: Данная статья посвящена анализу потенциальных угроз информационной безопасности интернет-магазинов, в которых реализована электронная коммерция. А также рассмотрен комплексный подход к защите интернет-магазина от различных угроз.

Ключевые слова: информационная безопасность, защита информации, атаки, DDoS-атаки, аудит, веб-сайт, электронная коммерция, уязвимости.

Annotation: This article is devoted to the analysis of threats to the information security of online stores, which implement e-commerce. And also considered a comprehensive approach to protecting an online store from various threats.

Keywords: information security, information protection, attacks, DDoS attacks, audit, website, e-commerce, vulnerabilities.

Анализ исследований, проводимых аналитическим центром PT Research, а также компанией PositiveTechnologies, осуществляющих проведение тестов на проникновение и аудит информационной безопасности показывают, что ошибки в защите веб-сайтов, в том числе интернет-магазины, по-прежнему остаются одним из наиболее распространенных недостатков обеспечения защиты информации. Такими ошибками, т.е. уязвимостями пользуются злоумышленники, совершая атаки на веб-сайты с целью кражи ценной информации. Также повышается вероятность последующего проникновения в

корпоративные информационные системы. Наиболее распространенными угрозами безопасности веб-сайтов являются:

Межсайтовый скриптинг (XSS–атаки). Межсайтовый скриптинг – одна из разновидностей атак на веб-системы, которая подразумевает внедрение вредоносного кода на определенную страницу сайта и взаимодействие этого кода с удаленным сервером злоумышленников при открытии страницы пользователем [3].

SQL-инъекции. Суть данной атаки – внедрение в данные (передаваемые через GET, POST запросы или значения Cookie) произвольного SQL кода с целью получить доступ к базе данных сайта [4].

Отсутствие обработки исключений. Исключение (от англ. exception) – это результат выполнения некорректного оператора, что привело к возникновению ошибки.

DDoS-атаки – распределенные сетевые атаки, которые также называются распределёнными атаками типа «отказ в обслуживании» (от англ. Distributed Denial of Service, DDoS). Этот тип атаки использует определенные ограничения пропускной способности, которые характерны для любых сетевых ресурсов [4].

Удаленное выполнение кода (RCE) – это компьютерная уязвимость, при которой происходит удаленное выполнение кода на взламываемом компьютере, сервере и т.п. Такая уязвимость является максимальной угрозой класса A1 по классификации открытого проекта обеспечения безопасности веб-приложений OWASP, а значит это гарантированный способ взлома сайтов и веб приложений. RCE-атаки являются одними из самых опасных уязвимостей.

Атаки на процесс аутентификации. Одним из наиболее ярких представителей таких атак является bruteforce. Bruteforce (атака полным перебором) – метод решения математических задач, сложность которого зависит от количества всех возможных решений. Сам же термин bruteforce обычно используется в контексте хакерских атак, когда злоумышленник пытается подобрать логин/пароль к какой-либо учетной записи или сервису.

Результатом успешной реализации угроз безопасности веб-приложений и атак злоумышленника может стать утечка или уничтожение конфиденциальных данных, заражение компьютеров пользователей вредоносным ПО, недоступность сервисов, финансовые и репутационные потери.

Значимой частью от всех веб-сайтов в Интернете являются онлайнмагазины. Помимо всех перечисленных проблем, у них также остро стоит проблема мошенничества с банковскими картами.

Так, объем несанкционированных операций с использованием платежных карт в 2018 году вырос на 44 процента, до 1,38 миллиарда рублей, количество таких операций увеличилось почти на треть: преступникам 417 тысяч раз удавалось разными способами получать деньги физических лиц.

Мошенничество с банковскими картами, так называемый фрод (от англ. fraud), становится возможен из-за использования данных добросовестного клиента мошенниками, вследствие их хищения через фишинг, скимминг, кликджекинг, прямую утечку данных [1].

Фишинг (от англ. fishing) – вид Интернет-мошенничества, который представляет собой противоправное действие, совершаемое с целью заставить то или иное лицо поделиться своей конфиденциальной информацией, например, паролем или номером кредитной карты. Зачастую такое мошенничество выглядит как пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать или обновить личные данные.

Скимминг – вид мошенничества с банковскими картами, представляющий преступные действия заключаются в том, что в банкоматах устанавливаются скрытые устройства, позволяющие считывать информацию с платежных карт в процессе транзакции [2].

Кликджекинг – это мошенническая технология для обмана пользователей интернета, основанная на том, что на странице кроме видимых элементов располагаются невидимые [2]. Невидимые кнопки, ссылки размещаются поверх видимых кнопок и ссылок – в местах, где кликают пользователи.

Соответственно, по клику происходит действие, которого пользователь не ожидал и которого не должно было быть. Такая техника может использоваться, например, для сбора персональных данных посетителей сайта без их ведома.

В онлайн-продажах страдает больше всего от подобного рода мошенничества именно торгово-сервисное предприятие, т.к. если его защита недостаточна и подобных транзакций происходит больше 1%, то платежная система может внести этот магазин в черный список и перестать обеспечивать передачу денег от покупателя продавцу, либо же применить какие-либо санкции.

Подобные уязвимости должны быть обнаружены и зафиксированы еще на этапе разработки веб-сайта: должен был проведен статический, динамический, интерактивный анализ, выявление аномалий в логике работы приложения.

Однако только ручное обнаружение и устранение уязвимостей, а также отслеживание мошеннических транзакций в самом сайте или приложении для торговли также часто не дает положительных результатов – команда разработчиков могут находить и исправлять тысячи уязвимостей, но злоумышленнику для проведения результативной атаки достаточно обнаружить всего одну. Следовательно, возникает необходимость в использовании специализированных средств и методов защиты вебприложений.

Таким образом, защита должна строиться по трем основным направлениям [5]:

1) Недопущение ошибок в коде при разработке веб-сайта. Этого можно добиться специальными техниками написания и тестирования программного кода, как например в Future Driven Development или Extreme Programming, где происходит непрерывное ревью работы программиста.

2) Применение специализированных технологий и механизмов для предотвращения вероятных внешних атак, как например, межсетевой экран уровня приложений, система обнаружения вторжений (решения типа ApplicationFirewall), система обнаружения вторжений (уровня сети и уровня узла), система Anti-DDoS, антивирус, криптографический пакет для шифрования. Такие технологии обладают встроенным функционалом

предупреждения и предотвращения вторжений и обеспечивают защиту от целенаправленных веб-атак, таких как переполнение буфера, SQL инъекции, Cross-Site-Scripting, изменение параметров запросов и других. Решения такого класса фильтруют запросы на доступ к приложению и блокируют все действия, которые не относятся к разрешенной активности пользователей. Также рекомендуется использование определенной парольной политики и проведение регулярного аудита компонентов веб-сайта.

3) Использование специальных технологий и сервисов для отсеивания мошеннических транзакций.

В выбранных направлениях для решения задач защиты от угроз мошенничества, несанкционированного доступа к платежным данным пользователей и защиты от уязвимостей web-приложений следует использовать комплексный подход.

Библиографический список:

1. Аналитическая система распознания мошеннических платежей – URL https://habr.com/ru/post/254683/ (дата обращения 12.12.2020).

2. Антифрод. Архитектура сервиса – URL: https://habr.com /ru/post/254037/ (дата обращения 12.12.2020).

3. Современные методы web-защиты. – URL: https://www. infowatch.ru/resources/blog/20207 (дата обращения 12.12.2020).

4. Защита сайта от хакерских атак — Nemesida WAF. – URL: https://habr.com/ru/company/pentestit/blog/282860/ (дата обращения 12.12.2020).

5. Известия Южного федерального университета. Технические науки. А.Ю. Оладько, В.С. Аткина «МОДЕЛЬ ЗАЩИТЫ ИНТЕРНЕТ-МАГАЗИНА» С. 74-80.