УДК 004.91
DOI: 10.18101/978-5-9793-1626-0-87-90

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЯ. ТОП-10 УЯЗВИМОСТЕЙ ПО OWASP

© **Конькова Анна Евгеньевна**
студент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
konkova@yandex.ru

© **Немчинова Татьяна Владимировна**
кандидат педагогических наук, доцент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
ntv05@mail.ru

Аннотация. Уязвимость — это недостаток в системе. Уязвимости позволяют менять ход работы программы, повышать права пользователей, раскрывать конфиденциальные данные. Как правило, возникают из-за ошибок в программировании, недостатков, допущенных при проектировании системы, слабых паролей и т. д. В статье рассматриваются вопросы, связанные с уязвимостью веб-приложений. И рассмотрено 10 самых критичных угроз безопасности веб-приложений.
Ключевые слова: уязвимость, веб-приложение, персональные данные, сервис

Для цитирования
Конькова А. Е., Немчинова Т. В. Обеспечение безопасности веб-приложения. Топ-10 уязвимостей по OWASP // Информационные системы и технологии в образовании, науке и бизнесе: материалы региональной научно-практической конференции с международным участием (Улан-Удэ, 1 июля 2021 г.) / отв. ред. А. А. Тонхоноева, науч. ред. Е. Р. Урмакшинова. Улан-Удэ: Изд-во Бурят. гос. ун-та, 2021. С. 87–90.

Один из основных мифов — веб-приложение безопасно благодаря использованию Firewall, IDS/IPS. Защита многих компаний во время использования HTML-кодов сводилась только лишь к установке нескольких пакетных фильтров. То есть по большому счету просматривались лишь первые четыре уровня модели OSI. При этом отметим, что каждый пакетный фильтр принципиально не может ни определить содержимое запросов, ни провести контент-анализ. Особенно критичной эта проблема стала, когда начали использоваться БД, скрипты, технологии Java, Flash, ActiveX и пр. С их появлением и распространением вся прежняя защита стала просто бесполезной [3].

Общая стратегия безопасности программного обеспечения основывается на трех основных принципах:

конфиденциальность — сокрытие определенных ресурсов или информации;

целостность — ожидание, что ресурс может быть изменен только соответствующим способом определенной группой пользователей; а в случае если данные повреждаются или неправильно изменяются, должна быть предусмотрена процедура восстановления;

доступность — требования о том, что ресурсы должны быть доступны авторизованному пользователю, внутреннему объекту или устройству.

Пандемия и последовавшие за ней ограничительные меры по всему миру нанесли серьезный удар не только по экономике, но и привычному распорядку жизни обычных граждан. По данным Ozon, в России за первую неделю пандемии сильно выросли продажи некоторых категорий товаров: пользователи купили на 200% больше подписок на игровые сервисы и онлайн-кинотеатры, вырос спрос на настольные игры (150%), товары для хобби и творчества (120%) и книги (110%)[1]. Все сайты электронной коммерции являются привлекательными целями для хакеров из-за личной и платежной информации, необходимой для совершения продажи. Даже если система не обрабатывает транзакции по картам напрямую, взломанный сайт может перенаправить клиентов на ложную страницу или изменить заказ, прежде чем он будет передан в платежный процессор. Взлом может иметь долгосрочные последствия как для покупателей, так и для продавцов.

По данным руководителя маркетинга PicsArt Анны Маиковой, на фоне пандемии пользователи потратили на мобильные приложения 111 млрд долл. — на 30% больше, чем в 2019 г. По прогнозам Sensor Tower, в ближайшие пять лет расходы пользователей на покупки внутри приложений и подписную модель будут расти со скоростью 19,5% и достигнут 270 млрд долл. — это в 2,5 раз больше, чем в 2020 г. При этом динамика App Store будет выше — 21% GAGR, тогда как Google Play — 17%[2]. Повышенным спросом у населения в данный период пользуются и веб-приложения. Такие как онлайн-банкинг, запись к врачу, доставка продуктов. Эти сервисы позволяют пользователям сэкономить время и получить нужную услугу «в один клик».

Используя то или иное веб-приложение, пользователь так или иначе вынужден предоставлять личные данные сервисам в обмен на возможность присоединиться и воспользоваться определенными услугами. Но зачастую веб-приложения не всегда способны обеспечить конфиденциальность и защиту персональных данных. И все это может привести к утечке огромных массивов данных, которые могут быть использованы мошенниками в корыстных целях. Кроме того, уязвимости веб-приложения могут вызвать его полную неработоспособность и, соответственно, финансовые убытки и репутационные потери.

По данным Газета.ru, персональные данные россиян действительно часто утекают в открытые источники или же становятся предметом купли-продажи. Согласно исследованию компании Dentsu Aegis Network, лишь 29% россиян считают, что их персональные данные защищены в достаточной степени[3].

Знание основных рисков безопасности поможет разработчику сделать веб-приложения надежнее. Существует множество организаций, которые занимаются

[1] Пандемия как стресс-тест: какие отрасли будут развиваться из-за вируса. URL: https://trends.rbc.ru/trends/industry/5e9034bf9a7947a07e906246 (дата обращения: 24.05.2021). Текст: электронный.

[2] Какие приложения будут пользоваться наибольшим спросом в ближайшие 5 лет: обзор главных трендов. URL: https://rb.ru/opinion/mobile-apps-trends/ (дата обращения: 24.05.2021). Текст: электронный.

[3] «Утечки неизбежны»: кто ответственен за персональные данные. URL: https://www.gazeta.ru/tech/2019/08/09_a_12567469.shtml (дата обращения: 24.05.2021). Текст: электронный.

информационной безопасностью и предоставляют в открытый доступ рекомендации по разработке и защите приложений. Среди них MITRE, Offensive Security, Positive Technologies. Далее рассмотрим проект некоммерческого фонда OWASP — Топ-10 уязвимостей веб-приложений (OWASP Top 10).

Цель данной работы является рассмотрение 10 самых критичных угроз безопасности веб-приложений. Доступно две редакции рейтинга с разницей в 4 года — за 2013 и 2017 гг. Проект OWASP TOP 10 подробно рассматривает каждый тип уязвимостей и дает рекомендации по их недопущению.

Существует общий перечень дефектов безопасности ПО — CWE (Common Weakness Enumeration), а также, база данных общеизвестных уязвимостей в ИБ — проект CVE (Common Vulnerabilitiesand Exposures). Дефекты безопасности — это ошибки, которые могут спровоцировать уязвимости. OWASP классифицирует уязвимости с помощью CWE.

При разработке веб-приложений полезно руководствоваться данным рейтингом. Топ-10 рисков по OWASP включают в себя: A1:2017 — Внедрение, A2:2017 — Недостатки аутентификации, A3:2017 — Разглашение конфиденциальных данных, A4:2017 — Внешние сущности XML (XXE), A5:2017 — Недостатки контроля доступа, A6:2017 — Некорректная настройка параметров безопасности, A7:2017 — Межсайтовое выполнение сценариев (XSS), A8:2017 — Небезопасная десериализация, A9:2017 — Использование компонентов известными уязвимостями, A10:2017 — Недостатки журналирования и мониторинга[1].

Как видно из рейтинга, самой распространенной атакой является внедрение, или инъекция. Такая атака становится возможной за счет того, что интерпретатору отправляются непроверенные данные, которые могут содержать вредоносный код. Например, sql-инъекции, которые позволяют извлекать, изменять, удалять содержимое баз данных, или инъекции команд операционной системы.

Также OWASP Top-10 ранжирует уязвимости по сложности эксплуатации, распространенности, сложности обнаружения и последствиям. Согласно OWASP, A1:2017 — Внедрение имеет сложность эксплуатации — 2, распространенность — 3, распространенность — 2, сложность обнаружения — 3 и последствия — 3.

Подробнее о каждом типе уязвимостей, причинах их возникновения и способах устранения можно прочитать на официальном сайте проекта https://wiki.owasp.org.

Таким образом, при создании веб-приложений необходимо уделять должное внимание безопасности. Проверять поступающую от пользователя информацию, не использовать распространенные пароли, правильно настраивать права доступа для пользователей и файлов самого приложения, внимательно относиться к используемым компонентам, таким как библиотеки, фреймворки и программные модули, а также следить за новостями в области информационной безопасности.

Сегодня, когда цифровизация используется во всех отраслях экономики, важность обеспечения безопасности приложений возрастает в геометрической прогрессии. Безопасность — это важнейшая составляющая качественного веб-

[1] Who is the OWASP Foundation? URL: https://owasp.org/ (дата обращения: 24.05.2021). Текст: электронный.

приложения. Поэтому нельзя оставлять без должного внимания относительно простые угрозы безопасности и нужно помнить, что помимо OWASP Top-10 существует множество других рисков, которые необходимо оценивать и учитывать.

Литература

1. Секреты хакеров. Безопасность Web-приложений — готовые решения / Дж. Скембрей, М. Шема, Й.-М. Чен, Д. Вонг. Москва: Вильямс, 2003. 384 с. Текст: непосредственный.

2. Китонов А. Ж., Баенова Г. М., Урынбасарова А. Ж. Вопросы безопасности веб-приложений // Физика и математика. 2020. № 13(65). С. 279–283. Текст: непосредственный.

3. Искадыров Р. Ю., Сырлыбаева Р. Р. Безопасность web-приложений // Актуальные проблемы социального, экономического и информационного развития современного общества: материалы всероссийской научно-практической конференции, посвященной 100-летию со дня рождения первого ректора БГУ (Уфа, 20 мая 2016 г.). Уфа: Аэтерна, 2016. С. 64–67. Текст: непосредственный.

ENSURING THE SECURITY OF THE WEB APPLICATION. TOP 10 OWASP VULNERABILITIES.

Anna E. Konkova
Student,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: konkova@yandex.ru

Tatyana V. Nemchinova
Cand. Sci. (Education), A/Prof.,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: ntv05@mail.ru

Abstract. A vulnerability is a flaw in the system. Vulnerabilities can change the course of the program, increase user rights, and disclose confidential data. As a rule, they arise due to programming errors, flaws in the design of the system, weak passwords, etc. This article discusses issues related to the vulnerability of web applications. And reviewed the 10 most critical web application security threats.
Keywords: vulnerability, web application, personal data, service