МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ВСЕРОССИЙСКАЯ ГРУППА ТЕОРИИ ИНФОРМАЦИИ IEEE
АКАДЕМИЯ ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ООО «ОТКРЫТЫЕ РЕШЕНИЯ»
ОБЩЕСТВО «ЗНАНИЕ» РОССИИ
ПРИВОЛЖСКИЙ ДОМ ЗНАНИЙ

XXII Международная
научно-техническая конференция

ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ, УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ

Сборник статей

Декабрь 2022 г.

Пенза

УДК 004
ББК 32.81я43+74.263.2+65.050.2я43
П781

П781 **ПРОБЛЕМЫ ИНФОРМАТИКИ В ОБРАЗОВАНИИ, УПРАВЛЕНИИ, ЭКОНОМИКЕ И ТЕХНИКЕ :**
сборник статей XXII Международной научно-технической конференции. – Пенза: Приволжский Дом знаний, 2022. – 356 с.

ISBN 978-5-8356-1800-2
ISSN 2311-0406

Под редакцией ***В.И. Горбаченко,*** доктора технических наук, профессора;
В.В. Дрождина, кандидата технических наук, профессора

Информация об опубликованных статьях предоставлена в систему Российского индекса научного цитирования (РИНЦ) по договору № 573-03/2014К от 18.03.2014.

ISBN 978-5-8356-1800-2
ISSN 2311-0406

© Пензенский государственный университет, 2022
© АННМО «Приволжский Дом знаний», 2022

XXII International
scientific and technical conference

PROBLEMS OF INFORMATICS IN EDUCATION, MANAGEMENT, ECONOMICS AND TECHNICS

December, 2022

Penza

УДК 004.056

РИСКИ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ: НЕБЕЗОПАСНЫЙ ДИЗАЙН

Б. А. Галактионова, С. Н. Катков

WEB APP SECURITY RISKS: INSECURE DESIGN

B.A. Galaktionova, S.N. Katkov

Аннотация. Статья рассматривает вопросы безопасности веб-приложений. В статье делается акцент на новую категорию уязвимостей списка OWASP – небезопасный дизайн.

Ключевые слова: небезопасный дизайн, веб-приложение, веб-безопасность, веб-сайт, уязвимость, безопасность веб-приложений, киберугроза.

Abstract. The article examines the security issues of web applications. The article focuses on a new category of vulnerabilities in the OWASP list: insecure design.

Key words: insecure design, web application, web security, website, vulnerability, web application security, cyber threat.

Безопасность веб-приложений – это раздел информационной безопасности, который занимается безопасностью веб-сайтов, веб-прило-жений и веб-служб. Проблемы веб-безопасности приложений становятся все более актуальными, в связи с их возрастающей интерактивностью, усложняющегося поведения и поддержки новых протоколов [1]. Доля приложений, содержащих уязвимости высокой степени риска, составила 62% в 2021-м году, что значительно больше показателя 2019 года – 50% [4].

Классификацией векторов атак и уязвимостей занимается сообщество OWASP (Open Web Application Security Project) – международная некоммерческая организация, сосредоточенная на анализе и улучшении безопасности программного обеспечения [5, 7]. OWASP составил список из 10-и самых опасных уязвимостей, которым могут быть подвержены интернет-ресурсы [2, 5] (рис. 1).

В данной работе мы остановимся на новой категории угроз на 2021 год – небезопасном дизайне. Она посвящена рискам, связанным с проектными и архитектурными недостатками, с призывом шире использовать моделирование угроз, шаблоны безопасного проектирования и эталонные архитектуры.

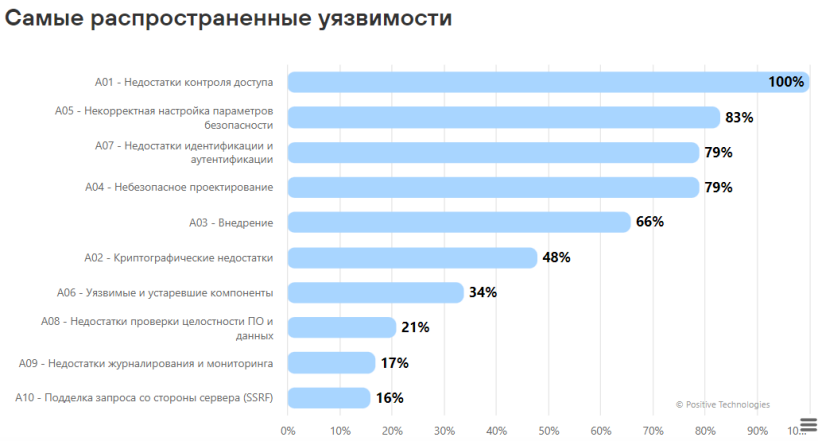

Рис. 1. Распределение уязвимостей по категориям
OWASP Top 10 – 2021 (доля приложений)

В среднем, данная уязвимость распространена на 42,51%, а максимум – на 77,25%. Общее количество встречаемости данной ошибки составляет 262,407 случаев на 2021 год.

Принцип «*Secure by Design*» подразумевает, что владелец сервиса стремится обеспечить безопасность на всех этапах производственного процесса – от идеи до вывода сервиса из эксплуатации. В противном случае, если дизайн является не стабильным еще на стадии планирования, приложение может быть не в состоянии противостоятьатакам и эксплойтам. Во избежание непредвиденных ситуаций, стоит изначально позаботиться о «фундаменте» веб-приложения. Это позволит на стадии «старт» обеспечить нужный уровень защиты и избежать значимых дефектов безопасности [3, 6, 7].

Стоит отметить, что не все риски категории «безопасный дизайн» устраняются успешной реализацией. Между этими понятиями есть существенная разница – разные первопричины и разные способы устранения. Безопасная реализация может иметь небезопасный дизайн, который по-прежнему делает веб-приложение уязвимым.

Но все же именно на ранних стадиях жизненного цикла разработки, планирования и проектирования, происходит основная работа над безопасным дизайном. Если мы ошибемся в самом начале, далее ошибку безопасности будет устранить сложнее, а в некоторых случаях невозможно.

Безопасный дизайн – это то, что гарантирует, что код надежно разработан и защищен от различных угроз.

Приведем наглядный пример небезопасного дизайна, который повлиял на репутацию американской технологической компании – Nvidia.

Nvidia – высокотехнологичная корпорация, разрабатывающая графические процессоры (GPU) и системы на чипе (SoC). Именно такая уязвимость, как небезопасный дизайн, в 2020 году не позволила пользователям ПК и геймерам приобрести новые графические процессоры Nvidia по рекомендованным розничным ценам. Компания не смогла справиться со спросом на свою продукцию, и многие клиенты остались ни с чем. Этим и воспользовались перекупщики.

В магазине было реализовано множество скрытых мер безопасности, которых оказалось недостаточно для описанного инцидента.

Данная компания не учла защиту своего сайта электронной торговли от ботов, которыми воспользовались спекулянты для массовой скупки видеокарт, которые изначально были ограничены.

После этого, злоумышленники перепродавали карты по завышенным ценам на аукционных сайтах. И для тех, кому действительно нужны были графические процессоры, пришлось выложить за GPU немалые суммы.

Для поддержки безопасности веб-приложения, важно знать и понимать каким угрозам и атакам может быть подвержено ваше программное обеспечение. Знание основ, позволяет тщательнее разработать приложение и корректное исправить уязвимости при их наличии. Достичь высокого уровня безопасности сложно, а поддерживать этот уровень защищённости – еще сложнее.

Библиографический список

1. Леонькова, И. П. Анализ методов обеспечения безопасности веб-приложений / И. П. Леонькова, А. И. Ларин. // Молодой ученый. – 2019. – № 12 (250). – С. 25-28.

2. OWASP Top Ten [Электронный ресурс]. – URL: https://owasp.org/www-project-top-ten/ (дата обращения: 02.11.2022.).

3. CWE [Электронный ресурс]. – URL: https://cwe.mitre.org/data/definitions/209.html (дата обращения: 05.11.2022.).

4. Positive Technologies. Уязвимости_и_угрозы_веб_приложений [Электронный ресурс]. – URL: https://www.ptsecurity.com/upload/corporate/ru ru/analytics/Уязвимости_и_угрозы_веб_приложений_A4_RUS_0004_02_JUL_06_2022.pdf (дата обращения: 05.11.2022.).

5. The OWASP Top 10 [Электронный ресурс]. – URL: https://www.hhs.gov/sites/default/files/owasp-top-10.pdf (дата обращения: 6.11.2022.).

6. Абрамова, Т. А. Актуальные угрозы безопасности веб-приложений и их характеристика / Т. А. Абрамова // Экономическое и социально-

политическое развитие России в условиях глобализации и цифровизации: сборник статей по материалам Международной научно-практической очной конференции. – Пенза: Пензенский государственный университет, 2022. – С. 7-12.

7. Абрамова, Т. А. Характеристики актуальных угроз безопасности веб-приложений / Т. А. Абрамова, С. Н. Катков, Д. А. Голдуева, А. Г. Петренко // Управление и экономика: исследование и разработка : сборник статей VI Международной научно-практической конференции. – Пенза: АННОО «Приволжский Дом знаний», 2021. – С. 131-135.

Галактионова Божена Андреевна
Катков Сергей Николаевич
Пензенский государственный университет,
г. Пенза, Россия

GalaktionovaB.A.
Katkov S.N.
PenzaStateUniversity,
Penza, Russia

УДК 004.7

СПОСОБЫ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ В ИНТЕРНЕТЕ

Р.Р. Гатин, В.В. Лебедев, Ю.Н. Матвеев

METHODS OF ANONYMITY ON THE INTERNET

R.R. Gatin, V.V. Lebedev, Y.N. Matveev

Аннотация. В статье рассматриваются способы, с помощью которых можно стать анонимным в Интернете.

Ключевые слова: прокси-сервер, сети Интернет, IP-адрес, идентификация, VPN.

Abstract. The article discusses the ways in which you can become anonymous on the Internet.

Key words: proxy server, internet networks, IP address, identification, VPN.

Каждый пользователь Интернета хоть раз задумывался о том, чтобы стать скрытным в сети. Анонимность в сети Интернет призвана обеспечить конфиденциальность, защиту персональных сведений, снижение контроля