Малявин М.Ю. Основные атаки и методы защиты в контексте обеспечения безопасности современных WEB-приложений // Международный журнал информационных технологий и энергоэффективности. – 2025. – Т. 10 № 3(53) с. 98–102

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ОСНОВНЫЕ АТАКИ И МЕТОДЫ ЗАЩИТЫ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ WEB-ПРИЛОЖЕНИЙ

Малявин М.Ю.
АНО ВО "МОСКОВСКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ - МОСКОВСКИЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ ИНСТИТУТ", Москва, Россия (109316, город Москва, Волгоградский пр-кт, д. 32 к. 11) e-mail: max-malyavin@bk.ru

В условиях стремительного развития веб-технологий и роста киберугроз обеспечение безопасности современных веб-приложений становится одной из приоритетных задач в сфере информационной безопасности. Цель данной статьи заключается в анализе и систематизации актуальных видов атак на веб-приложения, а также методов их предотвращения. В рамках исследования рассмотрены наиболее распространенные угрозы, а также систематизированы эффективные методы защиты. Ценность материалов работы заключается в возможности разработчикам и специалистам по информационной безопасности выбрать оптимальные стратегии и методы защиты веб-приложений. Предложенные в статье рекомендации могут быть использованы как основа для повышения уровня безопасности веб-систем и разработки более надежных приложений в условиях современных киберугроз.

Ключевые слова: Веб-разработка, веб-технологии, киберугроза, информационная безопасность.

THE MAIN ATTACKS AND METHODS OF PROTECTION IN THE CONTEXT OF ENSURING THE SECURITY OF MODERN WEB APPLICATIONS

Malyavin M.Yu.
MOSCOW UNIVERSITY OF HUMANITIES AND TECHNOLOGY - MOSCOW INSTITUTE OF ARCHITECTURE AND CIVIL ENGINEERING, Moscow, Russia (109316, Moscow, Volgogradsky prospekt, 32, bld. 11) e-mail: max-malyavin@bk.ru

In the context of the rapid development of web technologies and the growth of cyber threats, ensuring the security of modern web applications is becoming one of the priorities in the field of information security. The purpose of this article is to analyze and systematize current types of attacks on web applications, as well as methods to prevent them. The study examines the most common threats, as well as systematizes effective methods of protection. The value of the materials of the work lies in the opportunity for developers and information security specialists to choose the best strategies and methods for protecting web applications. The recommendations proposed in the article can used as a basis for improving the security of web systems and developing more reliable applications in the face of modern cyber threats.

Keywords: Web development, web technologies, cyber threat, information security, reliability, information security, vulnerability.

В последние годы веб-приложения становятся неотъемлемой частью цифровой экономики, обеспечивая работу множества сервисов, от электронной коммерции до государственных платформ. По данным аналитиков Market Research Future, по итогам 2024 года затраты на глобальном рынке веб-разработки достигли $57,31 млрд, что примерно на 5% больше, чем в 2023 году [1]. Такой рост свидетельствует о непрерывном развитии веб-

технологий и расширении их функциональности. Однако стремительное увеличение числа веб-приложений неизбежно приводит к росту киберугроз и делает информационную безопасность одним из ключевых вызовов. По результатам исследования BI.Zone, около 25% веб-уязвимостей, выявляемых ежемесячно, представляют высокий риск для кибербезопасности [2]. При этом, согласно их же отчетам, ежемесячно в мире обнаруживается порядка 1000 новых веб-уязвимостей, что демонстрирует сложность и динамичность угроз, с которыми сталкиваются разработчики и специалисты по информационной безопасности. В данных условиях эффективные методы защиты веб-приложений становятся критически важными. Организациям необходимо внедрять комплексные стратегии безопасности, учитывая актуальные виды атак и разрабатывая соответствующие защитные механизмы. Рассмотрение этих аспектов в рамках статьи позволит систематизировать угрозы и предложить наиболее действенные подходы к обеспечению надежной защиты современных веб-систем.

Итак, на фоне стремительного роста цифровизации и увеличения числа веб-приложений актуальность кибератак продолжает возрастать. Как отмечают П. Байраммырадов, Ш. Довлетназаров Ш. и Г. Гарягдыева, злоумышленники совершенствуют свои методы, используя уязвимости в веб-инфраструктуре для компрометации данных, финансовых потерь и нарушения работы сервисов [3]. Среди наиболее актуальных атак в 2025 году автором настоящей статьи выделяются следующие:

- SQL-инъекции (SQLi) – один из старейших, но по-прежнему эффективных способов атаки, позволяющий злоумышленникам получить несанкционированный доступ к базе данных через уязвимые запросы;
- XSS (межсайтовый скриптинг) – позволяет внедрять вредоносный код на веб-страницы, что ведет к краже данных пользователей или компрометации учетных записей;
- CSRF (межсайтовая подделка запросов) – эксплуатирует доверие веб-приложения к аутентифицированным пользователям, заставляя их неосознанно выполнять вредоносные действия;
- Credential Stuffing – атака, основанная на переборе украденных учетных данных с целью компрометации аккаунтов;
- Server-Side Request Forgery (SSRF) – позволяет атакующим отправлять произвольные запросы от имени веб-сервера, получая доступ к внутренним системам;
- Zero-Day-атаки – использование неизвестных уязвимостей до выпуска соответствующих исправлений, что делает их крайне опасными;
- DDoS-атаки – перегрузка серверов веб-приложения огромным количеством запросов, приводящая к отказу в обслуживании. Согласно Cloud Networks, в 2024 году количество DDoS-атак в России увеличилось на 32% по сравнению с 2023 годом, что подчеркивает их возрастающую угрозу [4].

С учетом постоянно меняющихся угроз и усложняющихся методов атак для защиты веб-приложений необходимо применять комплексный подход. Основные методы защиты включают: Web Application Firewall (WAF – фильтрация трафика для блокировки вредоносных запросов); контроль ввода данных (строгая валидация и экранирование пользовательского ввода для предотвращения SQL-инъекций и XSS-атак); многофакторная аутентификация

(MFA – защита от атак на учетные записи); защита от ботов и CAPTCHA (предотвращение автоматизированных атак, таких как Credential Stuffing); Rate Limiting и защита от DDoS (ограничение количества запросов для снижения нагрузки); журналирование и мониторинг (выявление подозрительной активности и предотвращение атак); обновление и патчинг ПО (минимизация риска эксплуатации уязвимостей Zero-Day).

С учетом представленных данных автором разработана Таблица 1, в которой систематизированы основные атаки на веб-приложения, соответствующие методы защиты, особенности их реализации и потенциальная эффективность. Данный анализ позволяет определить оптимальные стратегии безопасности в зависимости от типа угроз. Также в последнем столбце автором отражена потенциальная оценка эффективности каждого метода защиты при его корректном внедрении, основанная на экспертных данных, результатах тестирований и статистике выявленных атак. При этом, как отмечают М.М. Путято, А.С. Макарян, В.В. Лещенко и В.О. Немчинова, применение данных методов защиты в комплексе позволит значительно повысить уровень безопасности современных веб-приложений, снижая риски атак и сводя к абсолютному минимуму их последствия [5].

Таблица 1 - Рекомендации по применению методов защиты

№ п\ п	**Атака**	**Метод защиты**	**Особенности реализации**	**Эффективность**
1.	SQL-инъекция (SQLi)	Контроль ввода данных, WAF	Использование параметризованных запросов	95%
2.	XSS	Валидация и экранирование данных	Применение Content Security Policy (CSP)	90%
3.	CSRF	CSRF-токены, SameSite cookies	Генерация уникальных токенов для запросов	88%
4.	Credential Stuffing	MFA, защита от ботов	Ограничение количества неудачных входов	92%
5.	SSRF	Ограничение исходящих запросов	Использование allow/deny-листов адресов	85%
6.	Zero-Day-атаки	Обновления и мониторинг	Автоматизированное сканирование уязвимостей	80%
7.	DDoS-атака	Rate Limiting, WAF, защита на уровне CDN	Использование облачных решений для фильтрации трафика	93%

В результате проведенного исследования установлено, что обеспечение безопасности веб-приложений в 2025 году требует комплексного подхода, учитывающего не только известные угрозы, но и динамически изменяющийся ландшафт кибератак. Анализ актуальных данных и статистики показал, что увеличение числа веб-уязвимостей и рост атак, таких как SQL-инъекции, XSS, CSRF, а также усиление DDoS-атак, создают серьезные вызовы для разработчиков и специалистов по информационной безопасности. Систематизация методов

защиты позволяет определить наиболее эффективные стратегии противодействия различным видам атак. Так, например, использование параметризованных запросов практически полностью исключает риск SQL-инъекций, а CSP в сочетании с валидацией входных данных значительно снижает вероятность XSS-атак. Однако даже высокая эффективность отдельных решений не отменяет необходимости комплексного подхода, включающего постоянное обновление систем, мониторинг угроз и применение проактивных механизмов защиты.

По мнению автора настоящей статьи, наибольшую опасность представляют атаки, направленные на эксплуатацию уязвимостей нулевого дня, а также автоматизированные атаки, такие как подбор учетных данных (Credential Stuffing). В этих условиях повышается значимость таких механизмов, как многофакторная аутентификация, защита API и использование искусственного интеллекта для обнаружения аномального поведения. В перспективе киберугрозы будут становиться более сложными, что потребует не только технологических решений, но и повышения осведомленности разработчиков, пользователей и специалистов по информационной безопасности [6]. Исходя из этого, защита веб-приложений должна рассматриваться как непрерывный процесс, включающий анализ новых угроз, адаптацию существующих механизмов безопасности и использование интегрированных решений для минимизации рисков.

Список литературы

1. Веб-разработка (мировой рынок). Электронный ресурс. Режим доступа: https://www.tadviser.ru/index.php/Статья:Веб-разработка_(мировой_рынок) (дата обращения 17.02.2025 г.).
2. Безопасность веб-приложений. Электронный ресурс. Режим доступа: https://www.tadviser.ru/index.php/Статья:Безопасность_веб-приложений (дата обращения 17.02.2025 г.).
3. Байраммырадов П., Довлетназаров Ш., Гарягдыева Г. Атаки на веб-приложения: уязвимости и способы защиты // Вестник науки. 2024. №10 (79). С. 835-838.
4. Обзор крупнейших киберинцидентов 2024 года. Электронный ресурс. Режим доступа: https://cloudnetworks.ru/analitika/obzor-krupnejshih-kiberintsidentov-2024-goda/ (дата обращения 17.02.2025 г.).
5. Путято М.М., Макарян А.С., Лещенко В.В., Немчинова В.О. Анализ типовых уязвимостей при построении веб-приложений // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2022. №3 (306). С. 77-85.
6. Шутько Н. А. Теоретические понятия защиты web-приложений от уязвимостей // Вестник науки. 2022. №11 (56). С. 253-269.

References

1. Web development (global market). An electronic resource. Access mode: https://www.tadviser.ru/index.php/Статья:Web development_(global market) (date of issue 17.02.2025).
2. Web application security. An electronic resource. Access mode: https://www.tadviser.ru/index.php/Статья:Security of web applications (accessed 17.02.2025).

3. Bayrammyradov P., Dovetnazarov Sh., Garyagdieva G. Attacks on web applications: vulnerabilities and protection methods // Bulletin of Science. 2024. No. 10 (79). pp. 835-838.
4. An overview of the largest cyber incidents in 2024. An electronic resource. Access mode: https://cloudnetworks.ru/analitika/obzor-krupnejshih-kiberintsidentov-2024-goda / (accessed 17.02.2025).
5. Putyato M.M., Makaryan A.S., Leshchenko V.V., Nemchinova V.O. Analysis of typical vulnerabilities in building web applications // Bulletin of the Adygea State University. Series 4: Natural, mathematical and technical sciences. 2022. No. 3 (306). pp. 77-85.
6. Shutko N. A. Theoretical concepts of web application vulnerability protection // Bulletin of Science. 2022. No. 11 (56). pp. 253-269.