УДК 004.056.5 URL: https://ptsj.bmstu.ru/catalog/icec/insec/1041.html

БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

В.А. Бубнович bubnovichva@student.bmstu.ru
Е.В. Глинская glinskaya@bmstu.ru
SPIN-код: 5430-3023

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Представлены результаты исследования по улучшению защиты веб-приложений от ключевых угроз, таких как SQL-инъекции, межсайтовый скриптинг (XSS), DDoS-атаки и уязвимости API. Разработан многоуровневый подход к обеспечению безопасности, который включает как профилактические меры (валидация данных, ограничение прав доступа), так и активные механизмы защиты (системы предотвращения вторжений, пенет-тесты). Внедрение этих мер в жизненный цикл разработки приложений позволило снизить количество уязвимостей и повысить устойчивость приложений к современным кибератакам. Практическое применение методологии OWASP и тестирование защиты API подтвердили эффективность предложенных решений в условиях реальной эксплуатации.

Ключевые слова: защита данных, информационная безопасность, веб-приложения, киберпреступность, уязвимости API, XSS-атаки, DDoS-атаки

Введение. Безопасность веб-приложений — одна из ключевых задач в современном мире. Веб-приложения являются привлекательной целью для киберпреступников, стремящихся получить доступ к конфиденциальной информации или нарушить работу приложений. Основные угрозы, такие как SQL-инъекции и межсайтовый скриптинг (XSS), позволяют злоумышленникам использовать уязвимости в коде приложений для внедрения вредоносного кода и получения несанкционированного доступа к данным [1].

SQL-инъекции являются одной из самых опасных уязвимостей, поскольку они позволяют злоумышленникам манипулировать базами данных через ввод вредоносных запросов [2]. В свою очередь, XSS-атаки дают возможность злоумышленникам внедрять вредоносные скрипты, которые выполняются в браузерах пользователей и могут привести к краже их данных, нарушению функциональности приложения или другим негативным последствиям [3].

Также нельзя не упомянуть DDoS-атаки, которые представляют собой попытки перегрузить сервер веб-приложения, делая его недоступным для пользователей [4]. Для защиты от подобных атак современные компании внедряют системы предотвращения вторжений (IPS), которые позволяют

 ISSN 2541-8009

оперативно реагировать на подозрительный трафик и предотвращать блокировку серверов [5].

Уязвимости веб-приложений. Одной из главных уязвимостей, с которой сталкиваются современные веб-приложения, является SQL-инъекция. Атаки этого типа позволяют злоумышленникам манипулировать базами данных, внедряя вредоносные SQL-запросы через пользовательские формы ввода данных. Такие инъекции могут привести к утечке конфиденциальной информации, изменению или удалению данных, а также к нарушению работы системы [1, 2].

SQL-инъекции возникают из-за недостаточной проверки пользовательских данных и неправильной обработки входных данных. Чтобы предотвратить подобные атаки, разработчики должны применять методы валидации данных, ограничение прав доступа и внедрение безопасных методов взаимодействия с базами данных, таких как подготовленные выражения (prepared statements). Также рекомендуется проводить регулярные аудиты безопасности и тестирование на проникновение, что позволит выявить уязвимости до их эксплуатации злоумышленниками [6, 5].

Еще одной серьезной угрозой для веб-приложений служит межсайтовый скриптинг (XSS). Атаки этого типа позволяют злоумышленникам внедрять вредоносные скрипты на страницы веб-сайтов, которые затем выполняются в браузерах пользователей. XSS-атаки могут привести к краже данных пользователей, изменению содержимого страницы или к распространению вредоносного кода [3, 7].

Для защиты от XSS-атак необходимо правильно обрабатывать и фильтровать пользовательские данные, а также использовать механизмы ограничения доступа, такие как Content Security Policy (CSP). CSP позволяет ограничить выполнение непроверенного контента на веб-странице, что значительно снижает риск успешной XSS-атаки [8].

Защита веб-приложений. Один из наиболее эффективных методов защиты веб-приложений — использование систем предотвращения вторжений (IPS). Эти системы анализируют сетевой трафик в реальном времени и способны блокировать попытки атак, таких как DDoS и XSS. IPS также можно использовать для защиты от других типов атак, например, от попыток эксплуатации уязвимостей в коде или сетевой инфраструктуре [4, 5].

Системы предотвращения вторжений интегрируются в сетевую архитектуру приложения и обеспечивают автоматическую реакцию на подозрительную активность, что позволяет снизить риск возникновения критических инцидентов. Однако отметим, что IPS являются лишь частью комплексной стратегии безопасности, которая должна включать в себя регулярное тести-

рование на проникновение, обновление систем безопасности и мониторинг активности [6].

Тестирование на проникновение (пенет-тесты) — один из ключевых элементов обеспечения безопасности веб-приложений. Пенет-тесты позволяют выявить уязвимости на ранней стадии, оценить возможные сценарии атак и предложить меры по их устранению. Использование специализированных инструментов для тестирования, таких как OWASP ZAP и Acunetix, помогает разработчикам оперативно выявлять и устранять угрозы [2, 6].

Современные подходы к защите. Одной из современных тенденций в области безопасности веб-приложений является внедрение защитных механизмов уже на этапе разработки. Такие подходы, как DevSecOps, позволяют интегрировать меры безопасности в жизненный цикл разработки приложений, что позволяет уменьшить количество уязвимостей и повысить общую безопасность продукта [1].

В рамках подхода DevSecOps важным элементом служит автоматизация процессов тестирования и мониторинга. Это позволяет быстро выявлять и устранять уязвимости на всех этапах разработки, начиная с проектирования и заканчивая эксплуатацией приложения. Интеграция таких решений, как CI/CD (continuous integration/continuous delivery), с механизмами тестирования безопасности позволяет создавать приложения, которые изначально устойчивы к кибератакам [4, 9].

Безопасность API. С развитием веб-приложений и широким использованием API защита API стала важной частью общей безопасности. API позволяют приложениям взаимодействовать с внешними сервисами, но это открывает дополнительные уязвимости. Основные угрозы для API включают нарушение авторизации объектов, аутентификации, чрезмерное раскрытие данных и инъекции [10].

Для защиты API необходимо использовать строгие политики авторизации, аутентификации и ограничения доступа. Тестирование API на уязвимости с помощью таких инструментов, как пенет-тесты, помогает своевременно выявлять и устранять угрозы [10].

Заключение. В ходе исследования были изучены основные угрозы для веб-приложений, включая SQL-инъекции, XSS, DDoS-атаки и уязвимости API. Предложен многоуровневый подход к обеспечению безопасности, включающий как профилактические меры, так и активные механизмы защиты. Интеграция безопасности на этапе разработки, особенно с использованием методологии DevSecOps, показала свою эффективность в снижении количества уязвимостей и повышении устойчивости к атакам.

 ISSN 2541-8009

Достигнутый эффект заключается в углублении знаний в области защиты веб-приложений с акцентом на API Security. Практическое подтверждение предлагаемых решений основано на применении OWASP API Security Project и успешном тестировании предложенных мер защиты в реальных условиях.

Литература

[1] Шеркунов А.В. Безопасность веб-приложений. *Modern scientific research. II Междунар. науч.-практ. конф.: сб. ст.* Пенза, Наука и Просвещение (ИП Гуляев Г.Ю.), 2023, с. 101–103.

[2] Mungfaridah R., Riadi I. Web Server Security Analysis against Cross Site Scripting (XSS) Attacks using Penetration Testing. *International Journal of Computer Applications*, 2022, vol. 184, no. 30, pp. 45–52.

[3] Alsaffar M., Aljaloud S., Mohammed B.A., Al-Mekhlafi Z.G., Almurayziq T.S., Alshammari G., Alshammari A. Detection of Web Cross-Site Scripting (XSS) Attacks. *Electronics*, 2022, vol. 11, no. 14, art. no. 2212.

[4] Surbakti K.J., Tulloh R., Djibran M.N. Implementasi Anti-DDOS Menggunakan Intrusion Prevention System (IPS) terhadap Serangan DDOS. *Jurnal Informatika Universitas Pamulang*, 2023, vol. 8, no. 2, pp. 330–340.

[5] Patil N.V., Krishna C.R., Kumar K. KS-DDoS: Kafka streams-based classification approach for DDoS attacks. *The Journal of Supercomputing*, 2022, vol. 78, no. 6, pp. 8946–8976.

[6] Gandikota P.S.S.K., Valluri D., Mundru S.B., Yanala G.K., Sushaini S. Web Application Security through Comprehensive Vulnerability Assessment. *Procedia Computer Science*, 2023, vol. 230, pp. 168–182.

[7] Таволжанский А.В. Безопасность веб-приложений: лучшие практики и уязвимости. *Индустрия 1С. II регион. науч.-практ. конф.: сб. ст.* Брянск, Брянский гос. инж.-технол. ун-т, 2023, с. 342–346.

[8] Senkiv D.A. Audit as a Means of Ensuring Information Security of Web Applications and Used Computer Systems. *American Scientific Journal*, 2020, vol. 40–2 (40), pp. 54–57.

[9] Aladi C.C. Web Application Security: A Pragmatic Exposé. *Digital Threats: Research and Practice*, 2024, vol. 5 (2). https://doi.org/10.1145/3644394

[10] Idris M., Syarif I., Winarno I. Web Application Security Education Platform Based on OWASP API Security Project. *Emitter: International Journal of Engineering Technology*, 2022, pp. 246–261. https://doi.org/10.24003/emitter.v10i2.705

Поступила в редакцию 20.11.2024

Бубнович Виктория Андреевна — студентка кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Глинская Елена Вячеславовна — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Басараб Михаил Алексеевич, доктор физико-математических наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Бубнович В.А., Глинская Е.В. Безопасность веб-приложений. *Политехнический молодежный журнал*, 2025, № 3 (98). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1041.html

 ISSN 2541-8009

SECURITY IN THE WEB APPLICATIONS

V.A. Bubnovich bubnovichva@student.bmstu.ru
E.V. Glinskaya glinskaya@bmstu.ru
SPIN-code: 5430-3023

Bauman Moscow State Technical University, Moscow, Russian Federation

The article presents results of studying approaches to improve protection of the web applications from the key threats. Such threads include the SQL injections, cross-site scripting (XSS), DDoS attacks, and the API vulnerabilities. The paper proposes a developed multi-level approach to ensuring security, which includes both the prevention measures (data validation, access right limitation), and the active protection mechanisms (intrusion prevention systems, penetration tests). Introduction of these measures in the life cycle applications development makes it possible to reduce the number of vulnerabilities and increase applications resilience to the cyberattacks underway. Practical introduction of the OWASP methodology and the API security testing confirm efficiency of the proposed solutions in the real-life operation conditions.

Keywords: data protection, information security, web applications, cybercrime, API vulnerabilities, XSS attacks, DDoS attacks

Received 20.11.2024

Bubnovich V.A. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Glinskaya E.V. — Senior Lecturer, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Basarab M.A., Dr. Sci. (Phys.-Math.), Head of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Bubnovich V.A., Glinskaya E.V. Security in the Web applications. *Politekhnicheskiy molodezhnyy zhurnal*, 2025, no. 3 (98). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1041.html

