Анализ актуальных угроз и разработка подходов к защите веб - приложений

М.В. Шатурный

Финансовый университет при Правительстве Российской Федерации, Москва

Аннотация: В статье проведен анализ актуальных угроз и уязвимостей веб - приложений. На основании анализа предложены подходы к защите и рекомендации по обеспечению безопасности веб – приложений, учитывающие актуальные вызовы и проблемы. Статья может быть полезна специалистам по информационной безопасности, разработчикам программного обеспечения и руководителям организаций, заинтересованным в безопасности разрабатываемых или используемых веб – приложений.
Ключевые слова: киберугроза, кибератака, эксплуатация веб – уязвимостей, веб –приложение.

Введение

Современные веб – приложения получили широкое распространение и являются важным инструментом для бизнеса, обеспечивая взаимодействие с клиентами предоставляя доступ к различным сервисам. Также веб – приложения активно используются и в государственном секторе. По этой причине веб-приложения являются одной из главных целей киберпреступников. В связи с ускоренным развитием цифровой индустрии растет сложность веб – ресурсов, увеличивается объем обрабатываемых ими данных, разрабатываются и используются новые технологии. Вместе с тем, эволюционируют и киберугрозы, появляются новые уязвимости.

Согласно исследованиям компании Positive Technologies по итогам IV квартала 2023 года, количество атак на веб-приложения продолжает оставаться на лидирующих позициях в рейтингах [1]. К негативным последствиям атак на веб - приложения можно отнести: похищение пользовательских данных, недоступность ресурса, репутационный ущерб, ущерб, вызванный нарушением законодательных требований. Кроме того, веб – приложение может оказаться точкой входа во внутреннюю сетевую инфраструктуру организации, что создает риски последствий намного

большего масштаба. Поэтому развитие средств и мер защиты веб – ресурсов являются важной и актуальной задачей.

Цель исследования – анализ актуальных угроз и уязвимостей веб – приложений. Предложение компенсирующих мер и рекомендаций по обеспечению безопасности веб – ресурсов с учетом проведенного анализа.

Анализ угроз безопасности веб - приложений

По данным Positive technologies, за первые три квартала 2023 г. было выявлено на 44% больше атак на веб – приложения, чем в за весь 2022 г. Кроме того, отмечается, что злоумышленники активно применяют технику двойного вымогательства (заключается в получении выкупа и от организации, и от ее клиентов) [2].

По данным исследователей ReliaQuest, наиболее распространенные классы уязвимостей, эксплуатируемые киберпреступниками: повышение привилегий (26%), контроля доступа (13%), удаленное выполнения кода (13%) [3].

Рис. 1. Распространенные уязвимости 2023 г. [3]

К наиболее опасным уязвимостям веб-приложений, открытым и проэксплуатированным в 2023 году, можно отнести следующие:

- CVE-2023-0669. Небезопасная сериализация данных в продукте в GoAnywhere MFT.

- CVE-2023-34362. Уязвимость заключается во внедрении вредоносного SQL-кода в программное обеспечение MOVEit Transfer.

-CVE-2023-28121. Уязвимость заключается в получении привилегий, вплоть до администраторских в продукте WooCommerce Payments.

-CVE-2023-42793. Уязвимость заключается в обходе аутентификации в платформе TeamCity.

Наиболее резонансные веб-атаки 2023 года, повлекшие серьезные последствия:

- DDoS-атаки на веб-порталы Outlook, OneDrive и Azure компании Microsoft. Результат: нарушения функционирования облачных сервисов.

-DDoS-атаки на Amazon Web Services, Cloudflare и Google. Все атаки были отражены и оказались рекордными по количеству запросов в секунду.

-Атака на компанию JumpCloud методом целевого фишинга. Результат: похищение данных клиентов.

В 2023 году общее количество DDoS атак на веб приложения в России аналогично мировой тенденции выросло. Особенностью стало применение смешанных ботнетов, причем с российских серверов для обхода блокировок по GEOIP. Наблюдается трэнд на рост числа атак целью которых является остановка основной деятельности организации [4]. Наиболее активно атаковались следующие отрасли: государственный сектор (в том числе, критическая инфраструктура), финансовая и транспортная отрасли.

Российскими специалистами в области кибербезопасности выявлена новая уязвимость:

- BDU:2023-05857. Уязвимость в «1С-Битрикс: Управление сайтом» заключается в выполнении команд на сервере.

Наиболее резонансные кибератаки на российские веб приложения в 2023 году:

- Атака на CMS Bitrix. Результат: замена главной страницы сайта.

- Атака на приложение ОАО «РЖД». Результат: недоступность ресурса в течение двух дней.

Отмечены также массовые утечки данных с различных сайтов, причем в результате атак даже на небольшие компании.

Телекоммуникационные организации также привлекают внимание злоумышленников по причине обработки важных клиентские данные, такие как платежная информация и персональные данные

В соответствии с проведенным анализом атак на веб - приложения компанией «Вебмониторэкс» за 2023 год, наиболее частыми атаками на телеком являлись удалённое выполнение кода (RCE), межсайтовый скриптинг (XSS), превышение лимита ресурсов [5].

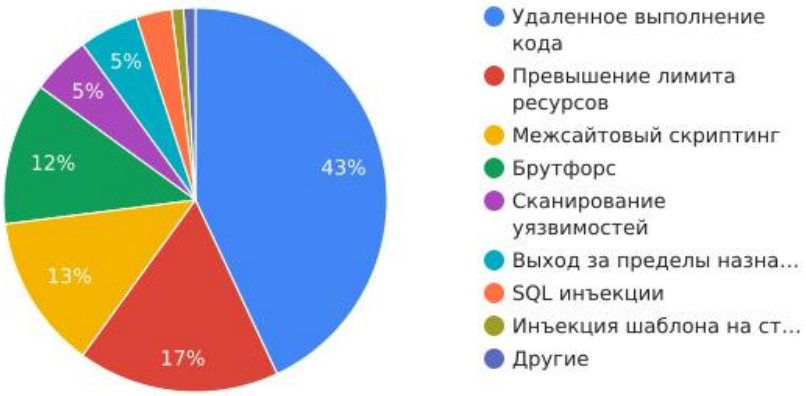

Рис. 2. Распространенные атаки на телекоммуникационные компании в 2023 г. [5].

К наиболее значимым проблемным вопросам применительно к безопасности веб – ресурсов можно отнести:

- большое количество уязвимостей в Open Source библиотеках (в частности Python и PHP) используемые в атаках на цепочку поставок [6];

- снижение порога входа в киберпреступность, обусловленный ростом рынка ресурсов по обучению кибератакам, количества вредоносного программного обеспечения, рассчитанного на относительно низкий уровень злоумышленника и применением ИИ [7];

- кадровый голод в отрасли информационной безопасности в целом и в области безопасности веб – приложений в частности [8];

- появление новых уязвимостей в связи с активным импортозамещением зарубежных программных продуктов [9];

- рост хактивизма [10], обусловленный геополитической обстановкой;

- снижение эффективности блокировки по IP, в связи с тем, что многие атаки на российские компании осуществлялись с серверов внутри страны [11];

- использование при кибератаках смешанных ботнетов. Особенность заключается в использовании нескольких вредоносных программ, что делает данные ботнеты универсальными. Данный инструмент появился недавно, поэтому у многих компаний отсутствуют соответствующие средства защиты [12].

Подходы к обеспечению безопасности веб – приложений с учетом актуальных тенденций

Анализ угроз последних лет демонстрирует непрерывный рост числа кибератак на веб – приложения, применение более изощренных техник, активное использование искусственного интеллекта нападающей стороной, снижение порога входа в киберпреступность, увеличение активности

хактивистов, политическую мотивированность атак. Отвечая требованиям рынка, веб – приложения увеличивают свою функциональность, применяя новые технологии и становясь более сложными, что неизбежно приводит к появлению новых уязвимостей. В связи с этим, методы обеспечения безопасности также должны совершенствоваться, учитывая новые трэнды и технологии.

Исходя из исследования веб - угроз и проблем безопасности 2023 года, можно выделить следующие подходы к защите веб – приложений:

1. Безопасная разработка. Применение практики безопасной разработки начинается с повышения осведомленности разработчиков ПО в вопросах актуальных уязвимостей и политики безопасности, принятой в организации. Важным аспектом является коммуникация между разработчиками ПО и специалистами по информационной безопасности. Для разрабатываемого продукта необходимо создать модель угроз и проанализировать риски информационной безопасности. Технические меры должны включать: проведение статического и динамического анализа кода на уязвимости, анализ Open Source библиотек, анализ компонентов ПО, анализ защищенности контейнеров, тестирование приложения при его развертывании, настройку и эксплуатацию межсетевого экрана уровня приложений.

2. Комплексная эшелонированная защита. Эшелонированный подход к защите подразумевает разделение информационной системы организации на уровни (эшелоны) для каждого из которых используются свои защитные средства и меры. В общем случае может состоять из следующих элементов:

- применение механизмов защиты веб – приложения на этапе его создания (с учетом уязвимостей и распространенных атак);
- защита сервера (-ов), на котором развернуто веб – приложение;

- межсетевой экран уровня приложений, его настройка и эксплуатация (адаптация с учетом выпуска релизов);

- средство защиты от DDoS;

- защита сетевой инфраструктуры (межсетевой экран, система обнаружения вторжений, отключение неиспользуемых портов, служб и тд.);

- защита «последней мили» со стороны поставщиков услуг связи;

- защита со стороны поставщиков облачных сервисов.

3. Участие в программах багбаунти (bug bounty). Российский рынок на данный момент представлен 3 платформами, реализующими данную программу: «Синклит» — «Киберполигон», «BI.ZONE Bug Bounty», и «Standoff 365 Bug Bounty».

4. Применение искусственного интеллекта. Проблему кадрового голода, наблюдаемого в отрасли кибербезасности может частично компенсировать использование искусственного интеллекта. Примером может служить автоматизация рутинных задач: определение отклонений в пользовательском поведении, рекомендательный ассистент, поиск взаимосвязей между разными событиями, определение контента, сгенерированного искусственным интеллектом.

5. Обмен данными об угрозах между организациями. В связи с возможным репутационным ущербом среди российских компаний, равно как и среди мировых не принято публично заявлять о произошедших у них инцидентах информационной безопасности. Подобного рода информация очень важна и может помочь другим компаниям быть готовыми к аналогичным инцидентам. Первым к данной коммуникации стало появление нового блока «Кейсы взломов» на прошедшей в 2023 г. конференции SOC Forum.

6. Шаблонизация решения по защите веб – приложений. Учет специфики деятельности организации и создание шаблонных решений по

обеспечению безопасности позволит увеличить оперативность реализации проектов для заказчиков.

Актуальным остается вопрос защиты веб – приложений от DDoS атак, в том числе с использованием смешанных ботнетов, а также развитие соответствующих средств и сервисов (аналог Cloudflare) по обеспечению данной защиты.

При менее глобальном подходе к результатам анализа киберугроз, можно дать следующие рекомендации по защите веб – приложений в современных реалиях:

- установка системы защиты от атак ботов непосредственно перед межсетевым экраном уровня приложений для снижения нагрузки на WAF;
- защита смежных ресурсов организации (мобильная версия сайта);
- оценка устойчивости веб – приложения к высоким нагрузкам;
- соблюдение политики информационной безопасности партнерами организации;
- включение модификации системы защиты в релизный цикл веб – приложения.

Заключение

Необходимо отметить важность развития средств, способов и мер защиты в соответствии с существующими, а возможно, и с будущими вызовами безопасности веб – ресурсов. Рекомендуется использовать разные базы данных с общеизвестными уязвимостями: BDU ФСТЭК, CVE MITRE, NVD NIST, а также данные из других источников. Ключевым аспектом является безопасная разработка, поскольку многие уязвимости закрываются еще на этом этапе. Это, в конечном счете, влияет на стоимость и эффективность системы защиты.

В работе исследованы современные проблемы безопасности веб – приложений, актуальные и наиболее эксплуатируемые уязвимости и методы их эксплуатации, а также предложены подходы и рекомендации по повышению уровня защищенности.

Литература

1. Positive Technologies Актуальные киберугрозы: IV квартал 2023 год. URL: ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/ (дата обращения 11.04.2024).

2. Positive Technologies Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть третья. URL: ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/ (дата обращения 13.04.2024).

3. 2023 Vulnerabilities: First-Quarter Highlights. URL: reliaquest.com/blog/2023-q1-vulnerabilities-cves/ (дата обращения 23.04.2024).

4. Защита веб-приложений в 2024 году. URL: anti-malware.ru/analytics/Threats_Analysis/Web-Apps-Security-AMLive-2024#part23 (дата обращения 26.04.2024).

5. Anti-Malware Атаки на веб-приложения в 2023 году: анализ действий злоумышленников. URL: anti-malware.ru/analytics/Threats_Analysis/Web-Application-Attack-2023 (дата обращения 30.04.2024).

6. Мыльников В. А. Автоматизация процессов поиска уязвимостей в исходном коде на этапе разработки программного приложения //Завалишинские чтения 23. – 2023. – С. 51-54.

7. Шаосюе Цзя Обзор правового регулирования сервисов генеративного искусственного интеллекта в Китае // Юридическая наука и практика. – 2024. – Т. 19. – №. 4. – С. 53-62.

8. Лившиц И. И. Проблемы подготовки специалистов в области информационной безопасности // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51. – №. 1. – С. 123-131.

9. Гайдукова М.О., Шушунова Т.Н. Проблемы импортозамещения программного обеспечения цифровой трансформации промышленных производств и поиск их оптимальных решений // Успехи в химии и химической технологии. Т. 36. 2022. № 1. – С. 20-22.

10. Кручковский К. С., Хакимов А. Ш., Петров И. П. Актуальные веб-уязвимости и способы защиты от них // Математическое и информационное моделирование: материалы Всероссийской конференции молодых ученых. Вып. 21. –Тюмень, 2023. – ТюмГУ-Press, 2023. – С. 357-365.

11. Отчет об атаках на онлайн-ресурсы российских компаний в 2023 году. URL: rt-solar.ru/analytics/reports/4113/ (дата обращения 21.04.2024).

12. Отчет о DDoS-атаках за третий квартал 2023 от StormWall. URL: stormwall.pro/otchet-o-ddos-atakah-2023-tretij-kvartal (дата обращения 26.04.2024).

References

1. Positive Technologies Aktual`ny`e kiberugrozy`: IV kvartal 2023 god. [Positive Technologies Actual cyber threats: IV quarter of 2023]. URL: ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/ (accessed 11.04.2024).

2. Positive Technologies Kiberbezopasnost` v 2023 2024 g.: trendy` i prognozy`. Chast` tret`ya. [Positive Technologies Cybersecurity in 2023–2024: trends and forecasts. The third part]. URL: ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/ (accessed 13.04.2024).

3. 2023 Vulnerabilities: First-Quarter Highlights. URL: reliaquest.com/blog/2023-q1-vulnerabilities-cves/ (accessed 23.04.2024).

4. Zashhita veb-prilozhenij v 2024 godu. [Web application protection in 2024]. URL: anti-malware.ru/analytics/Threats_Analysis/Web-Apps-Security-AMLive-2024#part23 (accessed 26.04.2024).

5. Anti-Malware Ataki na veb-prilozheniya v 2023 godu: analiz dejstvij zloumy`shlennikov. [Anti-Malware Attacks on web applications in 2023: an analysis of the actions of intruders]. URL: anti-malware.ru/analytics/Threats_Analysis/Web-Application-Attack-2023 (accessed 30.04.2024).

6. My`l`nikov V. A. Zavalishinskie chteniya 23. 2023. pp. 51-54.

7. Shaosyue Czzya Yuridicheskaya nauka i praktika. 2024. V. 19. №. 4. pp. 53- 62.

8. Livshicz I. I. Vestnik Dagestanskogo gosudarstvennogo texnicheskogo universiteta. Texnicheskie nauki. 2024. V. 51. №. 1. pp. 123-131.

9. Gajdukova M.O., Shushunova T.N. Uspexi v ximii i ximicheskoj texnologii V. 36. 2022. № 1. pp. 20-22.

10. Kruchkovskij K. S., Xakimov A. Sh., Petrov I. P. Aktual`ny`e veb-uyazvimosti i sposoby` zashhity` ot nix [Current web vulnerabilities and ways to protect against them], Matematicheskoe i informacionnoe modelirovanie: materialy` Vserossijskoj konferencii molody`x ucheny`. Rel. 21. Tyumen, 2023. TyumSU-Press, 2023. pp. 357 – 365.

11. Otchet ob atakax na onlajn-resursy` rossijskix kompanij v 2023 godu. [Report on attacks on online resources of Russian companies in 2023]. URL: rt-solar.ru/analytics/reports/4113/ (accessed 21.04.2024).

12. Otchet o DDoS-atakax za tretij kvartal 2023 ot StormWall. [DDoS Attacks Report for the third quarter of 2023 from StormWall].

URL: stormwall.pro/otchet-o-ddos-atakah-2023-tretij-kvartal (accessed 26.04.2024).

Дата поступления: 20.05.2024

Дата публикации: 11.07.2024