УДК 004.056.53

ЭВОЛЮЦИЯ УГРОЗ И УЯЗВИМОСТЕЙ WEB-САЙТОВ

Р.А. Божко[1], Т.А. Пулко[2]
[1]*Учреждение образования «Белорусская государственная академия связи», Минск, Беларусь*
[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

Аннотация. Уязвимости в безопасности всегда являются актуальной проблемой, на исследование которой администраторы веб-сайтов тратят много времени в целях обеспечения безопасности их работы. Эти уязвимости позволяют хакерам использовать, атаковать, проникать и влиять на данные веб-сайтов любых компаний. Для стабильной, бесперебойной и безопасной работы веб-сайта необходимо знать основную информацию об уязвимостях в безопасности онлайн-платформ.
Ключевые слова: безопасность веб-сайтов; уязвимость; защита информации; код; программное обеспечение; сканирование уязвимостей безопасности; инъекция; скриптинг; утечка данных; аутентификация.

EVOLUTION OF THREATS AND VULNERABILITIES OF WEB SITES

P.A. Bozhko[1], T.A. Pulko[2]
[1]*Educational Institution "Belarusian State Academy of Communications", Minsk, Belarus*
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Security vulnerabilities are always a pressing issue that website administrators spend a lot of time researching to ensure the security of their work. These vulnerabilities allow hackers to exploit, attack, penetrate and influence the data of websites of any companies. For stable, uninterrupted and secure operation of a website, it is necessary to know the basic information about security vulnerabilities of online platforms.
Keywords: website security; vulnerability; information protection; code; software; security vulnerability scanning; injection; scripting; data leakage; authentication.

Введение

С ростом числа интернет-пользователей и развитием цифровой экономики вопрос обеспечения безопасности онлайн-платформ становится все более актуальным. Уязвимости веб-сайтов могут привести к краже конфиденциальной информации, взлому сайта или другим серьезным проблемам, поэтому обнаружение и устранение уязвимостей есть важная задача для владельцев веб-сайтов и специалистов по информационной безопасности [1]. Обеспечение безопасности веб-сайтов является сложной задачей, требующей постоянного мониторинга и реагирования на уязвимости [2].

Основная часть

Уязвимость веб-сайта – это дефект или ошибка программного кода, неправильная конфигурация системы или какая-либо другая слабость веб-сайта, веб-приложения или его компонентов и процессов. Уязвимости веб- приложений позволяют злоумышленникам получить несанкционированный доступ к системам, процессам или важнейшим активам компаний [3]. Имея такой доступ, злоумышленники могут организовывать атаки, захватывать приложения, участвовать в повышении привилегий для кражи данных, вызывать масштабные сбои в работе служб и т. д. Любой элемент технологии будет содержать уязвимости [4]. Конечно, не существует никаких указаний на то, сколько уязвимостей может иметь каждый из них. Однако очень грубый метод

определения количества возможных уязвимостей основан на количестве строк кода. Другими словами, чем больше строк кода, тем больше количество возможных уязвимостей [5, 6]. Известно, что языки программирования позволяют быстро устранять уязвимости безопасности веб- приложений. Кроме того, имеются такие методы проверки уязвимостей сайта, как: метод локальной проверки (обнаружени уязвимостей путем непосредственной проверки исходного кода устройства и приложения, проверки и чтения библиотек (двоичных), таких как файлы .exe и т.д.), метод удаленной проверки (удаленное обнаружение уязвимостей через сетевые протоколы, суть которого заключается в удаленном обнаружении уязвимостей). [7].

К основным уязвимостям относятся: инъекции (уязвимости, возникающие вследствие передачи не проверенных данных, которые пользователь ввел интерпретатору в целях выполнения: LDAP, XXE, OS и SQL); уязвимость XSS (Cross-Site Scripting или XSS функционирует в JavaScript -считается не опасной для сервера, однако представляет опасность для пользователя); уязвимости CSRF (атака Cross-Site Request Forgery или CSRF предоставляет злоумышленнику возможность вынудить браузер жертвы осуществить отправку в уязвимое приложение определенного HTTP запроса); применение элементов с уязвимостями (такие элементы, как фреймворки, библиотеки и прочие программные модули функционируют с такими же полномочиями, как и приложение); незащищенные API (большая часть современных приложений зачастую содержат в себе веб-приложения клиентов, а также богатые API интерфейсы, которые доступны из мобильных приложений и через JavaScript в браузере- они работают по протоколам GWT, RPC, REST/JSON, SOAP/XML и др).[8]

Самым надежным на данный момент является рейтинг топ 10 уязвимостей от проекта OWASP (Open Web Application Security Project) – это открытый проект обеспечения безопасности веб-приложений. На документ OWASP Top 10 часто ссылаются при упоминании наиболее распространенных недостатков безопасности веб приложений [9]:

A1 Внедрение кода. Инъекционные недостатки как SQL, NoSQL, OS и LDAP, возникают, когда ненадежные данные отправляются интерпретатору как часть команды или запроса.

A2 Некорректная аутентификация и управление сессией.

A3 Межсайтовый скриптинг. «Многие веб-приложения и API не защищают конфиденциальные данные, такие как финансовые, медицинские и PII.

A4 Нарушение контроля доступа. Многие старые или слабо сконфигурированные XML-процессоры оценивают ссылки на внешние сущности в документах XML. Внешние объекты могут быть использованы для раскрытия внутренних файлов с использованием обработчика URI файла, внутренних общих файлов, внутреннего сканирования портов, удаленного выполнения кода и атак типа отказ в обслуживании.

A5 Небезопасная конфигурация. Ограничения на то, что разрешено пользователям, прошедшим проверку подлинности, часто не выполняются должным образом.

A6 Утечка чувствительных данных. Наиболее часто встречающаяся проблема – это неправильная конфигурация системы. Обычно это результат небезопасных конфигураций по умолчанию, неполных или специальных конфигураций, открытого облачного хранилища, неправильно сконфигурированных заголовков HTTP и подробных сообщений об ошибках, содержащих конфиденциальную информацию.

A7 Недостаточная защита от атак (NEW). Ошибки XSS возникают, когда приложение включает не доверенные данные на новой веб-странице без правильной проверки или экранирования, или обновляет существующую веб-страницу

с предоставленными пользователем данными с помощью API-интерфейса браузера, который может создавать HTML или JavaScript.

A8 Подделка межсайтовых запросов. Небезопасная десериализация часто приводит к удаленному выполнению кода.

A9 Использование компонентов с известными уязвимостями. Компоненты как библиотеки, фреймворки и другие программные модули, работают с теми же привилегиями, как и приложение. Если уязвимый компонент используется, такая атака может облегчить серьезную потерю данных или захват серверов.

A10 Недостаточное журналирование и мониторинг. Недостаточная регистрация и мониторинг в сочетании с отсутствующей или неэффективной интеграцией с реагированием на инциденты позволяют атакующим продолжать атаковать системы, поддерживать постоянство, склоняться к большему количеству систем и подделывать, извлекать или удалять данные.

Проблемы, выделенные в отчетах OWASP, не просто статичны – они развиваются, и мы должны быть готовы к тому, что они будут видоизменяться и дальше. В таблице представлены уязвимости, наиболее актуальные в 2021 году и наиболее актуальные на 2025 год с учетом новых тенденций и прогнозов/

Эволюция уязвимостей
Evolution of vulnerabilities

уязвимость	2021	Прогноз 2025
API1	Нарушение контроля доступа	Расширенная авторизация на уровне сломанных объектов (BOLA)
API2	Сбои в криптографии	Атаки аутентификации, основанной на ИИ
API3	Внедрение кода	Сложные действия по свойствам объектов и манипулированию данными
API4	Небезопасное проектирование	Искусственное потребление ресурсов:
API5	Небезопасная конфигурация	Уязвимости BFLA (Broken Function Level Authorization) с использованием машинного обучения.
API6	Уязвимые и устаревшие компоненты	Несанкционированный доступ к данным на основе контекста.
API7	Ошибки идентификации и аутентификации	Усиленные SSRF-активности с использованием облачной альтернативы.
API8	Нарушение целостности данных программного обеспечения	Уязвимости из-за неправильной конфигурации безопасности в микросервисах.
API9	Ошибки мониторинга и недостаточное ведение журналов	Динамический контроль запасов API
API10	Подделка запросов со стороны сервера	Небезопасное использование API с использованием ИИ-ботов

Заключение

Обеспечение безопасности веб-сайтов требует постоянного мониторинга и реагирования на уязвимости. Продолжительность мониторинга и реагирования на уязвимости являются ключевыми факторами в обеспечении безопасности веб-сайтов. Эффективные методы обнаружения уязвимостей и соответствующие меры безопасности должны постоянно совершенствоваться и адаптироваться к новым угрозам для обеспечения эффективной защиты веб-ресурсов. Важно уделять внимание обучению персонала и его осведомленности о современных методах атак, чтобы поддерживать ресурс в защищенном состоянии.

Список использованных источников

1. Шакиров А.А. Зарипова Р.С. (2019) Современные тенденции web-разработки. Russian Journal of Education and Psychology. (3), 85-88.
2. Гибадуллин Р.Ф., Вершинин И.С., Глебов Е.Е. (2023) Разработка приложения для ассоциативной защиты файлов. Инженерный вестник Дона.
3. Юртаев В.В., Николаева С.Г. (2023) Базы данных как уязвимость организации. Технологический суверенитет и цифровая трансформация. Международная научно-техническая конференция. 256-260.
4. Gizatullin Z., Nuriev M. (2022) Modeling the electromagnetic compatibility of electronic means under the influence of interference through the power supply network.
5. Злыгостев Д.Д., Зарипова Р.С. (2017) Информационная безопасность как инструмент обеспечения экономической безопасности предприятий. Инновации в информационных технологиях, машиностроении и автотранспорте: сборник материалов Международной научно-практической конференции. 23-25.
6. Gibadullin R.F., Nikonorov V.V. (2021) Development of the system for automated incident management based on open-source software.
7. Чудинов Н.В., Халидов А.А. (2022) Разработка программного комплекса для защиты программ от нелегального использования. Современные цифровые технологии: проблемы, решения, перспективы, национальная (с международным участием) научно-практическая конференция. 140-142.
8. Шутько Н.А. (2022) Теоретические понятия защиты web-приложений от уязвимостей. Международный научный журнал «ВЕСТНИК НАУКИ» . (11)
9. Алекперов З.А. (2019) Национальный Исследовательский Университет Информационных Технологий Механики и Оптики Россия, «Научно-практический электронный журнал Аллея Науки». (5)

References

1. Shakirov A.A. Zaripova R.S. (2019) Modern trends in web development. Russian Journal of Education and Psychology. (3), 85-88.
2. Gibadullin R.F., Vershinin I.S., Glebov E.E. (2023) Development of an application for associative file protection. Engineering Bulletin of the Don.
3. Yurtaev V.V., Nikolaeva S.G. (2023) Databases as an organization's vulnerability. Technological sovereignty and digital transformation. International scientific and technical conference. 256-260.
4. Gizatullin Z., Nuriev M. (2022) Modeling the electromagnetic compatibility of electronic means under the influence of interference through the power supply network.
5. Zlygostev D.D., Zaripova R.S. (2017) Information security as a tool for ensuring the economic security of enterprises. Innovations in information technology, mechanical engineering and motor transport: collection of materials of the International scientific and practical conference. 23-25.
6. Gibadullin R.F., Nikonorov V.V. (2021) Development of the system for automated incident management based on open-source software.
7. Chudinov N.V., Khalidov A.A. (2022) Development of a software package to protect programs from illegal use. Modern digital technologies: problems, solutions, prospects, national (with international participation) scientific and practical conference. 140-142.
8. Shutko N.A. (2022) Theoretical concepts of protecting web applications from vulnerabilities. International scientific journal "BULLETIN OF SCIENCE". (11)
9. Alekperov Z.A. (2019) National Research University of Information Technologies, Mechanics and Optics Russia, "Scientific and practical electronic journal Alley of Science". (5)

Сведения об авторах

Божко Р.А., начальник военной кафедры, учреждение образования «Белорусская государственная академия связи», vk@bsac.by
Пулко Т.А., канд. техн. наук, доц., доцент кафедры защиты информации факультета информационной безопасности учреждения образования «Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pulko@bsuir.by

Information about the authors

Bozhko R.A., Head of the Military Department, educational institution "Belarusian State Academy of Communications", vk@bsac.by
Pulko T.A., Cand. Sci. (Tech.)), Associate Professor, Associate Professor of the Department of Information Security, Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", pulko@bsuir.by.