УДК: 004.056

Янов И.В.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Киреева Н.В.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ОСНОВНЫЕ УГРОЗЫ И УЯЗВИМОСТИ ВЕБ-САЙТОВ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Аннотация. Статья посвящена вопросам обеспечения безопасности веб-сайтов в условиях роста числа кибератак. Рассматриваются основные угрозы, включая уязвимости по классификации OWASP Top-10, методы защиты – двухфакторная аутентификация, WAF, пентест и обучение персонала. Подчеркивается важность комплексного подхода к обеспечению безопасности, сочетающего технические и организационные меры для защиты данных и репутации организации.

Ключевые слова: веб-сайт, безопасность, кибератака, OWASP, WAF, 2FA, пентест, уязвимости, шифрование, мониторинг.

С бурным развитием интернета веб-ресурсы стали неотъемлемой частью бизнеса, коммуникаций и досуга. Однако их широкое распространение сделало их привлекательной целью для киберпреступников. Веб-сайты зачастую содержат личные и финансовые данные пользователей, а также могут использоваться как плацдарм для дальнейших атак.

В условиях стремительного роста числа угроз обеспечение информационной безопасности веб-приложений приобретает критическое значение. По данным компании Positive Technologies, в 2024 г. на веб-ресурсы в России приходилось 45 % всех кибератак, что показывает остроту проблемы [4].

Проект OWASP (Open Web Application Security Project, открытый проект безопасности веб-приложений [2]) формирует рейтинг наиболее опасных уязвимостей веб-приложений. В последнем OWASP TOP-10 (2021) были выделены следующие типовые угрозы:

1. Нарушение контроля доступа (Broken Access Control).
2. Ошибки в реализации криптографических алгоритмов (Cryptographic Failures).
3. Инъекционные уязвимости (Injection).
4. Недостатки архитектуры и проектирования (Insecure Design);
5. Неправильная настройка конфигураций (Security Misconfiguration);
6. Использование устаревших или небезопасных компонентов.
7. Проблемы с идентификацией и аутентификацией.

8. Нарушение целостности данных и ПО.

9. Отсутствие надлежащего логирования и мониторинга;

10. Подделка серверных запросов (SSRF).

Среди типичных векторов атак можно выделить SQL-инъекции, XSS (межсайтовый скриптинг), CSRF (подделка запросов), а также ошибки в настройке безопасности. SQL-инъекции позволяют злоумышленникам вмешиваться в работу баз данных и извлекать конфиденциальную информацию. XSS-атаки позволяют внедрять вредоносный код в страницы сайта, а CSRF может принудить пользователя к нежелательным действиям от имени его учетной записи.

Исследования компании «Лаборатория Касперского» показывают увелечение количества кибератак на веб-приложения на 38 % в 2024 г. по сравнению с предыдущти годом. Данные пресс-службы компании «Лаборатория Касперского» показывают, что в 2024 г. было официально зафиксировано 1 811 562 707 кибератак (при этом учитывались атаки с участием вредоносного ПО, предотвращенные средствами защиты и специалистами данной компании). Кроме того, специалисты компании указали, что за 2024 г. увеличился на 12 % объем инцидентов, которые связаны с различными мобильными устройствали с операционной системой Android.

Безопасность веб-сайтов обеспечивается с использованием различных методов. Одним из таких является применение двухфакторной аутентификации (2FA) и ориентирование на сложные пароли. Совместно это дает ощутимое снижение возможности несанкционнированного доступа, риск взлома.

Исследования Group-IB показывают, что 2FA снижает вероятность взлома учетных записей на 60 %, но не может являться абсолютной защитой. Совсеменные тенденции и технологии подрахумевают различные способы обхода данных мер защиты:

1. Социальная инженерия: манипулирование пользователями для получения доступа.

2. OAuth: использование уязвимостей открытой авторизации.

3. Brute-Force: перебор кодов, особенно при использовании устаревшего оборудования.

4. Сгенерированные ранее токены: использование резервных кодов, полученных злоумышленником.

5. Cookie-файлы сеанса: их кража для доступа к аккаунту без пароля и 2FA. Злоумышленники используют перехват сеансов, межсайтовый скриптинг, вредоносное ПО или Evilginx для захвата cookie.

6. SIM-jacking: получение контроля над номером телефона жертвы для перехвата SMS-кодов 2FA через обращение к оператору или вредоносные приложения.

Вследствии этого возникает необходимость применять дополнительные способы защиты, чтобы использование 2FA было эффективным [3], в

частности, рекомендуется не передавать временные или запасные ключи защиты; создавать сложные, из множества символов пароли; применять уникальные пароли для важных аккаунтов, использовать физические ключи для аутентификации; изучать популярныи тактики социальной инженерии. Говоря о сложности пароля, нужно понимать, что длина и сложность пароля это разные грани вопроса. Исследования Национального института стандартов и технологий (NIST) [4] показывают, что сложные пароли с различными символами и длинные пароли надежнее и риск взлома значительно ниже, например, взлом 12-символьного пароля занимает около 2000 лет.

Важной составляющей устранения уязвимостей являются регулярные обновления CMS, плагинов и серверного ПО. Качественные и частые обновления CMS показывают поддержку разработчиками и устранение уязвимостей.

С помощью веб-аппликационного межсетевого экрана (WAF) анализируется трафик и блокируются подозрительные запросы, что предотвращает SQL-инъекции и XSS-атаки. Данные пользователей защищаются протоколом HTTPS и шифрованием баз данных. WAF представляет комплексное решение, позволяющее защитить веб-приложения от множества атак, таких как: SQL-инъекции; XSS; инъекция локальных или удаленных файлов (LFI/RFI); PHP-инъекции; боты; Brute-force и другие методы перебора данных.

Важным методом защиты веб-сайтов от киберугроз, выявляющий уязвимости до злоумышленников, является тестирование на проникновение (пентест). По способу доступа к системе выделяют: внешние тесты и внутренние тесты. В зависимости от объема информации, доступной пентестеру, существуют разные подходы к пентесту:

- Black Box (черный ящик): полное отсутствие информации (имитация атаки извне);
- White Box (белый ящик): полный доступ к архитектуре (глубокий анализ);
- Gray Box (серый ящик): частичное знание системы (баланс между реализмом и полнотой).

Тестирование на проникновение является одной из ключевых мер обеспечения информационной безопасности веб-сайтов.

Другим значимым источником угроз информационной безопасности является человеческий фактор, приводящий к утечкам данных и взломам. Более трети инцидентов происходят из-за недостаточной осведомленности пользователей, использования ненадежных паролей и фишинга.

Для снижения рисков необходимо:

1. Регулярно обучать сотрудников основам кибербезопасности, используя практические примеры и актуальные данные об угрозах.

2. Внедрять технические средства, такие как многофакторная аутентификация и системы мониторинга, для минимизации ошибок и предотвращения несанкционированного доступа.

Обеспечение безопасности веб-сайтов требует комплексных мер, включая технические (WAF, шифрование, двухфакторная аутентификация) и организационные (мониторинг, тестирование, обучение сотрудников). С помощью комплексного подхода можно обеспечить минимизацию рисков и защитить данные пользователей и репутацию организации.

Вопросы обеспечения безопасности веб-сайтов требуют комплексного подхода, включающего как технические меры, так и организационные [1]. Активные и своевременные методы внедрения актуальных методов защиты, таких WAF, двухфакторная аутентификация и шифрование является крайне необходимым и своевременным решением на ряду с устранением текущих уязвимостей, связанных с увеличением числа кибератак. Использование постоянного мониторинга, тестирования и обучения сотрудников остаются основными и предпочтительными инструментами в борьбе с киберугрозами. Таким образом, только комплексный подход позволит минимизировать риски и защитить как данные пользователей, так и репутацию организации.

Список использованных источников:

1. Масалков А.С. Особенности киберпреступлений в России: инструменты нападения и защиты информации [Текст] / А.С. Масалков. М.: ДМК Пресс, 2018. 226 с.

2. Открытый проект обеспечения безопасности веб-приложений. URL: https://owasp.org/www-project-top-ten//.

3. NetSec.news. Портал для профессионалов и компаний, заинтересованных в защите своих данных и цифровых инфраструктур. URL: https://www.netsec.news/summary-of-the-nist-password-recommendations-for-2021/.

4. Positive Technologies. Лидер в области кибербезопасности, ориентированной на результат. URL:// https://global.ptsecurity.com/#analytics.

Yanov I.V.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Kireeva N.V.
Volga Region State University of
Telecommunications and Informatics, Samara

THE MAIN THREATS AND VULNERABILITIES OF WEBSITES AND METHODS OF PROTECTION AGAINST THEM

Abstract. The article is devoted to the issues of ensuring the security of websites in the context of an increasing number of cyber attacks. The main threats are considered, including vulnerabilities according to the OWASP Top-10 classification, protection methods – two-factor authentication, WAF, pentest and staff training. The importance of an integrated approach to security is emphasized, combining technical and organizational measures to protect the organization's data and reputation.

Keywords: website, security, cyberattack, OWASP, WAF, 2FA, pentest, vulnerabilities, encryption, monitoring.