Научная статья
Original article
УДК 004.424

# АТАКИ НА ВЕБ-КОНТЕНТ

ATTACKS ON WEB CONTENT

**Кобылко Андрей Эленович,** аспирант, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kurinaaa@rambler.ru

**Kobylko Andrey Elenovich**, post-graduate student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kurinaaa@rambler.ru

**Аннотация.** Чтобы управлять безопасностью веб-сайта, нужна максимальная прозрачность трафика, обращающегося к веб-сайту. Наблюдение за угрозами или вредоносной активностью в трафике в режиме реального времени позволит реагировать в режиме реального времени. В статье описаны виды атак на веб-контент.

**Annotation.** To manage website security, you need maximum visibility into the traffic accessing your website. Real-time monitoring of threats or malicious activity in your traffic will allow you to react in real time. The article describes the types of attacks on web content.

**Ключевые слова:** Атака, информационная безопасность, веб-контент.

**Keywords:** Attack, information security, web content.

Расширенные решения для веб-безопасности могут помочь визуализировать не только типы трафика, источники, протоколы, полосу пропускания и скорость передачи пакетов. Но помимо этого, они должны агрегировать эти данные, чтобы показать вам законный и вредоносный трафик. Во время проектирования должны определить тип атаки, к которой относится сеансовый.

Кроме того, у вас должен быть доступ к историческим и криминалистическим данным, чтобы получить полный контекст текущей атаки и в целях поиска угроз.

Данные о трафике в реальном времени — объемы трафика, источники, пропускная способность, скорость передачи пакетов и т. д.

Исторические данные — просматривайте данные о трафике за несколько недель или месяцев, чтобы понять исторические тенденции для текущих угроз. События безопасности — просмотрите, какие атаки поражали сайт прямо сейчас или в прошлом, а также какие сеансы относятся к какому типу атаки.

Эксплойты и уязвимости обнаруживаются каждый день. Чтобы действовать на опережение и предотвращать уязвимости, вам следует внедрить решение, которое поможет разработчикам приступить к созданию приложения. Самозащита приложений в реальном времени (RASP) перехватывает код, когда он передается в систему управления версиями, и предупреждает об известных атаках и атаках нулевого дня. Это может предотвратить появление уязвимого кода еще до того, как он будет запущен в производство.

RASP может по умолчанию обеспечивать защиту от OWASP Top 10, известных атак и атак нулевого дня, а также может защищать устаревшие и сторонние приложения, упакованные с программным обеспечением.

Без интеграции с SIEM любое решение для обеспечения безопасности веб-сайтов будет бесполезным для команды SOC. Никто не хочет добавлять «еще один экран» для просмотра.

Если команда использует систему управления информацией и событиями безопасности (SIEM), убедитесь, что инструменты безопасности веб-сайта интегрированы с ней. Это позволит вам использовать данные и оповещения из решений по обеспечению безопасности для создания оповещений SIEM, а также для проведения анализа безопасности и расследований.

Гибкое развертывание — обеспечьте быстрое развертывание всех компонентов решения безопасности без внесения изменений в базовые системы. Это экономит время, предотвращает сложные проекты внедрения и позволяет равномерно применять меры безопасности к новым и устаревшим системам.

SLA — убедитесь, что поставщик решения обязуется соблюдать SLA для реагирования на атаки, и что это SLA приемлемо с точки зрения целевого времени восстановления (RTO).

Ценообразование — инвестируйте столько, сколько необходимо, чтобы получить полное покрытие всех важных векторов угроз. Безопасность имеет большое значение и может значительно снизить риск катастрофического взлома. Имейте в виду, что каждое нарушение обходится организациям в среднем в 8 миллионов долларов.

Соответствие — убедитесь, что решение поддерживает все нормативные акты и отраслевые стандарты, которым необходимо соответствовать: HIPAA, PCI/DSS , SOX , GDPR , FERPA и т. д.

Отдайте предпочтение специализированному решению для обеспечения безопасности веб-сайтов

Безопасность веб-сайтов — это дисциплина, которая сильно развилась за последние два десятилетия благодаря специализированным решениям, таким как технология защиты от DDoS-атак, WAF, защита от ботов и безопасность API. Даже общие методы обеспечения безопасности, такие как регистрация событий и поведенческое профилирование, должны быть

адаптированы, чтобы быть эффективными для анализа веб-трафика и угроз веб-приложений.

При выборе поставщика постарайтесь оценить, предлагает ли выбранный вами провайдер безопасность веб-сайтов как часть огромного пакета услуг или рассматривает безопасность приложений как основную часть своего бизнеса. Мы советуем отдавать предпочтение поставщикам с большим опытом и специализированными технологиями, особенно подходящими для решения задач безопасности приложений.

Imperva предоставляет комплексное решение для обеспечения безопасности веб-сайтов, предоставляя все инструменты, необходимые для защиты критически важного веб-сайта или веб-приложения. У нас есть внутренняя исследовательская группа по безопасности, которая анализирует данные из тысяч организаций и помогает вам защититься от новейших угроз.

Imperva — это решение для обеспечения безопасности с широкими возможностями настройки, которое позволяет добавлять правила или исключения в соответствии с рабочими процессами бизнеса и предотвращать нарушение работы пользователей. Он поставляется с расширенными функциями контроля доступа, включая многофакторную аутентификацию, которую можно легко внедрить без внесения изменений в существующие приложения, и детальный контроль доступа на основе ролей (RBAC) для ИТ-систем.

Решение для обеспечения безопасности приложений Imperva включает в себя:

Защита от DDoS -атак — поддерживайте бесперебойную работу в любых ситуациях. Предотвратите любой тип DDoS-атаки любого масштаба, препятствующий доступу к веб-сайту и сетевой инфраструктуре.

WAF — облачное решение разрешает законный трафик и предотвращает нежелательный трафик, защищая приложения на периферии, а шлюз WAF обеспечивает безопасность приложений и API внутри сети. WAF также

облегчает развертывание в организации мер контроля доступа, таких как многофакторная аутентификация.

Управление ботами — анализирует трафик ботов для выявления аномалий, выявляет плохое поведение ботов и проверяет его с помощью механизмов проверки, которые не влияют на пользовательский трафик. Управление репутацией также позволяет отфильтровывать нежелательный трафик на основе источников, географических данных, шаблонов или черных списков IP-адресов.

Защита от захвата учетных записей — использует процесс обнаружения на основе намерений для выявления и защиты от попыток захвата учетных записей пользователей в злонамеренных целях. Это может помочь смягчить внутренние угрозы и защитить от повышения привилегий и горизонтального перемещения.

Безопасность API — защищает API, гарантируя, что только желаемый трафик может получить доступ к конечной точке API, а также обнаруживая и блокируя использование уязвимостей.

Аналитика атак — эффективно и точно устраняйте реальные угрозы безопасности и реагируйте на них с помощью действенной аналитики на всех уровнях защиты. Использует машинное обучение и аналитику рисков для данных, чтобы обрабатывать миллионы предупреждений, выявлять подозрительный доступ к данным и определять приоритеты угроз.

RASP — защитите свои приложения изнутри от известных атак и атак нулевого дня. Быстрая и точная защита без подписи или режима обучения.

CDN — повысьте производительность веб-сайта и сократите расходы на пропускную способность с помощью CDN, предназначенной для разработчиков. Кэшируйте статические ресурсы на периферии, ускоряя API и динамические веб-сайты.

**Литература**

1. Ван Хайтао Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного

интеллекта, Технологии и приложения сетевой безопасности, 2018 (3): 60-63.

2. Чжэн Яньфан Исследования и практика применения искусственного интеллекта и технологий анализа в системе ситуационной осведомленности информационной безопасности Мир цифровых коммуникаций, 2018, № 160 (4): 229.
3. Чжэн Фан Информационная безопасность в эпоху искусственного интеллекта, Исследования в области информационной безопасности, 2017, 3 (11): 966-967.
4. Дэн Вэньбинь Проблемы и меры противодействия надзору за информационной безопасностью в эпоху искусственного интеллекта Информационная безопасность Китая, 2018 г., 106 (10): 106-108.

**References**

1. Wang Haitao Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, Network Security Technology and Application, 2018 (3): 60-63.
2. Zheng Yanfang Research and Practice of Artificial Intelligence Application and Analysis Technology in Information Security Situational Awareness System Digital Communication World, 2018, No.160 (4):229.
3. Zheng Fang Information Security in the Age of Artificial Intelligence, Information Security Research, 2017, 3 (11): 966-967.
4. Deng Wenbing Challenges and Countermeasures for Information Security Supervision in the Age of Artificial Intelligence China Information Security, 2018, 106 (10): 106-108.

*© Кобылко А.Э., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №7/2022.*

**Для цитирования:** Кобылко А.Э. АТАКИ НА ВЕБ-КОНТЕНТ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №7/2022.