Вебмониторэкс
защита веб-приложений и API

Веб-атаки на российские компании в 1 полугодии 2025 года

Отчет об атаках на веб-приложения российских компаний с января по июнь 2025 года

Оглавление

Введение

Сегодня веб-приложения – это неотъемлемая часть инфраструктуры многих компаний независимо от отрасли и масштаба бизнеса. В то же время большой объем функционала, обработка персональных и конфиденциальных данных, доступ к различным сегментам ИТ-инфраструктуры компании делают веб-приложения одной из основных целей киберпреступников.

Данный отчет отражает картину того, какие веб-уязвимости чаще всего пытаются эксплуатировать злоумышленники, какие типы атак активно используют и какие веб-угрозы наиболее актуальны для различных отраслей.

Аналитика составлена на основе большого массива агрегированных данных о разных типах атак на клиентов Вебмониторэкс, безопасность которых обеспечивается одноименной платформой защиты веб-приложений, микросервисов и API. Для отчета была проанализирована информация о более чем 170 крупных организациях из различных отраслей, включая госсектор, ИТ, ритейл, финансы, здравоохранение, промышленность, телеком и др.

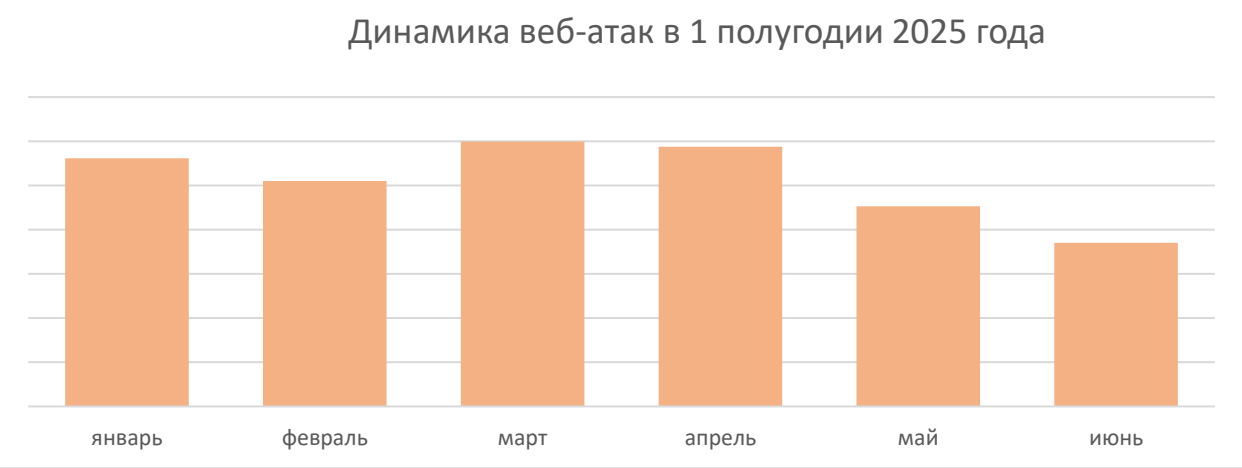
Отчетный период составляет **январь – июнь 2025 года**. Приведена статистика атак в динамике с детализацией на каждый месяц полугодия. Также сделаны выводы об отраслевой специфике атак и угрозах, наиболее актуальных для конкретных сфер экономики.

В отчете представлены ключевые веб-угрозы, которые были зафиксированы решением **ПроWAF**. Это межсетевой экран уровня веб-приложений, входящий в состав облачной платформы «Вебмониторэкс». Особенности ПроWAF:

- обеспечивает защиту веб-приложений без снижения производительности вне зависимости от нагрузки. Автоматически масштабируется вместе с веб-приложением;
- интеллектуальный анализ запросов снижает уровень ложных срабатываний, сохраняя доступность веб-приложения для легитимных пользователей;
- имеет встроенные сканеры для обнаружения уязвимостей, как на основе трафика приложения, так и за счет сканирования внешнего периметра;
- собственный отдел детектов непрерывно работает над улучшением качества обнаружения атак и расширением базы бессигнатурных детектов. Применяется глубокий анализ трафика для распознавания разных форматов данных;
- простой и понятный интерфейс, быстрая настройка продукта. Администрирование ПроWAF в среднем не превышают 15 минут в день.

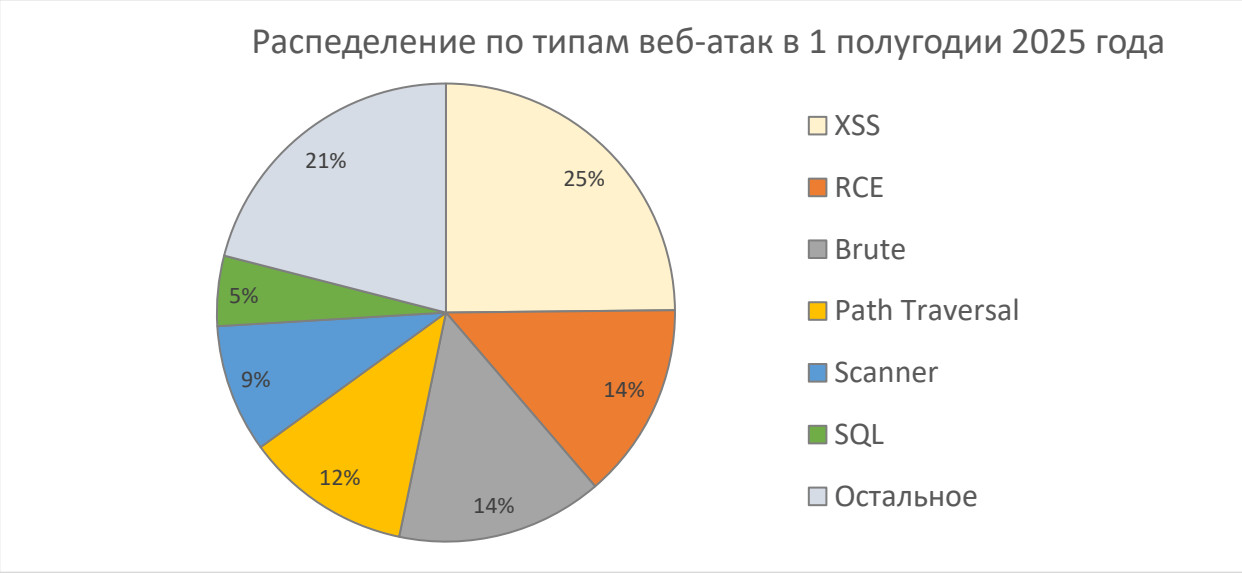
Общая статистика. Как атаковали веб-приложения

С каждым годом количество веб-атак на ресурсы российских компаний растет. С января по июнь 2025 года этот показатель превысил **600 млн веб-атак.**



Топ атак, которые пытались реализовать злоумышленники:

- XSS (межсайтовый скриптинг);
- RCE (удаленное исполнение кода);
- Brute-force;
- Path Traversal (попытки получить доступ к файловой системе через ошибки в фильтрации запросов к приложению).



Самые распространенные типы атак

Cross-site Scripting, XSS

Самой частой веб-атакой, с которой столкнулись компании в отчетном периоде, оказался **межсайтовый скриптинг** (Cross-site Scripting, XSS) – **25% выявленных атак.** XSS-атака предполагает, что злоумышленник пытается внедрить вредоносный код в веб-страницу. Пользователь вводит на сайте свои логины, пароли, данные банковской карты или выполняет другие действия — и всё это попадает в руки атакующего.

Различают несколько видов межсайтового скриптинга:

- **Хранимый XSS (англ. Stored XSS)**

  Вредоносный код заранее внедрен на HTML-страницу приложения. Этот код постоянно отображается в браузере всех пользователей.

- **Отраженный XSS (англ. Reflected XSS)**

  Для произведения атаки злоумышленнику необходимо спровоцировать пользователя перейти по специально сформированной ссылке.

- **DOM-based XSS**

  Уязвимость, при которой вредоносный JavaScript выполняется в браузере жертвы из-за неправильной обработки данных в DOM (Document Object Model – структура HTML-страницы).

Remote Code Execution (RCE) и Brute-force

Удаленное выполнение кода (англ. Remote Code Execution, RCE) предполагает, что злоумышленник пытается выполнить определенные команды операционной системы, в которой запущено уязвимое веб-приложение. В случае успеха он сможет, например:

- влиять на целостность, доступность и конфиденциальность данных веб-приложения;
- получать контроль над операционной системой и сервером, которые обеспечивают работу веб-приложения;
- распространить атаку далее по сети организации или на другие веб-приложения, которые находятся на атакованном сервере.

Доля RCE-атак в отчетном периоде **составила 14%,** что делает угрозу второй по распространенности после XSS.

Такую же долю **(14%)** составили попытки **перебора пароля (брутфорс).** Причем в абсолютном большинстве случаев речь идет не просто о переборе словарных паролей, а о **credential stuffing**. Это тип брутфорса, при реализации которого злоумышленник пытается подобрать пароль к учетной записи пользователя путём перебора ранее утекших комбинаций и похожих на них. Очевидно, что этот тренд связан с большим объемом учетных данных, которые попали в руки злоумышленников за последние годы. Теперь киберпреступники пытаются проверить эти комбинации на всех возможных ресурсах.

Path Traversal

Атака обхода пути занимает **12%** в общем объеме выявленных угроз. Это тип атаки, которая позволяет злоумышленнику получить доступ к конфиденциальным файлам и каталогам, хранящимся в файловой системе веб-приложения с помощью изменения существующих путей к файлам через параметры системы.

Подобная уязвимость возникает из-за некорректной фильтрации пользовательских данных при запросе пользователем файлов или директорий через веб-приложение.

SQL-инъекции

Атака этого типа реализуется из-за недостаточной фильтрации входных пользовательских данных, путем внедрения специально сконструированного SQL-запроса. Уязвимость к подобной атаке позволяет злоумышленнику внедрить в выполняемый запрос к базе данных произвольный SQL-код, получив возможность доступа к конфиденциальным данным, их изменению, а также выполнению операций по администрированию СУБД. В отчетном периоде **5%** событий ИБ было связано с попытками внедрения SQL-инъекций.

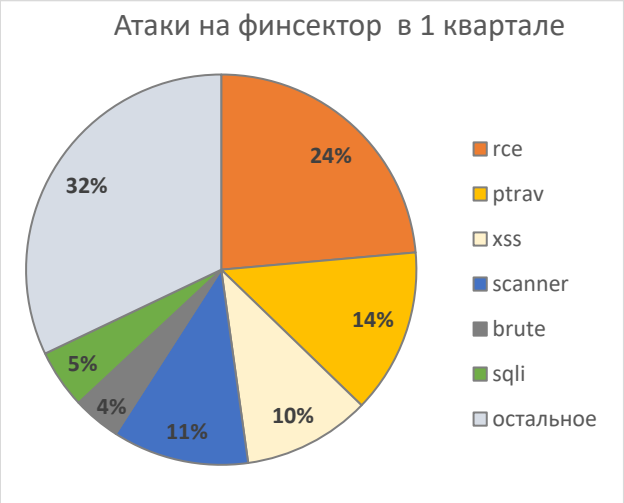
Какие отрасли атаковали?

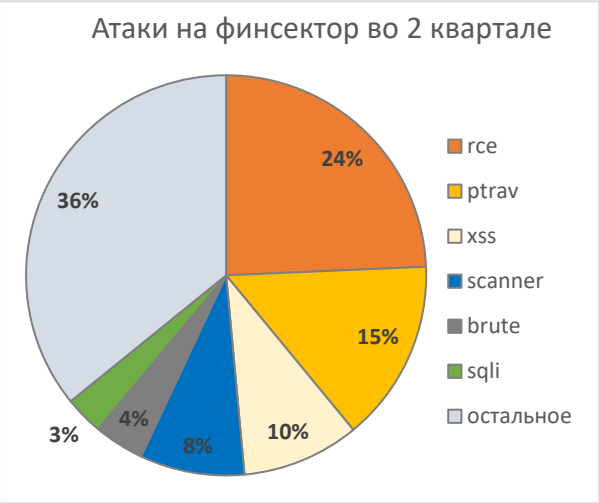
Финансовый сектор

Чаще всего кибердарам подвергались представители **финансового сектора.** В среднем на одну организацию отрасли в 1 полугодии было совершено **4,1 млн веб-атак.**

Самой актуальной угрозой для финансовых компаний стали попытки **удаленного исполнения вредоносного кода в серверной части приложения (RCE)**. С ними было связано **24%** выявленных в отрасли событий ИБ. Поскольку RCE позволяет выполнить произвольный код на сервере, в случае успеха злоумышленник получает полный контроль над системой. Это открывает перед ним массу возможностей: кража денег и данных клиентов, компрометация транзакций, установка бекдоров и другого ВПО для продвижения по внутренним системам банка. Для реализации подобной атаки хакерам нужно обладать достаточно высоким уровнем квалификации. В отличие от любителей, которые просто ищут доступные в интернете сервисы и действуют на удачу, профессионалы имеют конкретную цель, применяют проверенные техники и тактики, используют сложное, хорошо замаскированное вредоносное ПО.

Еще **четверть атак** на веб-приложения в организациях из финсектора была связана с уязвимостью обхода пути – **Path Traversal**. Ее злоумышленники часто используют в качестве подготовительного этапа к более серьезным действиям, например, RCE или SQL-инъекции. Например, через Path Traversal можно обнаружить версию ПО, на котором работает сайт, и, если она уязвима (например, Log4j, Fastjson, старый WordPress), реализовать RCE.





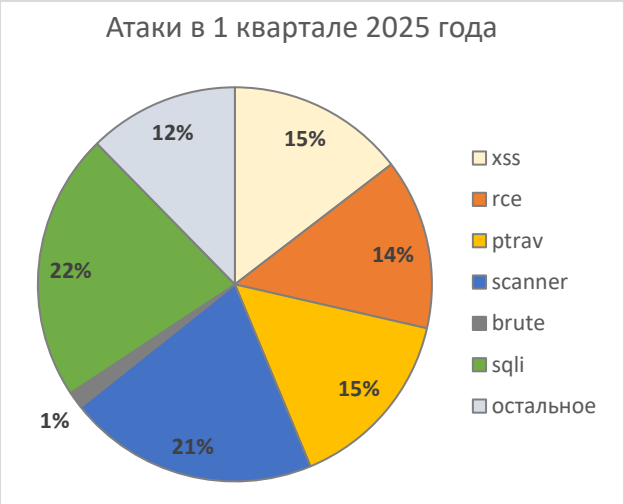
ИТ-сектор

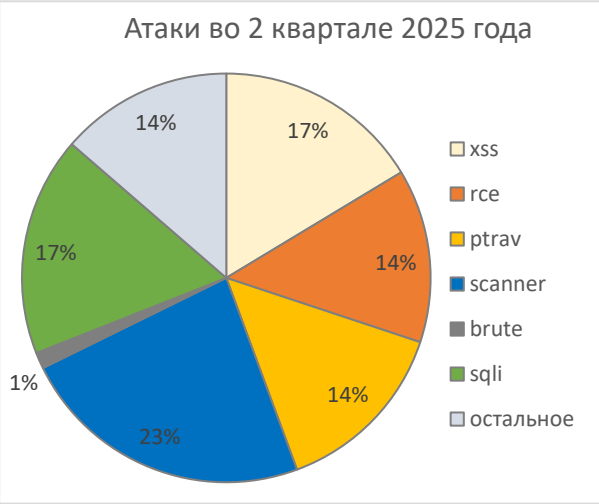
Среднее количество веб-атак на одну ИТ-организацию в 1 полугодии составило **2,6 млн.** Для отрасли наиболее актуальными веб-угрозами в отчетном периоде стали **SQL-инъекции** и **сканирование автоматизированными средствами (в том числе ботами)**. На них пришлось примерно **по 20%** зафиксированных атак. Это может свидетельствовать о том, что злоумышленники сначала собирают информацию о компонентах веб-приложения (используемое ПО и его версии, структура API и т.п.) и проверяют его на наличие уязвимостей. А после реализуют атаку, используя полученную информацию.

SQL-инъекции – это взлом базы данных приложения (через уязвимость злоумышленник вмешивается в запросы, которые приложение делает к своей базе данных). Атаки данного класса особенно критичны на фоне активного спроса на ИТ-аутсорсинг. Компании, предоставляющие такие

услуги, имеют множество клиентов и хранят информацию о них в своих базах данных (исходные коды, API-ключи, токены, данные о конфигурации инфраструктуры и т.п.). Все это может упростить злоумышленникам атаку на целевую организацию через ее подрядчика.

Примерно равные доли **(по 15%)** заняли другие популярные уязвимости: SQL, Path Traversal, RCE. Это скорее указывает на то, что для ИТ-отрасли актуальны практически все типы основных веб-угроз и компаниям необходимо сконцентрироваться на закрытии всех ключевых уязвимостей.

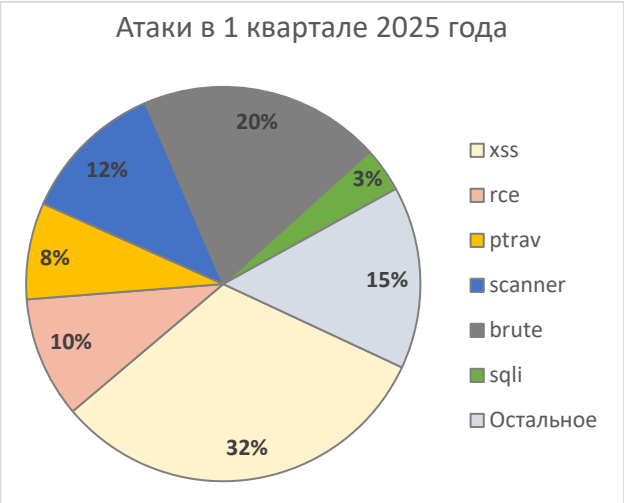


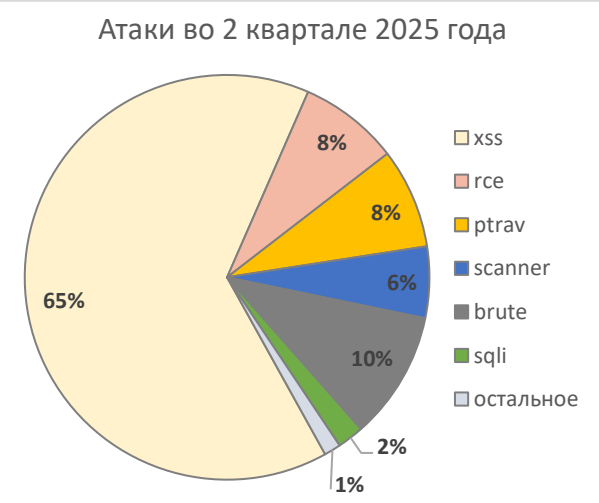


Электронная коммерция

По количеству зафиксированных веб-атак в расчете на одну организацию данная отрасль занимает третье место – в среднем на один онлайн-магазин было совершено **1,2 млн** веб-атак. **Межсайтовый скриптинг (XSS)** составил половину (**почти 50%**) всех веб-угроз, с которыми столкнулась отрасль в отчетном периоде. Чаще всего вредоносный код при XSS-атаке встраивается в интерактивные элементы сайта, которых в онлайн-магазинах достаточно много (строка поиска, отзывы, страница оплаты). Обилие пользовательского ввода и динамического контента делают XSS-атаки такой насущной проблемой для интернет-коммерции. К тому же обычному пользователю сложно заметить подмену контента и распознать фишинговую составляющую веб-приложения.

На втором месте после XSS находится **брутфорс (перебор пароля)**, на который приходится **14%** зафиксированных в отчетном периоде веб-атак. Актуальность данной уязвимости для e-commerce связана с тем, что многие покупатели используют один и тот же логин и пароль на разных сервисах. Так как за последние пару лет в сети оказалось огромное количество персональных данных, включая учетные данные, злоумышленники тестирую уже скомпрометированные комбинации на разных ресурсах.





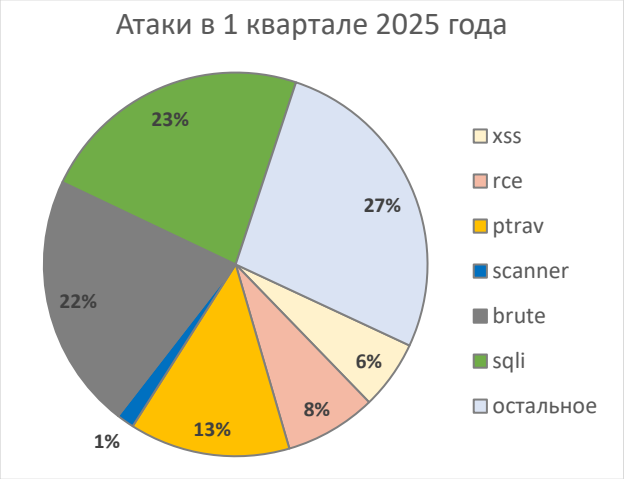
Государственный сектор

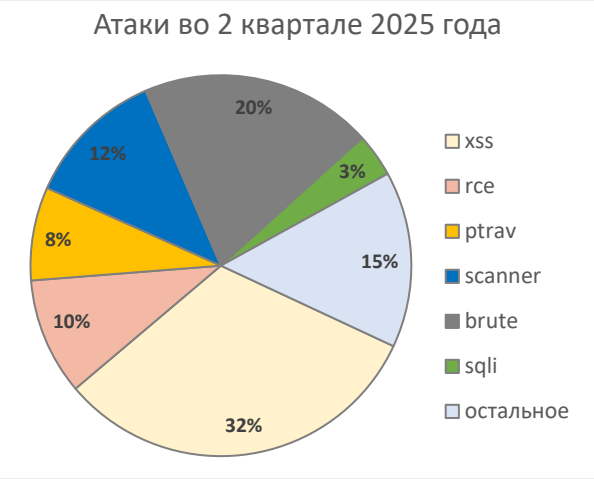
Для госорганизаций основной проблемой в 1 полугодии стал **перебор пароля (брутфорс)**. С попытками взлома учетных записей связана половина веб-атак на госсектор. Госсектор — это единственная отрасль, где брутфорс стабильно находится на 1 месте в перечне атак на веб. При этом в абсолютном большинстве случаев речь идет о **credential stuffing**. При этом типе брутфорса злоумышленник пытается подобрать пароль к учетной записи пользователя путём перебора ранее утекших данных и похожих комбинаций. Такие незаконные действия могут проводиться вручную или с использованием специализированного программного обеспечения (ботов), а также осуществляться с тысяч IP-адресов.

Преобладание брутфорса связано с тем, что учетные записи на различных государственных порталах есть практически у каждого гражданина, однако лишь небольшой процент пользователей задумывается о безопасности своих аккаунтов. Большинство же использует одинаковые или похожие учетные данные на разных ресурсах, что усугубляется многочисленными утечками последних лет. А взломав аккаунт пользователя, злоумышленник может не только получить всю информацию о человеке, но и совершать различные нелегитимные действия.

Целью киберпреступников могут быть как личные кабинеты граждан, так и учетные данные сотрудников ведомств. В этом случае может быть скомпрометирована гостайна, секретная и стратегическая информация. А если злоумышленники подберут логин и пароль к учетной записи администратора сети, то последствия атаки могут быть серьезными для всего госсектора.

Еще **15%** атак на веб-сайты государственных организаций связано с **SQL-инъекциями**. Как в случае с ИТ-компаниями, для злоумышленников ценность составляет доступ к базам данных. В них могут храниться не только конфиденциальные данные граждан, но и гостайна, информация о бюджетах ведомств, раскрытие структуры органов власти, техническая информация об интеграции между разными государственными системами и т.п.





Самые распространённые уязвимости

В данном разделе представлены уязвимости (CVE), которые злоумышленники чаще всего пытались проэксплуатировать в 1 полугодии 2025 года. Все попытки эксплуатации были выявлены и заблокированы продуктом ПроWAF.

> **CVE (Common Vulnerabilities and Exposures)** – стандартизированный идентификатор уязвимостей в программном обеспечении, используемый в кибербезопасности. Каждой уязвимости присваивается уникальный идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок.

Самые распространненные CVE 1 полугодия с долями в общем объеме атак:

1. **CVE-2021-44228 (59%)**

Уязвимость в библиотеке логирования, позволяющая злоумышленникам выполнять произвольный код на сервере путем отправки специально сформированных данных, которые затем логируются.

2. **CVE-2021-28169 (13%)**

Уязвимость в веб-сервере, позволяющая обойти ограничения и получить доступ к защищенным ресурсам через двойное кодирование пути в запросах.

3. **CVE-2009-4679 (3%)**

Уязвимость обхода директорий, позволяющая атакующим включать и выполнять произвольные локальные файлы через специальные последовательности в параметрах запроса.

4. **CVE-2009-4202 (3%)**

Уязвимость, связанная с обходом директорий, позволяет атакующим включать и выполнять произвольные локальные файлы через специальные последовательности в параметрах запроса.

5. **CVE-2010-0157 (3%)**

Уязвимость обхода директорий, позволяющая атакующим включать и выполнять произвольные локальные файлы через специальные последовательности в параметрах запроса.

6. **CVE-2017-9841 (3%)**

Уязвимость в инструменте тестирования PHP-кода, позволяющая атакующим выполнять произвольный PHP-код через специально сформированные HTTP-запросы.

7. **CVE-2010-0467 (2%)**

Уязвимость обхода директорий, позволяющая атакующим читать произвольные файлы через специальные последовательности в параметрах запроса.

8. **CVE-2010-0942 (2%)**

Уязвимость обхода директорий, позволяющая атакующим читать произвольные файлы через специальные последовательности в параметрах запроса.

Как видно, абсолютное большинство атак связано с попытками эксплуатации **CVE-2021-44228 (Log4Shell)**. Уровень ее опасности составляет 10 из 10 по шкале CVSS. Это критическая дыра в популярной библиотеке Log4j, последняя используется для записи логов (журналов событий) в Java-приложениях. Уязвимость относится к классу Remote Code Execution (RCE).

В случае ее успешной эксплуатации, злоумышленники могут исполнять на атакованном сервере произвольный код. Потенциально это позволяет им захватить полный контроль над системой.

Как это работает:

1. Любая запись в лог (например, ошибка "User *{имя}* не найден") обрабатывается Log4j.
2. Если вместо имени вписать вредоносный код, Log4j автоматически выполнит его.
3. Далее сервер связывается с управляющим сервером и загружает вредоносное ПО на атакованную систему.

Популярность Log4Shell объясняется несколькими фактами. Во-перых, эта библиотека используется практически везде. Во-вторых, эксплуатация уязвимости не требует от хакера особых навыков. В-третьих, в случае успеха, злоумышленник получает практически неограниченный контроль над инфорастуктурой жертвы.

Далее следует уязвимость **CVE-2021-28169,** с попытками эксплуатации которой связаны еще **13%** атак. Это уязвимость в сервере **Eclipse Jetty** (популярный Java-сервер для веб-приложений). Она позволяет злоумышленнику читать произвольные файлы на сервере из-за некорректной обработки путей (атака типа **Path Traversal**). Для данной уязвимости уже выпущен патч безопасности, тем не менее в корпоративной среде еще достаточно необновленных систем, что играет на руку злоумышленникам.

Примечательно, что большинство уязвимостей, которые пытались эксплуатировать злоумышленники в 1 полугодии, были обнаружены 10-15 лет назад. Тем не менее они все равно часто встречаются в хакерском арсенале. Это объясняется тем, что эксполойты для них тоже существуют давно, они доступны, понятны и часто автоматизированы.

Также это ошибки в достаточно популярных продуктых, которые используются повсеместно, что значительно увеличивает частоту их эксплуатации. Важно, что патчи безопасности для данных CVE выпущены также много лет назад. Однако не все компании обновили свои системы и остаются уязвимыми к таким веб-атакам.

Выводы

- С января по июнь 2025 года эксперты Вебмониторэкс зафиксировали более **600 млн** веб-атак на онлайн-ресурсы клиентов.
- Наиболее атакуемой отраслью в отчетном периоде стали **финансы**, где на одну организацию в среднем пришлось **4, 1 млн атак**. На втором месте **ИТ** – в среднем на одну компанию было совершено **2,6 млн веб-атак**.
- Среднее число веб-атак на одну **госорганизацию** в отчетном периоде составило **966 тыс.**
- Четверть всех атак с января по июнь – это **XSS (межсайтовый скриптинг)**. В топе также RCE (удаленное исполнение кода), брутфорс и Path Traversal (попытки получить доступ к файловой системе через ошибки в фильтрации запросов к приложению).
- Среди веб-уязвимостей, которые пытались проэксплуатировать злоумышленники, почти **60%** составляет **CVE-2021-44228 (Log4Shell).**
- В целом в большинстве атак злоумышленники стараются найти старые веб-уязвимости, возраст которых составляет 10-15 лет.