

Поддержите миссию OWASP по улучшению безопасности программного обеспечения с помощью инициатив с открытым исходным кодом и обучения сообщества. [Пожертвуйте сейчас!](#)

[Магазин](#)[ТЫ ГЛАВ](#)[Пожертвовать](#)[агазин](#)[Присоединиться](#)[СОБЫТИЯ](#)[О](#)[Q](#)[Присоединиться](#)

Десятка лучших OWASP

[Watch](#)

341

[Star](#)

1,158

[Основной](#)[Переводческие усилия](#)[Спонсоры](#)[Данные 2025 г.](#)

Важное примечание:

Десятка лучших OWASP 2025

Текущий статус проекта по состоянию на сентябрь 2024 г.:

- Мы планируем объявить о выпуске **OWASP Top 10:2025** в первой половине 2025 года.
- Сбор данных (сейчас - декабрь 2024 г.)** : пожалуйста, предоставьте статистику тестирования на проникновение ваших приложений.

[Следите за обновлениями!](#)

OWASP Top 10 — это стандартный документ по повышению осведомленности для разработчиков и безопасности веб-приложений. Он представляет собой широкий консенсус относительно наиболее критических рисков безопасности для веб-приложений.

Фонд OWASP® работает над повышением безопасности программного обеспечения посредством возглавляемых сообществом проектов по разработке программного обеспечения с открытым исходным кодом, сотен отделений по всему миру, десятков тысяч членов, а также путем проведения локальных и международных конференций.

Информация о проекте

- [OWASP Top 10:2021](#)
- [Создание OWASP Top 10](#)
- [OWASP Top 10:2021 — презентация к 20-летию \(PPTX\)](#)



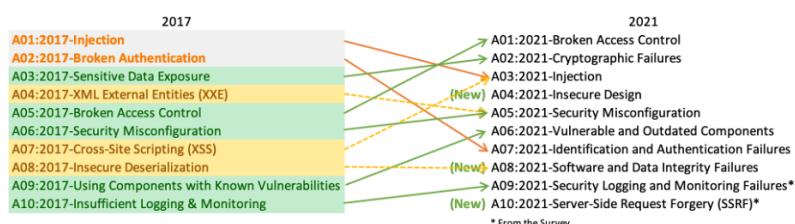
Флагманский проект

Разработчики во всем мире признают его первым шагом на пути к более безопасному кодированию.

Компании должны принять этот документ и начать процесс обеспечения того, чтобы их веб-приложения минимизировали эти риски. Использование OWASP Top 10, возможно, является самым эффективным первым шагом к изменению культуры разработки программного обеспечения в вашей организации в ту, которая производит более безопасный код.


10 основных рисков безопасности веб-приложений

В Топ-10 2021 года добавлены три новые категории, четыре категории с измененными названиями и областью действия, а также проведена некоторая консолидация.



 Документация

 Строитель

 Защитник

• [Предыдущая версия \(2017\)](#)

Загрузки или социальные ссылки

• [OWASP Топ 10 2017](#)
• [Другие языки → вкладка «Попытки перевода»](#)

Социальный

[Твиттер](#)

Репозиторий кода репо

Лидеры

[Эндрю ван дер Сток](#)
[Брайан Глас](#)
[Нил Смитлайн](#)
[Торстен Гиглер](#)

Предстоящие глобальные мероприятия OWASP

[OWASP Global AppSec EC 2025](#)

◦ 26-30 мая 2025 г.

[OWASP Global AppSec USA 2025 — Вашингтон, округ Колумбия](#)

◦ 3-7 ноября 2025 г.

[OWASP Global AppSec USA 2026 – Сан-](#)

- **A01:2021-Broken Access Control**

Франциско, Калифорния

поднимается с пятой позиции; 94% приложений были протестированы на наличие какой-либо формы сломанного контроля доступа. 34 списка общих уязвимостей (CWE), сопоставленных с Broken Access Control, имели больше случаев в приложениях, чем любая другая категория.

- 2-6 ноября 2026 г.

- **A02:2021-Криптографические сбои**

поднимаются на одну позицию вверх на #2, ранее известные как Разоблачение конфиденциальных данных, что было скорее общим симптомом, чем основной причиной. Здесь снова основное внимание уделяется сбоям, связанным с криптографией, которые часто приводят к раскрытию конфиденциальных данных или компрометации системы.

- **A03:2021-Внедрение** опускается на третью позицию. 94% приложений были протестированы на наличие той или иной формы внедрения, и 33 CWE, сопоставленные с этой категорией, занимают второе место по частоте встречаемости в приложениях. В этом выпуске к этой категории теперь относится межсайтовый скриптинг.

- **A04:2021-Небезопасный дизайн** — это новая категория 2021 года, в которой основное внимание уделяется рискам, связанным с недостатками дизайна. Если мы действительно хотим «двигаться влево» как отрасль, это требует более широкого использования моделирования угроз, безопасных шаблонов и принципов проектирования и эталонных архитектур.

- **A05:2021-Security Misconfiguration**
поднимается с #6 в предыдущем выпуске; 90% приложений были протестированы на наличие той или иной формы неправильной конфигурации. С ростом перехода на высококонфигурируемое программное обеспечение неудивительно, что эта категория поднимается. Бывшая категория XML External Entities (XXE) теперь является частью этой категории.
- **A06:2021-Уязвимые и устаревшие компоненты** ранее назывались «Использование компонентов с известными уязвимостями» и занимают 2-е место в опросе сообщества Top 10, но также имели достаточно данных, чтобы попасть в Top 10 с помощью анализа данных. Эта категория поднялась с 9-го места в 2017 году и является известной проблемой, которую мы с трудом тестируем и оцениваем риск. Это единственная категория, в которой нет общих уязвимостей и воздействий (CVE), сопоставленных с включенными CWE, поэтому в их оценках учитываются эксплойты и веса воздействия по умолчанию 5,0.
- **A07:2021-Identification and Authentication Failures** ранее называлась Broken Authentication и сползает со второй позиции вниз, а теперь включает CWE, которые больше связаны с ошибками идентификации. Эта категория по-прежнему является неотъемлемой частью Топ-10, но возросшая доступность стандартизированных фреймворков, похоже, помогает.

- **A08:2021-Software and Data Integrity Failures** — это новая категория 2021 года, которая фокусируется на предположениях, связанных с обновлениями программного обеспечения, критическими данными и конвейерами CI/CD без проверки целостности. Одно из самых высококовзвешенных воздействий от данных Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS), сопоставленных с 10 CWE в этой категории. Небезопасная десериализация с 2017 года теперь является частью этой более крупной категории.
- **A09:2021-Security Logging and Monitoring Failures** ранее был Insufficient Logging & Monitoring и добавлен из отраслевого опроса (#3), переместившись с #10 ранее. Эта категория расширена за счет включения большего количества типов сбоев, ее сложно тестировать, и она недостаточно хорошо представлена в данных CVE/CVSS. Однако сбои в этой категории могут напрямую влиять на видимость, оповещение об инцидентах и криминалистику.
- **A10:2021-Server-Side Request Forgery** добавлен из опроса сообщества Top 10 (#1). Данные показывают относительно низкий уровень заболеваемости с покрытием тестирования выше среднего, а также рейтинги выше среднего для Exploit и Impact potential. Эта категория представляет собой сценарий, в котором члены сообщества безопасности говорят нам, что это важно, хотя это не

проиллюстрировано в данных на данный
момент.

 [Редактировать на GitHub](#)

[HOME](#) [PROJECTS](#) [CHAPTERS](#) [EVENTS](#) [ABOUT](#)



[КОНФИДЕНЦИАЛЬНОСТЬ](#) [КАРТА САЙТА](#) [КОНТАКТ](#)

Open Web Application Security Project, OWASP, Global AppSec, AppSec Days, AppSec California, SnowFROC, LASCON и логотип OWASP являются товарными знаками OWASP Foundation. Если не указано иное, весь контент на сайте защищен лицензией Creative Commons Attribution-ShareAlike v4.0 и предоставляется без гарантии обслуживания или точности. Для получения дополнительной информации см. наш [Общий отказ от ответственности](#). OWASP не одобряет и не рекомендует коммерческие продукты или услуги, что позволяет нашему сообществу оставаться нейтральным по отношению к поставщикам с коллективной мудростью лучших умов в области безопасности программного обеспечения во всем мире. Авторские права 2024, OWASP Foundation, Inc.

Подборка наших корпоративных сторонников



PROMON

DEFECTDOJO



HITACHI
Inspire the Next



aikido

Cydrill
Code responsibly



monzo

[Станьте корпоративным сторонником](#)