Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Безопасность веб-приложений: аудит и типовые уязвимости

Почему дыры в сайте и личном кабинете — риск для всей компании и как найти их раньше хакеров

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У компаний до 50 рабочих мест почти всегда есть публичные веб-сервисы: сайт, личный кабинет, магазин, веб-доступ к 1С или CRM. Делал их подрядчик, безопасность никто не проверял, обновления не ставятся. О дырах владелец узнаёт постфактум — когда база клиентов уже продаётся или через сайт зашли в сеть. Штрафы за утечку персданных с 30.05.2025 — миллионы рублей.

Почему это важно бизнесу

- Веб-приложение — входная дверь в сеть: сайт на одном сервере с почтой, CRM и базой 1С открывает атакующему путь ко всей инфраструктуре
- Утечка клиентской базы — штраф до 15 млн ₽ за первый случай (свыше 100 тыс. субъектов) и 1–3% годовой выручки за повторный (с 30.05.2025)
- Простой сайта или личного кабинета — остановка продаж: восстановление после взлома из проверенного бэкапа занимает часы, без бэкапа — дни
- Малый бизнес атакуют автоматически: боты сканируют все сайты подряд, известные дыры в CMS и плагинах эксплуатируются в первые же дни
- Данные клиентов в продаже — потеря доверия, отток и иски; репутацию восстанавливать дольше, чем сайт

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

24 часа

на первичное уведомление Роскомнадзора о факте утечки персданных; ещё 72 часа — на результаты…

152-ФЗ, ст. 21, ч. 3.1

до 15 млн ₽

штраф за первую утечку данных свыше 100 тыс. субъектов ПДн; за неуведомление об инциденте — до…

КоАП РФ, ст. 13.11 (ред. 420-ФЗ)

1–3%

годовой выручки — оборотный штраф за повторную утечку: не менее 20 млн ₽ и не более 500 млн ₽

КоАП РФ, ст. 13.11 (ред. 420-ФЗ)

10

категорий рисков OWASP Top 10:2021 — базовый объём нашего аудита, от A01 Broken Access Control…

OWASP Top 10:2021

5 попыток

входа до блокировки IP на час — порог в нашем шаблоне fail2ban (maxretry=5) для админ-панелей…

шаблон ITfresh, fail2ban

72 часа

наш норматив на установку критических патчей CMS и плагинов; плановые обновления — еженедельно…

регламент сопровождения ITfresh

РЕАЛИЗАЦИЯ 1 ИЗ 3

IDOR в личном кабинете: любой клиент видел чужие заказы

Что настраиваем

Оптовая торговая компания, ~40 рабочих мест, Москва

Как мы это делаем

1. Аудит по OWASP Top 10: личный кабинет отдавал счета по ссылке вида /orders/4812/invoice.pdf без проверки владельца заказа
2. Перебор идентификатора в URL из-под тестовой учётки открыл документы других клиентов: реквизиты, суммы, адреса доставки
3. Причина: контроль доступа был только на уровне меню интерфейса, серверная проверка принадлежности объекта отсутствовала
4. Исправление: проверка владельца по сессии на каждом запросе к объекту, непредсказуемые UUID вместо сквозной нумерации, автотест на доступ к чужим ID в регрессии

РЕЗУЛЬТАТ

Уязвимость класса A01 Broken Access Control жила в кабинете два года — с момента сдачи подрядчиком. Формально это готовая утечка персданных: по нормам с 30.05.2025 — риск штрафа в миллионы рублей, плюс уход клиентов, чьи цены и объёмы закупок увидели бы конкуренты.

КЛЮЧЕВОЙ НЮАНС

Проверка «вошёл ли пользователь» не равна проверке «его ли это данные». Каждый запрос к объекту должен валидировать владельца на сервере — это первый пункт нашего чек-листа аудита.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Сайт «сделали и забыли»: веб-шелл через устаревший плагин

Что настраиваем

Производственная компания, сайт-каталог на WordPress

Как мы это делаем

1. Хостер прислал жалобу на рассылку спама с аккаунта; сайт не обновлялся с момента запуска — больше трёх лет
2. Разбор: в wp-content/uploads лежали посторонние PHP-файлы — веб-шелл, залитый через уязвимость загрузки файлов в устаревшем плагине
3. Через шелл атакующие читали wp-config.php с кредами базы и рассылали спам; в базе — форма заявок с телефонами клиентов
4. Лечение: чистая переустановка ядра и плагинов, удаление шелла, смена паролей и ключей (AUTH_KEY и солей), запрет исполнения PHP в uploads, fail2ban на wp-login.php

РЕЗУЛЬТАТ

Домен успел попасть в спам-листы, деловая переписка компании неделю уходила в спам у контрагентов. Цена инцидента — простой, чистка репутации домена и внеплановые работы; профилактикой было бы одно плановое обновление в месяц.

КЛЮЧЕВОЙ НЮАНС

CMS без регулярных обновлений — вопрос времени, а не вероятности. Обновления ядра и плагинов плюс запрет исполнения PHP в каталогах загрузки закрывают самый массовый вектор атак.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Веб-доступ к 1С опубликован в интернет без защиты

Что настраиваем

Компания сферы услуг, база 1С:Бухгалтерия на своём сервере

Как мы это делаем

1. Инвентаризация внешнего периметра: на публичном IP найдена публикация базы 1С через Apache — доступна всему интернету по HTTP без шифрования
2. В журнале регистрации 1С — многодневный перебор паролей по списку типовых логинов; у части пользователей базы пароль не был задан вообще
3. Исправление: HTTPS с сертификатом, доступ к публикации только с IP офиса и через VPN, обязательные пароли и отключение неиспользуемых пользователей 1С
4. Дополнительно: отдельный каталог публикации с default.vrd, обратный прокси с базовой аутентификацией перед 1С и алерт на серии неудачных входов

РЕЗУЛЬТАТ

База со всей бухгалтерией, зарплатами и контрагентами сутками стояла открытой под перебором. Успешный вход дал бы утечку персданных сотрудников и полную картину финансов компании — при том что «дыра» создана одной галочкой при публикации.

КЛЮЧЕВОЙ НЮАНС

Публикация 1С на веб-сервере — полноценное веб-приложение со всеми его рисками: только HTTPS, ограничение по IP или VPN и парольная политика в самой базе. Внешний периметр инвентаризуем регулярно.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Сайт «сделали и забыли»**
  CMS, плагины и библиотеки не обновляются годами; известные уязвимости боты эксплуатируют автоматически — иногда в первые дни после публикации патча.
- ✕ **Проверяют вход, но не права**
  Приложение проверяет логин, но не владельца данных: перебором ID в адресе любой клиент видит чужие документы и заказы (IDOR).
- ✕ **«Сырые» SQL-запросы «временно»**
  Параметры из форм подставляются прямо в текст запроса вместо параметризованных запросов — классическая SQL-инъекция позволяет выгрузить всю базу клие…
- ✕ **Нет лимитов на попытки входа**
  Пароли админки подбираются ботами неделями без препятствий: ни блокировок (fail2ban), ни лимитов запросов (nginx limit_req), ни двухфакторной аутенти…
- ✕ **Служебные панели открыты всем**
  Админки, тестовые поддомены и phpMyAdmin доступны из интернета, часто со стандартными или общими паролями.
- ✕ **Подробные ошибки на боевом сервере**
  Стек-трейсы, версии ПО и пути в сообщениях об ошибках подсказывают атакующему, что именно эксплуатировать; display_errors на проде должен быть выключ…
- ✕ **Ответственность не закреплена**
  Подрядчик сдал сайт, договор закончился — обновлять и закрывать дыры формально некому, инцидент обнаруживают клиенты.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Обновить CMS, плагины и серверное ПО; удалить неиспользуемые модули и темы
- HTTPS везде (Let's Encrypt с автопродлением certbot), уникальные пароли и 2FA для вс…
- Ежедневные резервные копии сайта и БД с хранением вне хостинга и проверкой восстанов…
- Лимиты попыток входа (fail2ban, maxretry=5), закрыть тестовые поддомены и служебные…

НОРМАЛЬНО

- Ежегодный внешний аудит по OWASP Top 10 плюс регулярный автоскан (OWASP ZAP baseline…
- WAF перед сайтом (ModSecurity + OWASP Core Rule Set), nginx limit_req на формы входа…
- Минимальные права: разработчик не админ прода, доступы персональные, ключи вместо па…
- План реагирования: уведомление Роскомнадзора в 24 часа, результаты расследования — в…

ХОРОШО

- Проверки в CI/CD: SAST, DAST (OWASP ZAP) и аудит зависимостей (composer audit, npm a…
- Пентест критичных систем ежегодно и после крупных доработок
- Мониторинг: серии неудачных входов, контроль целостности файлов, аномальный трафик —…
- Контроль сторонних скриптов: заголовки CSP, атрибуты SRI, инвентаризация всех интегр…

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Вы знаете все свои веб-ресурсы: сайт, личные кабинеты, веб-версии 1С/CRM, тестовые поддомены?
- [ ] Внешние специалисты хотя бы раз проверяли безопасность вашего сайта или веб-приложения?
- [ ] CMS, плагины и библиотеки сайта обновляются регулярно, а не «как поставили при запуске»?
- [ ] Вход в админ-панель защищён: сложный пароль, 2FA, ограничение по IP?
- [ ] Формы входа защищены от перебора паролей: лимиты попыток, блокировки, капча?
- [ ] Персональные данные клиентов на сайте передаются и хранятся в зашифрованном виде?
- [ ] Резервные копии сайта и базы хранятся отдельно от хостинга, и вы проверяли восстановление?
- [ ] Определено, кто и в какой срок действует, если сайт взломали или обнаружена утечка?
- [ ] Подрядчик, делавший сайт, до сих пор отвечает за его безопасность по договору?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит безопасности сайта и веб-приложений: OWASP Top 10, админ-панели, формы, API, зависимости
- Устранение уязвимостей: обновления CMS и библиотек, WAF, HTTPS, заголовки безопасности, лимиты запросов
- Приведение сайта в соответствие 152-ФЗ: согласия, хранение персданных, уведомления Роскомнадзора
- Сопровождение: регулярные обновления, мониторинг, резервные копии, повторные проверки после доработок

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 OWASP Top 10:2021 — категории рисков A01–A10 (owasp.org — 2021)

02 OWASP Web Security Testing Guide v4.2 — методика тестирования (owasp.org — 2020)

03 OWASP Application Security Verification Standard 5.0 (owasp.org — 2025)

04 OWASP Core Rule Set 4.x — правила WAF для ModSecurity (coreruleset.org — 2024)

05 nginx: ngx_http_limit_req_module — лимиты запросов на формы входа и API (nginx.org — 2025)

06 MDN: Content-Security-Policy и Subresource Integrity (developer.mozilla.org — 2025)

07 152-ФЗ ст. 21 и КоАП ст. 13.11 в ред. 420-ФЗ — уведомления и штрафы за уте… (publication.pravo.gov.ru — 2025)

08 ИТС 1С: публикация информационных баз на веб-серверах (its.1c.ru — 2025)

Основано на официальной документации продуктов и нашей практике внедрения.