ORBITDESK / ВЕБ-ПРИЛОЖЕНИЕ

Отчёт о безопасности

orbitdesk.example

Это учебный пример вымышленного отчёта, а не результат реального сканирования. Все данные, запросы и обнаруженные проблемы придуманы, реальные клиентские данные не используются.

Критический	Высокий	Средний	Приватность
01	02	01	02

Категория приватности частично совпадает с уровнями риска — это одни и те же проблемы, а не отдельные ошибки.

01 / ГЛАВНОЕ ДЛЯ ВАШЕЙ КОМАНДЫ

Наибольший риск — возможность доступа к приватной переписке без авторизации. Также необходимо исправить механизмы начисления кредитов и управления доступом к вложениям. Причина первых трёх проблем — недостаточная проверка прав на сервере или избыточное доверие данным, поступающим от клиента.

Продукт и технологии

Вымышленный SaaS-сервис для командной работы: чаты, обмен файлами и платные кредиты для доступа к дополнительным функциям.

React · TypeScript · Supabase · PostgreSQL

Учебные сценарии включают роли: гость, пользователь A и пользователь B. Все чаты, файлы и балансы являются вымышленными.

Находки по приоритету

Критический

CMA-01 · Supabase RPC · chat_previews

Последние сообщения из чужих чатов доступны без авторизации

> **Влияние на бизнес**
>
> Гость может увидеть превью приватных разговоров. Последнее сообщение может содержать конфиденциальную информацию — договорённости, контакты и прочее.

Что происходит в учебном сценарии

В учебном сценарии для доступа к странице чатов нужен вход в систему, однако функция chat_previews выдаёт последнее сообщение тестового чата гостю без пользовательской сессии.

Причины возникновения риска

Функция приложения позволяет выполнять вызов без пользовательской сессии и не проверяет, участвует ли пользователь в чате. Защита страницы не распространяется на отдельный запрос.

Учебное наблюдение

```
УЧЕБНЫЙ ЗАПРОС
POST https://api.orbitdesk.example/rest/v1/rpc/chat_previews
Сессия пользователя: отсутствует

СМОДЕЛИРОВАННЫЙ ОТВЕТ · HTTP 200
{ "chat": "fixture-chat-A",
  "last_message": "Учебное приватное сообщение A" }

Ожидается: отказ в доступе.
```

Необходимые изменения

- Запретить анонимный вызов функции. Для каждого возвращаемого чата проверять наличие сессии и участие в нём пользователя.
- Пересмотреть права EXECUTE и правила доступа к данным. Для функций с расширенными правами внедрить явную проверку принадлежности объектов.
- Провести тестирование для гостя, участника чата и других пользователей с использованием синтетических данных.

Как принять исправление

Гость получает отказ. Пользователь A видит только свой тестовый чат. Пользователь B не видит его превью.

Высокий

CMA-02 · Billing API · credit_grant

Кредиты начисляются по флагу из браузера без оплаты.

> **Влияние на бизнес**
>
> Пользователь может получить платные ресурсы без покупки, что приводит к прямым расходам сервиса и подрывает надёжность баланса.

Что происходит в учебном сценарии

В учебной модели сервер принимает от тестового клиента параметр paid: true и увеличивает баланс с 0 до 500, при этом подтверждённого платежа нет.

Причины возникновения риска

Начисление кредитов зависит от клиентского параметра. Сервер не проверяет подтверждённый платёж, его сумму и владельца заказа.

Учебное наблюдение

```
УЧЕБНАЯ МОДЕЛЬ
Пользователь: fixture-user-A
Баланс до: 0
Клиентский параметр: paid = true
Подтверждённый платёж: отсутствует
Баланс после: 500

Ожидается: баланс остаётся 0.
```

Необходимые изменения

- Начислять кредиты только после того, как сервер проверит статус платежа и подлинность уведомления от платёжного провайдера.
- На сервере определять сумму и получателя по заказу. Изменение флага на клиенте не должно влиять на баланс.
- Обеспечить идемпотентность начисления: повторное уведомление о платеже не должно приводить к повторному начислению кредитов.

Как принять исправление

Флаг paid: true на клиенте не влияет на баланс. Подтверждённый тестовый платёж приводит к начислению кредитов только один раз, повтор события не даёт дополнительного начисления.

Высокий

CMA-03 · Storage · private attachments

Приватное вложение доступно пользователю из другого чата

> **Влияние на бизнес**
>
> Знание ссылки позволяет получить доступ к файлу вне контекста разрешённого разговора. Защита сообщений не гарантирует защиту вложений.

Что происходит в учебном сценарии

В учебном сценарии файл fixture-attachment-A привязан к чату A. Пользователь B получает ответ HTTP 200 по ссылке на файл, хотя не является участником чата A.

Причины возникновения риска

Доступ к файлу не зависит от прав участника. Сложное имя файла не заменяет контроль доступа.

Учебное наблюдение

```
УЧЕБНАЯ МОДЕЛЬ ДОСТУПА
Объект: fixture-attachment-A
Владелец: тестовый чат A
Запрос: пользователь B
Участник чата A: нет
Смоделированный ответ: HTTP 200

Ожидается: HTTP 403 или 404.
```

Необходимые изменения

- Перед предоставлением файла или временной ссылки проверять, является ли пользователь участником чата.
- Организовать закрытое хранилище и установить правила доступа к объектам, а не только к сообщениям.
- Не сохранять приватные вложения в общие кеши, которые остаются доступными после смены пользователя.

Как принять исправление

Владелец тестового файла получает доступ, пользователь другого чата и гость — отказ.

Средний

CMA-04 · Browser · credential storage

Пароль сохраняется в хранилище браузера

> **Влияние на бизнес**
>
> При выполнении стороннего JavaScript-кода на странице или получении доступа к профилю браузера может быть раскрыт сохранённый пароль. Однако наличие записи само по себе не означает, что доступ уже был получен.

Что происходит в учебном сценарии

В рамках учебного сценария после авторизации в localStorage остаётся поле saved_password, но для восстановления интерфейса пароль не требуется.

Причины возникновения риска

Форма сохраняет введённые учётные данные вместе с пользовательскими настройками.

Учебное наблюдение

```
УЧЕБНОЕ НАБЛЮДЕНИЕ
Хранилище: localStorage
Ключ: saved_password
Значение: [учебное значение скрыто]
Запись сохраняется после завершения входа.
```

Необходимые изменения

Исключить сохранение паролей в localStorage и sessionStorage, удалить уже имеющиеся записи.

Воспользоваться механизмом сессии, предусмотренным системой авторизации. Хранить настройки интерфейса отдельно от учётных данных.

Как принять исправление

После авторизации и выхода из системы пароль не должен присутствовать в браузерных хранилищах.

План исправления

Сначала	CMA-01	Ограничить анонимный доступ к превью чатов и проверить права участников
До запуска	CMA-02 · CMA-03	Связать кредиты с подтверждёнными платежами и обеспечить защиту приватных вложений
Следом	CMA-04	Удалите сохранённые пароли и проверьте механизм хранения сессии.

Исправление завершено, если разрешённые сценарии функционируют, запрещённые — блокируются, а изменения проверены на тестовых данных.