ОТЧЁТ / ВЕБ-САЙТ И API

Отчёт о проверке веб-сайта и API

Учебный стенд Atlas Shop · Контроль доступа веб-сайта и API

ВЫВОД ДЛЯ РУКОВОДИТЕЛЯ

Три сценария показывают нарушения контроля доступа

В демонстрационной модели сервер недостаточно проверяет владельца объекта, право на функцию и границу организации.

HIGH

3 находки

учебный пример

ЧТО ПРОВЕРИЛИ

01 **Объекты**

принадлежность заказа пользователю

02 **Функции**

доступ к административному экспорту

03 **Организации**

изоляция данных арендаторов

04 **Роли**

матрица разрешённых действий

ПРИОРИТЕТНАЯ НАХОДКА

HIGH · ДЕМОНСТРАЦИЯ

Доступ к чужому заказу по ID

Контролируемый запрос вернул синтетический заказ другой организации. Интерфейс его скрывает, однако API не применяет то же правило принадлежности.

Карточка, доказательство и ретест >

DEMO-01

ВЫСОКИЙ РИСК · УЧЕБНЫЙ СТЕНД

Доступ к чужому заказу по ID

Риск: чтение заказа и данных клиента за пределами разрешённой организации.

ЗАПРОС В КОНТРОЛИРУЕМОМ СЦЕНАРИИ

```
GET /api/orders/7814
```

КОНТРОЛИРУЕМОЕ ПОДТВЕРЖДЕНИЕ

✓ 01	**Ожидаемо**	Пользователь организации alpha не получает заказ организации beta: HTTP 403 или 404.
✓ 02	**Фактически**	API вернул HTTP 200 и синтетические поля чужого заказа после замены только order_id.
✓ 03	**Граница**	Массовое извлечение не выполнялось; все записи созданы специально для учебного стенда.

ВОЗМОЖНОЕ ВЛИЯНИЕ

Заказы и клиенты

В реальном сервисе номера заказов, состав покупки, контакты и адрес доставки могли бы стать доступны пользователю другой организации.

ГРАНИЦЫ ВЫВОДА

Без массового извлечения

Данные массово не выгружались. Производственная система не проверялась. Вывод относится только к вымышленному Atlas Shop.

ИСПРАВЛЕНИЕ И ПОВТОРНАЯ ПРОВЕРКА

1 Проверять объект

Загружать заказ вместе с owner_id и tenant_id из доверенного серверного контекста.

2 Закрыть все пути

Применить правило к просмотру, скачиванию, изменению и экспорту заказа.

3 Провести ретест

Свой заказ: 200. Чужой заказ: 403/404. Соседние id не раскрывают существование объекта.

ИСТОЧНИК OWASP API Security Top 10 · API1: Broken Object Level Authorization · owasp.org/API-Security

02 / ГРАНИЦЫ И МЕТОДИКА

Что именно проверялось

Полный отчёт фиксирует среду, роли, разрешённые действия и ограничения выводов.

ПАРАМЕТР	ЗАФИКСИРОВАННОЕ УСЛОВИЕ
Объект	Вымышленный учебный сервис Atlas Shop: веб-интерфейс и REST API.
Среда	Изолированный стенд с синтетическими заказами и двумя организациями.
Роли	Пользователь, менеджер организации и администратор платформы.
Фокус	Авторизация на уровне объекта, функции и организации.
Не выполнялось	Нагрузочное тестирование, социальная инженерия, массовое извлечение.

ПОСЛЕДОВАТЕЛЬНОСТЬ ПРОВЕРКИ

01 **Карта ролей**

Определены субъект, объект, организация и действие.

02 **Позитивный сценарий**

Проверена законная операция со своим объектом.

03 **Негативный сценарий**

Заменены id, роль или организация.

04 **Ручная валидация**

Сравнены ожидаемый и фактический ответы.

ВАЖНО

Доказательства полностью синтетические

Реальные системы не проверялись. В рабочем отчёте указываются фактические версии, время, идентификаторы запросов и защищённые приложения.

03 / РЕЕСТР РИСКОВ

Три учебные находки

Приоритет связывает достижимость сценария, ценность данных и ширину затронутого процесса.

ID	НАХОДКА	РИСК	ПРИЧИНА	СТАТУС
DEMO-01	Доступ к чужому заказу по id	Высокий	Нет проверки объекта	Открыта
DEMO-02	Экспорт клиентов для менеджера	Высокий	Нет проверки функции	Открыта
DEMO-03	tenant_id принимается из запроса	Средний	Ослаблена изоляция	Открыта

КАК ЧИТАТЬ ПРИОРИТЕТ

Высокий

Нарушена значимая граница доступа. Исправление требуется до расширения функции.

Средний

Сценарий подтверждён, но влияние зависит от роли и фактического состава данных.

Не оценено

Недостаточно подтверждений. Наблюдение не называется уязвимостью.

МАРШРУТ НАХОДКИ



DEMO-02 ВЫСОКИЙ РИСК

Экспорт клиентов без права на функцию

Роль менеджера вызывает административную операцию напрямую через API.

КОНТРОЛИРУЕМЫЙ ЗАПРОС

```
POST /api/admin/customers/export Role: manager
```

ОЖИДАЕМО

HTTP 403. Нужна роль platform_admin и отдельное разрешение export_customers.

ФАКТИЧЕСКИ В УЧЕБНОЙ МОДЕЛИ

HTTP 202. Сервер создал задачу и вернул ссылку на синтетический CSV-файл.

ПОДТВЕРЖДЕНИЕ

Пункт меню скрыт для менеджера. Прямой POST с его действительным токеном создаёт экспорт. Без токена сервер отвечает 401: аутентификация есть, авторизация функции отсутствует.

ВЛИЯНИЕ НА БИЗНЕС

Экспорт концентрирует данные многих клиентов в одном файле и увеличивает масштаб возможного раскрытия.

ПЕРВОПРИЧИНА

Ограничение реализовано только в интерфейсе. Контроллер проверяет сессию, но не право export_customers.

ИСПРАВЛЕНИЕ

Добавить серверную policy-проверку до постановки задачи. Связать ссылку с инициатором и ограничить срок её жизни. Записывать субъект и область экспорта в журнал.

КРИТЕРИЙ РЕТЕСТА

manager: 403 без задачи;
platform_admin с правом: 202;
администратор без права: 403.

DEMO-03 СРЕДНИЙ РИСК

Ослаблена изоляция организаций

API доверяет tenant_id, полученному из параметра обычного пользователя.

КОНТРОЛИРУЕМЫЙ ЗАПРОС

```
GET /api/invoices?tenant_id=beta Session tenant: alpha
```

ОЖИДАЕМО

Параметр игнорируется. Область выбирается только из доверенной серверной сессии.

ФАКТИЧЕСКИ В УЧЕБНОЙ МОДЕЛИ

HTTP 200. Ответ содержит два синтетических счёта организации beta.

ПОДТВЕРЖДЕНИЕ

Штатный запрос отправляет tenant_id=alpha. После замены на beta структура ответа сохраняется, а маркеры записей меняются на другую организацию. Без tenant_id сервер возвращает 400.

ВЛИЯНИЕ НА БИЗНЕС

В многопользовательском сервисе нарушение границы организаций может раскрывать финансовые документы.

ПЕРВОПРИЧИНА

Обязательный параметр ошибочно считается доверенным и напрямую участвует в фильтре репозитория.

ИСПРАВЛЕНИЕ

Удалить tenant_id из публичного контракта обычной роли. Передавать область из авторизационного контекста на уровень репозитория и применять ко всем чтениям, подсчётам и экспортам.

КРИТЕРИЙ РЕТЕСТА

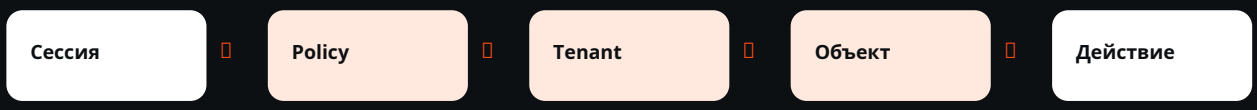
Пользователь alpha получает только alpha при любых tenant_id. Переключение возможно лишь через разрешённый процесс.

07 / ИСПРАВЛЕНИЕ

Устранить общую причину

Три находки объединяет отсутствие единого серверного решения об авторизации.

ЦЕЛЕВАЯ СХЕМА



ПЛАН РАБОТ

ПРИОР.	РАБОТА	ВЛАДЕЛЕЦ	КРИТЕРИЙ
P1	Единая policy-функция	Разработка	Объект, функция и tenant проверяются до операции
P1	Негативные тесты ролей	QA	Матрица allow/deny выполняется в CI
P1	Защита экспорта	Backend	Policy, журнал и срок жизни ссылки
P2	Tenant context	Архитектор	Область берётся из доверенной сессии
P2	Ретест	Проверяющий	Исходные и соседние сценарии закрыты

ЧТО НЕ СЧИТАЕТСЯ ИСПРАВЛЕНИЕМ

Скрытие кнопки, смена числовых идентификаторов на UUID, фильтрация только в браузере и созданная задача без внедрения не устраняют причину. Решение должно применяться сервером к каждой значимой операции.

08 / ПОВТОРНАЯ ПРОВЕРКА

Критерии принятия результата

Статус «исправлено» появляется только после проверки внедрённой версии.

ID	ПОЗИТИВНЫЙ ТЕСТ	НЕГАТИВНЫЙ ТЕСТ	КРИТЕРИЙ
DEMO-01	Свой заказ: 200	Чужой заказ: 403/404	Принято после повтора
DEMO-02	Администратор с правом: 202	Менеджер: 403 без задачи	Принято после повтора
DEMO-03	Своя организация: данные	Чужая организация: нет данных	Принято после повтора

ПРОТОКОЛ РЕТЕСТА

01 **Зафиксировать версию** — Номер сборки, среду и время проверки.

02 **Повторить исходный запрос** — Те же роль, объект и условие.

03 **Проверить соседние пути** — Просмотр, изменение, экспорт и скачивание.

04 **Сохранить доказательство** — Ответ, журнал решения и итоговый статус.

ГРАНИЦА ПОДТВЕРЖДЕНИЯ

Ретест подтверждает согласованный сценарий в указанной версии. Он не является бессрочной гарантией и не оценивает новые функции автоматически.

09 / ПРИЛОЖЕНИЕ

Матрица доступа и ориентиры

Минимальный набор для воспроизведения логики и проверки границ решения.

РОЛЬ	ОБЪЕКТ	ДЕЙСТВИЕ	ОЖИДАЕМОЕ РЕШЕНИЕ
user	свой заказ	читать	Разрешить
user	чужой заказ	читать	Запретить
manager	свои клиенты	читать	Разрешить
manager	все клиенты	экспорт	Запретить
platform_admin	все клиенты	экспорт	Только с export_customers
user	чужая организация	счета	Запретить

МЕТОДИЧЕСКИЕ ОРИЕНТИРЫ

01	**OWASP API Security Top 10 2023**	API1: Broken Object Level Authorization; API5: Broken Function Level Authorization.
02	**OWASP ASVS 4.0.3**	Раздел V4: управление доступом и принцип запрета по умолчанию.
03	**CWE-639 / CWE-862 / CWE-284**	User-controlled key, missing authorization и improper access control.

КОНЕЦ ПУБЛИЧНОГО ОБРАЗЦА

Реальный отчёт формируется только по согласованному и разрешённому контуру.

audit-bezopasnosti.pro · info@audit-bezopasnosti.pro · +7 902 204-00-02