

Звіт про тестування на проникнення

Застосунок «ShopDemo» (вигаданий): інтернет-магазин із порталом клієнта та REST API

Це демонстраційний звіт на вигаданому застосунку. Усі дані, назви та значення вигадані. Жодного реального клієнта, компанії, IP-адреси чи особи не існує.

Дата звіту	2026-03-12
Версія	1.0
Класифікація	Конфіденційно (демонстраційний зразок)
Підготував	Veiltrack

1. Підсумок для керівництва

Veiltrack провів тестування на проникнення вебзастосунку та REST API вигаданого інтернет-магазину «ShopDemo» на копії продуктивного середовища (staging). Метою було перевірити, чи може клієнт магазину побачити чужі дані або обійти захист облікових записів.

Виявлено **4 зауваження**: 1 високого, 1 середнього, 1 низького рівня та 1 інформаційне. Найважливіше: **будь-який авторизований клієнт може переглядати рахунки інших клієнтів**, змінюючи число в адресі запиту. Це витік персональних і фінансових даних, його слід усунути першим.

Загальний ризик: підвищений. Критичних проблем, що дають повний контроль над системою, не знайдено. Але одна помилка контролю доступу вже достатня для витоку даних, а відсутність обмеження спроб входу полегшує підбір паролів. Усі зауваження усуваються без перебудови системи, зазвичай за кілька днів роботи розробників.

Рівень	Кількість	Що це означає
Високий	1	Потрібне негайне виправлення
Середній	1	Виправити протягом 30 днів
Низький	1	Виправити в плановому порядку
Інформаційний	1	Рекомендація щодо зміцнення

2. Обсяг, правила проведення та методологія

Об'єкт	Вигаданий застосунок «ShopDemo»: вебпортал клієнта (https://staging.shopdemo.example.com) та REST API (https://api.staging.shopdemo.example.com, версія v1)
Середовище	Staging-копія продуктивного середовища зі знеособленими тестовими даними. Продуктивне середовище не тестувалося
Вікно тестування	2026-03-02 ... 2026-03-06, 10:00 ... 18:00 (UTC+2). Джерело тестування: 203.0.113.10, 203.0.113.11
Облікові записи	Два тестові клієнти (customer-a, customer-b) та один тестовий адміністратор (admin-test). Усі створені замовником для тесту
Модель доступу	Сірий ящик: відомі документація API та облікові записи, вихідний код недоступний
Дозволено	Перевірка авторизації й автентифікації, аналіз запитів і відповідей, перевірка конфігурації, обмежене за кількістю тестування логіну на тестових акаунтах
Заборонено	Атаки на відмову в обслуговуванні, соціальна інженерія, доступ до реальних даних, зміна чи видалення чужих даних, обхід фізичних засобів захисту, тестування сторонніх сервісів
Стандарти й методики	OWASP Web Security Testing Guide (WSTG), OWASP API Security Top 10 2023, NIST SP 800-115. Оцінка ризику: CVSS v3.1

Звіт не є сертифікацією чи гарантією відсутності інших вразливостей. Він описує стан застосунку на момент тестування в межах узгодженого обсягу.

Етапи методу: Розвідка та вивчення документації API → Моделювання загроз за ролями (клієнт А, клієнт В, адміністратор) → Ручна перевірка авторизації, автентифікації та конфігурації → Підтвердження та безпечна фіксація доказів, знеособлення даних → Підготовка рекомендацій і звіту

3. Зауваження

SD-001. Порушення авторизації на рівні об'єкта (BOLA) в рахунках

ID	SD-001	Рівень	Високий
Категорія	Порушений контроль доступу на рівні об'єкта (OWASP API1:2023)	CWE	CWE-639
CVSS v3.1	7.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N		
Уражена точка	GET /api/v1/invoices/{id}		

Опис

Кінцева точка повертає рахунок за числовим ідентифікатором, але не перевіряє, що рахунок належить поточному користувачеві. Авторизований клієнт може отримати рахунки інших клієнтів, послідовно змінюючи ідентифікатор. Ідентифікатори послідовні, тому перелік не потребує вгадування.

Вплив на бізнес

Витік персональних даних клієнтів (ім'я, адреса, склад замовлення, суми) та фінансової інформації. Можливі порушення вимог законодавства про захист персональних даних, репутаційні втрати, ризик цільового шахрайства. Додатково поле примітки до рахунка можна змінювати через суміжний запит, тому оцінено ще й обмежений вплив на цілісність.

Докази

Облікові дані, токени та персональні дані знеособлені. Знімки екрана наведено в додатку до повної версії звіту (в демонстраційному зразку не включені).

```
GET /api/v1/invoices/10482 HTTP/1.1
Host: api.staging.shopdemo.example.com
Authorization: Bearer eyJ***[masked]***
(токен customer-a)
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{ "id": 10482,
  "customer": "J*** D***",
  "email": "j***@example.com",
  "total": "1 2** UAH",
  "owner_id": 3917 }
(рахунок належить іншому клієнту, не customer-a)
```

Кроки відтворення

- Увійти під тестовим акаунтом customer-a і відкрити власний рахунок, зафіксувати його ідентифікатор.
- Надіслати той самий запит із ідентифікатором рахунка, що належить тестовому акаунту customer-b.
- Переконатися, що відповідь має код 200 і містить дані customer-b.
- Зафіксувати результат у знеособленому вигляді; інші ідентифікатори не перебирати.

Рекомендації

- Перевіряти на сервері, що рахунок належить поточному користувачеві (або що в нього є відповідна роль), перед поверненням даних.
- Застосувати політику «заборонено за замовчуванням» для всіх об'єктних кінцевих точок.
- Як додатковий захід використати непослідовні ідентифікатори (UUID). Це не заміняє перевірку власника.
- Додати автоматизований тест: клієнт А не може читати й змінювати об'єкти клієнта В.

Критерій ретесту

Запит із токеном customer-a до рахунка customer-b повертає 403 або 404; тест на власність об'єктів входить до CI.

Зауваження SD-002 ... SD-004

SD-002. Відсутнє обмеження спроб входу

Середній

CVSS v3.1	6.5 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
Уражена точка	POST /api/v1/auth/login
Опис	Кінцева точка входу не обмежує кількість спроб і не вводить затримку чи блокування. Це створює ризик підбору паролів та атак із використанням витеклих пар «логін-пароль» (credential stuffing). Перевірку виконано на тестових акаунтах в обмеженому обсязі.
Рекомендації	Обмеження за акаунтом та IP, експоненційні затримки, тимчасове блокування, CAPTCHA після серії невдач, багатфакторна автентифікація, сповіщення про підозрілі входи.

SD-003. Докладні повідомлення про помилки розкривають версію фреймворку

Низький

CVSS v3.1	3.7 AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Уражена точка	Кілька кінцевих точок API (відповіді 500)
Опис	Відповіді з помилкою містять технічні деталі, зокрема назву та версію серверного фреймворку (у демонстрації: «ShopFramework 4.2.x»). Це спрощує підбір відомих вразливостей для цієї версії.
Рекомендації	Повертати загальні повідомлення про помилку з ідентифікатором запиту, технічні подробиці писати лише в журнал, вимкнути режим налагодження на всіх середовищах.

SD-004. Відсутні заголовки безпеки

Інформаційний

CVSS v3.1	не застосовується
Уражена точка	Вебпортал (усі сторінки)
Опис	Не виявлено заголовків: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, X-Frame-Options (або frame-ancestors у CSP), Referrer-Policy, Permissions-Policy. Самі по собі вони не дають вразливості, але зменшують захист за іншої помилки.
Рекомендації	Додати перелічені заголовки на рівні вебсервера чи проксі, CSP впроваджувати спочатку в режимі звітування.

4. Пріоритетність усунення та ретест

Коли	ID	Дія	Орієнтовна складність
Виправити першим	SD-001	Серверна перевірка власника об'єкта, тест на авторизацію	Середня (1-3 дні)
Протягом 30 днів	SD-002	Обмеження спроб входу, MFA, сповіщення	Середня (2-4 дні)
Протягом 30 днів	SD-003	Загальні повідомлення про помилки, вимкнути debug	Низька (до 1 дня)
Коли буде зручно	SD-004	Додати заголовки безпеки	Низька (до 1 дня)

Ретест виконується за умовами пакета. Після виправлень Veiltrack перевіряє кожне зауваження за критерієм ретесту та випускає оновлену версію звіту. Обсяг і строки ретесту визначаються обраним пакетом.

Це демонстраційний звіт на вигаданому застосунку. Усі дані, назви та значення вигадані. Жодного реального клієнта, компанії, IP-адреси чи особи не існує.

Хочете такий звіт для свого застосунку? veiltrack.io/pentest