RAPORT Z TESTU PENETRACYJNEGO

Aplikacja webowa i API

Portal klienta B2B
Ocena separacji organizacji, dostępu i odzyskiwania konta

Wersja 1.1 po reteście
Raport wydany 19 sierpnia 2026

KOD PROJEKTU	OKNO TESTOWE	WERSJA
PT24-2026-081	12-13.08.2026	1.1 / RETEST

Materiał referencyjny bez danych rzeczywistego klienta

PENTEST24.PL

SEKCJA 01

Podsumowanie dla osób decyzyjnych

Test wykazał istotną lukę w separacji organizacji oraz błąd w procesie odzyskiwania konta. Najważniejsze poprawki zostały wdrożone i potwierdzone w reteście.

1	1	2	3
KRYTYCZNE	WYSOKIE	ŚREDNIE	NISKIE

Najważniejszy wniosek

Kontrola dostępu do faktur była wykonywana w interfejsie, ale nie w warstwie API. Zwykły użytkownik mógł wskazać identyfikator innej organizacji i pobrać jej dokumenty rozliczeniowe. Poprawka przeniosła decyzję autoryzacyjną do wspólnej warstwy serwerowej.

Wpływ biznesowy

Potencjalny incydent obejmowałby poufność danych klientów, obowiązki kontraktowe, obsługę incydentu oraz ryzyko utraty zaufania. Nie stwierdzono dowodów wykorzystania poza uzgodnionym testem.

Stan napraw

Zamknięte	WEB-01, WEB-02 i WEB-05. Poprawki potwierdzone w uzgodnionym zakresie retestu.
Ograniczone	WEB-03. Dodano dane korelacyjne, pełny próg alertowy pozostaje w planie.
Planowane	WEB-04 i WEB-06. Termin właścicielski: kolejny cykl wydawniczy.

Priorytety

- **Natychmiast:** egzekwować autoryzację zasobu w API i sprawdzić podobne endpointy.
- **Do 14 dni:** ujednolicić tokeny resetu, testy regresji i logowanie zdarzeń dostępu.
- **Do 30 dni:** dokończyć alerty między tenantami oraz redukcję danych diagnostycznych.

SEKCJA 02

Zakres, reguły i metodyka

Ocena objęła portal B2B oraz powiązane API w modelu grey box. Prace prowadzono według pisemnej autoryzacji i uzgodnionych Rules of Engagement.

Cel	Ocena separacji organizacji, odporności procesu logowania, odzyskiwania konta i bezpieczeństwa API.
Zakres	portal.example.test, api.example.test/v1, role: użytkownik, księgowość, administrator organizacji.
Model	Grey box. Trzy konta testowe, opis ról, kolekcja API i dane demonstracyjne.
Okno	12-13 sierpnia 2026, 09:00-18:00 CEST.
Wyłączenia	Testy przeciążeniowe, płatności rzeczywiste, system pocztowy i dostawcy zewnętrzni.
Autoryzacja	Pisemna zgoda właściciela celu, kontakt alarmowy i warunki natychmiastowego przerwania.

Przebieg prac

01	**Przygotowanie**	Autoryzacja, zakres, role, dane testowe, kontakty i warunki STOP.
02	**Test ręczny**	Autoryzacja, sesje, API, logika biznesowa i granice tenantów.
03	**Walidacja**	Powtórzenie, ocena wpływu, bezpieczny dowód i eliminacja false positive.
04	**Raport i retest**	Priorytety napraw, omówienie oraz niezależne potwierdzenie poprawek.

Podstawy oceny

Zakres kontrolny oparto na OWASP Web Security Testing Guide, OWASP ASVS, OWASP API Security Top 10 i praktykach PTES. Ryzyko oceniano z uwzględnieniem CVSS 3.1 oraz wpływu na proces biznesowy.

Granice wniosku

Raport opisuje stan wskazanego zakresu i wersji w czasie testu. Nie stanowi gwarancji braku innych podatności ani certyfikatu zgodności. Istotna zmiana kodu, konfiguracji lub architektury może wymagać ponownej oceny.

WEB-01

KRYTYCZNE ZAMKNIĘTE

Dostęp do faktur innej organizacji przez zmianę identyfikatora

Obszar	API / kontrola dostępu / separacja tenantów
Wpływ	Odczyt dokumentów i danych rozliczeniowych innych klientów.
Warunki	Zwykłe konto dowolnej organizacji oraz identyfikator zasobu.
Klasyfikacja	OWASP A01: Broken Access Control / CVSS 3.1: 9.1

Opis techniczny

Interfejs ukrywał faktury innych organizacji, ale endpoint API sprawdzał jedynie ważność sesji. Nie weryfikował relacji użytkownika z organizacją wskazaną w ścieżce. Zmiana identyfikatora zwracała dokumenty innego klienta.

Dowód

```
GET /v1/organizations/2002/invoices HTTP/1.1
Host: api.example.test
Authorization: Bearer [REDACTED]

HTTP/1.1 200 OK
{"invoice_id":"INV-2048","organization_id":2002}
```

Przyczyna

Decyzja autoryzacyjna była rozproszona między interfejsem a kontrolerami API. Brakowało wspólnej warstwy, która wiązała każdy obiekt z zaufanym kontekstem tenantów z sesji.

Rekomendacja

Egzekwować autoryzację zasobu po stronie serwera dla każdego żądania. Organizację wyznaczać z zaufanego kontekstu sesji albo jednoznacznie sprawdzać relację użytkownik-organizacja. Dodać testy regresji dla macierzy rola-organizacja-operacja oraz alerty dla prób dostępu między tenantami.

Wynik retestu

Endpoint zwracał 403 dla użytkownika spoza organizacji. Sprawdzono listę, szczegóły, pobieranie PDF i eksport CSV. Nie stwierdzono obejścia w uzgodnionym zestawie przypadków.

WEB-02

WYSOKIE ZAMKNIĘTE

Token resetu hasła pozostaje aktywny po pierwszym użyciu

Obszar	Uwierzytelnienie / odzyskiwanie konta
Wpływ	Ponowne przejęcie konta przez osobę posiadającą wcześniej ujawniony link.
Warunki	Dostęp do wcześniejszego tokenu przed upływem 60 minut.

Opis

Po ustawieniu nowego hasła token nie był oznaczany jako wykorzystany. Ten sam link pozwalał ponownie zmienić hasło do czasu wygaśnięcia. Zwiększało to wpływ przejętej skrzynki lub ujawnionego adresu URL.

Rekomendacja

Przechowywać skrót tokenu, oznaczać go jako wykorzystany w tej samej transakcji co zmiana hasła oraz unieważniać pozostałe tokeny użytkownika. Skrócić czas życia i nie umieszczać tokenów w logach analitycznych.

Wynik retestu

Po pierwszym użyciu token zwracał ogólną odpowiedź 400. Test równoległy potwierdził atomowe oznaczenie wykorzystania. Starsze tokeny tego samego użytkownika zostały unieważnione.

WEB-03

ŚREDNIE OGRANICZONE

Brak alertu dla seryjnych prób dostępu między tenantami

Aplikacja rejestrowała odpowiedzi 403, ale log nie zawierał identyfikatora organizacji źródłowej i docelowej. Utrudniało to wykrycie systematycznej enumeracji. Dodano dane korelacyjne bez treści dokumentów; próg alertowy pozostaje do wdrożenia.

Rekomendacja: emitować osobne zdarzenie bezpieczeństwa, korelować liczbę unikalnych celów i alarmować przy wzorcu wskazującym enumerację, bez zapisywania danych biznesowych w logu.

SEKCJA 05

Rejestr ustaleń

Poniższa tabela porządkuje wszystkie ustalenia, ich priorytet oraz stan po uzgodnionym reteście.

ID	USTALENIE	RYZYKO	STATUS
WEB-01	Dostęp do faktur innej organizacji	Krytyczne	Zamknięte
WEB-02	Token resetu wielokrotnego użycia	Wysokie	Zamknięte
WEB-03	Brak alertu dla enumeracji tenantów	Średnie	Ograniczone
WEB-04	Nadmierne dane diagnostyczne w odpowiedzi	Średnie	Planowane
WEB-05	Brak ograniczenia prób kodu zaproszenia	Niskie	Zamknięte
WEB-06	Niespójna polityka nagłówków ochronnych	Niskie	Planowane
WEB-07	Jawna wersja komponentu w błędzie API	Niskie	Zamknięte

Mechanizmy, które zadziałały poprawnie

- Tokeny sesji miały bezpieczne atrybuty i były unieważniane po zmianie hasła.
- Upload plików ograniczał typ, rozmiar i miejsce wykonania.
- Konta administracyjne wymagały MFA, a operacje krytyczne były rejestrowane.
- Dane w środowisku testowym nie zawierały informacji rzeczywistych klientów.

Pozytywna obserwacja potwierdza działanie w sprawdzonym scenariuszu i czasie testu. Nie jest gwarancją odporności poza zakresem.

SEKCJA 06

Plan naprawczy

Plan łączy pilność techniczną z wpływem biznesowym i kolejnością wdrożeń. Każdy punkt ma właściciela, termin oraz kryterium zamknięcia.

TERMIN	PRIORYTET	DZIAŁANIE	KRYTERIUM ZAMKNIĘCIA
0-24 h	Natychmiast	Zablokować dostęp między tenantami, przejrzeć logi i wskazać podobne endpointy.	403 poza tenantem, brak regresji dla ról uprawnionych.
1-14 dni	Wysoki	Wspólna warstwa autoryzacji, jednorazowe tokeny resetu i testy regresji.	Pokrycie macierzy ról i atomowe zużycie tokenu.
15-30 dni	Średni	Korelacja zdarzeń, alerty enumeracji i redukcja danych diagnostycznych.	Alert testowy oraz brak danych wrażliwych w logach.
Kolejny cykl	Doskonalenie	Threat modeling nowych przepływów i testy autoryzacji w CI.	Kontrola bezpieczeństwa jako warunek wydania.

Zasada zamknięcia

Ustalenie jest zamknięte, gdy poprawka działa dla opisanej ścieżki, nie powoduje regresji u ról uprawnionych i obejmuje rozsądny zestaw wariantów tego samego mechanizmu. Commit, zrzut ekranu lub deklaracja wdrożenia nie zastępują retestu.

Odpowiedzialność

Product owner	Priorytet biznesowy, komunikacja z klientami i akceptacja ryzyka resztkowego.
Zespół aplikacyjny	Poprawki autoryzacji, tokenów i odpowiedzi diagnostycznych.
Security / SOC	Zdarzenia bezpieczeństwa, korelacja i progi alertowe.
QA	Testy regresji ról, tenantów i procesu odzyskiwania konta.

SEKCJA 07

Wynik retestu

Retest przeprowadzono 19 sierpnia 2026 na wersji wdrożonej do środowiska testowego. Obejmował ustalenia WEB-01, WEB-02 i WEB-05 oraz podstawowe przypadki regresji.

USTALENIE	WYNIK	DOWÓD ZAMKNIĘCIA
WEB-01	ZAMKNIĘTE	403 poza tenantem dla listy, szczegółów, PDF i CSV. Brak regresji dla kont uprawnionych.
WEB-02	ZAMKNIĘTE	Token jednorazowy. Równoległe użycie oraz starsze tokeny odrzucone.
WEB-05	ZAMKNIĘTE	Limit prób, opóźnienie progresywne i zdarzenie bezpieczeństwa bez ujawnienia kodu.

Próba kontrolna

```
GET /v1/organizations/2002/invoices HTTP/1.1
Host: api.example.test
Authorization: Bearer [REDACTED]

HTTP/1.1 403 Forbidden
{"error":"access_denied"}
```

Zakres wniosku

Retest nie był pełnym ponownym pentestem aplikacji. Zmiany niezwiązane z raportem, nowe funkcje oraz elementy poza zakresem pozostały nieweryfikowane.

Następny krok

Dokończyć WEB-03, WEB-04 i WEB-06 w zaplanowanym cyklu, następnie przeprowadzić krótką weryfikację zmian. Przy większej zmianie architektury zalecany jest ponowny test zakresu wysokiego ryzyka.

O tym dokumencie

To publiczny przykład struktury raportu przygotowany bez danych rzeczywistego klienta, działających sekretów i informacji poufnych. Zakres, dowody oraz zalecenia w projekcie komercyjnym są zawsze dopasowane do testowanego systemu.

pentest24.pl/wycena-pentestu

kontakt@pentest24.pl