BREACHROAD
SECURITY ENGINEERING

BR-SAMPLE-WEB-2026-01
WERSJA 1.0

PUBLICZNA PRÓBKA · BEZ DANYCH KLIENTA

Test penetracyjny aplikacji webowej i API

Northbridge Commerce — fikcyjna organizacja demonstracyjna

PRZYGOTOWANE PRZEZ BREACHROAD

KAROL RAPACZ · CEO · OSCP · PNPT

15 LIPCA 2026

OKNO TESTÓW: 06–10 LIPCA 2026

KLASYFIKACJA: PUBLICZNA DEMONSTRACJA

SYNTHETIC / SAFE TO SHARE

BR / SAMPLE NOTICE

Przeczytaj przed użyciem próbki

To realistyczna demonstracja standardu raportowania Breachroad. Organizacja, systemy, identyfikatory, zapytania i ustalenia są fikcyjne. Dokument nie przedstawia projektu klienta, włamania ani danych produkcyjnych.

00 / INDEX

Zawartość raportu

01 / EXECUTIVE

Podsumowanie zarządcze

01 / CEL

Ustalić, czy uwierzytelniony klient może przekroczyć granicę tenanta, zmienić stan płatności albo zachować dostęp po zdarzeniu bezpieczeństwa konta.

02 / WYNIK OGÓLNY

WYSOKIE RYZYKO

Test potwierdził dwie luki wysokiego ryzyka. Konto o niskich uprawnieniach mogło odczytać fakturę innego tenanta, a webhook bez podpisu zmieniał stan płatności. Żaden scenariusz nie wymagał uprawnień administracyjnych.

03 / KONSEKWENCJA BIZNESOWA

Połączona ścieżka tworzy ryzyko poufności i nadużycia finansowego: dane klienta i faktury przekraczają granicę izolacji, a następnie zaufany stan płatności może zostać zmieniony poza prawidłowym przepływem operatora.

04 / KONTROLE, KTÓRE ZADZIAŁAŁY

MFA było wymagane dla administratorów, endpointy administracyjne odrzucały role klientów, walidacja uploadu blokowała aktywną treść, a test nie potwierdził SQL injection ani zdalnego wykonania kodu.

Metryka projektu

TESTOWANE SYSTEMY app.example.test · api.example.test · auth.example.test	**JAWNE WYŁĄCZENIA** Denial of service, socjotechnika, infrastruktura zewnętrznego operatora płatności i dostęp do danych innych niż syntetyczne rekordy testowe.
MODEL TESTU Test grey-box z użyciem dwóch odizolowanych tenantów klienta oraz testowej roli wsparcia. Konfiguracja zbliżona do produkcyjnej; wyłącznie dane syntetyczne.	**OGRANICZENIA OCENY PUNKTOWEJ** Pentest próbkuje uzgodnione ścieżki ataku w określonym czasie. Nie gwarantuje wykrycia każdej podatności ani niezmienności środowiska po zakończeniu prac.

Ryzyko i ustalenia

0	2	2	1	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

ID	USTALENIE	CVSS	RYZYKO
BR-01	Dostęp do faktury innego tenanta przez brak autoryzacji obiektowej	7.1	WYSOI
BR-02	Webhook płatności bez podpisu akceptowany przez logikę biznesową	7.5	WYSOI
BR-03	Refresh token pozostaje ważny po zmianie hasła	6.5	ŚREDN
BR-04	Proces odzyskiwania ujawnia zarejestrowane adresy e-mail	5.3	ŚREDN
BR-05	Content Security Policy dopuszcza niebezpieczne skrypty inline	3.1	NISKIE
BR-06	Zdarzenia bezpieczeństwa nie zawierają kontekstu granicy tenanta	–	INFO

04 / ATTACK PATH

Potwierdzona ścieżka ataku

Istotne ryzyko jest czytelniejsze jako jedna sekwencja niż jako zestaw niepowiązanych alertów.

STEP 01	Przejęte konto klienta o niskich uprawnieniach
STEP 02	Identyfikator faktury pozyskany z prawidłowego procesu
STEP 03	API nie egzekwuje własności obiektu
STEP 04	Zwrócone dane faktury innego tenanta
STEP 05	Webhook bez podpisu zmienia zaufany stan płatności

05 / ROADMAP

Plan naprawczy

01

0–7 dni

Wymusić autoryzację obiektową przy odczycie faktur. Odrzucać każdy webhook bez poprawnego podpisu przed przetworzeniem danych biznesowych. Przejrzeć logi pod kątem odwołań między tenantami i ruchu webhook bez podpisu.

02

Do 30 dni

Scentralizować politykę autoryzacji, dodać negatywne testy izolacji tenantów, obrócić sekrety webhooków, unieważniać aktywne sesje po zmianie hasła i odzyskaniu konta oraz ograniczyć zapytania do procesu odzyskiwania.

03

Do 90 dni

Wprowadzić regresyjne testy bezpieczeństwa do CI, monitorować odmowy granicy tenantów i błędy weryfikacji podpisu oraz powtarzać test po istotnych zmianach tożsamości lub płatności.

Szczegółowe ustalenia

BR-01 / FINDING 01

WYSOKIE | CVSS 7.1

Dostęp do faktury innego tenanta przez brak autoryzacji obiektowej

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

PRAWDOPODOBIEŃSTWO	WPŁYW	SUGEROWANY WŁAŚCICIEL
Wysokie — jedno uwierzytelnione żądanie i identyfikator w poprawnym formacie	Wysoki — ujawnienie danych klienta i rozliczeń poza granicą tenanta	API / Produkt

PRZYCZYNA ŹRÓDŁOWA

Endpoint weryfikuje sesję i identyfikator faktury, ale nie wiąże obiektu z tenantem uwierzytelnionego użytkownika.

ZANONIMIZOWANY DOWÓD

```
GET /v1/invoices/inv_demo_9d3 z <TENANT_A_TOKEN> zwrócił H
TTP 200 oraz tenant_id: tenant_demo_b.
```

NAPRAWA

Egzekwować własność tenanta w warstwie dostępu do danych, domyślnie odrzucać i dodać negatywne testy dla każdej referencji oraz roli.

KRYTERIA AKCEPTACJI RETESTU

Tenant A otrzymuje 404/403 dla każdej trasy faktury Tenanta B; brak różnic metadanych; testy obejmują listę, detal, PDF i eksport.

ODNIESIENIA

CWE-639 · OWASP API1:2023 · WSTG-ATHZ-04

BR-02 / FINDING 02

WYSOKIE

CVSS 7.5

Webhook płatności bez podpisu akceptowany przez logikę biznesową

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

PRAWDOPODOBIEŃSTWO	WPŁYW	SUGEROWANY WŁAŚCICIEL
Wysokie — publiczny endpoint nie wymaga poprawnego podpisu operatora	Wysoki — możliwość nadania zaufanego stanu „opłacone” poza przepływem operatora	**Płatności / Backend**

PRZYCZYNA ŹRÓDŁOWA	Weryfikacja podpisu uruchamia się tylko wtedy, gdy nagłówek istnieje; brak wartości przechodzi do obsługi zdarzenia.
ZANONIMIZOWANY DOWÓD	`POST /v1/webhooks/payment bez X-Payment-Signature zwrócił HTTP 202 i zmienił status demonstracyjnej faktury na paid.`
NAPRAWA	Weryfikować surowe body przed parsowaniem, odrzucać brak lub błąd podpisu, wymusić tolerancję czasu i idempotency oraz obrócić sekret.
KRYTERIA AKCEPTACJI RETESTU	Brakujące, błędne, powtórzone i wygasłe podpisy są odrzucane przed zmianą stanu; poprawne fixture przechodzi tylko raz.
ODNIESIENIA	CWE-345 · OWASP API10:2023 · WSTG-BUSL-02

BR-03 / FINDING 03

ŚREDNIE CVSS 6.5

Refresh token pozostaje ważny po zmianie hasła

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

PRAWDOPODOBIEŃSTWO	WPŁYW	SUGEROWANY WŁAŚCICIEL
Średnie — wymaga posiadania wcześniej wydanego refresh tokenu	Wysoki — istniejąca sesja może przetrwać zmianę poświadczeń wykonaną z powodów bezpieczeństwa	Tożsamość

PRZYCZYNA ŹRÓDŁOWA

Reset hasła zmienia poświadczenie, ale nie zwiększa generacji sesji ani nie unieważnia rodzin refresh tokenów.

ZANONIMIZOWANY DOWÓD

```
Token wydany przed resetem uzyskał nowy access token po za
kończeniu resetu i wysłaniu powiadomienia do użytkownika.
```

NAPRAWA

Unieważniać wszystkie rodziny refresh tokenów przy zmianie i odzyskaniu hasła; dodać widoczne zarządzanie sesjami oraz telemetrię zdarzeń.

KRYTERIA AKCEPTACJI RETESTU

Każdy token sprzed resetu jest odrzucany; aktywne sesje wygasają, a zdarzenie zawiera kontekst konta i urządzenia.

ODNIESIENIA

CWE-613 · OWASP ASVS V3 · WSTG-SESS-06

BR-04 / FINDING 04

ŚREDNIE CVSS 5.3

Proces odzyskiwania ujawnia zarejestrowane adresy e-mail

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

PRAWDOPODOBIEŃSTWO	WPŁYW	SUGEROWANY WŁAŚCICIEL
Wysokie — zdalne, nieuwierzytelnione i możliwe do automatyzacji	Niski do średniego — ułatwia phishing, credential stuffing i profilowanie prywatności	Tożsamość / UX

PRZYCZYNA ŹRÓDŁOWA	Treść i czas odpowiedzi różnią się dla zarejestrowanego i nieznanego adresu.
ZANONIMIZOWANY DOWÓD	`Znany adres zwrócił metadane kanału odzyskiwania; nieznany — odmienny kod i długość odpowiedzi.`
NAPRAWA	Zwracać jeden komunikat, wyrównać obsługę, ograniczyć częstotliwość i wykrywać wzorce enumeracji.
KRYTERIA AKCEPTACJI RETESTU	Znane i nieznane konta mają równoważny status, strukturę body i praktyczny rozkład czasu.
ODNIESIENIA	CWE-204 · OWASP ASVS V2 · WSTG-IDNT-04

BR-05 / FINDING 05

NISKIE

CVSS 3.1

Content Security Policy dopuszcza niebezpieczne skrypty inline

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

PRAWDOPODOBIEŃSTWO	WPŁYW	SUGEROWANY WŁAŚCICIEL
Niskie — test nie potwierdził niezależnego punktu injection	Niski samodzielnie — osłabienie warstwy ochronnej przy przyszłym błędzie injection	Frontend

PRZYCZYNA ŹRÓDŁOWA	Polityka produkcyjna zawiera unsafe-inline bez nonce lub hashy.
ZANONIMIZOWANY DOWÓD	`Content-Security-Policy zawiera script-src self unsafe-inline; próbkowane strony nie używają nonce.`
NAPRAWA	Przenieść kod inline do zasobów statycznych, wdrożyć nonce lub hashe i najpierw uruchomić ostrzejszą politykę w report-only.
KRYTERIA AKCEPTACJI RETESTU	Brak unsafe-inline; wszystkie przepływy działają z wymuszoną CSP, a naruszenia są monitorowane.
ODNIESIENIA	CWE-693 · OWASP Secure Headers Project

BR-06 / FINDING 06

INFO CVSS –

Zdarzenia bezpieczeństwa nie zawierają kontekstu granicy tenanta

Bez oceny CVSS

PRAWDOPODOBIEŃSTWO	WPŁYW	SUGEROWANY WŁAŚCICIEL
Luka operacyjna	Wolniejsze dochodzenie i słabszy materiał dowodowy przy podejrzeniu ruchu między tenantami	Platforma / SOC

PRZYCZYNA ŹRÓDŁOWA

Logi aplikacji zapisują trasę i użytkownika, ale nie właściciela obiektu, tenant docelowy ani decyzję autoryzacji.

ZANONIMIZOWANY DOWÓD

```
Nie można było skorelować zdarzeń faktur jednocześnie z tenantem aktora i właściciela obiektu.
```

NAPRAWA

Logować tenant aktora i celu, typ obiektu, decyzję i trace ID bez danych wrażliwych; alarmować przy próbie niedopasowania.

KRYTERIA AKCEPTACJI RETESTU

Kontrolowane odrzucone żądanie tworzy pełne, wyszukiwalne zdarzenie i uzgodniony sygnał detekcji.

ODNIESIENIA

OWASP ASVS V7 · NIST SP 800-92

07 / COVERAGE

Macierz pokrycia

OBSZAR	WYNIK	UWAGI
Uwierzytelnianie i odzyskiwanie	CZĘŚCIOWO	Potwierdzono problem cyklu sesji; MFA i jednorazowość tokenu resetu zadziałały.
Autoryzacja i tenanty	NIEZALICZONE	Potwierdzono brak autoryzacji obiektowej przy pobieraniu faktury.
Logika biznesowa i płatności	NIEZALICZONE	Aplikacja przyjmowała webhook bez podpisu.
Obsługa danych wejściowych	ZALICZONE	W testowanych ścieżkach nie potwierdzono użytecznego injection.
Pliki i integracje	ZALICZONE	Ograniczenia uploadu i callbacków zadziałały w próbkowanych przypadkach.
Logowanie i detekcja	CZĘŚCIOWO	Zdarzenia istniały, lecz brakowało kontekstu granicy tenanta i błędów podpisu.

08 / RETEST

Plan retestu

Retest powinien użyć pierwotnych żądań oraz dwóch odizolowanych tenantów. Zamknięcie wymaga serwerowej kontroli własności na każdej trasie faktur, weryfikacji podpisu fail-closed przed obsługą webhooku, testu unieważniania sesji i pokrycia regresyjnego. Sama zmiana kodu nie oznacza zamknięcia.

01	OTWARTE — pierwotny wpływ nadal można odtworzyć
02	GOTOWE DO RETESTU — klient deklaruje wdrożenie poprawki
03	ZAMKNIĘTE — pierwotny wpływ nie jest już możliwy
04	CZĘŚCIOWO ZAMKNIĘTE — ryzyko spadło, ale kryteria nie są spełnione

Metodyka i źródła

CVSS v3.1 + business context

Ryzyko łączy wykazany wpływ biznesowy i warunki wykorzystania. CVSS v3.1 jest przejrzystym odniesieniem technicznym, ale nie zastępuje kontekstu środowiska. Każdy wynik liczbowy ma podany wektor.

OWASP · PTES · NIST

Struktura próbki korzysta z zaleceń raportowania OWASP WSTG, kryteriów PTES i NIST SP 800-115. Identyfikatory, dowody, komponenty, naprawa oraz kryteria retestu zachowują pełną śledzalność.

OWASP WSTG — Reporting Structure

PTES — Reporting

NIST SP 800-115

FIRST — CVSS v3.1 Specification

OWASP OPTRS