

Pentest-Bericht

Kundenportal Beispielwerk

Prüfzeitraum
01.–04.09.2026

Fachliche Bewertung
Franz Bettag

Berichtsstand
09.09.2026

Version
PT-2026-001 · 1.0

Ergebnis in Kürze

Drei illustrative Findings: Ein Fehler mit hoher Priorität ermöglicht das Lesen von Daten eines anderen Mandanten. Zwei Findings mittlerer Priorität betreffen einen erreichbaren Diagnose-Endpunkt und eine zu weitreichende Fehlerausgabe.

1 Hoch

2 Mittel

Status · 09.09.2026

Ein Fix zur Nachprüfung bereit. Ein Finding offen. Ein Finding nachgeprüft und geschlossen.

Fiktives Muster · öffentlich

Alle Systeme, Daten und Ergebnisse sind frei erfunden. Dies ist kein Kundenbericht.

Prüfumfang und Ergebnisse

Kundenportal Beispielwerk

Freigegebene Systeme	portal.example.test, api.example.test · HTTPS
Testzugänge	Je ein reguläres Testkonto für Mandant A und B; ausschließlich synthetische Daten.
Prüf Schwerpunkte	Anmeldung, Objektberechtigungen der API und Informationspreisgabe über erreichbare Dienste.

Ausgeschlossen

Interne Netze, umfassende Cloud-IAM-Prüfungen, native Mobile-Apps, Social Engineering, Full Red Team sowie Hardware, Firmware und OT. Keine Lasttests, Betriebsunterbrechungen oder Zugriffe auf reale Kundendaten.

Ergebnisübersicht

Finding	Priorität	Status	Verantwortlich
F-01 API-Zugriff über Mandantengrenzen	Hoch	Nachprüfung ausstehend	API-Team
F-02 Diagnose-Endpunkt	Mittel	Offen	Betrieb
F-03 Fehlerausgabe	Mittel	Geschlossen	Web-Team

Priorität beschreibt den Handlungsbedarf anhand von Auswirkung und Voraussetzungen. Der ausführliche Befund zeigt, wie daraus eine überprüfbare Aufgabe wird. Die Prüfung gilt für die vereinbarten Systeme und den dokumentierten Zeitraum.

Fiktives Muster · öffentlich

Alle Systeme, Daten und Ergebnisse sind frei erfunden. Dies ist kein Kundenbericht.

F-01 · API-Zugriff über Mandantengrenzen

Priorität

Hoch

Status

Nachprüfung ausstehend

Verantwortlich

API-Team

Betroffen

api.example.test · GET /v1/invoices/:id

Auswirkung und Voraussetzung

Ein angemeldetes Konto von Mandant A konnte im Musterfall eine Rechnung von Mandant B lesen. Dazu war eine gültige Rechnungs-ID des anderen Mandanten nötig. Diese ID stammt hier aus dem zweiten autorisierten Testkonto. Belegt ist ein lesender Zugriff; Änderungen oder Zugriffe ohne Anmeldung wurden damit nicht nachgewiesen.

Beispielbeleg

```
GET /v1/invoices/B-1042
Host: api.example.test
Sitzung: autorisiertes Testkonto A
```

```
HTTP 200
invoice_id: B-1042
tenant: B
total_eur: 120.00
```

Erwartet: Zugriff verweigert, ohne Daten von Mandant B zurückzugeben. Beobachtet: Die Antwort enthielt die synthetische Rechnung des anderen Mandanten.

Behebung

Bei jedem Objektzugriff die Mandantenzugehörigkeit serverseitig aus der authentifizierten Sitzung ableiten und gegen das angefragte Objekt prüfen. Dieselbe Regel auf weitere Rechnungs-Endpunkte anwenden. Automatisierte Negativtests mit zwei getrennten Mandanten ergänzen.

Nachprüfung und Abschlusskriterium

Das API-Team hat den Fix im Muster am 8. September bereitgestellt. Die Nachprüfung steht aus. Für den Abschluss müssen Zugriffe A → B und B → A abgewiesen werden; eigene Rechnungen müssen weiter abrufbar sein. Ergebnis und geprüfter Versionsstand werden danach im Finding festgehalten.

Findings-Update

Kundenportal Beispielwerk

Berichtsstand
09.09.2026

Prüfzeitraum
01.–04.09.2026

Ein Fix zur Nachprüfung bereit. Ein Finding offen. Ein Finding nachgeprüft und geschlossen.

Finding	Priorität	Status	Verantwortlich	Nächster Schritt / Nachprüfung
F-01 API-Zugriff über Mandantengrenzen	Hoch	Nachprüfung ausstehend	API-Team	Zugriffe zwischen beiden Testmandanten und auf eigene Rechnungen prüfen. Abschluss nach bestandenem Test.
F-02 Diagnose-Endpunkt	Mittel	Offen	Betrieb	Externen Zugriff sperren. Nachprüfung nach Bereitstellung des Fixes vereinbaren.
F-03 Fehlerausgabe	Mittel	Geschlossen	Web-Team	Am 08.09. in Muster-Build 1.4.2 nachgeprüft: keine internen Diagnosedaten mehr in der Antwort.

Bis zum nächsten Austausch

API-Team und Prüfer stimmen den Termin für F-01 ab. Operations nennt den Bereitstellungstermin für F-02. Änderungen am Scope werden vor weiteren Prüfungen vereinbart.

Übergabe ins Kundensystem

Finding-ID, Priorität, Beleg, Verantwortlichkeit, Behebung und Nachprüfungsstand werden in Jira, Linear oder GitHub übernommen: im vereinbarten Format oder über einen bereitgestellten Zugang.

Nachprüfungen behobener Findings innerhalb des vereinbarten Scopes und der aktiven Vertragslaufzeit sind in allen Paketen enthalten.

Fiktives Muster · öffentlich

Alle Systeme, Daten und Ergebnisse sind frei erfunden. Dies ist kein Kundenbericht.