✓ Proofline

KOSTENLOSE VORLAGE

Fintech-API-Testcheckliste

Idempotenz, Geldbeträge, Autorisierung, SCA, Webhooks, Limits und Abgleich – die Prüfungen, die wir bei Payment-APIs durchführen.

> Für Payment-, Banking- und Karten-APIs. Bezug zu OWASP API Security Top 10 (2023) und gängigen PSD2-Anforderungen. Nutzen Sie einen eigenen Testmandanten und die Sandbox des Anbieters – niemals echte Kundendaten.

1. Geldbeträge

	PRÜFPUNKT	PRIO	VERANTW. / NOTIZ
☐	Beträge in ganzzahligen Minor Units oder Decimal-Typen – nie Gleitkomma; Fälle wie 0,1 + 0,2 testen.	HOCH	
☐	Währungsexponent berücksichtigt (JPY 0, EUR 2, BHD 3 Nachkommastellen); nicht unterstützte Währungen abgelehnt.	HOCH	
☐	Grenzwerte: 0, negativ, Minimum, Maximum, Maximum+1, sehr große Zahlen, zu viele Nachkommastellen.	HOCH	
☐	Rundungsregeln für FX, Gebühren und Splits dokumentiert und getestet (Summe der Teile = Gesamtbetrag).	MITTEL	
☐	Limits (pro Transaktion, täglich, monatlich) serverseitig durchgesetzt, auch bei parallelen Requests.	MITTEL	

2. Idempotenz & Nebenläufigkeit

	PRÜFPUNKT	PRIO	VERANTW. / NOTIZ
☐	POST Zahlung/Überweisung unterstützt einen Idempotency-Key; gleicher Key + gleicher Body liefert das ursprüngliche Ergebnis.	HOCH	

☐	Gleicher Key + anderer Body wird abgelehnt (z. B. 422), nicht stillschweigend verarbeitet.	HOCH	
☐	Parallele Duplikate (Race) erzeugen genau eine Transaktion; Saldo unterschreitet nie das erlaubte Minimum.	HOCH	
☐	Client-Timeouts und Retries: Ergebnis abrufbar (GET per Referenz) ohne Doppelbelastung.	MITTEL	
☐	Zustandsübergänge erzwungen (z. B. keine Erstattung einer ausstehenden oder bereits erstatteten Zahlung).	MITTEL	

3. Authentifizierung & Autorisierung (OWASP API1, API2, API5)

	PRÜFPUNKT	PRIO	VERANTW. / NOTIZ
☐	BOLA: Jede Objekt-ID (Konto, Zahlung, Empfänger, Karte) wird gegen den Aufrufer geprüft; mit IDs eines zweiten Mandanten testen.	HOCH	
☐	Autorisierung auf Funktionsebene: Kundentokens können keine Admin-/Backoffice-Endpunkte aufrufen.	HOCH	
☐	Tokens: Ablauf, Widerruf, Audience-/Issuer-Prüfung; alg=none und Key-Confusion abgelehnt.	HOCH	
☐	OAuth2-Scopes nach Least Privilege und je Endpunkt durchgesetzt.	MITTEL	
☐	401/403/404-Antworten verraten nicht die Existenz fremder Ressourcen.	MITTEL	

4. Starke Kundenauthentifizierung (PSD2 / SCA)

	PRÜFPUNKT	PRIO	VERANTW. / NOTIZ
☐	SCA dort ausgelöst, wo erforderlich (Zahlungsauslösung, neuer Empfänger, sensible Daten); Ausnahmen nur regelkonform.	HOCH	
☐	Dynamic Linking: Der Authentifizierungscode ist an Betrag und Empfänger gebunden; jede Änderung macht ihn ungültig.	HOCH	
☐	OTP/Challenge: begrenzte Versuche, Ablauf, keine Wiederverwendung, Rate Limit pro Nutzer und Gerät.	MITTEL	
☐	3-D-Secure-Flows (frictionless, Challenge, Fehler, Timeout) mit Testkarten des Acquirers getestet.	MITTEL	

5. Eingabevalidierung & Datenexposition (API3, API8)

	PRÜFPUNKT	PRIO	VERANTW. / NOTIZ
☐	IBAN/BIC, Kartennummern validiert (Prüfsumme) und nie vollständig zurückgegeben; PAN maskiert, CVV nie gespeichert oder ausgegeben.	HOCH	

☐	Mass Assignment: Clients können Status, Saldo, Gebühr, Eigentümer oder KYC-Felder nicht setzen.	HOCH	
☐	Responses enthalten nur benötigte Felder; keine internen IDs, Stacktraces oder Fremddaten.	MITTEL	
☐	Unicode, sehr lange Strings und Injection-Payloads in Referenzen/Verwendungszwecken sicher behandelt (inkl. Exporte/CSV).	MITTEL	

6. Webhooks & Callbacks

	PRÜFPUNKT	PRIO	VERANTW. / NOTIZ
☐	Webhook-Signaturen geprüft (HMAC + Zeitstempel); wiederholte oder unsignierte Events abgelehnt.	HOCH	
☐	Handler sind idempotent: doppelte und ungeordnete Events führen nicht zu Doppelbuchungen.	HOCH	
☐	Retries mit Backoff; Dead-Letter-Behandlung und Alarmierung getestet.	MITTEL	
☐	Ausgehende Callback-URLs gegen SSRF validiert (keine internen Adressen).	MITTEL	

7. Zuverlässigkeit, Limits & Performance (API4)

	PRÜFPUNKT	PRIO	VERANTW. / NOTIZ
☐	Rate Limits pro Client/Key mit 429 + Retry-After; teure Endpunkte (Suche, Exporte, Kontoauszüge) begrenzt.	HOCH	
☐	Paginierung mit erzwungener maximaler Seitengröße an allen Listen-Endpunkten.	HOCH	
☐	Lasttest für Monatsende-/Zahltag-Spitzen; p95/p99- und Fehlerraten-Schwellen in k6 definiert.	MITTEL	
☐	Ausfälle nachgelagerter Systeme (Kernbank, Kartenprozessor, KYC-Anbieter) führen zu klaren, retry-sicheren Fehlern; Circuit Breaker getestet.	MITTEL	

8. Ledger, Abgleich & Audit

	PRÜFPUNKT	PRIO	VERANTW. / NOTIZ
☐	Doppelte-Buchführung-Invarianten gelten nach jedem Test (Soll = Haben, keine verwaisten Buchungen).	HOCH	
☐	Täglicher Abgleich mit PSP-/Bankdateien erkennt und meldet Abweichungen.	HOCH	
☐	Audit-Log für sensible Aktionen (wer, was, wann) ist unveränderlich und enthält keine Secrets.	MITTEL	
☐	Zeitzonen und Cut-off-Zeiten (Tagesende, Bankfeiertage, Zeitumstellung) getestet.	MITTEL	

☐	API-Versionierung und Deprecation-Policy mit alten Clients getestet.	NIEDRIG	

© Proofline · Kostenlose Vorlage, darf intern genutzt und angepasst werden. Keine Rechtsberatung.