MUSTERBERICHT — KEINE ECHTEN KUNDENDATEN

Sicherheitsbewertung

Penetrationstest — Webanwendung

Auftraggeber	Beispiel GmbH (fiktiv)
Testzeitraum	03.–14. August 2026
Scope	Webanwendung app.beispiel.tld inkl. API
Durchgeführt von	Christian Noack — CN Interactive Systems
Methodik	Manuelles Testing, orientiert an OWASP Testing Guide

Management Summary

Im Rahmen des vereinbarten Penetrationstests wurde die Webanwendung app.beispiel.tld auf Sicherheitslücken geprüft. Insgesamt wurden vier Schwachstellen identifiziert, davon eine mit kritischer und eine mit hoher Priorität. Die kritische Schwachstelle ermöglichte eine vollständige Umgehung der Authentifizierung und wurde dem Auftraggeber umgehend, noch vor Abschluss des Tests, gemeldet.

Schweregrad	Anzahl
Kritisch	1
Hoch	1
Mittel	1
Niedrig	1

Einzelfunde

SQL-Injection im Login-Formular

Kritisch

Betroffen: /login (Parameter „user")
Auswirkung: Vollständige Authentifizierungsumgehung möglich. Ein Angreifer könnte sich ohne gültige Zugangsdaten als beliebiger Nutzer anmelden.
Nachweis: 1) POST-Request an /login senden. 2) Im Feld „user" den Payload ' OR '1'='1 einsetzen. 3) Anmeldung erfolgt ohne gültiges Passwort.
Empfehlung: Parametrisierte Queries (Prepared Statements) statt String-Konkatenation verwenden. Eingaben serverseitig validieren.

Fehlende Rate-Limitierung beim Login

Hoch

Betroffen: /login
Auswirkung: Automatisiertes Ausprobieren von Zugangsdaten (Brute-Force) ist ohne Sperre oder Verzögerung möglich.
Nachweis: Wiederholte fehlgeschlagene Login-Versuche wurden ohne Sperrung, Captcha oder Verzögerung akzeptiert.
Empfehlung: Rate-Limiting und Account-Lockout nach mehreren Fehlversuchen einführen, ergänzt um Multi-Faktor-Authentifizierung.

Veraltete TLS-Konfiguration

Mittel

Betroffen: api.beispiel.tld
Auswirkung: Unterstützung veralteter Protokollversionen erhöht die Angriffsfläche für Man-in-the-Middle-Szenarien.
Nachweis: TLS-Handshake unterstützte TLS 1.0/1.1 sowie schwache Cipher Suites.
Empfehlung: Veraltete Protokollversionen und schwache Cipher Suites serverseitig deaktivieren, nur TLS 1.2+ zulassen.

Ausführliche Fehlermeldungen im Produktivbetrieb

Niedrig

Betroffen: Diverse Endpunkte
Auswirkung: Stacktraces und interne Pfade werden bei Serverfehlern an den Client ausgegeben und erleichtern Angreifern die Aufklärung.
Nachweis: Ein fehlerhafter Request löste eine ausführliche Fehlerseite mit internen Pfadangaben aus.
Empfehlung: Generische Fehlerseiten im Produktivbetrieb ausgeben, Details nur serverseitig loggen.

Retest

Nach Behebung der gemeldeten Schwachstellen wird jeder Fund erneut gezielt geprüft. Der Retest-Vermerk bestätigt je Fund, ob dieser vollständig behoben, teilweise behoben oder weiterhin offen ist.
