TSBSec

MUSTER – ANONYMISIERTES BEISPIEL

PENETRATIONSTEST – ERGEBNISBERICHT

Externer Penetrationstest der Web-Anwendung und des Perimeters

Musterkunde GmbH (anonymisiert)

Auftraggeber	Musterkunde GmbH (anonymisiert)
Testzeitraum	12.–16. Mai 2026
Testart	Grey-Box, extern
Umfang	1 Web-Anwendung, 12 externe Hosts
Methodik	OWASP Testing Guide, BSI-Durchführungskonzept
Einstufung	Vertraulich

TSB Top Sec Bau GmbH
Neufeldtstr. 6, 24118 Kiel

info@tsbsec.de
+49 15778716239

Inhalt

1. Management-Summary

Im Auftrag der Musterkunde GmbH hat TSBSec vom 12. bis 16. Mai 2026 einen Penetrationstest der öffentlich erreichbaren Web-Anwendung und der externen Netzwerk-Infrastruktur durchgeführt. Ziel war es, ausnutzbare Schwachstellen aus Sicht eines externen Angreifers zu identifizieren und zu bewerten.

GESAMTBEWERTUNG

19 Befunde gesamt

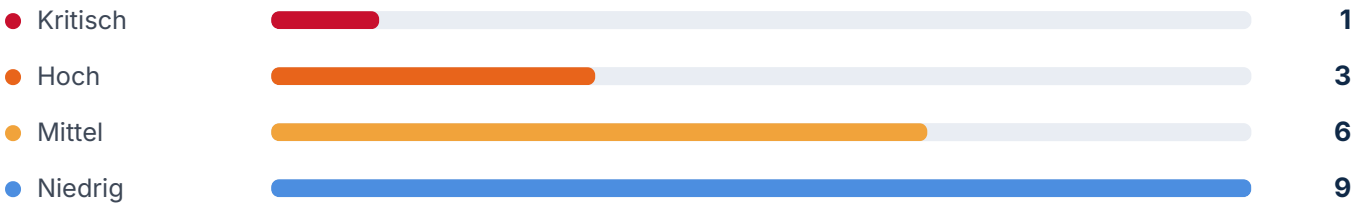
Nach Behebung erreichbar: A

Die Sicherheitslage ist insgesamt solide, weist jedoch klaren Handlungsbedarf auf. Eine kritische Schwachstelle (SQL-Injection im Kundenportal) erlaubte den Zugriff auf Datenbankinhalte und muss vorrangig behoben werden. Drei Befunde hoher Kritikalität betreffen fehlende Zugriffskontrollen und eine veraltete Komponente mit bekannter Schwachstelle.

Positiv fielen die konsequente TLS-Konfiguration, aktivierte Multi-Faktor-Authentifizierung für administrative Zugänge und ein sauberes Patch-Management der Server-Betriebssysteme auf. Nach Behebung der priorisierten Maßnahmen ist ein Sicherheitsniveau von A erreichbar.

3. Ergebnisübersicht

SCHWEREGRAD — 19 BEFUNDE GESAMT



ID	Befund	Schweregrad	CVSS	Status
F-01	SQL-Injection im Kundenportal	Kritisch	9.1	Geschlossen
F-02	Fehlende Autorisierung an der Bestell-API	Hoch	8.2	In Arbeit
F-03	Veraltete Bibliothek mit bekannter Schwachstelle	Hoch	7.5	Offen

4. Ausgewählte Befunde

Nachfolgend die drei schwerwiegendsten Befunde in gekürzter Form. Der vollständige Bericht enthält für jeden Befund Nachweis, Risikoeinschätzung und detaillierte Empfehlung.

F-01 SQL-Injection im Kundenportal

Kritisch · CVSS 9.1

BESCHREIBUNG	Der Suchparameter des Kundenportals war nicht ausreichend gegen SQL-Injection abgesichert. Über eine manipulierte Anfrage ließen sich beliebige Datenbankabfragen ausführen.
AUSWIRKUNG	Auslesen von Kundendaten, Zugangsdaten-Hashes und internen Konfigurationswerten. Vollständige Kompromittierung der Anwendungsdatenbank möglich.
EMPFEHLUNG	Ausschließlich parametrisierte Abfragen (Prepared Statements) verwenden, Eingaben serverseitig validieren und die Datenbankberechtigungen nach dem Prinzip der geringsten Rechte einschränken.
STATUS	Geschlossen

F-02 Fehlende Autorisierung an der Bestell-API

Hoch · CVSS 8.2

BESCHREIBUNG	Ein authentifizierter Nutzer konnte durch Ändern der Objekt-ID auf Bestellungen anderer Kunden zugreifen (Insecure Direct Object Reference).
AUSWIRKUNG	Unbefugter Zugriff auf fremde Bestell- und Rechnungsdaten über die gesamte Kundenbasis.
EMPFEHLUNG	Serverseitige Autorisierungsprüfung für jeden Objektzugriff einführen; Objektreferenzen nicht fortlaufend und ohne Berechtigungsbezug vergeben.
STATUS	In Arbeit

F-03 Veraltete Bibliothek mit bekannter Schwachstelle

Hoch · CVSS 7.5

BESCHREIBUNG	Eine im Frontend eingesetzte JavaScript-Bibliothek war mehrere Hauptversionen veraltet und für eine öffentlich dokumentierte Schwachstelle anfällig.
AUSWIRKUNG	Möglichkeit von Cross-Site-Scripting und Ausführung von Schadcode im Browser der Nutzer.
EMPFEHLUNG	Bibliothek auf die aktuelle Version aktualisieren und ein automatisiertes Abhängigkeits-Monitoring (Software Composition Analysis) einführen.
STATUS	Offen

5. Maßnahmen & Status

Übersicht des Behebungsstatus zum Zeitpunkt des Re-Tests (30. Mai 2026).

Geschlossen **14** In Arbeit **3** Offen **2**

6. Über den Test

Dieser Musterbericht zeigt Aufbau, Tiefe und Sprache eines TSBSec-Berichts. Alle Firmennamen, Adressen, Befunde und Zahlen sind frei erfunden und dienen ausschließlich der Veranschaulichung. Ein realer Bericht wird ausschließlich verschlüsselt und vertraulich an den Auftraggeber übergeben.

Kontakt: TSBSec · TSB Top Sec Bau GmbH · info@tsbsec.de · +49 15778716239 · tsbsec.de