TSBSec

SAMPLE – ANONYMISED EXAMPLE

PENETRATION TEST – FINDINGS REPORT

External penetration test of the web application and perimeter

Example Customer Ltd (anonymised)

Client	Example Customer Ltd (anonymised)
Test period	12–16 May 2026
Test type	Grey box, external
Scope	1 web application, 12 external hosts
Methodology	OWASP Testing Guide, BSI methodology
Classification	Confidential

TSB Top Sec Bau GmbH
Neufeldtstr. 6, 24118 Kiel

info@tsbsec.de
+49 15778716239

Contents

1. Management summary

On behalf of Example Customer Ltd, TSBSec conducted a penetration test of the publicly reachable web application and the external network infrastructure from 12 to 16 May 2026. The objective was to identify and assess exploitable vulnerabilities from the perspective of an external attacker.

OVERALL RATING

19 Findings in total

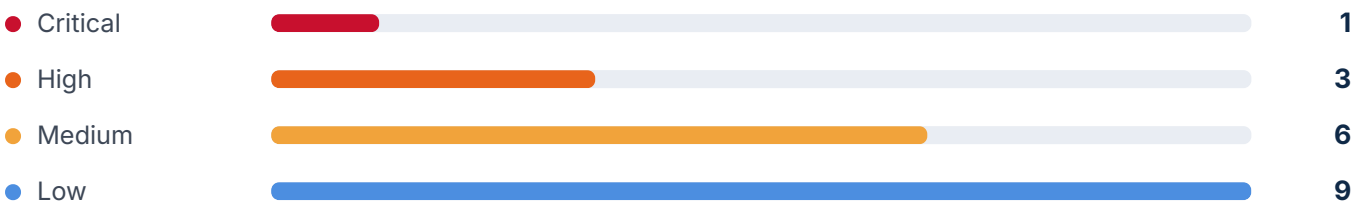
Achievable after remediation: A

The overall security posture is solid but shows clear need for action. One critical vulnerability (SQL injection in the customer portal) allowed access to database contents and must be remediated as a priority. Three high-severity findings concern missing access controls and an outdated component with a known vulnerability.

On the positive side, the consistent TLS configuration, enabled multi-factor authentication for administrative access and clean patch management of the server operating systems stood out. After remediating the prioritised measures, a security level of A is achievable.

3. Results overview

SEVERITY — 19 FINDINGS IN TOTAL



ID	Finding	Severity	CVSS	Status
F-01	SQL injection in the customer portal	Critical	9.1	Closed
F-02	Missing authorisation on the order API	High	8.2	In progress
F-03	Outdated library with a known vulnerability	High	7.5	Open

4. Selected findings

Below are the three most severe findings in abbreviated form. The full report contains evidence, risk assessment and a detailed recommendation for every finding.

F-01 SQL injection in the customer portal

● Critical · CVSS 9.1

DESCRIPTION	The customer portal's search parameter was insufficiently protected against SQL injection. A manipulated request allowed arbitrary database queries to be executed.
IMPACT	Reading of customer data, credential hashes and internal configuration values. Full compromise of the application database is possible.
RECOMMENDATION	Use parameterised queries (prepared statements) exclusively, validate input server-side and restrict database permissions following the principle of least privilege.
STATUS	Closed

F-02 Missing authorisation on the order API

● High · CVSS 8.2

DESCRIPTION	An authenticated user could access other customers' orders by changing the object ID (insecure direct object reference).
IMPACT	Unauthorised access to other customers' order and invoice data across the entire customer base.
RECOMMENDATION	Introduce a server-side authorisation check for every object access; do not assign object references sequentially and without a permission check.
STATUS	In progress

F-03 Outdated library with a known vulnerability

● High · CVSS 7.5

DESCRIPTION	A JavaScript library used in the frontend was several major versions out of date and vulnerable to a publicly documented issue.
IMPACT	Potential for cross-site scripting and execution of malicious code in users' browsers.
RECOMMENDATION	Update the library to the current version and introduce automated dependency monitoring (software composition analysis).
STATUS	Open

5. Remediation & status

Overview of the remediation status at the time of the re-test (30 May 2026).

● Closed **14** ● In progress **3** ● Open **2**

6. About this test

This sample report shows the structure, depth and language of a TSBSec report. All company names, addresses, findings and figures are fictitious and serve illustration only. A real report is handed over to the client exclusively in encrypted and confidential form.

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