GABRYSZ
PENTEST · NRW

VERTRAULICH · ANONYMISIERT

PENETRATION TEST REPORT · GBR-2026-014

Sicherheitsanalyse *MUSTERMANN LOGISTIK GMBH*

(Beispiel — frei erfunden, keine reale Firma)

Scope
External Web-App + Perimeter

Methodik
OWASP WSTG · PTES

Zeitraum
KW 14/2026 · 5 Tage

Datum
25. Juni 2026

Maik Gabrysz · Penetrationstests & Forensik · pentesting.gabrysz.de

EXECUTIVE SUMMARY · FÜR DIE GESCHÄFTSFÜHRUNG

Das Wichtigste in einem Satz

Im Test wurden **5 Schwachstellen** identifiziert, darunter **1 kritische**, die eine vollständige Übernahme der Kundendaten erlauben. Alle Befunde sind priorisiert und mit konkreten, umsetzbaren Maßnahmen versehen.

CRITICAL 1 HIGH 1 MEDIUM 2 LOW 1

ID	Schweregrad	CVSS	Finding
F-01	CRITICAL	9.1	SQL-Injection im Login-Formular
F-02	HIGH	8.1	Veraltete Komponente mit bekannter RCE (CVE-2024-XXXX)
F-03	MEDIUM	5.4	Session-Fixation nach Login
F-04	MEDIUM	5.3	Fehlende Security-Header am Perimeter
F-05	LOW	3.1	Ausführliche Fehlermeldungen (Information Disclosure)

▲ CRITICAL FINDING F-01 · WEB-APP CVSS 9.1

SQL-Injection im Login-Formular

Der Parameter „username" wird ungefiltert in eine SQL-Abfrage übernommen. Über eine UNION-basierte Injection lässt sich die komplette Benutzertabelle inklusive Passwort-Hashes auslesen — ohne gültige Zugangsdaten.

Auswirkung

Vollständige Kompromittierung der Kundendatenbank, Übernahme beliebiger Konten, DSGVO-meldepflichtiger Datenabfluss.

Proof of Concept

```
POST /login HTTP/1.1
Host: app.mustermann-logistik.example
Content-Type: application/x-www-form-urlencoded

username=admin' UNION SELECT id,email,pw_hash FROM users-- -&password=x

→ 200 OK
[{"id":1,"email":"admin@…","pw_hash":"$2y$10$Xk…"}]
```

Empfehlung

Ausschließlich parametrisierte Queries / Prepared Statements verwenden. Eingaben serverseitig validieren. WAF als zweite Schicht, nicht als Ersatz.

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

▲ HIGH FINDING F-02 · WEB-APP CVSS 8.1

Veraltete Komponente mit bekannter RCE (CVE-2024-XXXX)

Eine eingesetzte Bibliothek ist drei Major-Versionen veraltet und für eine öffentlich dokumentierte Remote-Code-Execution anfällig. Ein passender Exploit ist frei verfügbar.

Auswirkung

Codeausführung auf dem Applikationsserver, Brückenkopf ins interne Netz, Lateral Movement.

Proof of Concept

```
$ curl -s https://app.…/static/vendor.js | grep version
// libfoo v2.3.1  (aktuell: v5.x — CVE-2024-XXXX, CVSS 8.1)

$ nuclei -t cves/2024/CVE-2024-XXXX.yaml -u https://app.…
[CVE-2024-XXXX] [high] https://app.… → vulnerable
```

Empfehlung

Bibliothek auf eine gepatchte Version aktualisieren. Software-Inventar (SBOM) einführen, automatisiertes Dependency-Scanning in die CI/CD-Pipeline integrieren.

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H`

▲ MEDIUM FINDING F-03 · WEB-APP CVSS 5.4

Session-Fixation nach Login

Die Session-ID wird beim Login nicht erneuert. Ein Angreifer, der einem Opfer eine bekannte Session-ID unterschiebt, übernimmt nach dessen Anmeldung die Sitzung.

Auswirkung

Kontoübernahme im Kontext eines aktiven Nutzers.

Proof of Concept

```
# vor Login
Set-Cookie: SESSIONID=abc123

# nach erfolgreichem Login – identisch:
Set-Cookie: SESSIONID=abc123   ← nicht rotiert
```

Empfehlung

Session-ID bei jeder Privilegien-Änderung (Login) serverseitig neu generieren. Cookies mit Secure, HttpOnly und SameSite=Strict setzen.

`CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N`

▲ MEDIUM FINDING F-04 · WEB-APP CVSS 5.3

Fehlende Security-Header am Perimeter

CSP, HSTS und X-Frame-Options fehlen. Das erhöht die Ausnutzbarkeit von XSS und ermöglicht Clickjacking sowie Protokoll-Downgrade-Angriffe.

Auswirkung

Verstärkt andere Findings, erleichtert Phishing und Clickjacking.

Proof of Concept

```
$ curl -sI https://app.… | grep -iE 'content-security|strict-transport|x-frame'
# (keine Treffer)
```

Empfehlung

Strenge CSP, HSTS mit langer max-age + preload, X-Frame-Options: DENY, X-Content-Type-Options: nosniff zentral am Reverse Proxy setzen.

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

▲ LOW FINDING F-05 · WEB-APP CVSS 3.1

Ausführliche Fehlermeldungen (Information Disclosure)

Bei Fehlern werden Stacktraces samt Framework-Version, Dateipfaden und SQL-Fragmenten ausgegeben — wertvolle Aufklärung für Angreifer.

Auswirkung

Erleichtert die Vorbereitung gezielterer Angriffe (Recon).

Proof of Concept

```
HTTP 500 – Internal Server Error
PDOException: SQLSTATE[42S22] in /var/www/app/src/Db/Query.php:212
Stack trace: #0 /var/www/app/vendor/…
```

Empfehlung

Generische Fehlerseiten ausliefern, Details nur serverseitig loggen. Debug-Modus in Produktion deaktivieren.

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`