SYNTHETISCHER MUSTERBERICHT · Keine echte Prüfung, kein Zertifikat.

PRÜFBERICHT · SICHERHEIT & COMPLIANCE

Wie sicher ist example/demo-web?

example/demo-web · geprüft am 16.09.2026 · 12:00 UTC · Commit c0ffee420000

Noch nicht freigabefähig.

2 Punkte müssen vor dem nächsten Release erledigt sein. Danach ist der Stand freigabefähig, wenn die 5 zeitnahen Punkte eingeplant sind. 594 von 603 anwendbaren Prüfkriterien sind ohne Befund.

1.431 PRÜFKRITERIEN · 603 AUF DIESES PROJEKT ANWENDBAR

594 ohne Befund | 9 mit Befund | 828 nicht anwendbar

2	5	2
Sofort	Zeitnah	Ordnung
Von außen ausnutzbar oder Datenverlust möglich	Wichtig, in den nächsten Sprint	Dokumentation und Hygiene, kein akutes Risiko

Wer erledigt das: KI-Agent 4 × | Update & Release 2 × | Mensch entscheidet 3 ×

PRÜFZEITPUNKT	16.09.2026 · 12:00 UTC
REGELWERK	2026.09.3/sme-eu-web (Beispiel)
PRÜFPROFIL	commercial-v1 (Beispiel)
PRÜFWERKZEUG	MAVENS.mcp 0.8.5 (Beispiel)
COMMIT	c0ffee420000000000000000000000000a17e
AUFTRAGS-ID	run-demo-0001

Was jetzt zu tun ist

17 Einzeltreffer des Scans, nach Ursache zusammengefasst: 9 Aufgaben. Jede nennt, was passiert, wenn man sie liegen lässt, und wer sie erledigen kann.

SOFORT Vor dem nächsten Release. Angreifbar von außen oder Daten in Gefahr.

next aktualisieren: 16.2.6 → 16.3.3

2 bekannte Lücken · Kritisch

Update & Release

Verwendete Bausteine haben bekannte Sicherheitslücken. Angreifer könnten sie ausnutzen.
Behebung: Betroffene Pakete auf sichere Version updaten (pnpm audit zeigt die Pfade).

```
CVE-2026-75604 [CRITICAL] · behoben ab 15.5.24, 16.3.3
Next.js: Middleware / Proxy bypass in App Router applications (critical)
```

Zugangsdaten aus Code und Git-Historie entfernen - und prüfen, ob sie noch gelten

1 Stelle

Mensch entscheidet

Ein Zugangscode liegt im Klartext im Code. Jeder mit Zugriff könnte ihn missbrauchen.
Behebung: Secret in .env/.env.example verschieben und über Umgebungsvariable laden; gedrückten Wert rotieren.

```
config/example.env:12
```

ZEITNAH In den nächsten Sprint. Erhöht das Risiko, ist aber nicht direkt ausnutzbar.

2 weitere Bausteine mit bekannten Lücken aktualisieren

2 Pakete · Hoch

Update & Release

Verwendete Bausteine haben bekannte Sicherheitslücken. Angreifer könnten sie ausnutzen.
Behebung: Ein Update-Durchgang für alle Pakete, dann Testlauf und Release. Betroffene Pakete auf sichere Version updaten (pnpm audit zeigt die Pfade).

```
postcss: 8.4.31 → 8.5.12
ws: 8.18.3 → 8.21.0
```

Personenbezogene Daten aus Logs und Browser fernhalten

3 Stellen · 2 Dateien

KI-Agent

Personenbezogene Daten könnten in Protokolle oder den Browser gelangen. Das darf nicht passieren.
Behebung: PII nicht loggen (console.log/logger) und nicht an Client-Komponenten übergeben.

```
app/api/invite/route.ts:41
app/api/invite/route.ts:58
lib/server/billing.service.ts:120
```

CI-Actions und Images auf feste Versionen pinnen

2 Stellen

KI-Agent

Ein Bestandteil des Builds kann sich unbemerkt ändern. Manipulierte Aktionen oder Images laufen dann mit Zugriff auf Secrets.
Behebung: Actions auf vollen Commit-Hash pinnen, Images auf Digest.

```
.github/workflows/ci.yml
.github/workflows/ci.yml
```

Fehlende Schutz-Header setzen

1 Stelle

KI-Agent

Die App setzt keine Schutz-Header. Browser können Inhalte dann einbetten, Skripte fremder Herkunft ausführen oder unverschlüsselt laden.
Behebung: Strict-Transport-Security in next.config headers() oder am Reverse Proxy setzen.

```
missing security headers: Strict-Transport-Security
```

Injection- oder XSS-Muster beheben

1 Stelle

KI-Agent

Eingaben werden ungeprüft verarbeitet. Angreifer könnten Daten manipulieren oder Code einschleusen.
Behebung: Betroffene Stelle absichern; semgrep-Meldung zeigt die exakte Stelle.

```
lib/oauth.ts:58
```

ORDNUNG Kein akutes Risiko. Nachweise, Hygiene, Vorbereitung auf CRA- und DSGVO-Nachfragen.

Meldeweg und Support-Policy dokumentieren

1 Stelle

Mensch entscheidet

Ohne Meldeweg und Support-Zusage fehlt die Grundlage für die Pflichten des Cyber Resilience Act.
Behebung: SECURITY.md mit Meldeweg, Reaktionszeit und Support-Zeitraum ergänzen.

```
SECURITY.md
```

Verarbeitungsverzeichnis anlegen

1 Stelle

Mensch entscheidet

Verarbeitungszwecke und Rechtsgrundlagen sind nicht maschinenlesbar dokumentiert.
Behebung: processing_manifest.yaml anlegen: Zwecke, Rechtsgrundlagen, Kategorien, Aufbewahrung.

```
processing_manifest.yaml fehlt: Datenverarbeitungszwecke und Rechtsgrundlagen sind nicht maschinenlesbar dokumentiert
```

Was das für DSGVO, CRA und KI-Verordnung bedeutet

Der Scan prüft im Code, was sich dort prüfen lässt: technische Schutzmaßnahmen und das Vorhandensein der geforderten Nachweise. Ob ein Gesetz für den Betreiber gilt, ergibt sich nicht aus dem Code - dafür stehen bei jedem Instrument die Fragen, die der Betreiber beantworten muss.

DSGVO

Befund

Datenschutz-Grundverordnung. Gilt, sobald personenbezogene Daten verarbeitet werden - im Code sichtbar an Nutzerkonten, E-Mail-Adressen, Logs.

3 Pflichten mit Befund, 2 ohne Befund, 1 nicht prüfbar. Die Befunde stehen als Aufgaben im Hauptteil.

PFLICHT	ARTIKEL	ERGEBNIS	WAS DER SCAN SIEHT
Datenminimierung, Privacy by Design	Art. 5, 25	Befund	Personenbezogene Daten aus Logs und Browser fernhalten
Einwilligung vor Tracking	Art. 6, 7 · TDDDG §25	ohne Befund	Kein Befund im Code; Nachweis bzw. Schutzmaßnahme vorhanden.
Verarbeitungsverzeichnis	Art. 30	Befund	Verarbeitungsverzeichnis anlegen
Rechtsgrundlagen und Aufbewahrungsfristen	Art. 6, 5(1)(e), 17	nicht prüfbar	Nicht prüfbar, solange „Verarbeitungsverzeichnis anlegen“ offen ist.
Sicherheit der Verarbeitung, technisch	Art. 32	Befund	Zugangsdaten aus Code und Git-Historie entfernen - und prüfen, ob sie noch gelten · Fehlende Schutz-Header setzen · Injection- oder XSS-Muster beheben · next aktualisieren: 16.2.6 → 16.3.3 · 2 weitere Bausteine mit bekannten Lücken aktualisieren
Sicherheit der Verarbeitung, Nachweise	Art. 32	ohne Befund	Kein Befund im Code; Nachweis bzw. Schutzmaßnahme vorhanden.

Fragen an den Betreiber: (1) Werden personenbezogene Daten von EU-Bürgern verarbeitet, und in welcher Rolle (Verantwortlicher oder Auftragsverarbeiter)? (2) Gibt es ein Verarbeitungsverzeichnis außerhalb des Repositories? (3) Werden Daten an Dienstleister außerhalb der EU übertragen?

Cyber Resilience Act

Befund

Gilt für Produkte mit digitalen Elementen, die in der EU in Verkehr gebracht werden. Kernpflichten: Schwachstellen-Meldeweg, Support-Zeitraum, sichere Lieferkette.

4 Pflichten mit Befund, 0 ohne Befund. Die Befunde stehen als Aufgaben im Hauptteil.

PFLICHT	ARTIKEL	ERGEBNIS	WAS DER SCAN SIEHT
Meldeweg und koordinierte Offenlegung	Art. 13, Anhang I Teil II	Befund	Meldeweg und Support-Policy dokumentieren
Bekannte Schwachstellen in Komponenten	Anhang I Teil II Nr. 1	Befund	next aktualisieren: 16.2.6 → 16.3.3 · 2 weitere Bausteine mit bekannten Lücken aktualisieren
Integrität der Lieferkette und des Builds	Anhang I Teil II	Befund	CI-Actions und Images auf feste Versionen pinnen
Sichere Standardkonfiguration	Anhang I Teil I	Befund	Fehlende Schutz-Header setzen

Fragen an den Betreiber: (1) Wird das Produkt in der EU in Verkehr gebracht, und in welcher Rolle (Hersteller, Importeur, Händler)? (2) Ab wann und wie lange gilt der zugesagte Support-Zeitraum? (3) Existiert ein Meldeweg für Schwachstellen außerhalb des Repositories?

KI-Verordnung (AI Act)

nicht anwendbar

Gilt, wenn das Produkt ein KI-System ist oder eines einsetzt. Der Scan erkennt das an Model-SDKs, Modell-Endpunkten oder einem KI-System-Manifest im Code.

Im Code nicht anwendbar: no model SDK, model endpoint or AI system manifest found; Reg. (EU) 2024/1689 does not apply to this artifact

Hinweis: Der Scan sieht nur, was im Code steht. Wird KI außerhalb dieses Codes eingesetzt, etwa über angebundene Agenten oder externe Modelle, gilt die Verordnung trotzdem - dann sind die Fragen unten zu beantworten.

PFLICHT	ARTIKEL	ERGEBNIS	WAS DER SCAN SIEHT
Transparenz gegenüber Nutzern	Art. 50	nicht anwendbar	Nicht anwendbar: im Code kein Anknüpfungspunkt.
Verbotene Praktiken	Art. 5	nicht anwendbar	Nicht anwendbar: im Code kein Anknüpfungspunkt.
Einstufung und KI-System-Manifest	Art. 6, Anhang III	nicht anwendbar	Nicht anwendbar: im Code kein Anknüpfungspunkt.
Menschliche Aufsicht	Art. 14, 26(2)	nicht anwendbar	Nicht anwendbar: im Code kein Anknüpfungspunkt.
Protokollierung bei Hochrisiko	Art. 12, 26(6)	nicht anwendbar	Nicht anwendbar: im Code kein Anknüpfungspunkt.
KI-Verarbeitung im Verarbeitungsverzeichnis	DSGVO Art. 30	nicht anwendbar	Nicht anwendbar: im Code kein Anknüpfungspunkt.

Fragen an den Betreiber: (1) Setzt das Produkt KI ein, die außerhalb dieses Codes liegt (z. B. angebundene Agenten oder externe Modelle)? (2) Trifft das System Entscheidungen mit Wirkung auf Personen (Anhang III)? (3) In welcher Rolle: Anbieter oder Betreiber?

Was geprüft wurde

4 Regelquellen, 1.431 Kriterien, 20 Prüfverfahren. Ein Kriterium gilt als „ohne Befund“, wenn es auf dieses Projekt anwendbar ist, sein Verfahren gelaufen ist und nichts gemeldet hat. Nicht anwendbar sind z. B. Cloud- oder Kubernetes-Regeln in einem Projekt ohne solche Artefakte.

REGELQUELLE	KRITERIEN	ANWENDBAR	OHNE BEFUND	MIT BEFUND
MAVENS-Regelkatalog 2026.09.3	48	40	32	8
Semgrep · OWASP Top 10, Secrets, JavaScript p/owasp-top-ten + p/secrets + p/javascript	598	310	309	1
Gitleaks · Secret-Muster, inkl. Git-Historie 8.30.1	222	222	222	0
Trivy · Infrastruktur-Konfiguration 0.74.0	563	31	31	0
Summe	1.431	603	594	9

Schwachstellen-Datenbanken (pnpm audit, Trivy CVE-Datenbank): 3 Pakete mit bekannten Lücken. Datenbanken sind keine Kriterien und zählen nicht in die 1.431.

20 Prüfverfahren

PRÜFVERFAHREN	ERGEBNIS	UMFANG
Zugangsdaten im Code	Befund	412 eligible files scanned; 0 not examined
Zugangsdaten in der Git-Historie (Gitleaks)	ohne Befund	gitleaks scanned working tree and full history
Datenbank-Migrationen	ohne Befund	12 migration files scanned; 0 not examined
Mandantentrennung, statisch (RLS)	ohne Befund	9 tables tracked; RLS without policies defaults to deny; effective access not tested
Mandantentrennung, live (RLS)	übersprungen	DATABASE_URL not set
Abhängigkeiten (pnpm audit)	Befund	pnpm audit completed (6 advisories)
Abhängigkeiten (Trivy CVE)	Befund	trivy vulnerability scan completed
Personenbezogene Daten in Logs	Befund	188 of 188 eligible source files scanned
Anmeldung & Sessions	ohne Befund	64 auth-relevant files scanned (static heuristics)
DSGVO · Einwilligung	Befund	manifest missing, 0 tracking files without consent gate
DSGVO · Art. 32 Nachweise	ohne Befund	compliance/processing-manifest.yaml absent; Art. 32 declarations checked; operational effectiveness not verified
CRA-Bereitschaft	Befund	vulnerability intake, disclosure, support and patch policy checked
Software-Lieferkette	Befund	1 lockfile(s), 2 workflow(s), license and deploy declarations checked; operating effectiveness not verified
Statische Codeanalyse (Semgrep)	teilweise	semgrep p/owasp-top-ten completed over 402 files; 2 artifacts with limited coverage

PRÜFVERFAHREN	ERGEBNIS	UMFANG
Infrastruktur-Konfiguration (Trivy)	ohne Befund	trivy misconfiguration scan completed
Live-Header des Servers	nicht anwendbar	no deployment_url in the assurance profile; nothing was contacted
Vertrauenswürdigkeit der Pakete	ohne Befund	7 dependencies checked against lockfile and 25 popular names
Schutz-Header	Befund	3/4 headers configured, CSRF protection found, 240 files scanned
Datei-Uploads	ohne Befund	0 upload handler(s) examined in 188 source files
KI-Verordnung	nicht anwendbar	no model SDK, model endpoint or AI system manifest found; Reg. (EU) 2024/1689 does not apply to this artifact

Was dieser Bericht nicht prüft

Laufzeit und Angriffe
Alles basiert auf dem Quellcode. Kein Penetrationstest, keine Beobachtung des laufenden Systems. „Ohne Befund“ heißt: kein Muster im Code - nicht: unangreifbar.

Mandantentrennung, live (RLS) · übersprungen
DATABASE_URL not set. Dieses Verfahren gilt nicht als bestanden.

Statische Codeanalyse (Semgrep) · 2 Dateien nicht lesbar
lib/database.types.ts, app/components/story.tsx. Für diese Dateien gilt kein Ergebnis dieses Verfahrens.

Live-Header des Servers · nicht anwendbar
no deployment_url in the assurance profile; nothing was contacted

KI-Verordnung · nicht anwendbar
no model SDK, model endpoint or AI system manifest found; Reg. (EU) 2024/1689 does not apply to this artifact

Ausgeschlossen: Testcode · 1 Treffer
Beispiel-Zugangsdaten und Beispiel-PII in Tests zählen nicht als Befund.

Rechtlicher Kontext
Betreiber-, Markt- und Verarbeitungskontext stehen nicht im Code. Die Fragen im Abschnitt zu DSGVO, CRA und KI-Verordnung klären, ob und wie die Instrumente gelten.

Anhang: alle Fundstellen

Jede Aufgabe mit sämtlichen Fundstellen und Befund-IDs, in der Reihenfolge des Hauptteils. Schweregrade und Hinweise stammen unverändert aus dem gespeicherten Scannerergebnis.
7 Blocker · 2 Kritisch · 8 Hoch

Sofort · MAV-DEP-001 · next aktualisieren: 16.2.6 → 16.3.3

```
pnpm-lock · next >=16.0.0 <16.2.11: Next.js: Middleware / Proxy bypass in App Router applications (critical) · demo-dep-001
pnpm-lock.yaml · trivy CVE-2026-75604 [CRITICAL]: next@16.2.6 (fixed 15.5.24, 16.3.3) · demo-sca-001
```

Sofort · MAV-SEC-001 · Zugangsdaten aus Code und Git-Historie entfernen - und prüfen, ob sie noch gelten

```
config/example.env:12 · credential assignment pattern in config/example.env:12 · demo-sec-001
```

Zeitnah · MAV-DEP-001 · 2 weitere Bausteine mit bekannten Lücken aktualisieren

```
pnpm-lock · ws >=8.0.0 <8.21.0: ws: Memory exhaustion DoS from tiny fragments (high) · demo-dep-002
pnpm-lock.yaml · trivy CVE-2026-48779 [HIGH]: ws@8.18.3 (fixed 8.21.0) · demo-sca-002
pnpm-lock · postcss <=8.5.11: PostCSS: Arbitrary file read via attacker-controlled sourceMappingURL (high) · demo-dep-003
pnpm-lock.yaml · trivy CVE-2026-45623 [HIGH]: postcss@8.4.31 (fixed 8.5.12) · demo-sca-003
```

Zeitnah · MAV-PII-001 · Personenbezogene Daten aus Logs und Browser fernhalten

```
app/api/invite/route.ts:41 · Personal-data payload (email) reaches logger at app/api/invite/route.ts:41; transport redaction unknown · demo-pii-001
app/api/invite/route.ts:58 · Personal-data payload (userId) reaches logger at app/api/invite/route.ts:58; transport redaction unknown · demo-pii-002
lib/server/billing.service.ts:120 · Personal-data payload (userId) reaches logger at lib/server/billing.service.ts:120; transport redaction unknown · demo-pii-003
```

Zeitnah · MAV-SUPPLY-002 · CI-Actions und Images auf feste Versionen pinnen

```
.github/workflows/ci.yml · CI action is not pinned to a full commit: actions/checkout@v4 · demo-sup-001
.github/workflows/ci.yml · CI action is not pinned to a full commit: actions/setup-node@v4 · demo-sup-002
```

Zeitnah · MAV-HDR-001 · Fehlende Schutz-Header setzen

```
missing security headers: Strict-Transport-Security · demo-hdr-001
```

Zeitnah · MAV-SAST-001 · Injection- oder XSS-Muster beheben

```
lib/oauth.ts:58 · semgrep javascript.node-crypto.security.gcm-no-tag-length.gcm-no-tag-length: source pattern requires review (lib/oauth.ts:58) · demo-sast-001
```

Ordnung · MAV-CRA-001 · Meldeweg und Support-Policy dokumentieren

```
SECURITY.md · SECURITY.md must define vulnerability intake and coordinated disclosure · demo-cra-001
```

Ordnung · MAV-GDPR-001 · Verarbeitungsverzeichnis anlegen

```
processing_manifest.yaml fehlt: Datenverarbeitungszwecke und Rechtsgrundlagen sind nicht maschinenlesbar dokumentiert · demo-gdpr-001
```

Prüfverfahren

Automatisierte, regelbasierte Analyse des angegebenen Quellstands. Der Bericht übernimmt das gespeicherte Scannerurteil und dokumentiert gelaufene sowie ausgefallene Prüfschritte getrennt. Prioritäten und Zuständigkeiten folgen einer festen Tabelle je Regel; kein Sprachmodell bewertet Befunde beim Versand neu.

Geltungsbereich

Die Aussage gilt für das benannte Repository und den vollständigen Commit. Test-, Fixture- und Designdateien werden gezählt, aber nicht als Aufgabe geführt. Eine spätere Code-Version ist nicht Gegenstand dieses Berichts.

Bewertung und Grenzen

Dieser Bericht ist keine Zertifizierung, keine Rechtsberatung und kein manueller Penetrationstest. Organisatorische Maßnahmen, die Wirksamkeit von Korrekturen und nicht ausgeführte Prüfschritte sind nicht nachgewiesen.

Technischer Nachweis

Die SHA-256-Prüfsumme bezeichnet den gespeicherten Textbericht. Sie ist keine digitale Signatur dieses PDFs. Die Vorlage stellt das gespeicherte Ergebnis dar; sie führt keine neue Prüfung durch.

Technische Referenzen

Vorlage	mavens-assurance-report / 2.0
Auftrags-ID	run-demo-0001
Repository	example/demo-web
Commit	c0ffee420000000000000000000000000a17e
Tree-SHA	0000000000000000000000000000000000000000
Quellstand-Digest	sha256:0000000000000000000000000000000000000000000000000000000000000000
Prüfprofil	commercial-v1 (Beispiel)
Regelwerk	2026.09.3/sme-eu-web (Beispiel)
Richtlinie	remote-review-v1 (Beispiel)
Runner	synthetischer Musterlauf
Runner-Image	sha256:0000000000000000000000000000000000000000000000000000000000000000
Textbericht SHA-256	sha256:0000000000000000000000000000000000000000000000000000000000000000
Einzeltreffer	17 gesamt · 17 blockierend · 1 Prüfausfälle
App / IDE	Beispiel-App
Vorgangs-ID	workflow-demo-0001