WEBSITE SECURITY REPORT

Vollständige Sicherheitsanalyse

demobeboag.de

Demo BeBo AG – Investment Unternehmen

Analysedatum	01. April 2026
Gesamtbewertung	**D – Erhebliche Mängel**
Analysescope	demobeboag.de inkl. Subdomains & Mailinfrastruktur
Hosting	Vercel Inc. (CDN-Edge: fra1 – Frankfurt)
DNS / E-Mail	Muster-Hosting AG (musterhost.example) – Berlin/DE
SSL-Aussteller	Let's Encrypt R12 – gültig bis 31.05.2026
Methodik	Black-Box (passiv + aktiv, mit Genehmigung)
Tools	Nmap, Nikto, dnsrecon, dig, curl, swaks, openssl, gobuster, WPScan, Shodan InternetDB, crt.sh
Klassifizierung	**VERTRAULICH – nur für den Auftraggeber**

1. Executive Summary

Die Website demobeboag.de wurde einer vollständigen Black-Box-Sicherheitsanalyse unterzogen. Die Analyse umfasste HTTP-Header-Inspektion, DNS-Enumeration, Portscanning, SSL/TLS-Prüfung, E-Mail-Sicherheit, Directory-Bruteforce, CMS-Erkennung sowie eine manuelle Untersuchung der eingesetzten Technologien und Infrastruktur.

Die Gesamtbewertung lautet D – Erhebliche Mängel. Die Website weist 6 kritische und 5 mittelschwere Schwachstellen auf. Besonders hervorzuheben sind das vollständige Fehlen essenzieller HTTP-Sicherheitsheader, eine DSGVO-widrige Implementierung von Vercel Analytics ohne Cookie-Consent, ein potenzieller Subdomain-Takeover-Vektor über einen verwaisten Vercel-CNAME sowie eine fehlende SPF-Konfiguration die E-Mail-Spoofing begünstigt.

Alle gefundenen Schwachstellen sind ohne Infrastrukturwechsel behebbar. Der kritische Pfad für Sofortmaßnahmen umfasst ca. 4–8 Stunden Konfigurationsaufwand.

KRITISCH	WARNUNG	BESTANDEN	HINWEIS
6	5	3	3

1.1 Risikomatrix

ID	Befund	Kategorie	Schwere	CVSS est.
F-01	Fehlende HTTP-Sicherheitsheader (CSP, X-Frame, XCTO, Permissions)	Web	KRITISCH	7.4
F-02	CORS Wildcard (access-control-allow-origin: *)	Web	KRITISCH	7.1
F-03	Vercel Analytics ohne Cookie-Consent (DSGVO Art. 5, 13, 28)	Datenschutz	KRITISCH	–
F-04	Potenzieller Subdomain-Takeover (Vercel CNAME DEPLOYMENT_NOT_FOUND)	Infra	KRITISCH	8.1
F-05	Kein SPF-Record – E-Mail-Spoofing möglich	E-Mail	KRITISCH	6.5
F-06	DNSSEC nicht konfiguriert – DNS-Spoofing/Cache-Poisoning möglich	DNS	KRITISCH	6.8
F-07	SSL-Zertifikat läuft ab: 31.05.2026 (~53 Tage)	SSL/TLS	WARNUNG	5.3
F-08	Mailserver-Version exponiert (Muster-Hosting MailCore V55.0.1)	E-Mail	WARNUNG	4.3
F-09	Vercel-interne Deployment-IDs in Response-Headern	Infra	WARNUNG	3.7

F-10	Inkonsistente Redirect-Kette (HTTP→HTTPS Apex-Domain)	Web	**WARNUNG**	3.1
F-11	Sitemap veraltet (lastmod 2024-12-11, letzter Deploy 2026-04-07)	Web	**WARNUNG**	2.0
F-12	Kein IPv6 (AAAA-Record fehlt)	Infra	**HINWEIS**	–
F-13	security.txt fehlt (RFC 9116)	Web	**HINWEIS**	–
F-14	Shared Vercel-IP mit fremden Domains (fremdprojekt.example.com)	Infra	**HINWEIS**	–

2. Infrastruktur & Technologie-Stack

Die folgende Tabelle dokumentiert den vollständig rekonstruierten Infrastruktur-Stack auf Basis aller durchgeführten Reconnaissance-Maßnahmen.

Domain	demobeboag.de
www-Auflösung	www.demobeboag.de → CNAME deadbeefdeadbeef.vercel-dns-017.com
IP-Adressen	(alle Vercel fra1)
Hosting	Vercel Inc. (San Francisco, USA) – CDN-Edge Frankfurt (fra1)
Frontend	Statisches HTML/CSS/JS – kein WordPress, kein Next.js erkannt (WPScan bestätigt)
Webserver	Vercel Edge Network – HTTP/2, TLSv1.3
CDN / Cache	Vercel Edge Cache (x-vercel-cache: HIT, age: 136901s)
Analytics	Vercel Web Analytics (/_vercel/insights/script.js) – aktiv ohne Consent
Nameserver	ns1.musterhost.example | ns2.musterhost.example (Muster-Hosting AG, PowerDNS)
SOA / Registrar	Muster-Hosting AG – hostmaster.musterhost.example – Serial: 2026010101
Mailserver (MX)	mailin.musterhost.example (260.260.260.260) – Muster-Hosting AG, MailCore V55.0.1
SSL-Zertifikat	Let's Encrypt R12 – RSA 2048-bit – 02.03.2026 bis 31.05.2026
TLS-Protokoll	TLSv1.3 / TLS_AES_128_GCM_SHA256 / X25519MLKEM768 (Post-Quantum)
Offene Ports (Web)	TCP 80 (HTTP), TCP 443 (HTTPS) – alle anderen gefiltert/geschlossen
Offene Ports (Mail)	TCP 25 (SMTP offen) – 465/587/993/995 gefiltert
E-Mail-Auth	DMARC: v=DMARC1; p=reject | DKIM: o=~; t=y | SPF: NICHT VORHANDEN
DNSSEC	NICHT konfiguriert
IPv6 (AAAA)	NICHT konfiguriert
Autodiscover	_autodiscover._tcp → autoconfigure.musterhost.example:443 (Provider-E-Mail)

3. Detaillierte Findings

3.1 HTTP-Sicherheitsheader (F-01, F-02)

Die vollständige HTTP-Response-Header-Analyse zeigt ein unzureichendes Sicherheitsniveau. Fünf von sieben OWASP-empfohlenen Sicherheitsheadern fehlen vollständig.

Header	Wert	Status	Priorität
strict-transport-security	max-age=63072000	**Vorhanden**	–
content-security-policy	— nicht gesetzt —	**FEHLT**	HOCH
x-frame-options	— nicht gesetzt —	**FEHLT**	HOCH
x-content-type-options	— nicht gesetzt —	**FEHLT**	HOCH
permissions-policy	— nicht gesetzt —	**FEHLT**	HOCH
referrer-policy	— nicht gesetzt —	**FEHLT**	MITTEL
access-control-allow-origin	* (Wildcard!)	**KRITISCH**	HOCH
server	Vercel	**Info-Leak**	NIEDRIG

KRITISCH
F-01

Fehlende HTTP-Sicherheitsheader – CSP, X-Frame-Options, X-Content-Type-Options, Permissions-Policy

Vier essenzielle OWASP-empfohlene Sicherheitsheader fehlen vollständig. Ohne Content Security Policy sind XSS-Angriffe auf eingebettete Formulare und fremde Script-Injection möglich. Ohne X-Frame-Options kann die Seite in fremde iFrames eingebettet werden (Clickjacking). Ohne X-Content-Type-Options ist MIME-Sniffing durch Browser möglich was MIME-Confusion-Angriffe ermöglicht. Ohne Permissions-Policy haben Drittanbieter-Scripts unkontrollierten Zugriff auf Browser-APIs wie Kamera, Mikrofon und Standort.

Tool/Nachweis: Nikto: 'X-Frame-Options header is not present' | 'X-Content-Type-Options header is not set' | curl -sI → alle vier Header fehlen

Empfehlung: Alle fehlenden Header über vercel.json headers-Konfiguration setzen. CSP zunächst im Report-Only-Modus testen. Umsetzungsaufwand ca. 1–2 Stunden.

KRITISCH
F-02

CORS Wildcard – access-control-allow-origin: *

Der Server antwortet auf jeden Origin-Header mit einem Wildcard-Wert. Jede beliebige externe Website kann per JavaScript Anfragen an demobeboag.de stellen und Antworten lesen. Bei vorhandener API-Route (/api/hello gibt HTTP 200 zurück) ist dies ein direkter Angriffspfad für Cross-Site Request Forgery und Datenlecks. Nikto bestätigte: 'Retrieved access-control-allow-origin header: *'.

Tool/Nachweis: curl -sI https://www.demobeboag.de -H 'Origin: https://evil.com' → access-control-allow-origin: * | /api/hello → HTTP 200

Empfehlung: CORS auf die eigene Domain beschränken: access-control-allow-origin: https://www.demobeboag.de. Wildcard nur wenn ausschließlich öffentliche, nicht sensible Ressourcen ausgeliefert werden.

3.2 DSGVO – Vercel Analytics ohne Cookie-Einwilligung (F-03)

KRITISCH
F-03

Vercel Web Analytics trackt Besucher ohne Einwilligungsbanner

Das Script /_vercel/insights/script.js ist aktiv eingebunden und sendet bei jedem Seitenaufruf automatisch folgende Daten an Vercel-Server: vollständige URL (inkl. Pfad), Zeitstempel (Date.now()), Referrer-Informationen, Browser-Fingerprint (navigator.webdriver, userAgent), Session-Tracking sowie Routing-Daten. Dies geschieht ohne Einwilligungsbanner, ohne Opt-Out und ohne dass Vercel als Auftragsverarbeiter in der Datenschutzerklärung genannt wird. Gemäß Art. 5, 13 und 28 DSGVO sowie der ePrivacy-Richtlinie ist dies ein bußgeldbewehrter Datenschutzverstoß (bis zu 4% des Jahresumsatzes oder 20 Mio. EUR).

Tool/Nachweis: curl https://www.demobeboag.de/_vercel/insights/script.js → Script aktiv, sendet pageview/url/referrer/timestamp/session ohne Einwilligung

Empfehlung: Option A: Vercel Analytics vollständig deaktivieren im Vercel-Dashboard. Option B: Consent-Management-Plattform (z.B. Cookiefirst, Klaro) implementieren die Analytics erst nach aktiver Einwilligung lädt. AVV mit Vercel abschließen und Datenschutzerklärung aktualisieren.

3.3 Subdomain-Takeover-Risiko (F-04)

KRITISCH
F-04

Vercel CNAME deadbeefdeadbeef.vercel-dns-017.com gibt DEPLOYMENT_NOT_FOUND zurück

Der DNS-CNAME-Eintrag von www.demobeboag.de zeigt auf den Vercel-internen Hostnamen deadbeefdeadbeef.vercel-dns-017.com. Eine direkte HTTP-Anfrage an diesen Hostnamen ohne Host-Header gibt den Fehler 'x-vercel-error: DEPLOYMENT_NOT_FOUND' mit HTTP 404 zurück. Dies ist das klassische Signalmuster für einen potenziellen Subdomain-Takeover: Wenn das Vercel-Deployment gelöscht oder nicht mehr fest verknüpft ist, könnte ein Angreifer ein eigenes Vercel-Projekt mit demselben CNAME registrieren und die Domain vollständig übernehmen. Im Takeover-Szenario könnte ein Angreifer Phishing-Seiten unter www.demobeboag.de betreiben, gültige SSL-Zertifikate ausstellen und Besucher-Traffic abfangen.

Tool/Nachweis: dnsrecon: CNAME www.demobeboag.de → deadbeefdeadbeef.vercel-dns-017.com | curl https://deadbeefdeadbeef.vercel-dns-017.com → HTTP 404, x-vercel-error: DEPLOYMENT_NOT_FOUND

Empfehlung: Im Vercel-Dashboard prüfen ob das Deployment aktiv und die Domain korrekt verknüpft ist. Falls ein altes Deployment nicht mehr aktiv ist, CNAME-Eintrag entfernen oder Vercel-Projekt reaktivieren. Monitoring einrichten.

3.4 E-Mail-Sicherheit (F-05, F-08)

KRITISCH
F-05

Kein SPF-Record – E-Mail-Spoofing im Namen von @demobeboag.de möglich

Ein SPF TXT-Record für demobeboag.de fehlt vollständig (dig TXT liefert keinen SPF-Eintrag). Obwohl DMARC mit p=reject konfiguriert ist, greift DMARC nur wenn SPF oder DKIM einen positiven Identifier-Alignment-Treffer liefern. Ohne SPF ist dieses Alignment nicht gewährleistet. Swaks-Test bestätigt: Der Muster-Mailserver akzeptierte MAIL FROM:<fake@demobeboag.de> kommentarlos (250 2.1.0 Sender ok) und lehnte nur den externen Relay ab. Angreifer könnten Phishing-E-Mails im Namen des Unternehmens versenden die bei einigen Empfängern nicht als Spam erkannt werden.

Tool/Nachweis: dig demobeboag.de TXT +short → kein SPF-Eintrag | swaks: MAIL FROM:<fake@demobeboag.de> → 250 2.1.0 Sender ok

Empfehlung: SPF-Record anlegen: 'v=spf1 mx include:musterhost.example ~all' als TXT-Record im Provider-DNS-Panel. Anschließend DMARC-Alignment mit DKIM prüfen.

WARNUNG
F-08

Mailserver-Version vollständig exponiert: Muster-Hosting MailCore V55.0.1

Der Muster-Mailserver gibt seine vollständige Implementierungsversion in EHLO- und HELP-Antworten preis: 'Implementation Muster-Hosting AG, MailCore V55.0.1'.

Zusätzlich wird die Support-E-Mail postmaster@musterhost.example exponiert. Diese Informationen ermöglichen Angreifern gezielt nach veröffentlichten Schwachstellen für diese spezifische Softwareversion zu suchen.

Tool/Nachweis: nmap --script smtp-commands mailin.musterhost.example → '214-Implementation Muster-Hosting AG, MailCore V55.0.1'

Empfehlung: Provider-Kundensupport kontaktieren bezüglich SMTP-Banner-Einschränkung. Bei Managed-Hosting-Angeboten ist dies oft konfigurierbar.

3.5 DNS-Sicherheit (F-06)

KRITISCH
F-06

DNSSEC nicht konfiguriert – DNS-Cache-Poisoning möglich

DNSSEC ist für demobeboag.de nicht aktiviert. Ohne DNSSEC können DNS-Antworten durch Cache-Poisoning-Angriffe gefälscht werden. Ein Angreifer im gleichen Netzwerk oder mit Zugang zu einem anfälligen Resolver könnte DNS-Anfragen auf eigene Server umleiten und so den gesamten Web- und E-Mail-Traffic abfangen (Man-in-the-Middle). Dies ist insbesondere kritisch in Kombination mit dem fehlenden SPF-Record und dem potenziellen Subdomain-Takeover-Vektor.

Tool/Nachweis: dnsrecon: '[-] DNSSEC is not configured for demobeboag.de'

Empfehlung: DNSSEC über das Provider-Kundenpanel aktivieren. Muster-Hosting unterstützt DNSSEC für .de-Domains nativ. Aufwand ca. 30 Minuten.

3.6 SSL/TLS-Analyse (F-07)

WARNUNG
F-07

SSL-Zertifikat läuft in ~53 Tagen ab – Auto-Renewal muss verifiziert werden

Das Let's Encrypt Zertifikat (ausgestellt 02.03.2026) läuft am 31.05.2026 ab. Let's Encrypt erneuert Zertifikate normalerweise automatisch alle 60–90 Tage. Die verbleibende Laufzeit von ~53 Tagen deutet darauf hin, dass die Erneuerung bald fällig wird. Schlägt das Auto-Renewal fehl, ist die Website für alle Besucher unerreichbar. Zusätzlich fehlt die Apex-Domain (demobeboag.de ohne www) als Subject Alternative Name – nur www. ist im Zertifikat enthalten.

Tool/Nachweis: nmap ssl-cert: Not valid after: 2026-05-31T22:03:42 | openssl Subject: CN=www.demobeboag.de | SAN: DNS:www.demobeboag.de (kein Apex-SAN)

Empfehlung: Auto-Renewal in Vercel-Dashboard verifizieren. SSL-Monitoring mit Alert bei <30 Tagen Restlaufzeit einrichten (z.B. UptimeRobot). Apex-Domain in SAN aufnehmen lassen.

Positive TLS-Befunde

- TLSv1.3 aktiv – veraltete Protokolle (TLS 1.0/1.1, SSLv3) nicht verfügbar
- X25519MLKEM768 Key Exchange – Post-Quantum-resistenter Algorithmus aktiv
- HSTS: max-age=63072000 (2 Jahre) – HTTP wird vom Browser dauerhaft auf HTTPS erzwungen
- HTTP/2 aktiv – modernes, effizientes Protokoll
- Let's Encrypt CA – weitverbreitet und vertrauenswürdig

3.7 Weitere Findings (F-09 bis F-11)

WARNUNG
F-09

Vercel-interne Deployment-IDs und private IP in Response-Headern exponiert

Jede HTTP-Response enthält den Header x-vercel-id mit vollständiger interner Routing-Information (z.B. fra1::demo00-0000000000000-000000000000) inkl. Zeitstempel, Node-

	ID und Deployment-Hash. Nikto identifizierte zusätzlich eine private IP-Adresse im x-vercel-id Header (IP: 0a::00). Diese Informationen erleichtern die Infrastruktur-Reconnaissance erheblich. **Tool/Nachweis:** Nikto: 'IP address found in the x-vercel-id header. The IP is 0a::00' | curl -sI: x-vercel-id: fra1::demo00-0000000000000-000000000000 **Empfehlung:** Über vercel.json den x-vercel-id Header soweit möglich unterdrücken. Interne Routing-IDs sollten nicht in öffentlichen HTTP-Responses erscheinen.
WARNUNG F-10	**Inkonsistente Redirect-Kette für Apex-Domain** http://www.demobeboag.de → https://www.demobeboag.de (korrekt, 308). http://demobeboag.de → https://demobeboag.de/ (308, ohne www). https://demobeboag.de → https://www.demobeboag.de (307, temporär!). Die doppelte Redirect-Kette erzeugt unnötige Latenz, der 307-Status ist temporär statt permanent und kann Cookie-Probleme sowie inkonsistentes HSTS-Verhalten verursachen. **Tool/Nachweis:** curl -sI http://demobeboag.de → 308 zu https://demobeboag.de | curl -sI https://demobeboag.de → 307 zu https://www.demobeboag.de **Empfehlung:** In vercel.json sicherstellen dass alle Varianten (http/https, www/non-www) in einem einzigen permanenten 308-Redirect auf https://www.demobeboag.de enden.
WARNUNG F-11	**Sitemap.xml veraltet – lastmod-Datum stimmt nicht mit letztem Deploy überein** Die sitemap.xml enthält als lastmod-Datum den 2024-12-11, obwohl der HTTP Last-Modified-Header der Seite den 07.04.2026 ausweist. Eine veraltete Sitemap kann SEO-Performance beeinträchtigen und Suchmaschinen veranlassen die Seite seltener zu crawlen. **Tool/Nachweis:** curl https://www.demobeboag.de/sitemap.xml → <lastmod>2024-12-11</lastmod> | HTTP Header: last-modified: Tue, 07 Apr 2026 **Empfehlung:** Sitemap.xml bei jedem Deploy automatisch mit aktuellem Datum aktualisieren. Über Vercel Build-Hooks oder ein pre-deploy Script automatisierbar.

4. Positive Befunde

Befund	Details
Kein Open Mail Relay	RCPT TO externe Adressen korrekt mit 550 Relaying denied verweigert
Zone Transfer blockiert	AXFR an ns1.musterhost.example und ns2.musterhost.example schlägt fehl – korrekt konfiguriert
DMARC p=reject konfiguriert	v=DMARC1; p=reject – strengste verfügbare Richtlinie
HSTS mit 2 Jahren max-age	max-age=63072000 – Browser erzwingen dauerhaft HTTPS
TLSv1.3 mit Post-Quantum-Krypto	X25519MLKEM768 Key Exchange – zukunftssicher gegen Quantencomputer
Minimale Portexposition	Nur TCP 80 und 443 offen – keine Management-Ports, keine unnötigen Dienste
Kein Malware-/Blacklist-Eintrag	Shodan InternetDB zeigt vulns:[] für beide IPs – keine bekannten CVEs
HTTP/2 aktiv	Modernes Protokoll, verbesserte Performance und Multiplexing
SMTP STARTTLS verfügbar	E-Mail-Übertragung verschlüsselt möglich – korrekte EHLO-Konfiguration
Gobuster-/Nikto-Zugriff blockiert	Vercel WAF/Rate-Limiting blockiert automatisierte Scanner nach wenigen Requests

5. Maßnahmenplan

Alle Maßnahmen sind ohne Infrastrukturwechsel umsetzbar. Gesamtaufwand für Sofortmaßnahmen: ca. 4–8 Stunden.

5.1 Sofortmaßnahmen (0–48 Stunden)

#	Maßnahme	Umsetzung	Aufwand
1	HTTP-Security-Header setzen (CSP, X-Frame-Options, XCTO, Permissions-Policy, Referrer-Policy) via vercel.json	vercel.json → headers	1–2 Std.
2	CORS auf eigene Domain einschränken: access-control-allow-origin: https://www.demobeboag.de	vercel.json → headers	30 Min.
3	SPF-Record anlegen: v=spf1 mx include:musterhost.example ~all als TXT-Record bei Muster-Hosting	Provider-DNS-Panel	15 Min.
4	Vercel Analytics deaktivieren oder Cookie-Consent implementieren (DSGVO-Pflicht)	Vercel Dashboard + CMP	2–4 Std.
5	Vercel-Deployment-Verknüpfung prüfen – Subdomain-Takeover-Risiko bewerten und ausschließen	Vercel Dashboard → Domains	15 Min.

5.2 Kurzfristige Maßnahmen (1–4 Wochen)

#	Maßnahme	Umsetzung	Aufwand
6	DNSSEC aktivieren	Provider-Panel → DNS → DNSSEC	30 Min.
7	SSL Auto-Renewal in Vercel verifizieren + Monitoring-Alert bei <30 Tagen	Vercel Dashboard + UptimeRobot	30 Min.
8	Redirect-Kette vereinheitlichen: alle Varianten → https://www.demobeboag.de (308)	vercel.json → redirects	30 Min.
9	Sitemap.xml lastmod bei jedem Deploy automatisch aktualisieren	Build-Script / Vercel Hook	1 Std.
10	Datenschutzerklärung aktualisieren: Vercel als Auftragsverarbeiter + AVV abschließen	Datenschutzerklärung + Vercel DPA	2 Std.

5.3 Empfohlene vercel.json (behebt F-01, F-02, F-10)

```
{
  "headers": [{
    "source": "/(.*)",
    "headers": [
      { "key": "X-Frame-Options",        "value": "SAMEORIGIN" },
      { "key": "X-Content-Type-Options",  "value": "nosniff" },
      { "key": "Referrer-Policy",         "value": "strict-origin-when-cross-origin" },
      { "key": "Permissions-Policy",      "value": "camera=(), microphone=(), geolocation=()" },
      { "key": "Access-Control-Allow-Origin", "value": "https://www.demobeboag.de" },
      { "key": "Content-Security-Policy", "value": "default-src 'self'; script-src 'self' 'unsafe-inline'; report-uri /csp-report" }
    ]
  }],
  "redirects": [{
    "source": "/(.*)",
    "has": [{ "type": "host", "value": "demobeboag.de" }],
    "destination": "https://www.demobeboag.de/$1",
    "permanent": true
  }]
}
```

6. Verwendete Tools & Methodik

Tool	Version	Verwendung
Nmap	7.95	Portscanning, Service-Erkennung, SSL-Check, SMTP-Skripte
Nikto	2.5.0	HTTP-Header-Analyse, Pfad-Enumeration, Security-Header-Check
dnsrecon	Kali 2026	DNS-Enumeration, Subdomain-Bruteforce, DNSSEC-Prüfung
dig (DiG)	9.20.11-4	DNS-Records (A, MX, TXT, NS, SOA, AAAA, AXFR-Versuch)
curl	8.15.0	HTTP-Header, CORS-Test, Pfad-Enumeration, Response-Analyse
openssl	System	SSL/TLS-Zertifikatsprüfung, Cipher-Suite-Analyse
swaks	Kali 2026	SMTP-Relay-Test, E-Mail-Spoofing-Simulation
gobuster	3.8	Directory-Bruteforce (durch Vercel WAF blockiert)
WPScan	Kali 2026	CMS-Erkennung – WordPress ausgeschlossen
Shodan InternetDB	internetdb.shodan.io	IP-Reputation, CVE-Lookup, Hostname-Mapping
crt.sh	Certificate Transparency	Zertifikatshistorie, Subdomain-Enumeration

6.1 Rechtlicher Hinweis

Diese Sicherheitsanalyse wurde im Auftrag und mit ausdrücklicher Genehmigung des Betreibers von demobeboag.de durchgeführt. Sämtliche Tests erfolgten ausschließlich gegen Systeme für die eine Freigabe vorlag. Die Analyse dient der Verbesserung der Website-Sicherheit und ist als vertraulich zu behandeln. Eine Weitergabe an Dritte bedarf der ausdrücklichen Genehmigung des Auftraggebers.

CVSS-Scores sind Schätzungen aus Black-Box-Perspektive und können von einer vollständigen internen Prüfung abweichen. Kein Penetrationstest ersetzt eine vollständige, interne Sicherheitsprüfung.

Ende des Berichts – Erstellt: 08. April 2026 | VERTRAULICH