

Sicherheitsanalyse

Passive externe Prüfung der Website

www.beispiel.at

GESAMTEINSTUFUNG

Hoch

Es liegen erhebliche Risiken vor, etwa eine PHP-Version ohne Sicherheitsupdates. Zeitnah handeln.

Auftraggeber	Beispiel GmbH (Musterbericht)
Geprüfte Adresse	https://www.beispiel.at/
Prüfzeitpunkt	28.10.2026, 09:12
Bericht erstellt	28.10.2026, 09:15
Bericht-ID	R-A1B2C3D4E5
Bestellnummer	B-20261028-A1B2C

Diese Analyse beruht auf öffentlich abrufbaren Informationen: den Antworten des Servers, öffentlichen DNS-Einträgen und einem festen Katalog bekannter Fundstellen, die nur gelesen wurden. Sie ist kein Penetrationstest: Es wurden keine Schwachstellen aktiv ausgenutzt und keine Zugangsdaten probiert.

01

Management Summary

Die externe Prüfung von [www.beispiel.at](#) am 28.10.2026, 09:12 ergibt die Gesamteinstufung „Hoch“. Der Server meldet PHP 8.2.35; Supportstatus: Nur noch Sicherheitsupdates. Die HTTPS-Verbindung ist mit einem gültigen Zertifikat gesichert. Die erweiterten Prüfungen ergeben Handlungsbedarf in diesen Bereichen: Offengelegte Dateien, Plugins, JavaScript-Bibliotheken, Inhalte und Formulare, Cookies, E-Mail-Sicherheit. Insgesamt ergeben sich 13 Feststellungen mit Handlungsbedarf.

PHP-VERSION

PHP 8.2.35

Exakte Version erkannt

PHP-SUPPORT

Nur Sicherheit

Sicherheitsupdates bis 31.12.2026

BEKANNTE SCHWACHSTELLEN

0

Zuordnung anhand der exakten Version

HTTPS / TLS

gültig

TLSv1.3

SICHERHEITSHEDER

2 von 5 gesetzt

FESTSTELLUNGEN

13

ohne reine Hinweise

ANWENDUNG

WordPress

Version nicht erkennbar

OFFENGELEGTE DATEIEN

2

20 Fundstellen geprüft

E-MAIL-SICHERHEIT

SPF ja · DMARC none

beispiel.at

Priorisierte Maßnahmen

#	STUFE	MASSNAHME	ZEITRAHMEN
1	HOCH	WordPress-Debugprotokoll öffentlich WP_DEBUG_LOG im Live-Betrieb abschalten oder auf einen Pfad außerhalb des Webroots legen; Datei löschen.	Sofort
2	MITTEL	PHP 8.2 erhält nur noch Sicherheitsupdates Den Umstieg auf PHP 8.5 einplanen, rechtzeitig vor Ende des Sicherheitssupports.	Kurzfristig
3	MITTEL	Sicherheitsheader fehlt: Strict-Transport-Security (HSTS) Den Header „Strict-Transport-Security: max-age=31536000; includeSubDomains“ setzen — erst, wenn alle Subdomains per HTTPS erreichbar sind.	Kurzfristig
4	MITTEL	1 Plugin ist nicht aktuell Plugins aktualisieren und automatische Updates für Plugins einschalten.	Kurzfristig

#	STUFE	MASSNAHME	ZEITRAHMEN
5	MITTEL	jQuery 3.4.1 mit bekannten Schwachstellen jQuery auf mindestens 3.5.0 aktualisieren (bzw. das CMS-Theme oder Plugin, das die Bibliothek mitbringt).	Kurzfristig
6	NIEDRIG	PHP-Version wird öffentlich angezeigt In der php.ini „expose_php = Off“ setzen. Bei vielen Hostern geht das im Kundenmenü unter den PHP-Einstellungen.	Mittelfristig

02

Technische Analyse

2.1 PHP-Version und Erkennungsgrundlage

Ergebnis	Exakte Version erkannt
Erkannte Version	PHP 8.2.35
Distributionspaket	nicht erkennbar

QUELLE	ÜBERMITTELT WERT
X-Powered-By	PHP/8.2.35
HTML-Generator	Wordpress

2.2 PHP-Lifecycle

Versionsreihe	8.2
Status	Nur noch Sicherheitsupdates
Aktiver Support bis	31.12.2024
Sicherheitsupdates bis	31.12.2026
Aktuelles Release der Reihe	PHP 8.2.35

Derzeit unterstützte PHP-Versionen:

REIHE	STATUS	AKTIV BIS	SICHERHEIT BIS	AKTUELL
PHP 8.5	Aktiver Support	31.12.2027	31.12.2029	8.5.12
PHP 8.4	Aktiver Support	31.12.2026	31.12.2028	8.4.27
PHP 8.3	Nur noch Sicherheitsupdates	31.12.2025	31.12.2027	8.3.36
PHP 8.2	Nur noch Sicherheitsupdates	31.12.2024	31.12.2026	8.2.35

Quelle: php.net/releases/branches.php (mitgelieferter Stand), Stand 28.10.2026.

2.3 Bekannte Schwachstellen (CVE)

Für die erkannte Version sind in der NVD keine Schwachstellen mit passendem Versionsbereich verzeichnet.
Das ist der Stand der Datenbank zum Abrufzeitpunkt. Neue Schwachstellen werden laufend veröffentlicht, und die NVD bewertet nicht alle Einträge zeitnah.

2.4 HTTPS und TLS

Zertifikat	gültig und vertrauenswürdig
Ausgestellt für	beispiel.at, www.beispiel.at
Aussteller	Let's Encrypt R11
Gültig bis	30.11.2026 (noch 33 Tage)
Ausgehandeltes Protokoll	TLSv1.3
Umleitung http -> https	ja

2.5 Sicherheitsheader

HEADER	STATUS	BEFUND
Strict-Transport-Security	FEHLT	Fehlt. Browser dürfen die Website dann auch unverschlüsselt aufrufen.
Content-Security-Policy	FEHLT	Fehlt. Eine CSP begrenzt, welche Skripte und Inhalte der Browser ausführen darf, und dämpft so die Folgen von Cross-Site-Scripting.
X-Content-Type-Options	GESETZT	Gesetzt.
Referrer-Policy	GESETZT	Gesetzt.
X-Frame-Options / frame-ancestors	FEHLT	Fehlt. Fremde Websites könnten diese Seite unsichtbar einbetten (Clickjacking).

2.6 Weitere erkennbare Informationen

HTTP-Status der Startseite	200
Server-Header	Apache/2.4.62 (Debian)
Weiterleitungen	301 https://beispiel.at/ -> https://www.beispiel.at/

2.7 Anwendung und Erweiterungen

Erkanntes System	WordPress
Version	nicht erkennbar
Aktuelle Version	—
Supportende	—
Bekannte Schwachstellen (NVD)	nicht bestimmbar

PLUGIN	INSTALLIERT	AKTUELL	STAND	ZULETZT GEPFLEGT
Beispiel Slider	2.1.0	3.4.2	VERALTET	14.09.2026

Erkannt werden nur Plugins, deren Dateien auf der Startseite eingebunden sind. Die installierte Version stammt aus der readme.txt des Plugins oder — weniger verlässlich — aus dem ver-Parameter der eingebundenen Dateien. Für Plugins außerhalb des WordPress-Verzeichnisses (z. B. Premium-Plugins) liegen keine Vergleichsdaten vor.

2.8 JavaScript-Bibliotheken

BIBLIOTHEK	BEFUND	EINZELHEITEN
jQuery 3.4.1	2 CVE	CVE-2020-11022, CVE-2020-11023 — behoben in 3.5.0

2.9 Inhalte, Formulare und Cookies

Unverschlüsselt geladene Skripte/Styles 0

Unverschlüsselt geladene Bilder/Medien 1

Formulare mit http://-Ziel 0

Sichtbare Fehlermeldungen nein

COOKIE	SECURE	HTTPONLY	SAMESITE
PHPSESSID (Sitzung)	ja	ja	—

Erfasst wurden nur Name und Attribute der Cookies, die beim Aufruf der Startseite gesetzt werden — keine Werte.

2.10 Server-Software

KOMPONENTE	HERSTELLERSUPPORT	BEKANNTE SCHWACHSTELLEN
Apache HTTP Server 2.4.62 (Debian)	—	—

2.11 Verschlüsselung im Detail

Schlüssel EC, 256 Bit

Signaturverfahren ecdsa-with-SHA256

TLS 1.0 abgelehnt

TLS 1.1 abgelehnt

2.12 E-Mail-Sicherheit (DNS)

Domain	beispiel.at
Mailserver (MX)	mail.beispiel.at
SPF	v=spf1 mx include:_spf.mailanbieter.example ~all
DMARC	v=DMARC1; p=none; rua=mailto:dmarc@beispiel.at
CAA	nicht vorhanden

DKIM lässt sich von außen ohne Kenntnis des Selektors nicht prüfen und ist nicht bewertet.

2.13 Offengelegte Dateien und Fundstellen

ADRESSE	ERGEBNIS	BELEG
/.git/HEAD	NICHT OFFEN	—
/.env	NICHT OFFEN	—
/.svn/wc.db	NICHT OFFEN	—
/.DS_Store	NICHT OFFEN	—
/.htaccess	NICHT OFFEN	—
/phpinfo.php	NICHT OFFEN	—
/info.php	NICHT OFFEN	—
/server-status	NICHT OFFEN	—
/backup.zip	NICHT OFFEN	—
/backup.sql	NICHT OFFEN	—
/dump.sql	NICHT OFFEN	—
/error_log	NICHT OFFEN	—
/.well-known/security.txt	FEHLT	Kontakt für Sicherheitsmeldungen (RFC 9116)
/wp-config.php.bak	NICHT OFFEN	—
/wp-config.php~	NICHT OFFEN	—
/wp-config.old	NICHT OFFEN	—
/wp-content/debug.log	GEFUNDEN	Datei enthält PHP-Fehlermeldungen mit Zeitstempel
/wp-content/uploads/	NICHT OFFEN	—
/wp-json/wp/v2/users	NICHT OFFEN	—

ADRESSE	ERGEBNIS	BELEG
/xmlrpc.php	GEFUNDEN	Antwort „XML-RPC server accepts POST requests only.“

„Nicht offen“ heißt: unter dieser Adresse wurde nichts gefunden, was eindeutig zur jeweiligen Datei passt. Gelesen wurden je Adresse höchstens 8 KB; Inhalte wurden nicht gespeichert. Eine vorgeschaltete Firewall kann einzelne Abrufe blockieren — „nicht offen“ ist daher kein Nachweis, dass eine Datei fehlt.

03

Feststellungen im Einzelnen

HOCH

PSC-EXP-WP-DEBUG · Sofort

WordPress-Debugprotokoll öffentlich

wp-content/debug.log ist lesbar und enthält Fehlermeldungen mit Pfaden und Details. Fundstelle: /wp-content/debug.log — Datei enthält PHP-Fehlermeldungen mit Zeitstempel. Der Inhalt wurde nicht gespeichert.

Empfehlung: WP_DEBUG_LOG im Live-Betrieb abschalten oder auf einen Pfad außerhalb des Webroots legen; Datei löschen.

MITTEL

PSC-PHP-SECURITY-ONLY · Kurzfristig

PHP 8.2 erhält nur noch Sicherheitsupdates

Für PHP 8.2 gibt es keine Fehlerkorrekturen mehr, nur noch Sicherheitsupdates — bis 31.12.2026 (noch 64 Tage).

Empfehlung: Den Umstieg auf PHP 8.5 einplanen, rechtzeitig vor Ende des Sicherheitssupports.

MITTEL

PSC-HDR-HSTS · Kurzfristig

Sicherheitsheader fehlt: Strict-Transport-Security (HSTS)

Fehlt. Browser dürfen die Website dann auch unverschlüsselt aufrufen.

Empfehlung: Den Header „Strict-Transport-Security: max-age=31536000; includeSubDomains“ setzen — erst, wenn alle Subdomains per HTTPS erreichbar sind.

MITTEL

PSC-WP-PLUGIN-OUTDATED · Kurzfristig

1 Plugin ist nicht aktuell

Installierte Version laut readme.txt, aktuelle laut wordpress.org: Beispiel Slider 2.1.0 -> 3.4.2. Veraltete Plugins sind die häufigste Ursache erfolgreicher Angriffe auf WordPress.

Empfehlung: Plugins aktualisieren und automatische Updates für Plugins einschalten.

MITTEL

PSC-JS-VULN · Kurzfristig

jQuery 3.4.1 mit bekannten Schwachstellen

CVE-2020-11022 (CVSS 6,1): Cross-Site-Scripting beim Einfügen von HTML aus nicht vertrauenswürdiger Quelle; CVE-2020-11023 (CVSS 6,1): Cross-Site-Scripting beim Einfügen von HTML mit <option>-Elementen.

Empfehlung: jQuery auf mindestens 3.5.0 aktualisieren (bzw. das CMS-Theme oder Plugin, das die Bibliothek mitbringt).

NIEDRIG PSC-PHP-DISCLOSURE · Mittelfristig

PHP-Version wird öffentlich angezeigt

Der Server nennt jedem Besucher die genaue PHP-Version. Das erleichtert gezielte Angriffe auf bekannte Schwachstellen dieser Version.

Empfehlung: In der `php.ini` „`expose_php = Off`“ setzen. Bei vielen Hostern geht das im Kundenmenü unter den PHP-Einstellungen.

NIEDRIG PSC-HDR-CSP · Mittelfristig

Sicherheitsheader fehlt: Content-Security-Policy

Fehlt. Eine CSP begrenzt, welche Skripte und Inhalte der Browser ausführen darf, und dämpft so die Folgen von Cross-Site-Scripting.

Empfehlung: Eine Content-Security-Policy schrittweise einführen: zunächst im Report-Only-Modus beobachten, dann scharf schalten.

NIEDRIG PSC-HDR-FRAMING · Mittelfristig

Sicherheitsheader fehlt: Schutz vor Einbettung (Clickjacking)

Fehlt. Fremde Websites könnten diese Seite unsichtbar einbetten (Clickjacking).

Empfehlung: Per CSP „`frame-ancestors 'self'`“ oder „`X-Frame-Options: SAMEORIGIN`“ festlegen, wer die Seite einbetten darf.

NIEDRIG PSC-HDR-SERVER · Mittelfristig

Server-Software und Version werden angezeigt

Der Server-Header lautet „`Apache/2.4.62 (Debian)`“. Versionsangaben helfen Angreifern bei der Auswahl passender Schwachstellen.

Empfehlung: Versionsangaben im Server-Header abschalten (Apache: `ServerTokens Prod`, nginx: `server_tokens off`).

NIEDRIG PSC-CONTENT-MIXED-PASSIVE · Mittelfristig

1 Bild oder Medium wird unverschlüsselt geladen

Browser zeigen dann kein vollständiges Schloss-Symbol; die Inhalte können unterwegs ausgetauscht werden.

Empfehlung: Bild- und Medienadressen auf `https://` umstellen.

NIEDRIG PSC-COOKIE-SAMESITE · Mittelfristig

Sitzungscookie ohne SameSite

Ohne SameSite-Angabe verlassen sich diese Cookies auf die Voreinstellung des Browsers: `PHPSESSID`.

Empfehlung: „`SameSite=Lax`“ (oder `Strict`) setzen (PHP: `session.cookie_samesite = Lax`).

NIEDRIG PSC-MAIL-DMARC-NONE · Mittelfristig**DMARC nur im Beobachtungsmodus (p=none)**

Gefälschte Mails werden gemeldet, aber nicht abgewiesen.

Empfehlung: Nach Auswertung der Berichte auf „p=quarantine“ und dann „p=reject“ umstellen.

NIEDRIG PSC-EXP-WP-XMLRPC · Mittelfristig**XML-RPC-Schnittstelle aktiv**

xmlrpc.php wird häufig für massenhafte Passwort-Rateversuche genutzt. Fundstelle: /xmlrpc.php — Antwort „XML-RPC server accepts POST requests only.“. Der Inhalt wurde nicht gespeichert.

Empfehlung: XML-RPC abschalten, wenn keine App oder Anbindung es braucht.

HINWEIS PSC-DNS-CAA · Zur Kenntnis**Kein CAA-Eintrag**

Ohne CAA darf jede Zertifizierungsstelle Zertifikate für die Domain ausstellen.

Empfehlung: Optional einen CAA-Eintrag für die tatsächlich genutzte Zertifizierungsstelle setzen (z. B. 0 issue "letsencrypt.org").

HINWEIS PSC-EXP-SECURITYTXT · Zur Kenntnis**Keine security.txt**

Unter /.well-known/security.txt (RFC 9116) fehlt eine Kontaktangabe für Sicherheitsmeldungen.

Empfehlung: Eine security.txt mit Contact- und Expires-Angabe veröffentlichen.

04

Maßnahmenplan

Sofortmaßnahmen

Innerhalb weniger Tage umsetzen.

- WP_DEBUG_LOG im Live-Betrieb abschalten oder auf einen Pfad außerhalb des Webroots legen; Datei löschen. (PSC-EXP-WP-DEBUG)

Kurzfristige Verbesserungen

In den nächsten Wochen umsetzen.

- Den Umstieg auf PHP 8.5 einplanen, rechtzeitig vor Ende des Sicherheitssupports. (PSC-PHP-SECURITY-ONLY)
- Den Header „Strict-Transport-Security: max-age=31536000; includeSubDomains“ setzen — erst, wenn alle Subdomains per HTTPS erreichbar sind. (PSC-HDR-HSTS)
- Plugins aktualisieren und automatische Updates für Plugins einschalten. (PSC-WP-PLUGIN-OUTDATED)
- jQuery auf mindestens 3.5.0 aktualisieren (bzw. das CMS-Theme oder Plugin, das die Bibliothek mitbringt). (PSC-JS-VULN)

Mittelfristige Empfehlungen

Im Zuge der nächsten Wartung einplanen.

- In der php.ini „expose_php = Off“ setzen. Bei vielen Hostern geht das im Kundenmenü unter den PHP-Einstellungen. (PSC-PHP-DISCLOSURE)
- Eine Content-Security-Policy schrittweise einführen: zunächst im Report-Only-Modus beobachten, dann scharf schalten. (PSC-HDR-CSP)
- Per CSP „frame-ancestors 'self'“ oder „X-Frame-Options: SAMEORIGIN“ festlegen, wer die Seite einbetten darf. (PSC-HDR-FRAMING)
- Versionsangaben im Server-Header abschalten (Apache: ServerTokens Prod, nginx: server_tokens off). (PSC-HDR-SERVER)
- Bild- und Medienadressen auf https:// umstellen. (PSC-CONTENT-MIXED-PASSIVE)
- „SameSite=Lax“ (oder Strict) setzen (PHP: session.cookie_samesite = Lax). (PSC-COOKIE-SAMESITE)
- Nach Auswertung der Berichte auf „p=quarantine“ und dann „p=reject“ umstellen. (PSC-MAIL-DMARC-NONE)
- XML-RPC abschalten, wenn keine App oder Anbindung es braucht. (PSC-EXP-WP-XMLRPC)

Grundsätzlich empfohlen

- PHP-Version, CMS, Erweiterungen und Themes regelmäßig aktualisieren und dafür einen festen Rhythmus einplanen.
- Das Ende des Sicherheitssupports der eingesetzten PHP-Reihe im Kalender vormerken und den Umstieg rechtzeitig testen.

- Regelmäßige, geprüfte Sicherungen außerhalb des Webserverns vorhalten.
- Für Anwendungen mit personenbezogenen Daten zusätzlich eine authentifizierte Prüfung oder einen Penetrationstest durchführen lassen.

05

Methodik und Grenzen

Durchgeführte Prüfungen

- Abruf der Startseite per HTTPS, ersatzweise per HTTP, mit einzeln geprüften Weiterleitungen.
- Ein einzelner Abruf per http://, um die Umleitung auf HTTPS zu prüfen.
- Ein TLS-Verbindungsaufbau zum Auslesen des Zertifikats und des ausgehandelten Protokolls.
- Auswertung der übermittelten HTTP-Kopfzeilen (u. a. X-Powered-By, Server, Sicherheitsheader) und des Generator-Hinweises im HTML.
- Abgleich der erkannten PHP-Version mit den offiziellen Supportzeiträumen und mit veröffentlichten Schwachstellen.
- Auswertung des Seitenquelltexts: CMS und Version, eingebundene WordPress-Plugins, JavaScript-Bibliotheken mit Versionsangabe, unverschlüsselt geladene Inhalte, Formularziele, sichtbare Fehlermeldungen.
- Auswertung der gesetzten Cookies (nur Name und Schutzattribute) und der Server-Software laut Kopfzeilen; Abgleich mit Herstellersupport und der NVD.
- Je ein Verbindungsversuch mit TLS 1.0 und TLS 1.1 sowie Auswertung von Schlüssel und Signatur des Zertifikats.
- Öffentliche DNS-Abfragen der Domain: MX, SPF, DMARC, CAA.
- Lesender Abruf von 20 bekannten Fundstellen (Tabelle 2.13) und — bei WordPress — der readme.txt eingebundener Plugins; je Abruf höchstens 8 KB, keine Weiterleitungen verfolgt, Inhalte nicht gespeichert. Abfrage der Plugin-Daten bei wordpress.org.

Verwendete Datenquellen

PHP-Supportzeiträume	php.net, Stand 28.10.2026
Schwachstellen	National Vulnerability Database (NIST), API 2.0, abgerufen 28.10.2026, 09:00
JavaScript-Bibliotheken	Kuratierte Liste mit CVE-Nummern (NVD, GitHub Advisories), Stand 29.10.2026
CMS und Plugins	api.wordpress.org; Supportzeiträume laut Hersteller
Zeitpunkt der Datenerhebung	28.10.2026, 09:12
Prüfdauer	2,1 s

Bewertungsregeln

Jede Feststellung beruht auf einer festen Regel, deren Kennung (z. B. PSC-PHP-EOL) im Bericht angegeben ist. Die Gesamteinstufung entspricht der schwerwiegendsten Feststellung. Ist die PHP-Version nicht bewertbar und liegt keine andere Feststellung vor, lautet die Einstufung „Unbekannt“ — nicht „Niedrig“.

STUFE	BEDEUTUNG
KRITISCH	Exakt erkannte Version mit veröffentlichter Schwachstelle der Bewertung CVSS 9,0 oder höher; öffentlich abrufbare Git-Daten, .env-Datei, Sicherungen oder Kopien der Konfiguration.
HOCH	PHP, CMS oder Server-Software ohne Sicherheitssupport; Schwachstelle CVSS 7,0–8,9; kein oder ungültiges HTTPS; unverschlüsselte Formulare; wegen Sicherheitsproblemen entfernte Plugins; öffentliche phpinfo- oder Fehlerprotokolle.
MITTEL	Fehlender Patchstand, veraltetes CMS oder Plugins, JavaScript-Bibliotheken mit bekannten Lücken, fehlendes HSTS, SPF oder DMARC, ungeschützte Sitzungscookies, TLS 1.0/1.1, bald ablaufendes Zertifikat.
NIEDRIG	Fehlende ergänzende Sicherheitsheader, öffentliche Versionsangaben, DMARC im Beobachtungsmodus, sichtbare Benutzernamen.
UNBEKANNT	Datenlage reicht für eine Einstufung nicht aus.

Nicht überprüfbar

- Der tatsächliche Patchstand des Servers, wenn die Version nicht oder nur teilweise übermittelt wird.
- Schwachstellen in Plugins und Themes, soweit sie nicht über Aktualität und Verzeichnisstatus erkennbar sind; Plugins, deren Dateien auf der Startseite nicht eingebunden sind; eigener Programmcode.
- Fundstellen außerhalb des geprüften Katalogs; Bibliotheken ohne Versionsangabe im Dateipfad; DKIM.
- Serverkonfiguration hinter dem Webserver: Datenbank, Dateirechte, Zugänge, Firewall, Protokollierung.
- Ob eine aufgeführte Schwachstelle in dieser Installation ausnutzbar ist.
- Bereiche hinter einer Anmeldung und Unterseiten außer der geprüften Adresse.

Keine aktive Schwachstellenausnutzung

Ausgewertet wurden die Informationen, die der Server jedem Besucher übermittelt, öffentliche DNS-Einträge und ein fester Katalog bekannter Fundstellen, die nur gelesen wurden. Es wurden keine Angriffe ausgeführt, keine Schwachstellen ausgenutzt, keine Zugangsdaten probiert, keine Formulare abgeschickt und keine Pfade über den Katalog hinaus geraten. Die Prüfung erfolgte nach Bestätigung der Berechtigung durch den Besteller. Diese Analyse ersetzt keinen Penetrationstest. Eine unauffällige externe Prüfung ist keine Bestätigung, dass die Website sicher ist.

Erstellt mit PHP Security Check · Mag. Christian Inzko · www.inzko.at