SICHERHEITSBERICHT

Schwachstellenanalyse Webshop

Nordlicht Wellness GmbH (fiktiv)

Dokument	Sicherheitsbericht – Webshop Schwachstellenanalyse
Auftraggeber	Nordlicht Wellness GmbH (fiktiv)
Webseite	https://www.nordlicht-wellness-shop.de (fiktiv)
Erstellt von	Vincent de Vries, Vincent de Vries IT-Sicherheitsdienste
Datum	15. April 2026
Klassifizierung	**VERTRAULICH**
Methodik	OWASP Web Security Testing Guide (WSTG v4.2)

Dieses Dokument enthält vertrauliche Informationen über Sicherheitslücken.
Weitergabe nur an autorisierte Personen.

1. Zusammenfassung

Im Rahmen eines autorisierten Sicherheitstests des Nordlicht-Wellness-Webshops wurden sieben Schwachstellen identifiziert, darunter zwei mit kritischem Schweregrad. Drei Schwachstellen wurden bereits während der Testphase durch das Entwicklungsteam behoben.

Die schwerwiegendste Schwachstelle — eine SQL-Injection im Suchfeld — hätte einem Angreifer vollständigen Zugriff auf die Kundendatenbank ermöglicht, einschließlich Zahlungsinformationen und persönlicher Daten. Diese wurde nach Meldung innerhalb von 4 Stunden behoben.

Alle identifizierten Schwachstellen erfordern lediglich grundlegende technische Kenntnisse zur Ausnutzung. Es wird dringend empfohlen, die verbleibenden offenen Befunde innerhalb der angegebenen Fristen zu beheben.

Testumfang

Metrik	Wert
Getestete Endpunkte	34 API-Endpunkte
Getestete Formulare	12
Identifizierte Schwachstellen	**7**
Davon kritisch/hoch	**4**
Testdauer	3 Werktage

Risikomatrix

Schweregrad	Anzahl	Behoben	Offen
Kritisch	2	1	**1**
Hoch	2	0	**2**
Mittel	2	1	**1**
Niedrig	1	1	0

Übersicht der Befunde

Nr.	Schwachstelle	Schweregrad	Status
1	SQL-Injection im Suchfeld	**Kritisch**	☑ **Behoben**
2	IDOR: Zugriff auf fremde Bestellungen	**Kritisch**	⚠ **Offen**

3	Stored XSS in Bewertungsformular	**Hoch**	⚠ **Offen**
4	Fehlende Preisvalidierung bei Gutscheinen	**Hoch**	⚠ **Offen**
5	Session-Fixation nach Login	**Mittel**	☑ **Behoben**
6	Fehlende Rate-Limitation auf Login-Endpunkt	**Mittel**	⚠ **Offen**
7	Informationsoffenlegung in Fehlerseiten	**Niedrig**	☑ **Behoben**

2. Befunde

2.1 SQL-Injection im Suchfeld

Eigenschaft	Details
Schwachstelle	SQL-Injection – Kundendatenbank
OWASP-Kategorie	A03:2021 – Injection
Schweregrad	**Kritisch**
Status	☑ **Behoben**

Beschreibung

Das Suchfeld auf der Startseite übergibt Benutzereingaben ohne Bereinigung direkt an die SQL-Datenbank. Durch gezielte Eingabe von SQL-Befehlen konnte die Datenbankstruktur ausgelesen und auf sämtliche Tabellen zugegriffen werden, einschließlich Kundendaten, Bestellungen und Zahlungsinformationen.

Reproduktionsschritte

1. Das Suchfeld auf der Startseite aufrufen.
2. Folgenden Text eingeben:

```
' UNION SELECT table_name FROM information_schema.tables --
```

3. Die Suchergebnisse zeigen alle Datenbanktabellen an.
4. Durch Anpassung der Abfrage können Spalten und Datensätze ausgelesen werden.

Auswirkung

Vollständiger Lesezugriff auf die gesamte Datenbank, einschließlich: Kundennamen, E-Mail-Adressen, Telefonnummern; Bestellhistorie und Zahlungsdaten; interne Administrationszugänge. Je nach Datenbankrechten wäre auch Schreibzugriff oder die Übernahme des Servers möglich.

Empfehlung

Prepared Statements: Alle Datenbankabfragen auf parametrisierte Queries umstellen.

Input Validation: Benutzereingaben serverseitig validieren und bereinigen.

Least Privilege: Datenbankbenutzer mit minimalen Rechten ausstatten.

2.2 IDOR: Zugriff auf fremde Bestellungen

Eigenschaft	Details
Schwachstelle	Insecure Direct Object Reference (IDOR)
OWASP-Kategorie	A01:2021 – Broken Access Control
Schweregrad	**Kritisch**
Status	**⚠ Offen**

Beschreibung

Bestellungen werden über fortlaufende numerische IDs referenziert (z. B. /bestellung/10042). Nach dem Login kann ein Benutzer die Bestellnummer in der URL ändern und erhält Zugriff auf Bestellungen anderer Kunden, einschließlich Name, Adresse, Telefonnummer und bestellter Produkte.

Reproduktionsschritte

1. Eine eigene Bestellung im Kundenkonto öffnen (z. B. /bestellung/10042).
2. Die Bestellnummer in der URL ändern (z. B. /bestellung/10041).
3. Die vollständigen Bestelldaten eines anderen Kunden werden angezeigt.

Auswirkung

Zugriff auf persönliche Daten aller Kunden. Verstoß gegen DSGVO Art. 32 (technische Schutzmaßnahmen). Durch automatisiertes Durchlaufen aller Bestellnummern könnten sämtliche Kundendaten extrahiert werden.

Empfehlung

Autorisierungsprüfung: Bei jedem Zugriff auf eine Bestellung prüfen, ob der angemeldete Benutzer der Eigentümer ist.

Nicht-vorhersagbare IDs: Fortlaufende IDs durch UUIDs ersetzen.

2.3 Stored XSS in Bewertungsformular

Eigenschaft	Details
Schwachstelle	Stored Cross-Site Scripting (XSS)
OWASP-Kategorie	A03:2021 – Injection
Schweregrad	**Hoch**
Status	**⚠ Offen**

Beschreibung

Das Feld „Ihre Bewertung“ auf Produktseiten akzeptiert HTML- und JavaScript-Code. Eingegebener Schadcode wird in der Datenbank gespeichert und bei jedem Seitenaufruf für alle Besucher ausgeführt.

Reproduktionsschritte

1. Ein beliebiges Produkt aufrufen und zum Bewertungsformular scrollen.
2. Im Feld „Ihre Bewertung“ folgenden Text eingeben:

```
<img src=x onerror=alert(document.cookie)>
```

3. Bewertung absenden.
4. Beim nächsten Aufruf der Produktseite wird ein Alert mit dem Session-Cookie angezeigt.

Auswirkung

Session-Diebstahl bei allen Besuchern der betroffenen Produktseite. Wenn ein Administrator die Bewertung im Backend aufruft, können seine Sitzungsdaten gestohlen und für eine vollständige Kontoübernahme verwendet werden.

Empfehlung

Output Encoding: Alle Benutzereingaben bei der Ausgabe HTML-encoden.

Content Security Policy: CSP-Header implementieren, um Inline-Skripte zu blockieren.

Input Sanitization: HTML-Tags serverseitig entfernen oder escapen.

2.4 Fehlende Preisvalidierung bei Gutscheinen

Eigenschaft	Details
Schwachstelle	Fehlende serverseitige Eingabevalidierung
OWASP-Kategorie	A04:2021 – Insecure Design
Schweregrad	**Hoch**
Status	**⚠ Offen**

Beschreibung

Der Mindestbetrag für Geschenkgutscheine (10,00 €) wird nur im Browser durchgesetzt. Durch Änderung des HTML-Attributs „min“ kann ein Gutschein für 0,01 € erstellt werden. Der Server akzeptiert den Wert ohne Prüfung.

Reproduktionsschritte

1. Im Webshop einen Geschenkgutschein auswählen.
2. Mit Entwicklerwerkzeugen (F12) das Eingabefeld suchen.
3. Das „min“-Attribut von „10“ auf „0.01“ ändern.
4. Wert 0,01 eingeben und zum Warenkorb hinzufügen.
5. Checkout abschließen — ein Gutschein über 0,01 € wird ausgestellt.

Auswirkung

Unbegrenzte Erstellung von Gutscheinen zum Minimalpreis. Gutscheine können als Rabatt eingesetzt werden, was direkten finanziellen Schaden verursacht.

Empfehlung

Mindestbeträge serverseitig durchsetzen. Clientseitige Validierung dient nur der Benutzerfreundlichkeit, niemals der Sicherheit.

2.5 Session-Fixation nach Login

Eigenschaft	Details
Schwachstelle	Session-Fixation
OWASP-Kategorie	A07:2021 – Identification and Authentication Failures
Schweregrad	**Mittel**
Status	☑ **Behoben**

Beschreibung

Nach einem erfolgreichen Login wurde die bestehende Session-ID beibehalten, anstatt eine neue zu generieren. Ein Angreifer könnte einem Opfer eine vorher bekannte Session-ID unterschieben und nach dem Login des Opfers dessen Sitzung übernehmen.

Empfehlung

Nach jedem erfolgreichen Login eine neue Session-ID generieren (session_regenerate_id() in PHP). Diese Maßnahme wurde umgesetzt.

2.6 Fehlende Rate-Limitation auf Login-Endpunkt

Eigenschaft	Details
Schwachstelle	Fehlende Rate-Limitation
OWASP-Kategorie	A07:2021 – Identification and Authentication Failures
Schweregrad	**Mittel**
Status	⚠ **Offen**

Beschreibung

Der Login-Endpunkt (/api/auth/login) erlaubt unbegrenzte Anmeldeversuche ohne Verzögerung oder Sperrung. In einem Test konnten 500 Passwörter pro Minute getestet werden.

Auswirkung

Brute-Force-Angriffe auf Benutzerkonten sind ohne Einschränkung möglich. Insbesondere Konten mit schwachen Passwörtern sind gefährdet.

Empfehlung

Rate Limiting: Maximal 5 Anmeldeversuche pro IP pro Minute.

Account Lockout: Nach 10 Fehlversuchen das Konto temporär sperren.

CAPTCHA: Nach 3 Fehlversuchen ein CAPTCHA einblenden.

2.7 Informationsoffenlegung in Fehlerseiten

Eigenschaft	Details

Schwachstelle	Informationsoffenlegung
OWASP-Kategorie	A05:2021 – Security Misconfiguration
Schweregrad	**Niedrig**
Status	☑ **Behoben**

Beschreibung

Bei serverseitigen Fehlern (HTTP 500) wurde ein detaillierter PHP-Stacktrace angezeigt, einschließlich Dateipfaden, Datenbankverbindungsstrings und Framework-Versionen. Diese Informationen erleichtern gezielte Angriffe.

Empfehlung

Detaillierte Fehlermeldungen nur in Log-Dateien schreiben. Benutzern eine generische Fehlerseite anzeigen. debug=false in der Produktionsumgebung setzen. Diese Maßnahme wurde umgesetzt.

3. Allgemeine Empfehlungen

3.1 Sofortmaßnahmen (innerhalb 48 Stunden)

1. Befund 2 beheben — IDOR auf Bestellungen: Autorisierungsprüfung implementieren.

2. Befund 3 beheben — XSS in Bewertungen: Output Encoding einführen.

3.2 Kurzfristig (innerhalb 2 Wochen)

3. Befund 4 beheben — Gutschein-Preisvalidierung serverseitig durchsetzen.

4. Befund 6 beheben — Rate Limiting auf Login-Endpunkt.

3.3 Mittelfristig (innerhalb 1 Monat)

5. Content Security Policy — CSP-Header für alle Seiten konfigurieren.

6. Nicht-vorhersagbare IDs — Fortlaufende Nummern durch UUIDs ersetzen.

7. Web Application Firewall — WAF als zusätzliche Schutzschicht implementieren.

8. Security-Awareness-Training — Entwicklerteam für OWASP Top 10 schulen.

9. Regelmäßige Sicherheitstests — Penetrationstests in den Entwicklungszyklus integrieren.

4. Getestete Bereiche ohne Befund

Die folgenden Bereiche wurden getestet und als sicher eingestuft:

Bereich	Ergebnis
CSRF-Schutz	Sicher – CSRF-Tokens korrekt implementiert
Passwort-Reset	Sicher – Token kryptografisch stark, läuft nach 1h ab
Datei-Upload	Sicher – Dateitypen und Größe serverseitig validiert
TLS-Konfiguration	Sicher – TLS 1.3, HSTS aktiviert, A+ Rating
Cookie-Sicherheit	Sicher – HttpOnly, Secure, SameSite=Strict
Directory Traversal	Sicher – Pfade korrekt normalisiert

5. Testverfahren & Methodik

Methodik: OWASP Web Security Testing Guide (WSTG v4.2)

Testdauer: 3 Werktage (12.–14. April 2026)

Testmodus: Gray-Box – Tester hatte ein reguläres Kundenkonto

Testumfang:

Zugangskontrolle und Autorisierung • Eingabevalidierung und Injection • Geschäftslogik • Authentifizierung und Sitzungsmanagement • API-Sicherheit • Informationsoffenlegung • Kryptografie und TLS

Es wurden keine Daten verändert, gelöscht oder unbefugt eingesehen. Alle Tests wurden im Rahmen der vereinbarten Testbedingungen durchgeführt.

Bericht erstellt von Vincent de Vries

Vincent de Vries IT-Sicherheitsdienste

Julius-Vosseler-Straße 110d, 22527 Hamburg

contact@vdevries.nl · vdevries.nl