

Technischer Bericht

Security P0 – Angebotsgenerator

WAMAS Lift & Store Angebot

Standard · Deutsch (de-DE)

Login-Limit, HTTPS/Cookie Secure und starkes Passwort-Hashing

Marek Sobona / WLS Generator

LOGIMAT

SCHÄFER

WAMAS®

SSI SCHÄFER

V 1.0 · 28.10.2026

Inhaltsverzeichnis

1 Über dieses Dokument.....	4
1.1 Zweck.....	4
1.2 Lesen dieses Dokuments.....	4
1.3 Dokumentinformationen.....	4
2 Ausgangslage und Scope.....	5
2.1 Abgleich mit PO-00153-EN.....	5
2.2 Was P0 umfasst – und was nicht.....	5
3 Umgesetzte Massnahmen.....	6
3.1 P0-1 Login-Rate-Limit.....	6
3.2 P0-2 HTTPS, Cookie Secure, Netz.....	8
3.3 P0-3 Passwort-Hashes.....	9
4 Deploy und Verifikation.....	10
4.1 Stand 28.10.2026.....	10
4.2 Kurz-Checkliste Betrieb.....	10
5 Stolperfallen.....	11
6 Praxisbeispiele.....	12
6.1 Sperre auslösen (Test).....	12
6.2 Hash-Upgrade beobachten (Admin).....	12
7 Offene Punkte (nicht P0).....	13
8 Quellenverzeichnis.....	14

1 Über dieses Dokument

1.1 Zweck

Dieses Dokument beschreibt die **P0-Sicherheitsmassnahmen**, die am 28.10.2026 am WAMAS Lift & Store Angebotsgenerator (CH, Port 8100) umgesetzt, gemergt und deployed wurden. Es dient als Nachweis gegenüber der SSI SCHÄFER **Secure Development Policy** (PO-00153-EN) und als Betriebsleitfaden für Administratoren.

1.2 Lesen dieses Dokuments

- UI-Bezeichnungen stehen **fett**.
- Konfigurationsschlüssel und API-Pfade stehen in `monospace`.
- Screenshots und API-Nachweise stammen vom Live-System
`https://angebot.mareksobona.synology.me/` bzw. vom Host `127.0.0.1:8100`.

1.3 Dokumentinformationen

Merkmal	Angabe
Titel	Security P0 – Angebotsgenerator
Produkt / Release	WAMAS Lift & Store Angebot
Dokumentversion	1.0
Stand	28.10.2026
Autor	Marek Sobona / WLS Generator
Zielgruppe	Administratoren, Entwickler, ISMS-Ansprechpartner
Grundlage	CWA Secure Development Policy PO-00153-EN v1.00; PR #2; Deploy ui-p0-5db45ac auf Port 8100

2 Ausgangslage und Scope

2.1 Abgleich mit PO-00153-EN

Der Angebotsgenerator ist eine FastAPI-Web-App mit Login, Rollen, Docker-Betrieb und Kundendaten. Die Ausnahme für «minor tool development» (Abschnitt 3 der Policy) greift **nicht**. Es gilt die volle Secure-Development-Policy.

Quelle: CWA Security SW.pdf (PO-00153-EN v1.00), Abgleichbericht WLS_Angebot_Security_Abgleich_PO-00153.md.

2.2 Was P0 umfasst – und was nicht

Umgesetzt wurden nur die drei **P0**-Punkte:

1. Login-Brute-Force-Schutz (Rate-Limit / Sperre)
2. HTTPS-Pfad: Secure-Cookie, HSTS, engeres Port-Bind
3. Starkes Passwort-Hashing (PBKDF2 600k) und Abschalten schwacher Legacy-Varianten

Nicht Bestandteil dieses Releases: CI/SAST/SCA, Dependency-Pins, Security-Header-Set (CSP usw.), /docs abschalten, Pentest (das sind **P1/P2**).

Hinweis

International auf Port 8110 (wamas-ls-angebot-intl) wurde **nicht** geändert.

3 Umgesetzte Massnahmen

3.1 P0-1 Login-Rate-Limit

Nach wiederholten Fehlversuchen antwortet POST /api/auth/login mit **HTTP 429**. Standardwerte (konfigurierbar über WAMAS_LOGIN_*):

Schwelle	Wert	Wirkung
Fehlversuche pro Benutzer	5 / 15 Min.	Sperre 15 Min.
Fehlversuche pro IP	30 / 15 Min.	Sperre 15 Min.
Audit	audit.jsonl	Zeit, Benutzername, IP – kein Passwort/Token

Tab. 1: Login-Limiter

Geprüfte API-Antwort bei Sperre:

```
{"detail": "Zu viele Anmeldeversuche. Bitte später erneut versuchen."}
```

Abb. 1: JSON bei HTTP 429

Login Rate-Limit (HTTP 429)

Antwortkörper nach wiederholten Fehlversuchen:

```
{"detail": "Zu viele Anmeldeversuche. Bitte später erneut versuchen."}
```

Erwartung: HTTP 429 nach mehreren Fehlversuchen pro Benutzer.

Abb. 2: API-Nachweis Rate-Limit

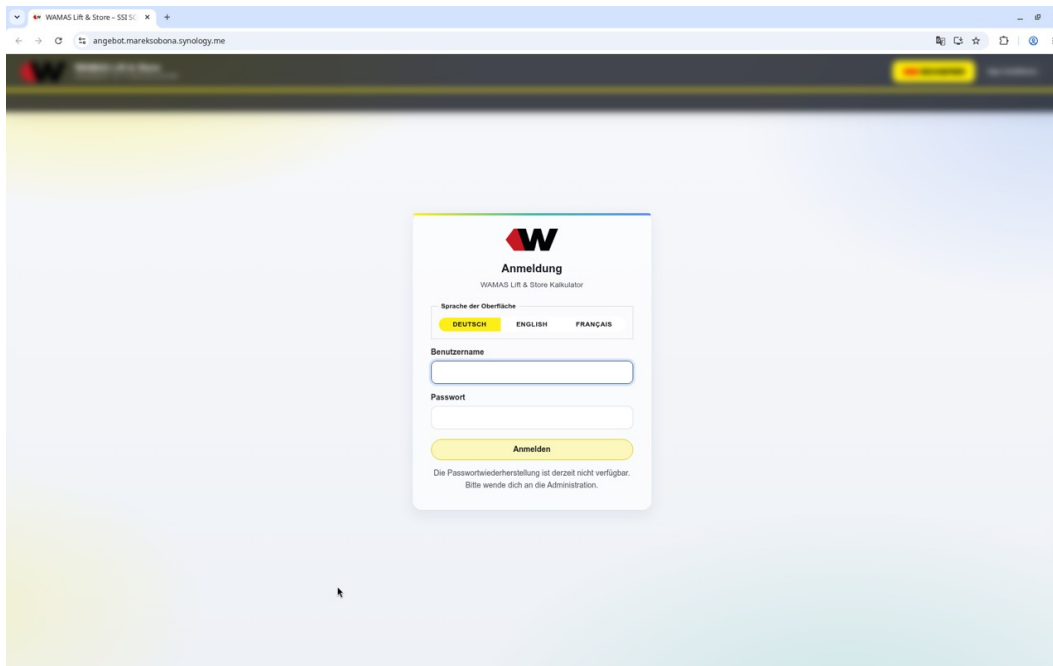


Abb. 3: Anmeldemaske

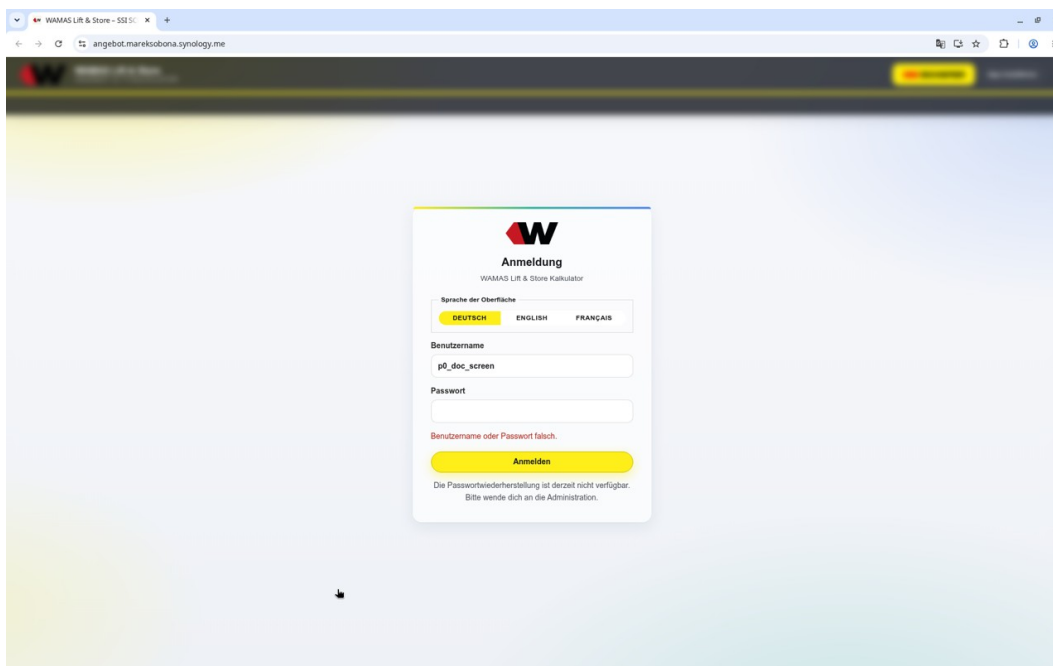


Abb. 4: Fehlermeldung nach falschem Passwort

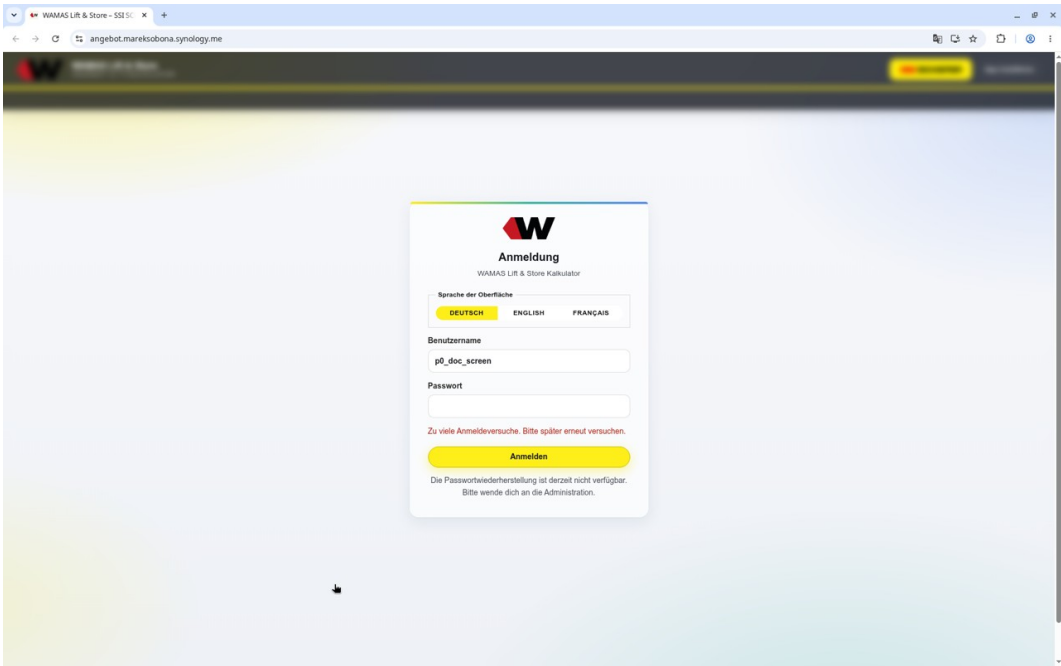


Abb. 5: Sperre in der Oberfläche

Quelle: Live-Test 28.10.2026, Wegwerf-Benutzer p0_doc_* / p0_doc_screen (kein Produktivkonto).

3.2 P0-2 HTTPS, Cookie Secure, Netz

Einstellung	Wert	Wirkung
WAMAS_PUBLIC_URL	https://angebot.mareksobona.synology.me/	Secure-Cookie + App-HSTS
WAMAS_TRUST_PROXY	1	X-Forwarded-For für Limiter vertrauenswürdig
WAMAS_CORS_ORIGINS	öffentliche Origin + localhost	enge Allowlist
Compose-Ports	127.0.0.1:8100 und 192.168.0.70:8100	kein offenes 0.0.0.0; LAN für Synology-Proxy

Tab. 2: HTTPS- und Netz-Konfiguration

Nachweis Health + HSTS-Header (öffentlich über nginx):

API Health + HSTS (öffentlich)

```
HTTP/2 200
server: nginx
date: Wed, 28 Oct 2026 11:43:34 GMT
content-type: application/json
content-length: 201
strict-transport-security: max-age=15552000

Body:
{"ok":true,"status":"ok","service":"WAMAS Lift & Store Calculator","modules":["license","it","offer"],"appVersion":"3.0.0","wamasProductVersion":"2.8","pdf":{"available":true,"provider":"libreoffice"}}
```

Abb. 6: Health 200 und Strict-Transport-Security

Achtung

Nur 127.0.0.1:8100 reicht nicht, wenn der Synology-Reverse-Proxy die LAN-IP 192.168.0.70 anspricht. Deshalb zusätzlich LAN-Bind in `docker-compose.override.yml` auf dem Host.

3.3 P0-3 Passwort-Hashes

Aspekt	Vorher	Nachher
Primärformat	PBKDF2 ca. 120k, viele Legacy-Kandidaten	pbkdf2_sha256\$600000\$...
Schwache Varianten	u. a. reines SHA-256	nur noch einmalig zum Upgrade
Legacy-Feld <code>password</code>	akzeptiert	ignoriert, beim Login entfernt
Bestehende Benutzer	–	beim nächsten Login automatisch migriert

Tab. 3: Hash-Migration

Hinweis

Ein Passwort-Reset ist für die Migration **nicht** nötig. Beim nächsten erfolgreichen Login wird der Hash angehoben.

4 Deploy und Verifikation

4.1 Stand 28.10.2026

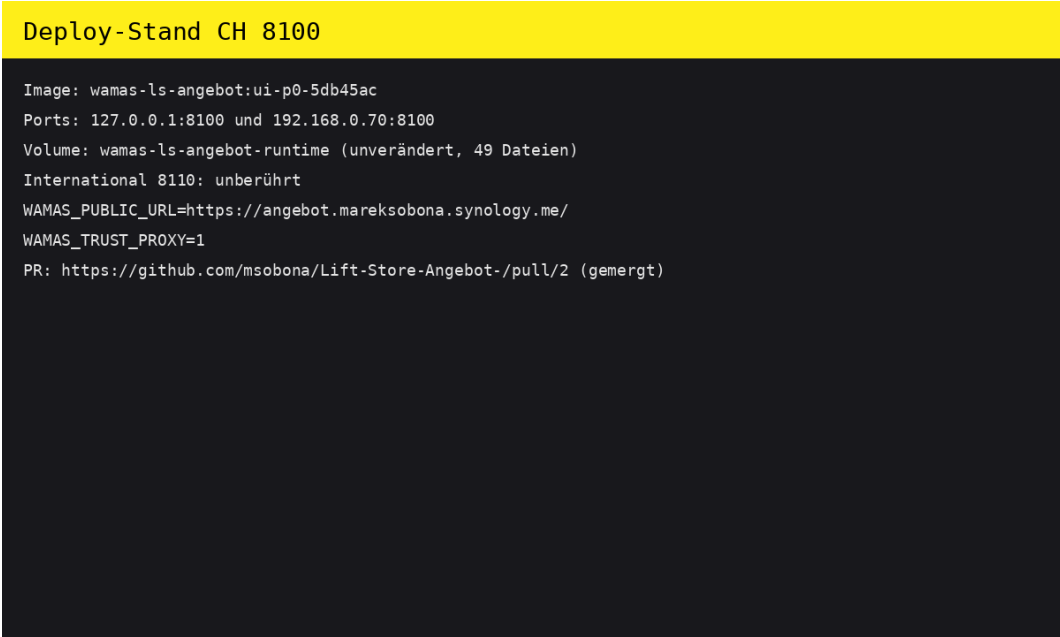


Abb. 7: Deploy-Stand

Element	Wert
PR	https://github.com/msobona/Lift-Store-Angebot-/pull/2 (gemergt in cursor/design-2027-f0f0)
Image	wamas-ls-angebot:ui-p0-5db45ac
Container	wamas-ls-angebot
Volume	wamas-ls-angebot-runtime (49 Dateien, unverändert)
Health lokal/öffentlich	HTTP 200

Tab. 4: Deploy-Nachweis

4.2 Kurz-Checkliste Betrieb

1. https://angebot.mareksobona.synology.me/api/health → 200, Header strict-transport-security vorhanden.
2. Login mit gültigem Konto → Session-Cookie mit Secure hinter HTTPS.
3. Fünf falsche Passwörter mit Testbenutzer → Meldung «Zu viele Anmeldeversuche...» / HTTP 429.
4. International 8110 weiterhin erreichbar und unverändert.

5 Stolperfallen

- Rate-Limit gilt **pro Benutzername und IP**. Tests mit dem eigenen Admin-Konto können dich 15 Minuten aussperren.
- `WAMAS_TRUST_PROXY=1` nur setzen, wenn wirklich ein vertrauenswürdiger Reverse Proxy davor sitzt.
- Compose-Warnung «volume already exists» ist unkritisch, solange der Volume-Name `wamas-ls-angebot-runtime` bleibt.
- Altes Image `ui-95f3f90` liegt als gestoppter Vorgänger-Container vor und kann bei Bedarf zurückgerollt werden.

6 Praxisbeispiele

6.1 Sperre auslösen (Test)

1. Anmeldemaske öffnen.
2. Benutzer `p0_doc_test` und beliebiges falsches Passwort fünfmal absenden.
3. Erwartung: Hinweis **Zu viele Anmeldeversuche. Bitte später erneut versuchen.**

6.2 Hash-Upgrade beobachten (Admin)

1. Mit bestehendem Konto einmal erfolgreich anmelden.
2. In der Runtime-Benutzerdatei prüfen, dass der Hash mit `pbkdf2_sha256$600000$` beginnt und kein Klartext-/SHA-256-Legacy-Feld `password` mehr existiert.

7 Offene Punkte (nicht P0)

In den Unterlagen nicht beschrieben

P1: CI mit pytest, Bandit/pip-audit/Trivy; Dependencies pinnen; Security-Header; /docs in Prod aus; Bootstrap-Passwort nicht ins Docker-Log.

P2: Threat Model, ASVS-Mapping, Retention/Löschkonzept, dokumentierte Reviews, Staging, einmaliger Pentest/DAST.

8 Quellenverzeichnis

Kürzel	Dokument / Artefakt
PO-00153	CWA Security SW.pdf – Secure Development Policy v1.00
ABGL	WLS_Angebot_Security_Abgleich_PO-00153.md
PR2	GitHub Pull Request #2 – P0 Security Fixes
IMG	Docker-Image wamas-ls-angebot:ui-p0-5db45ac