WOMsys

OWASP MASVS L1 — Zelfevaluatie

versie 2026 Q2 · publieke versie (zonder productie-screenshots)

Onderdeel	Waarde
Standaard	OWASP Mobile Application Security Verification Standard (MASVS) v2.1.0
Niveau	MASVS-L1 (Standard) — passend voor zakelijke werkapps zonder financiële transacties of medische gegevens
Scope	WOMsys monteurs-app (Android, Capacitor 7.4) en bijbehorende backend; tevens de WOMsys-webapplicatie waar relevant voor authenticatie
Opgesteld door	DC WebApps (Dennis Ceulemans)
Datum	1 juni 2026 (revisie 2026 Q2)

Status: In v4.0 is Multi-Factor Authentication (MFA) op basis van TOTP volledig geïmplementeerd en in productie geverifieerd — op zowel de webapplicatie als de native Android-app. In deze 2026 Q2-revisie is **media-/signed-URL-beveiliging** als expliciet toetsingspunt opgenomen, zijn de exported-componenten preciezer beschreven en zijn de Firebase- en AVG-formuleringen verfijnd. Daarmee staan **39 van de 40** toetsingspunten op groen; het enige resterende punt (optionele certificate pinning) staat bewust op de roadmap.

1. Inleiding

Dit document beschrijft de uitkomst van een zelfevaluatie van de WOMsys monteurs-app tegen de OWASP Mobile Application Security Verification Standard (MASVS), editie v2.1.0, niveau L1. Niveau L1 (“Standard”) is bedoeld voor apps die persoonsgegevens en zakelijke informatie verwerken, maar geen betalingen of zeer gevoelige gegevens. L1 dekt de fundamentele beveiligingsmaatregelen die in elke productie-app aanwezig moeten zijn. Niveau L2 en R (Resilience) zijn bedoeld voor banking-apps en apps die actief tegen reverse engineering moeten worden beschermd, en zijn niet van toepassing op WOMsys.

1.1 Versiehistorie

Versie	Wijzigingen
v1.0 · 28 mei 2026	Eerste zelfevaluatie; zeven quick-wins geïdentificeerd.
v2.0 · 29 mei 2026	Alle zeven quick-wins doorgevoerd: allowBackup=false, FLAG_SECURE, wachtwoord-policy, gelaagde brute-force-lockout, WebView-hardening, deep-link-beperking en npm audit fix.
v3.0 · 29 mei 2026	Firebase Crashlytics geïntegreerd en via live verbinding met de Firebase Console geverifieerd.
v4.0 · 30 mei 2026	Multi-Factor Authentication (TOTP) volledig geïmplementeerd op webapp én Android-app: organisatiebrede afdwinging, verplichte QR-enrollment, eenmalige recovery codes en MFA-audit-logging.
v4.1 · 30 mei 2026	Privacyverklaring samengevoegd tot één canonieke URL (womsys.nl/privacy.html).
2026 Q2 · 1 jun 2026	Media-/signed-URL-beveiliging als toetsingspunt toegevoegd en op beide domeinen gehandhaafd; access-token ook in de Android Keystore; exported-componenten en release-signing geverifieerd in de APK; Firebase (Crashlytics/FCM) en bijbehorende gegevensverwerking transparant gemaakt; overgestapt op een kwartaal-versieschema.

● **Groen** = geïmplementeerd en operationeel. ● **Roadmap** = bewust uitgesteld als grotere feature of optionele opt-in.

2. MASVS-STORAGE — Veilige opslag op het toestel

Vereiste	Status	Toelichting
Geen gevoelige bedrijfsdata permanent op het toestel	● Groen	De app bevat zelf geen klant- of werkorderdata; alles wordt bij gebruik opgehaald van de server en blijft daar.
Tokens in versleutelde opslag	● Groen	Toegangs- en refresh-token worden opgeslagen in de Android Keystore via @aparajita/capacitor-secure-storage (hardware-ondersteunde opslag). In de browserversie staat het token in de standaard, sandboxed browseropslag — een hardware-keystore bestaat niet in browsers. Geverifieerd in de APK.
Logout wist lokale gevoelige data	● Groen	Bij uitloggen worden alle tokens uit de Keystore verwijderd.
Foto's worden niet onbeschermd op toestel bewaard	● Groen	Foto's worden direct na het maken naar de server geüpload; er blijven geen losse bestanden buiten de app-omgeving achter.
App-data uitgesloten van Android auto-backup	● Groen	android:allowBackup="false" in AndroidManifest.xml. Geverifieerd in de gecompileerde APK.
Schermbeveiliging — FLAG_SECURE (screenshots + recents)	● Groen	FLAG_SECURE wordt in MainActivity.onCreate() vóór super.onCreate() gezet en defensief herzet in onResume(). Screenshots zwart, recents-thumbnail leeg, screen-mirroring geblokkeerd. Zie bewijsstuk 10.1.

3. MASVS-CRYPTO — Cryptografie

Vereiste	Status	Toelichting
Geen zelfgeïmplementeerde crypto	● Groen	Alle cryptografische functies komen uit standaard, breed gebruikte bibliotheken (Node.js crypto, bcrypt, jsonwebtoken).
Wachtwoorden veilig gehasht	● Groen	Gehasht met bcrypt (sterke, langzame eenrichtingsfunctie). Plain-text wachtwoorden komen nergens voor.
Refresh-tokens veilig opgeslagen	● Groen	Opgeslagen als SHA-256 hash; nooit in leesbare vorm.
JWT digitaal ondertekend	● Groen	Ondertekend met een server-side secret (HS256). Tokens kunnen niet worden vervalst zonder de secret.
Sleutels niet hardcoded in de app	● Groen	De Android-app bevat geen secrets of API-keys; authenticatie verloopt via gebruikersnaam + wachtwoord (en TOTP-code).

4. MASVS-AUTH — Authenticatie en sessiebeheer

Vereiste	Status	Toelichting
Sterke server-side authenticatie	● Groen	Authenticatie vindt server-side plaats; de app vertrouwt nooit op client-side checks.
Sessie verloopt automatisch	● Groen	JWT verloopt na 24 uur; daarna is opnieuw inloggen of een refresh-token nodig.

Vereiste	Status	Toelichting
Sessie onmiddellijk intrekbaar	● Groen	Bij verlies/diefstal kan een beheerder de actieve sessie van een gebruiker binnen één seconde ongeldig maken (token_versie++).
Refresh-tokens server-side intrekbaar	● Groen	Refresh-tokens zijn server-side gehashed opgeslagen en kunnen per gebruiker worden ingetrokken.
Rol-gebaseerde toegangscontrole	● Groen	Alle endpoints en menu-items zijn beschermd door expliciete rechten per rol (rechten-tabel + tenant-isolatie per bedrijf).
Afscherming van mediabestanden (foto's/pasjes)	● Groen	Geüploade bestanden zijn niet anoniem opvraagbaar. Elke foto/pasje wordt geserveerd via een per-bestand ondertekende, kortlevende URL (HMAC-SHA256, circa 1 uur geldig); zonder geldige handtekening volgt HTTP 401. Gehandhaafd op zowel app.womsys.nl als monteurs.womsys.nl en gescoped per bedrijf.
Audit-logboek voor gevoelige acties	● Groen	Logins (geslaagd/mislukt/lockout), MFA-events, gebruikersbeheer, sessie-intrekking en werkorder-acties worden centraal gelogd. Filterbaar overzicht; automatische bewaartermijn 1 jaar.
Brute-force bescherming (defense-in-depth)	● Groen	Express rate-limit op /api/auth/login (30 verzoeken per IP per 15 min) als netwerk-vangnet + persistente username-lockout (10 mislukte pogingen per gebruikersnaam per 15 min) met audit-trail (login.locked_out). Zie bewijsstuk 10.2.
Wachtwoord-policy bij registratie en wijziging	● Groen	Minimaal 10 tekens, met hoofd-/kleine letter, cijfer en speciaal teken; niet in de common-list en mag de gebruikersnaam niet bevatten. Server-side gevalideerd op 4 plekken; frontend toont de eisen vooraf.
Multi-Factor Authentication (MFA / TOTP)	● Groen	Geïmplementeerd (v4.0). TOTP (RFC 6238) via Google/Microsoft Authenticator, Authy en 1Password. Beschikbaar op de webapplicatie én de native Android-app. Organisatiebeheerders kunnen 2FA bedrijfsbreed verplicht stellen; gebruikers zonder 2FA worden bij de eerstvolgende login gedwongen tot QR-enrollment vóórdat toegang wordt verleend. Bij activering worden eenmalige recovery codes gegenereerd. Alle MFA-events worden gelogd. Zie bewijsstukken 10.4 t/m 10.7.

5. MASVS-NETWORK — Netwerk

Vereiste	Status	Toelichting
Alle verkeer versleuteld via TLS	● Groen	Uitsluitend HTTPS; geen onversleutelde fallback. Geldige SSL-certificaten op app.womsys.nl en monteurs.womsys.nl.
Vaste, geverifieerde server-URL	● Groen	De app praat uitsluitend met de eigen WOMsys-server. Capacitor allowNavigation is beperkt tot het eigen domein; geen runtime-configureerbare endpoints; geen open redirects.
Geen gevoelige data in URL-parameters	● Groen	Alle gevoelige gegevens worden via request body of headers verzonden, nooit in URL query strings. De ondertekende media-URL's bevatten enkel een tijdelijke, niet-geheime handtekening — geen inloggegevens of persoonsgegevens.

Vereiste	Status	Toelichting
Certificate pinning	● Roadmap	Optioneel binnen MASVS-L1. Niet standaard geïmplementeerd vanwege MDM-/TLS-inspectie-compatibiliteit (sommige organisaties gebruiken eigen TLS-inspectie). Op aanvraag activeerbaar per organisatie.

6. MASVS-PLATFORM — Platform-interactie

Vereiste	Status	Toelichting
Minimale toestelrechten	● Groen	Alleen camera, locatie, notificaties en (optioneel) biometrie — elk met duidelijke werkreden. Geen contacten, sms, oproepgeschiedenis of bestanden.
App-componenten niet onnodig geëxporteerd	● Groen	Alleen MainActivity is exported (vereist voor LAUNCHER). De FileProvider en alle eigen app-componenten staan op exported=false. Enkele standaard framework-receivers (Firebase/FCM, profile-installer) zijn exported maar afgeschermd met systeem-/signature-permissies (o.a. c2dm SEND, DUMP) — geen eigen aanvalsvector. Geverifieerd in de APK.
Veilige WebView-instellingen	● Groen	webContentsDebuggingEnabled=false (productie), allowMixedContent=false, androidScheme=https, allowNavigation strikt beperkt tot het eigen domein, geen cleartextTraffic in manifest.
Deep-link validatie	● Groen	AndroidManifest bevat alleen MAIN + LAUNCHER. Geen custom schemes of host-filters = geen deep-link aanvalsvector.
Geen onveilige Android-componenten	● Groen	Geen IPC, geen content providers voor extern gebruik, geen custom intent filters voor externe apps.

7. MASVS-CODE — Code- en buildkwaliteit

Vereiste	Status	Toelichting
Modern, actief onderhouden framework	● Groen	Capacitor 7.4, Node.js 20.x (LTS), React 18 en PostgreSQL 16 — alle actief onderhouden door grote communities. Minimum ondersteunde Android-versie: API 23 (Android 6.0).
Server-side input-validatie	● Groen	Alle inputs worden server-side gevalideerd (geen vertrouwen op client-side checks).
Productie-build zonder debug-artefacten	● Groen	Release-APK's worden gebouwd zonder console-debug en ontwikkelaar-flags; webContentsDebuggingEnabled=false en de app is niet debuggable. Digitaal ondertekend met een vaste release-keystore (CN=WOMsys Monteurs) — geverifieerd in de APK (v1+v2 signing) — zodat updates verifieerbaar van dezelfde uitgever komen.
Dependencies regelmatig geüpdatet (npm audit)	● Groen	npm audit fix toegepast op backend, web-frontend en monteurs-frontend. Resterende bevindingen zitten in dev-dependencies (build-tooling) zonder runtime-impact. Plan: maandelijkse herhaling + bij elke release.

Vereiste	Status	Toelichting
Crash- en foutmonitoring	● Groen	Firebase Crashlytics SDK geïntegreerd in de Android-app via Firebase BoM; live verbinding met de Firebase Console bevestigd (v3.0). Crashlytics is een dienst van Google (Firebase); zie sectie 9 voor de bijbehorende gegevensverwerking. Zie bewijsstuk 10.3.

8. MASVS-RESILIENCE — Anti-tampering en anti-reverse engineering

Niet van toepassing op niveau L1. Resilience-controles zijn uitsluitend vereist voor MASVS-R (apps die actief beschermen tegen reverse engineering, zoals bank-, betalings- of DRM-apps). WOMsys verwerkt geen betalingen of high-value data; alle gevoelige logica draait server-side. Bij een geslaagde reverse-engineering-aanval op de app blijft de server-side autorisatie volledig intact.

9. Aanvullende privacy- en AVG-maatregelen (buiten MASVS-scope)

In OWASP MASVS v2.1.0 zijn privacy-aspecten verspreid over meerdere categorieën in plaats van als één losse categorie te bestaan. De onderstaande maatregelen vallen daarmee deels buiten de strikte MASVS-scope, maar zijn opgenomen omdat ze relevant zijn voor zakelijke afnemers en voor naleving van de AVG.

Vereiste	Status	Toelichting
Privacyverklaring beschikbaar	● Groen	Live op womsys.nl/privacy.html (AVG-conform). Eén canonieke verklaring voor zowel het webplatform als de monteurs-app.
Gegevensopslag binnen de EU	● Groen	Platform- en bedrijfsgegevens worden uitsluitend binnen de EU opgeslagen (Strato en Hetzner, Duitsland). Voor pushmeldingen en crashdiagnose verwerkt Google (Firebase Cloud Messaging / Crashlytics) beperkte technische gegevens (toestel-/installatie-ID, diagnostische crashdata); deze kunnen buiten de EU worden verwerkt onder de EU-modelcontractbepalingen (SCC's) en Google's aanvullende waarborgen.
Dataminimalisatie	● Groen	Alleen gegevens die nodig zijn voor de werkfunctionaliteit worden verwerkt. Geen advertenties en geen commerciële tracking of verkoop van gegevens. Voor crashdiagnose en pushmeldingen gebruikt de app Firebase (Crashlytics + Cloud Messaging, Google); de Firebase-SDK registreert standaard Google-componenten en een advertentie-ID-permissie, die WOMsys niet voor advertenties of profilering inzet.
Recht op inzage en verwijdering	● Groen	Verzoeken worden via de bedrijfsbeheerder verwerkt; gegevens kunnen worden geëxporteerd of geanonimiseerd.
Audit-log met bewaartermijn	● Groen	Audit-events worden 1 jaar bewaard en daarna automatisch opgeschoond via een nachtelijke achtergrondtaak — conform het AVG-principe van dataminimalisatie.

10. Bewijsstukken

Onderstaande screenshots dienen als visueel bewijs van de geïmplementeerde maatregelen. De FLAG_SECURE-, brute-force- en Crashlytics-bewijzen zijn gemaakt op 29 mei 2026; de MFA-bewijzen (10.4 t/m 10.7) op 30 mei 2026, in de productie-omgeving.

10.1 Schermbeveiliging (FLAG_SECURE)

Wanneer een gebruiker probeert een screenshot te maken van een willekeurig scherm binnen de app, vervangt Android de inhoud automatisch door een zwart vlak. Alleen de systeem-statusbalk is nog zichtbaar — geen WOMsys-data. Hetzelfde effect treedt op in het recents-overzicht en bij screen-mirroring.

(Schermafbeelding op aanvraag — in deze publieke versie weggelaten omdat de afbeelding productiedata toont.)

10.2 Brute-force detectie + persistente audit-trail

Na 10 mislukte aanmeldingen voor een account binnen 15 minuten blokkeert het systeem de volgende poging (login.locked_out) en legt het event vast in het audit-logboek met aantal pogingen en tijdsvenster. Succesvolle logins van een ander account werken ongehinderd door — de lockout is gericht op het aangevallen account.

(Schermafbeelding op aanvraag — in deze publieke versie weggelaten omdat de afbeelding productiedata toont.)

10.3 Crash- en foutmonitoring (Firebase Crashlytics)

Na integratie van de Crashlytics SDK heeft de Firebase Console de app gedetecteerd en de verbinding bevestigd. De boodschap “App detected and we're waiting for a crash!” bevestigt dat de SDK actief is en met de Firebase-backend communiceert.

(Schermafbeelding op aanvraag — in deze publieke versie weggelaten omdat de afbeelding productiedata toont.)

10.4 Tweestapsverificatie bij het inloggen (TOTP)

Na het invoeren van gebruikersnaam en wachtwoord vraagt de applicatie om de 6-cijferige TOTP-code uit de authenticator-app. Zonder geldige code wordt geen toegang verleend — de tweede factor is verplicht.

(Schermafbeelding op aanvraag — in deze publieke versie weggelaten omdat de afbeelding productiedata toont.)

10.5 Verplichte 2FA-enrollment bij login

Een gebruiker zonder 2FA in een organisatie waar 2FA verplicht is, wordt bij login gedwongen tot het instellen ervan: een QR-code (plus handmatige sleutel) voor de authenticator-app, gevolgd door verificatie met een code. Pas na succesvolle activering wordt toegang verleend.

(Schermafbeelding op aanvraag — in deze publieke versie weggelaten omdat de afbeelding productiedata toont.)

10.6 Self-service beheer en organisatiebrede afdwinging

Gebruikers beheren hun eigen 2FA (activeren, nieuwe recovery codes genereren, uitschakelen). Beheerders zien de adoptiegraad en kunnen 2FA voor de hele organisatie verplicht stellen.

(Schermafbeelding op aanvraag — in deze publieke versie weggelaten omdat de afbeelding productiedata toont.)

10.7 Audit-logging van authenticatie- en 2FA-gebeurtenissen

Alle relevante gebeurtenissen worden vastgelegd: mfa.setup_started, mfa.enabled, mfa.login.success/failed, bedrijf.mfa.required.enabled/disabled en login.locked_out. Per event worden tijdstip, gebruiker, IP-adres en details bewaard.

(Schermafbeelding op aanvraag — in deze publieke versie weggelaten omdat de afbeelding productiedata toont.)

11. Samenvatting

Van de toetsingspunten in deze evaluatie:

- **39 punten** staan op groen — geïmplementeerd en operationeel.
- **0 punten** staan open — alle quick-wins zijn doorgevoerd, MFA is volledig geïmplementeerd en media-/signed-URL-beveiliging is op beide domeinen gehandhaafd.
- **1 punt** staat op de roadmap — optionele certificate pinning.

De belangrijkste sterke punten van WOMsys ten aanzien van mobiele beveiliging:

- Geen bedrijfsgegevens permanent op het toestel — tokens in de Android Keystore (app) en in sandboxed browseropslag (web).
- Geüploade foto's en pasjes zijn niet anoniem opvraagbaar: uitsluitend via per-bestand ondertekende, kortlevende URL's, gehandhaafd op beide domeinen.
- Schermbeveiliging via FLAG_SECURE blokkeert screenshots, recents-thumbnail en screen-mirroring app-breed.
- Multi-Factor Authentication (TOTP) op webapp én Android-app, met organisatiebrede afdwinging en eenmalige recovery codes.
- Sessies zijn binnen één seconde server-side intrekbaar bij verlies of diefstal van een toestel.
- Gelaagde brute-force bescherming: netwerk-rate-limit per IP + persistente username-lockout met audit-trail.
- Centraal audit-logboek met filterbare beheerinterface en automatische bewaartermijn van één jaar.
- Wachtwoord-policy met complexity-eisen en common-list-check, gevalideerd op alle aanmaak- en wijzigingspaden.
- Strikte scheiding per bedrijf en rol-gebaseerde toegang voor alle data en functies.
- Real-time crash- en foutmonitoring via Firebase Crashlytics (geverifieerde verbinding).
- EU-hosting (Duitsland) en AVG-compliance, inclusief privacyverklaring; Firebase verwerkt beperkte technische data onder SCC's (zie sectie 9).

12. Roadmap

- Certificate pinning (optioneel, activeerbaar per organisatie i.v.m. MDM-compatibiliteit). Bewust niet standaard geactiveerd om compatibel te blijven met corporate TLS-inspectie / MDM-omgevingen. Geschat: 2-3 uur ontwikkeltijd.

Externe pentest: nog niet uitgevoerd. Een externe penetratietest of audit staat open en wordt op verzoek ingepland met een door uw organisatie aangewezen partij; bevindingen worden meegenomen in een volgende release.

13. Conclusie

WOMsys voldoet aan vrijwel alle eisen van MASVS-L1 (editie v2.1.0). Van de **40 toetsingspunten** staan er **39 op groen**; het enige resterende punt — optionele certificate pinning — staat bewust op de roadmap als opt-in. Alle quick-wins zijn doorgevoerd, crash-monitoring is toegevoegd met een live geverifieerde verbinding, Multi-Factor Authentication (TOTP) is volledig geïmplementeerd en in productie geverifieerd op zowel de webapplicatie als de Android-app, en geüploade media zijn afgeschermd met ondertekende, kortlevende URL's. Er zijn geen kritieke beveiligingsgaten geïdentificeerd.

De combinatie van server-side autorisatie, verplichte tweestapsverificatie, afgeschermde media, centrale audit-logging, EU-hosting, sessie-intrekking binnen één seconde, gelaagde brute-force bescherming, app-brede schermbeveiliging en real-time crash-monitoring maakt WOMsys passend voor inzet binnen organisaties met een strikt beveiligingsbeleid — ook internationaal.

DC WebApps · Dennis Ceulemans
Van IJsendijkstraat 87, 1442 CJ Purmerend · KvK 99326922 · info@dcwebapps.nl · info@womsys.nl