Responsible Disclosure Program

Scope

Assets:

- https://www.cm.be/nl/toepassingen/cm-gezondheidsacademie
- https://www.mc.be/fr/services-en-ligne/souscrire-assurance
- https://www.ckk-mc.be/online-dienste/versicherung-abschliessen
- https://www.cm.be/nl/toepassingen/zoek-een-zorgverlener-je-buurt
- https://www.mc.be/fr/services-en-ligne/rechercher-prestataire
- https://www.ckk-mc.be/online-dienste/leistungserbringer
- https://www.cm.be/nl/toepassingen/online-aangifte-ziekenhuisopname
- https://www.mc.be/fr/services-en-ligne/demande-intervention-hospitalisation
- https://www.ckk-mc.be/online-dienste/antrag-erstattung-krankenhausrechnung
- https://www.cm.be/nl/contact/contactformulier
- https://www.mc.be/fr/contact/formulaire
- https://www.ckk-mc.be/kontakt/formular
- https://www.cm.be/nl/contact/cm-in-je-buurt
- https://www.mc.be/fr/services-en-ligne/points-de-contact
- https://www.ckk-mc.be/online-dienste/kontaktpunkte
- https://www.cm.be/dimona
- https://www.mc.be/fr/services-en-ligne/dimona
- https://www.ckk-mc.be/online-dienste/dimona
- https://www.cm.be/nl/toepassingen/ezvk-aanvragen
- https://www.mc.be/fr/services-en-ligne/commander-ceam
- https://www.ckk-mc.be/online-dienste/ekvk-beantragen
- https://www.cm.be/jongeren
- https://www.cm.be/nl/toepassingen/toestemming-verwerking-medische-gegevens
- https://www.mc.be/fr/services-en-ligne/consentement-gdpr
- https://www.ckk-mc.be/online-dienste/einverstaendiserklaerung-gdpr
- https://www.cm.be/nl/doccle-documenten-raadplegen
- https://www.mc.be/fr/services-en-ligne/doccle
- https://www.ckk-mc.be/online-dienste/doccle
- https://www.cm.be/nl/toepassingen/gele-klevers
- https://www.mc.be/fr/services-en-ligne/commander-vignettes
- https://www.ckk-mc.be/online-dienste/aufkleber-bestellen
- https://www.cm.be/nl/toepassingen/welke-verzekering-past-bij-jou
- https://www.cm.be/nl/aanvraag-verzekeringsvoorstel
- https://www.cm.be/nl/toepassingen/bereken-je-premie
- https://www.cm.be/nl/jobs/vacaturelijst
- https://www.mc.be/fr/jobs/offres-emploi
- https://www.cm.be/nl/jobs/vacaturelijst/vacaturedetail
- https://www.mc.be/fr/jobs/offres-emploi/detail-offre
- https://www.cm.be/nl/jobs/alerts-beheer
- https://www.cm.be/nl/toepassingen/bereken-zelf-je-terugbetaling
- https://www.mc.be/fr/services-en-ligne/tarifs-officiels-remboursements
- https://www.ckk-mc.be/online-dienste/honorare-rueckerstattungen
- https://www.cm.be/nl/toepassingen/vergelijking-ziekenhuistarieven
- https://www.mc.be/fr/services-en-ligne/prix-hopitaux-belgique
- https://www.ckk-mc.be/online-dienste/krankenhaus-kosten-belgien
- https://www.cm.be/nl/toepassingen/aanmelden-op-mijn-cm
- https://www.mc.be/fr/services-en-ligne/connexion-ma-mc
- https://www.ckk-mc.be/online-dienste/sso-onboarding
- https://www.ckk-mc.be/online-dienste/meine-ckk
- https://www.cm.be/nl/lid-worden/je-bent-aangesloten-bij-een-ander-ziekenfonds
- https://www.mc.be/fr/services-en-ligne/affiliation-autre-mutualite
- https://www.ckk-mc.be/online-dienste/einschreibung-andere-krankenkasse
- https://www.cm.be/nl/toepassingen/communicatievoorkeuren-beheren
- https://www.mc.be/fr/services-en-ligne/preferences-de-communication
- https://www.ckk-mc.be/online-dienste/kommunikationspraeferenzen
- https://www.cm.be/nl/toepassingen/wat-kost-orthodontie

- https://www.cm.be/nl/toepassingen/mijn-cm-verzekeringen
- https://www.mc.be/fr/services-en-ligne/apercu-assurances
- https://www.ckk-mc.be/online-dienste/uebersicht-versicherungen
- https://www.cm.be/nl/domiciliering-zorgpremie-aanvragen

Vulnerabilites/tests in scope:

- All vulnerabilities described in the OWASP ASVS.
- Vulnerabilities that lead to data leakage of personal data.
- Bruteforcing as long as requests stay below the 5 requests per second.

Vulnerabilites/tests out of scope:

- Disruptive tests(D/DOS, ...)
- Phishing attacks
- Physical tests/attacks (breaking-in, bypassing physical access controls, ...)
- API key disclosure without business impact
- Self-XSS
- Verbose messages/files/directory listings without business impact
- CORS misconfiguration
- Missing cookie flags with the exception of sessie related cookie flags
- Missing security headers
- Cross-site Request Forgery without business impact
- Autocomplete attributes on web forms
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking
- Email spoofing, SPF, DMARC or DKIM
- Email bombing
- HTTP Request smuggling without business impact
- Banner grabbing/Version disclosure
- Open poorten without business impact
- Weak SSL configurations en SSL/TLS scan reports
- Disclosing API keys without business impact
- Same-site scripting
- Arbitrary file upload without business impact
- Blind SSRF without business impact
- Cookie Information Disclosure without business impact
- HTML injection without business impact

Hall of Fame

Name	Surname	Nickname	Critical	High	Medium
Robbe	Verwilghen	GrumpinouT	0	0	2