

Programma voor Verantwoorde Openbaarmaking

Bug Bounty & Beveiliging — Aureus IA SPRL

1. Toepassingsgebied

Binnen scope: app.aureussocial.be (hoofdapplicatie), REST API v1.

Buiten scope: aureusia.com (bedrijfswebsite), DDoS-aanvallen, social engineering, kwetsbaarheden van derden zonder PoC.

2. Beloningen

Ernst	Type	Beloning
Kritiek	RCE, SQLi, volledige DB-toegang, auth bypass	500-2.000 EUR
Hoog	IDOR op INSZ/loongegevens, opgeslagen XSS, SSRF	200-500 EUR
Gemiddeld	CSRF op kritieke acties, informatielekken	50-200 EUR
Laag	Gereflecteerde XSS, ontbrekende headers, open redirect	Hall of Fame

3. Gedragsregels

1. Geen toegang tot gegevens van andere gebruikers.
2. Geen exfiltratie van persoonsgegevens (INSZ, lonen, IBAN).
3. Geen destructieve aanvallen of denial of service.
4. Niet testen in productie zonder voorafgaande toestemming.
5. Melden via security@aureusia.com met beschrijving, PoC en impact.

4. Proces

1. Ontvangst: Bevestiging binnen 48 uur.
2. Triage: Ernstbeoordeling binnen 5 werkdagen.
3. Correctie: Patch volgens ernst (kritiek: 24u, hoog: 7d, gemiddeld: 30d).
4. Beloning: Betaling na validatie van de fix.
5. Openbaarmaking: Gecoordinateerde publicatie na 90 dagen of na fix.

5. Safe Harbor

Onderzoekers die deze regels respecteren zullen niet juridisch worden vervolgd. Wij verbinden ons ertoe geen gerechtelijke procedures te starten tegen onderzoekers die te goeder trouw handelen.

6. Contact

Email: security@aureusia.com — Talen: FR, NL, EN, DE