Programme de Divulgation Responsable

Bug Bounty & Securite — Aureus IA SPRL

1. Perimetre

Dans le perimetre : app.aureussocial.be (application principale), API REST v1.

Hors perimetre : aureusia.com (site corporate), attaques DDoS, social engineering, vulnerabilites tierces sans PoC.

2. Recompenses

Severite	Type	Recompense
Critique	RCE, SQLi, acces BDD complet, bypass auth	500-2.000 EUR
Haute	IDOR sur donnees NISS/salaire, XSS stocke, SSRF	200-500 EUR
Moyenne	CSRF sur actions critiques, information disclosure	50-200 EUR
Basse	XSS reflete, headers manquants, open redirect	Hall of Fame

3. Regles d'engagement

1. Ne pas acceder, modifier ou supprimer des donnees d'autres utilisateurs.
2. Ne pas exfiltrer de donnees personnelles (NISS, salaires, IBAN).
3. Ne pas effectuer d'attaques destructives ou de deni de service.
4. Ne pas tester en production sans accord prealable.
5. Reporter via security@aureusia.com avec description, PoC et impact.

4. Processus

1. Reception : Accuse de reception sous 48h.
2. Triage : Evaluation severite sous 5 jours ouvrables.
3. Correction : Patch selon severite (critique: 24h, haute: 7j, moyenne: 30j).
4. Recompense : Paiement apres validation du fix.
5. Disclosure : Publication coordonnee apres 90 jours ou apres fix.

5. Safe Harbor

Les chercheurs respectant ces regles ne feront l'objet d'aucune poursuite legale. Nous nous engageons a ne pas initier de procedure judiciaire contre les chercheurs agissant de bonne foi.

6. Contact

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