

Programm zur verantwortungsvollen Offenlegung

Bug Bounty & Sicherheit — Aureus IA SPRL

1. Geltungsbereich

Im Geltungsbereich: app.aureussocial.be (Hauptanwendung), REST API v1.

Ausserhalb: aureusia.com (Firmenwebsite), DDoS-Angriffe, Social Engineering, Schwachstellen Dritter ohne PoC.

2. Belohnungen

Schweregrad	Typ	Belohnung
Kritisch	RCE, SQLi, voller DB-Zugriff, Auth-Bypass	500-2.000 EUR
Hoch	IDOR auf INSZ/Gehaltsdaten, gespeichertes XSS, SSRF	200-500 EUR
Mittel	CSRF bei kritischen Aktionen, Informationsleck	50-200 EUR
Niedrig	Reflektiertes XSS, fehlende Header, Open Redirect	Hall of Fame

3. Verhaltensregeln

1. Keinen Zugriff auf Daten anderer Benutzer.
2. Keine Exfiltration personenbezogener Daten (INSZ, Gehälter, IBAN).
3. Keine destruktiven Angriffe oder Denial of Service.
4. Kein Testen in Produktion ohne vorherige Zustimmung.
5. Meldung über security@aureusia.com mit Beschreibung, PoC und Auswirkung.

4. Prozess

1. Empfang: Bestätigung innerhalb von 48 Stunden.
2. Triage: Schweregradbewertung innerhalb von 5 Werktagen.
3. Behebung: Patch nach Schweregrad (kritisch: 24h, hoch: 7T, mittel: 30T).
4. Belohnung: Zahlung nach Validierung der Korrektur.
5. Offenlegung: Koordinierte Veröffentlichung nach 90 Tagen oder nach Fix.

5. Safe Harbor

Forscher, die diese Regeln einhalten, werden keiner rechtlichen Verfolgung ausgesetzt. Wir verpflichten uns, keine rechtlichen Schritte gegen gutgläubig handelnde Forscher einzuleiten.

6. Kontakt

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