Pheonix5981 Security — Security Research Summary

Contact: willworachat@gmail.com | Report date: 2026-07-02

Target	OSL
Platform	Bugcrowd
Engagement dates	2026-06-15 to 2026-06-21
Reports submitted	0 (drafted, not filed)
Outcome	NOT SUBMITTED (patched)

Scope Tested

trade-glb.osl.com API surface (183 endpoints mapped from JS bundle) — KYC, deposit/withdrawal, spot trading, user management, broker/affiliate, fiat, retail-asset endpoints. Bitget/upex white-label platform.

Methodology Applied

P10 recon checklist (subdomain enumeration, JS mining, API surface mapping), H11 web checklist (IDOR across all major object types — all blocked, correctly scoped to JWT).

Coverage

Full IDOR sweep across mapped API surface; API key detail flow; rate-limit behavior.

Outcome / Findings Summary

One Medium finding (Java stack-trace/class-name disclosure on affiliate endpoints) was confirmed live but the vendor patched globally within hours, before a screenshot/PoC could be captured — not submitted due to reproducibility and reputation-risk concerns. All IDOR vectors tested came back correctly scoped. $0.