# Pheonix5981 Security

Security Research Summary · Contact: willworachat@gmail.com · Report date: 2026-07-02

## Memento RESOLVED

**Platform:** YesWeHack
**Program dates:** Research 2026-05 to 2026-06-05; program complete
**Coverage:** ~45% of total surface — unauthenticated API layer thoroughly tested; authenticated layer blocked by a broken login flow

### SCOPE TESTED

Memento's DeFi asset-management protocol (DFM), specifically its testnet web application and two API namespaces (/dd/ authenticated operations, /dcd/ public chain data) across five EVM-compatible testnets.

### METHODOLOGY APPLIED

- H11 broken-access-control checklist — systematically tested whether authenticated-only endpoints enforced their auth requirement
- H3 JWT signature-verification testing — identified a complete authentication-bypass class
- P10 systematic recon via JS bundle mining to map all 85 API endpoints before testing

### OUTCOME

> A Critical-severity JWT signature-verification bypass (forgeable authentication token) was identified and closed as a duplicate of an existing report. A High-severity broken-access-control finding — multiple endpoints intended to require authentication (fee data, order data, session-counter mutation, and a soulbound-token IDOR) were reachable without any valid credential — was submitted and closed as “requires the fix to succeed” (RTFS), the platform's designation for an already-tracked/expected-fix scenario. A separate pre-authentication code-execution lead was found already patched before submission. The program's login flow itself was broken throughout the engagement, which capped testable coverage of the authenticated surface at roughly 5%.