Security assessments for software that matters.

**Dr.-Ing. Mario Heiderich, Cure53**
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

# Cure53 Security Assessment of ERA Wallet mobile apps, crypto, API & TX flows, Management Summary, 08.2026

Cure53, Dr.-Ing. M. Heiderich, Dr. A. Pirker, C. Lüders, Dr. D. Bleichenbacher, M. V. S. Lima

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a penetration test and source code audit conducted against the ERA wallet mobile applications and Serverpod RPC API.

To give some context regarding the assignment's origination and composition, ERA Wallet (HWLT FZE) contacted Cure53 in June 2026. The test execution was scheduled for August 2026, namely in CW32. To achieve full coverage across the agreed scope, Cure53 dedicated eighteen testing days to the engagement. Project execution was managed end-to-end, spanning initial setup, testing, and report finalization, by a specialized team of five senior security testers.

The work was split into four separate work packages (WPs), defined as:

- **WP1**: White-box pen.-tests & code audits against ERA mobile applications
- **WP2**: White-box pen.-tests & code audits against ERA Transaction Construction
- **WP3**: White-box pen.-tests & code audits against ERA QR & BC-UR flows
- **WP4**: White-box pen.-tests & code audits against ERA Serverpod RPC API

The assessment utilized a white-box evaluation model. Operating with comprehensive access, the Cure53 testing team was supplied with source repositories, build binaries, system documentation, and elevated credentials to enable deep diagnostic analysis across all scope items.

Preparations for the assessment were finalized in late July 2026 (CW31) to guarantee an unhindered operational kickoff. Real-time collaboration was maintained through a dedicated joint Slack channel connecting key project contributors from both ERA and Cure53.

Operational communication proceeded seamlessly, supported by a clear and thoroughly prepared project scope that minimized routine clarification requests. Testing executed without notable technical roadblocks. Throughout the engagement, Cure53 provided regular progress updates and conducted live reporting for all identified findings directly within the joint Slack workspace.

Testing yielded broad coverage across all defined work packages, unearthing twenty-eight security-related items. Cure53 categorized these discoveries into fifteen technical vulnerabilities requiring direct remediation and thirteen lower-severity general weaknesses that represent opportunities for overall system hardening.

**Dr.-Ing. Mario Heiderich, Cure53**
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

**Identified Vulnerabilities**

- HWL-01-002 WP1: DoS of Android app via serialized intents (Medium) **Fixed**
- HWL-01-007 WP4: Unauthenticated endpoints leak user data (Medium) **Fixed**
- HWL-01-009 WP4: Unauthorized device linking to account via fingerprint (High) **Fixed**
- HWL-01-010 WP4: Unauthenticated memory exhaustion DoS of API (High) **Fixed**
- HWL-01-011 WP4: Unauthenticated device attestation API due to asserts (High) **Fixed**
- HWL-01-014 WP4: IP spoofing via X-Forwarded-For header (Info) **Fixed**
- HWL-01-015 WP4: DoS in anonymous rate-limited endpoints (Low) **Fixed**
- HWL-01-016 OOS: Open redirect in /tap/return endpoint (Low) **Fixed**
- HWL-01-017 WP4: Insecure randomness for generating device attestation (Low) **Fixed**
- HWL-01-018 WP4: TRON RPC proxy allows unauthenticated broadcast (Medium) **Fixed**
- HWL-01-019 WP1: Supabase exposes multiple internal files (Low) **Fixed**
- HWL-01-021 WP1: Plaintext storage of contacts and UR wallet code (Medium) **Fixed**
- HWL-01-024 WP3: Decompression bomb DoS via crafted UR codes (Low) **Fixed**
- HWL-01-026 WP1/WP3: Signed QR reply accepted without validation (Low) **Fixed**
- HWL-01-027 WP1: Multiple bypasses in PIN lock mechanism (High) **Fixed**

**Miscellaneous Issues**

- HWL-01-001 WP1: Android application supports outdated SDK versions (Low) **Fixed**
- HWL-01-003 WP4: Non-constant time comparison of secrets (Info) **Fixed**
- HWL-01-004 WP4: Path traversals in RPC proxy & moonpay API endpoints (Low) **Fixed**
- HWL-01-005 WP1: PIN brute-forcing due to weak PBKDF2 parameters (Medium) **Fixed**
- HWL-01-006 WP4: Docker container running with root privileges (Info) **Fixed**
- HWL-01-008 WP4: Insufficient HMAC check in Onramper endpoints (Low) **Fixed**
- HWL-01-012 WP4: Path traversal in Onramper and preview API endpoints (Low) **Fixed**
- HWL-01-013 WP4: Insufficient HMAC check on MoonPay session creation (Low) **Fixed**
- HWL-01-020 WP3: Insecure parsing of UR codes could result in exceptions (Info) **Fixed**
- HWL-01-022 WP1: ECDSA malleability due to missing length check (Low) **Fixed**
- HWL-01-023 WP1: Inclusion of sensitive Keychain data in iOS backups (Low) **Fixed**
- HWL-01-025 WP1: Use of weak cryptographic libraries (Info) **Fixed**
- HWL-01-028 WP1: Biometric verification bypass in iOS (Medium) **Fixed**

Physical hardware wallets required for live transaction signing were not provisioned prior to project execution, as this operational dependency was identified at kickoff, preventing physical device shipment. To maintain assessment momentum, Cure53 utilized a provided simulation framework. Consequently, certain hardware-dependent features could not be validated in a production-equivalent physical environment.

While preliminary testing showed a reasonable baseline, extended assessment of the mobile applications exposed core architectural gaps. Key findings included insecure local storage of unencrypted sensitive data (HWL-01-021) and trivial bypass techniques targeting the PIN validation mechanism (HWL-01-027) and native biometric APIs (HWL-01-028).

**Dr.-Ing. Mario Heiderich, Cure53**
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Assessment of the backend API revealed systemic security gaps characterized by widespread authentication and access control failures. Exposed endpoints allowed unauthenticated parties to extract sensitive user data (HWL-01-007), enabled unauthorized account linking via public fingerprints (HWL-01-009), and permitted complete backend Denial of Service (DoS) (HWL-01-010). In addition, essential authorization mechanisms proved ineffective in production-representative configurations (HWL-01-011), while the proxy service allowed unauthenticated actors to broadcast arbitrary transactions (HWL-01-018).

Following the active testing phase, ERA acted decisively to remediate all identified security flaws. Cure53 reviewed and verified the newly deployed updates, confirming that all vulnerabilities and weaknesses were successfully fixed. This prompt response significantly strengthened the security controls across the mobile application ecosystem.

Cure53 would like to thank Grigorii Siabruk, Dan Mutsvanga, Igor Skladchikov, and Ochir Mandzhiev from the ERA Wallet (HWLT FZE) team for their excellent project coordination, support and assistance, both before and during this assignment.