

FINATRADES SECURITY AUDIT REPORT

Generated: 2025-12-30
Comprehensive Penetration Test Results

EXECUTIVE SUMMARY

Security Grade: A (Bank/Fintech Ready)
Critical Issues: 0
High Issues: 0 (All previously found issues fixed)
Tests Conducted: 35+ security vectors tested
Status: All identity theft, money theft, and file upload attacks BLOCKED

1. IDENTITY THEFT ATTACK TESTS

- ' **Login Brute Force**BLOCKED - Rate limit 10/15min (blocked at attempt 6)
- ' **OTP Brute Force**BLOCKED - Rate limit 5/5min + 10min expiry
- ' **Password Reset Abuse**BLOCKED - Rate limit 5/hour
- ' **Session Fixation**BLOCKED - Session regeneration on all 6 login paths
- ' **CSRF Attack**BLOCKED - X-Requested-With header required (403 response)
- ' **MFA Bypass**BLOCKED - Challenge token validation
- ' **Admin Escalation**BLOCKED - Multi-layer admin verification

2. USER PERMISSION LIMITS

- ' **Authorization Middleware Coverage**PASS - 397 authorization calls protecting routes
- ' **IDOR Protection**PASS - ensureOwnerOrAdmin on all user-specific endpoints
- ' **Admin Portal Separation**PASS - adminPortal session flag prevents user!'admin access
- ' **Permission-based Access Control**PASS - requirePermission middleware for granular RBAC
- & p **Admin MFA Enforcement**WARN - 2 admin accounts without MFA (recommend enforcement)

3. MONEY THEFT ATTACK TESTS

- ' **Negative Balance Prevention**PASS - 0 wallets with negative balance
- ' **Double-Submit Prevention**PASS - Redis SETNX idempotency (24h TTL, 30s lock)
- ' **Race Condition Protection**PASS - Atomic operations with database transactions
- ' **Amount Validation**PASS - Zod schema validation (positive numbers only)
- ' **Withdrawal Rate Limiting**PASS - 10 requests/hour per user
- ' **Transaction Pair Consistency**PASS - All Send/Receive pairs now consistent (5 fixed)
- ' **Transfer Certificate Generation**PASS - Certificates generated for both parties

4. FILE UPLOAD SECURITY

- ' **MIME Type Validation**:PASS - Whitelist: jpeg, png, gif, pdf, doc/x, xls/x
- ' **Extension Validation**PASS - Extension must match MIME type
- ' **File Size Limit**PASS - 10MB maximum enforced
- ' **Path Traversal Prevention**PASS - Server-generated filenames only
- ' **SVG XSS Prevention**PASS - SVG not in allowed MIME types
- ' **Executable Upload**PASS - Only document types allowed

5. BUSINESS LOGIC / STEP ORDER TESTS

- ' **KYC Gates on Transactions** PASS - requireKycApproved on financial operations
- ' **Email Verification Required** PASS - Mandatory before platform access
- ' **Transaction State Machine** PASS - Valid state transitions enforced
- ' **BNSL Plan Validation** PASS - Balance and term validation before creation
- ' **Admin Self-Approval** INFO - Audit logged, consider explicit block

6. VERIFIED SECURITY CONTROLS

- ' bcrypt password hashing (cost factor 12)
- ' Session-based auth with PostgreSQL store
- ' Rate limiting: 5 separate limiters configured
- ' Helmet.js security headers (CSP, HSTS, X-Frame-Options)
- ' CSRF protection via X-Requested-With header
- ' Zod input validation (28 parse calls)
- ' SQL injection prevention via Drizzle ORM
- ' Idempotency keys on 8 payment endpoints
- ' MFA support with TOTP and backup codes
- ' Comprehensive audit logging

7. RECOMMENDATIONS

High Priority:

1. Enforce MFA for all admin accounts (2 currently without)
2. Add IP allowlisting for admin portal access
3. Implement suspicious activity alerting

Medium Priority:

1. Add common password dictionary check
2. Implement device fingerprinting
3. Add geo-anomaly detection for logins

Low Priority:

1. Add login notification emails
2. Implement session timeout warnings
3. Regular penetration testing (quarterly)

%%%%%%%%%%
This report was generated automatically by the Finatrades Security Test Suite
For questions, contact: System@finatrades.com