Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Management Summary: Rockwell Ventures BitNote Web, Infra & Crypto, Security Assessment by Cure53, 01.2024

Cure53, Dr.-Ing. M. Heiderich, Dr. M. Conde Pena, Dr. D. Bleichenbacher, MSc. R. Peraglie

Cure53, a Berlin-based IT security consultancy, has been compiled following the completion of a Cure53 penetration test and source code audit against the BitNote web application. The project originated from initial discussions with Rockwell Ventures management in October 2023.

After confirmation, the security review was scheduled for CW03 of January 2024 and conducted by four highly skilled professionals from the Cure53 team. To ensure comprehensive coverage, twelve working days were dedicated to the analysis.

For optimal structuring and tracking of tasks, the examination was split into four separate work packages (WPs):

- **WP1**: White-box pentests & source code audits against BitNote web UI & infra
- **WP2**: White-box pentests & source code audits against BitNote web crypto

To ensure a smooth start and efficient audit, Cure53 was provided with a comprehensive set of supporting materials beforehand. This included source code, URLs, documentation, test accounts, and other relevant assets. The testing team leveraged these resources during the pre-engagement preparations, which were completed the week before the active review period (CW02). With full access to all relevant resources allowed Cure53 was able to employ a white-box penetration testing methodology for a thorough evaluation.

A dedicated and secure Slack channel streamlined communication between both teams throughout the penetration test. This facilitated open dialogue and quick collaboration on progress, findings, and any issues that arose. This, combined with comprehensive preparation beforehand, contributed to a smooth and efficient pentest with minimal obstacles.

After achieving extensive coverage over the scope elements defined in the two WPs, Cure53 identified nine findings. Notably, five were actual security vulnerabilities, while the remaining four were best practice recommendations or minor issues. This low number, especially for a first-time audit, reflects positively on the overall security posture of the scope.

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Identified Vulnerabilities

- RVE-01-001 WP1: Persistent XSS in blockchain via sharing (Critical)
- RVE-01-002 WP1: Persistent XSS in note via export (Critical)
- RVE-01-004 WP1: Insufficient master password policy (Medium)
- RVE-01-005 WP2: Transaction origin phishing attack on referral address (Low)
- RVE-01-007 WP1: Full password decryption for biometric authentication (Medium)

Miscellaneous Issues

- RVE-01-003 WP1: Absent Content Security Policy (Medium)
- RVE-01-006 WP2: Security non-reinstatable post-MP compromise (Info)
- RVE-01-008 WP2: Side-channel attack hardening guidance (Low)
- RVE-01-009 WP2: Note sender/receiver unbound to share links (Low)

While the overall audit results were encouraging, the attack surface found in the areas in scope was broader in what concerned the web UI (WP1). The BitNote web application (WP1) revealed two concerningly and therefore critical rated issues, which both address persistent XSS vulnerabilities. In contrast, WP2 revealed only minor issues, including a single low-severity vulnerability and a few improvement suggestions. Immediate remediation was crucial to protect user experience before going live, and the BitNote team commendably prioritized addressing these, alongside other findings, swiftly and effectively, fixing the critically-rated vulnerabilities during the testing phase and the rest shortly after. The following list showcases, which findings were already addressed by the BitNote team:

Resolved Vulnerabilities and Issues:

- RVE-01-001 WP1: Persistent XSS in blockchain via sharing (Critical)
- RVE-01-002 WP1: Persistent XSS in note via export (Critical)
- RVE-01-003 WP1: Absent Content Security Policy (Medium)
- RVE-01-005 WP2: Transaction origin phishing attack on referral address (Low)
- RVE-01-007 WP1: Full password decryption for biometric authentication (Medium)
- RVE-01-009 WP2: Note sender/receiver unbound to share links (Low)

Please note that, in order to resolve RVE-01-007, the biometric authentication feature was temporarily removed in its entirety.

Initially, the BitNote web application (WP1) raised security concerns, requiring significant improvements before launch. Fortunately, the cryptography (WP2) impressed with its sound implementation, needing minimal adjustments. Due to the implementation of the aforementioned fixes, the web application has made commendable progress towards achieving robust security. However, maintaining this positive trajectory requires regular testing of both the application and cryptography to ensure all new features and updates adhere to the same high security standards.

Cure53 would like to thank Rockwell and Michael from the Rockwell Ventures team for their excellent project coordination, support, and assistance, both before and during this assignment.