Fine penetration tests for fine websites

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

Cure53 Security Assessment of Tequity Web App UIs, Games, APIs & Infra, Management Summary, 05.2025

Cure53, Dr.-Ing. M. Heiderich, M. Pedhapati, C. Luders, MSc. D. Weißer, J. Hector, A. Belkahla, A. Pirker, Dr. M. Conde

Cure53, a Berlin-based IT security consulting firm, has been contracted to conduct a penetration test and source code audit of the Tequity web application. The work was requested by Tequity in March 2025 and carried out by Cure53 precisely during CW20 and CW21 2025.

For this security assessment, a dedicated team consisting of eight senior security testers was assembled and thoroughly briefed on the project objectives and scope. These testers were responsible for all phases of the project, including the initial preparations, the execution of the testing activities, and the final delivery of the project outcomes. To ensure the expected level of coverage was achieved, a total of twenty-nine person-days were allocated and subsequently invested in the project.

To organize and structure the scope of work optimally, four work packages (WPs) were delineated:

- **WP1**: White-box penetration tests & audits against Tequity web frontends & UIs
- **WP2**: White-box pen.-tests & audits against Tequity backend components & APIs
- **WP3**: White-box pen.-tests & audit against multiple Tequity singleplayer games
- **WP4**: White-box pen.-tests & audit against multiple Tequity multiplayer games

For the purpose of this white-box penetration test, Cure53 was granted comprehensive access, encompassing source code, relevant URLs, and necessary test credentials. Preparations for the engagement were finalized in CW19 of May 2025, facilitating an efficient commencement of the testing phase. A dedicated Slack channel served as the primary communication medium between the Cure53 and Tequity teams. This setup fostered seamless information exchange, minimizing queries due to the well-defined scope and the absence of significant obstacles encountered during testing.

Throughout the assessment, Cure53 maintained regular communication, providing timely status updates and promptly reporting identified issues via the shared Slack channel. The testing efforts achieved good coverage across the defined objectives (WP1-WP4).

The overall outcome of the audit indicates that the Tequity platform exhibits a mature implementation with strong underlying application logic and security foundations. This conclusion is supported by the limited number of identified flaws and the absence of any High or Critical severity findings.

The reported issues primarily suggest areas for refinement, such as enhancing client-side security practices and strengthening backend cryptographic implementations, rather than indicating fundamental systemic weaknesses. These findings include unauthenticated IDORs, the presence of hardcoded secrets, the use of weak AES-CBC, and a potential Denial-of-Service (DoS) vector arising from rate-limiting deficiencies.

Furthermore, the platform's gameplay and fairness mechanisms, including RTP calculations, random number generation, and input validation across games, were observed to be well-managed and consistently favoring the house under testing. Common attack scenarios, such as payload manipulation, race conditions, and overpayment attempts, appear to be effectively mitigated by robust server-side protections, which incorporate secure coding practices for input handling, authorization, and randomness.

In summary, the platform shows strong resistance to high-risk vulnerabilities that could impact revenue or fairness.

Cure53 would like to thank Krzysztof Opałka and Ricardo Ferreira from the Tequity team for their project coordination, support and assistance, both before and during this assignment.