Security assessments for software that matters.

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

Cure53 Security Audit of Aurorium Apps, Admin & API, Management Summary, 03.2026

Cure53, Dr.-Ing. M. Heiderich, C. Lüders, M. Piechota, M. V. S. Lima, A. Belkahla, Y. Yuan, BSc. M. Astner

Cure53, an IT security consultancy based in Berlin, conducted a penetration test, source code audit, and security assessment of the Aurorium application stack. The work was requested by AURORIUM GROUP PTE. LTD. in February 2026, and all tests were performed by Cure53 over a two-week time frame in March 2026, specifically during CW12 and CW13.

A total of twenty-eight workdays were allocated to reach the depth and breadth of research expected for this project. The testing conducted for this audit was divided into four distinct Work Packages (WPs) for execution efficiency, as follows:

- **WP1**: White-box pen.-tests & code audits against Aurorium backend & API
- **WP2**: White-box pen.-tests & code audits against Aurorium Electron app
- **WP3**: White-box pen.-tests & code audits against Aurorium mobile app
- **WP4**: White-box pen.-tests & code audits against Aurorium website & auth

Note on Scope Adjustment: It is worth mentioning that the original scope included a fifth WP focusing on the Aurorium admin panel. However, the client requested removing this facet during the active review stage. All designated days were thereafter dispersed among the other four WPs for enhanced evaluation.

Cure53 was provided with full visibility into the platform's architecture, including the underlying source code, target URLs, comprehensive technical documentation, and functional test-user credentials. For this purpose, a white-box methodology was adopted, and a team comprising seven accomplished security analysts was assigned to the project’s preparation, execution, and finalization.

All preparatory actions were completed in March 2026, namely in CW11, to ensure testing could proceed without hindrance or delay. Communications were facilitated via a dedicated, shared Slack workspace deployed to combine the workspaces of AURORIUM and Cure53, thereby creating an optimal collaborative working environment. All participatory personnel and relevant stakeholders from both parties were invited to partake throughout the test preparations and discussions.

The execution phase was notably efficient, characterized by a well-defined scope that precluded technical bottlenecks or the need for extensive clarification. Throughout the assessment, Cure53 provided consistent progress reports. Per the project's setup, live-reporting was successfully utilized to fast-track the disclosure of specific, high-priority findings via the shared Slack channel.

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

A total of thirty-five findings were identified in this round of testing, eighteen of which were classified as exploitable security vulnerabilities and the remaining seventeen as miscellaneous lower-risk deficiencies. It should be noted that the total number of issues is relatively high, and the original findings reflected the brittleness of the current security posture. In addition, several Critical and High impact faults were detected, including four Critical flaws that directly undermined the platform's primary operations, particularly regarding user anonymity and data integrity, which was highly concerning.

However, it should be noted that the audit was immediately followed by a comprehensive remediation phase. All identified issues have since been fully or partially mitigated.

It is safe to say that nearly all issues have been properly addressed, and the critical vulnerabilities highlighted in the original report no longer pose a threat to the platform's ecosystem. Given the architectural changes and patches applied, the application stack has successfully neutralized the severe attack vectors.

In conclusion, this 2026 assessment of the Aurorium application stack confirms that the backend services, desktop client, mobile applications, and public website under review are now in significantly better shape from a security perspective.

Cure53 would like to thank Andrew Filipchik and Illia Kaplan from the AURORIUM GROUP PTE. LTD. team for their excellent project coordination, support, and assistance, both before and during this assignment.