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 St8 Web App, API & Infrastructure, Management Summary, 02.2026

Cure53, Dr.-Ing. M. Heiderich, M. Wege, Dipl.-Ing. A. Inführ, MSc. J. Moritz, J. Hector, M. Elrod

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a penetration test and source code audit against the St8 web application complex.

Regarding the timeline and setup, the project originated from preliminary discussions held with ST8 Innovations Limited stakeholders in November 2025. The agreed testing scope comprised twenty-four person-days of active diagnostic evaluation. Cure53 deployed six experienced security analysts during CW06 to complete the assessment across target systems.

The scope of work was structured as five individual work packages (WPs) specifying the primary features for inspection during this iteration of testing:

- **WP1**: White-box pen.-tests and code audits of Backoffice UI
- **WP2**: White-box pen.-tests of Backoffice API/GraphQL & backend
- **WP3**: White-box pen.-tests & code audits of Backoffice app authn & authz
- **WP4**: White-box pen.-tests of Backoffice app Team Management feature
- **WP5**: Configuration review & gray-box pen.-tests of cloud infrastructure

The engagement utilized a hybrid strategy, as a white-box analysis was applied to WP1-WP4, and a gray-box model was leveraged for WP5. To support thorough execution, St8 provided the assessment team with direct access to application source code, operational environments, test user credentials, and necessary architectural artifacts.

Scoping and administrative setups concluded in late January 2026 (CW05) to enable an unhindered operational kickoff. Project collaboration was maintained through a dedicated Slack workspace connecting active team members from both St8 and Cure53.

Testing executed smoothly without notable operational or technical disruptions, supported by thorough pre-engagement setup. Cure53 maintained routine progress briefings and communicated notable discoveries as testing unfolded. To support rapid visibility, live reporting was selectively provided for designated findings using shared Markdown documentation.

Cure53 achieved comprehensive diagnostic coverage across work packages WP1 through WP5, identifying eighteen total findings for client remediation. The assessment team classified seven items as exploitable security vulnerabilities and eleven items as general security weaknesses representing minor risks or opportunities for systemic hardening.

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

While numerous findings were documented, Cure53 assesses the primary security posture of the St8 web application to be adequate. However, the volume of identified issues indicates substantial opportunity for security hardening.

Demonstrating strong responsiveness, the St8 engineering team initiated remediation efforts immediately after the assessment. St8 successfully fixed or mitigated all of the reported issues, prioritizing and resolving all exploitable security vulnerabilities in the immediate aftermath of active testing.

Going forward, Cure53 advises St8 to maintain a continuous security improvement model and schedule regular third-party audits alongside major platform updates.

Cure53 would like to thank Yurii Semeniuk and Almaz Nazipov from the ST8 Innovations Limited team for their excellent project coordination, support, and assistance, both before and during this assignment.