Fine penetration tests for fine websites

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

Cure53 Security Assessment of DeepL Web & API Management Summary January 2022

Cure53, Dr.-Ing. M. Heiderich, Dipl.-Ing. A. Inführ, BSc. B. Walny, MSc. F. Fäßler, MSc. S. Moritz

Cure53, which is a Berlin-based IT security consultancy, completed a comprehensive security assessment of the DeepL Web Application UI, connected API and underlying servers (labeled as *DPL-01*). The project was requested by DeepL GmbH (now DeepL SE) in early June 2021 and then scheduled for Q3 2021. As for the precise timeline and specific resources, Cure53 completed the examination in September, namely in CW35 of 2021.

The assessment conducted by Cure53 entailed a mixed-box penetration test against the DeepL Translator Web Application and connected backend APIs and servers. For optimal structuring and tracking of tasks, the work was split into five separate work packages (WPs):

- **WP1**: Grey-Box Penetration-Tests against DeepL Translator Web-App UI
- **WP2**: Grey-Box Penetration-Tests against DeepL Translator Backend & API
- **WP3**: Grey-Box Penetration-Tests against DeepL Translator Admin Webapp
- **WP4**: Grey-Box Penetration-Tests & Scans of the DeepL IP Ranges & Hosts
- **WP5**: White-Box Review against DeepL Keycloak Configuration & Hardening

By investigating the scope through a range of methods, the Cure53 team could collect sufficient evidence to formulate a holistic verdict on the robustness of the DeepL web security premise.

A team of five Cure53 testers, all with expertise matching the project's goals, invested a total of fourteen-and-a-half person-days into this assignment. Cure53 was given access to the application rolled-out on a staging environment, test-users as well as configuration files.

The project progressed effectively on the whole. All preparations were done in CW34 to foster a smooth transition into the testing phase. Over the course of the engagement, the communications were done using a private, dedicated and shared Slack channel joined by all relevant team members. The discussions throughout the preparatory phase and the test execution period were very prompt and productive. Ongoing interactions positively contributed to the overall outcomes of this project. Further, the scope was well-prepared and clear, with no noteworthy roadblocks encountered during the test.

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

The Cure53 team managed to get very good coverage over the WP1-5 scope items. Among eleven security-relevant discoveries, four were classified to be security vulnerabilities and seven to be general weaknesses with lower exploitation potential.

For a project of this scale, the number of issues is not excessive and the scope appears to be quite robust. No flaws received Critical scores. Cure53 notes that the DeepL application compound is well managed and does not expose too many weaknesses. None of the issues would be classified as the so-called low-hanging fruit that are easy to spot. It is noticeable that the DeepL team has their security matters under control and prioritized as needed.

As a final stage of this project in Q1 2022, Cure53 engaged in and completed a phase of fix verification, inspecting how the DeepL Translator Web UI & API scope has improved over time and in relation to the communicated findings. DeepL shared several diffs for Cure53 to review. In this realm, the testing team is happy to report that all four vulnerabilities have been properly addressed, with recommendations stemming from the assessment followed correctly.

To conclude, this September 2021 assessment confirms that the DeepL web complex is now significantly stronger and more stable in terms of security posture. From Cure53's perspective, reasonable steps were being taken to ensure that good fixes were crafted and took effect on the DeepL Translator Website UI and backend API.

In Cure53's expert opinion, this project now represents a solid security premise at DeepL SE for the DeepL Translator Web Application UI, connected API and underlying server. The application compound is currently well-protected against a broad number of web application attack vectors. One can argue that the outcome highlights the development team's commitment to maintaining security features with due diligence and adherence to best practices.

Cure53 would like to thank the DeepL SE team for their excellent project coordination, support and assistance, both before and during this assignment.