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 Ahrefs Web, API & Infra, Management Summary, 04.-06.2024

Cure53, Dr.-Ing. M. Heiderich, BSc. C. Kean, L. Herrera, M. Pedhapati, H. Jaiswal

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a penetration test and security assessment of the Ahrefs' web application front-end aspects and UI, back-end components and API endpoints, and underlying infrastructure and servers. Cure53 was engaged by Ahrefs Pte. Ltd. in April 2024 to conduct this security assessment in late April & early May 2024 (CW17-18).

In terms of the exact timeline and specific resources allocated to *AHR-03*, Cure53 completed the research in CW18/2024 as planned. As can be seen, this was the third assessment that Cure53 had already performed against Ahrefs’ scope item. For this iteration, a total of twenty days were invested to achieve the expected coverage for this task.

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

- **WP1**: Gray-box pentests and assessments against Ahrefs web UI & frontend
- **WP2**: Gray-box pentests and assessments against Ahrefs API & backend
- **WP3**: Gray-box pentests and assessments against Ahrefs server & infrastructure

As you can see, a gray-box testing methodology was used to facilitate a comprehensive assessment. The client provided full access to all necessary resources, including URLs, test credentials, and any additional access points. A dedicated team of five senior security testers managed the project from planning through execution to completion. All preparatory activities were completed by the end of April 2024 (CW16), ensuring a smooth start to the test.

Effective communication was maintained throughout the audit via a dedicated Slack channel shared by both the Ahrefs Pte. Ltd. and Cure53 teams. This platform facilitated the participation of all relevant personnel from both parties.

The clearly defined scope and open communication channels minimized the need for cross-team requests. Cure53 provided regular status updates on test progress and related findings, although live reporting was deemed unnecessary..

This test achieved comprehensive coverage and identified a total of ten findings within the defined scope. None of the findings were assigned a *critical* severity rating, which is a great sign for Ahrefs, one was assigned a *high* severity rating, and the rest were assigned *medium* and lower severity ratings. Four of the ten findings were classified as security vulnerabilities, while the remaining six were classified as less exploitable weaknesses.

This relatively moderate number of vulnerabilities indicates a mostly positive security posture for the Ahrefs components in scope. However, Cure53 noted that there is room for improvement, particularly with regard to cross-site scripting (XSS) vulnerabilities. However, it is worth noting that the Ahrefs team addressed all of the *high* and *medium* rated vulnerabilities shortly after the pentest & assessments.

To verify and confirm the implemented fixes, Cure53 performed retests and code reviews in the form of a diff inspection to validate the effectiveness of the implemented fixes and the resulting security improvements for the assessed components.

The now well-established security foundation of the Ahrefs website compound, coupled with the prompt remediation efforts of the Ahrefs team, ensures the production readiness of the assessed features. Cure53 is confident that the features described in this document are ready for production deployment.

Cure53 would like to thank Efim Mirochnik, Igor Pikovets, Mauricio Fernandez, and Joris Giovannangeli from the Ahrefs Pte. Ltd. team for their excellent project coordination, support, and assistance, both before and during this assignment.