Management Summary: Cake DeFi UI, API & Server Security Assessment by Cure53, 04.2022

Cure53, Dr.-Ing. M. Heiderich, N. Hippert, MSc. R. Peraglie, BSc. B. Walny

Cure53, which is a Berlin-based IT security consultancy, completed a security assessment against the user-facing parts of the Cake Pte. Ltd. software complex, spanning the Cake DeFi UI, backend API, and underlying servers. The project executed by Cure53 entailed a penetration test and a general review of the observable security premise. By investigating the scope through a range of methods, Cure53 acquired evidence-based knowledge about the scope and can now issue a verdict about its robustness.

In the frames of this cooperation, a team of four Cure53 testers, all with expertise matching the project's goals, invested a total of thirteen person-days into this assignment. The work was predominantly carried out in February 2022, namely CW06 through CW07, with the main tasks ascribed to two distinct Work Packages (WPs).

- **WP1**: Grey-box penetration tests against Cake DeFi web UI and JavaScript
- **WP2**: Grey-box penetration tests against Cake DeFi backend API and server

Prior to highlighting the contents of the two WPs, it is important to comment on the methods employed for this project. The overarching approach was a grey-box methodology. The Cure53 testing team was given information on how to create and leverage test-users and test-data, accompanied by test-supporting documentation and API documentation. This level of clarity of the scope also meant neither technical nor other problems occurred during the assessment.

The Cake Pte. Ltd. team responsible for the application in scope was highly engaged in making sure that the envisioned attack surface is fully test-ready by the project's start date set for the February project. Dedication to preparatory stages enabled timely and efficient progress of this Cure53 assessment. For each of the aforementioned components in scope, Cure53 conducted security reviews and penetration testing.

Communications during this engagement took place in a dedicated, private and shared Slack channel, which connected the Cake Pte. Ltd. and Cure53 workspaces and enabled the involved team members from both sides to join in. Keeping the Cake Pte. Ltd. team apprised of the progress, the Cure53 team reported the number and headlines of the spotted findings on an almost daily basis.

Live-reporting was executed using the same communications channel, leading to several timely fixes being authored by Cake Pte. Ltd. developers. Speaking of the findings, the Cure53 testers have made ten security-relevant discoveries on the Cake DeFi web application scope. Three problems were categorized as vulnerabilities and seven as general weaknesses.

Generally speaking, the overall volume of findings detected should be considered relatively moderate for a framework of this complexity and magnitude. This is evidently a positive indication regarding the security posture of the components and aspects included in this particular scope. Notably, all findings were assigned *Medium*-severity ratings or even lower. Additionally, the majority were only considered general weaknesses that are trivially easy to address and mitigate.

Throughout the testing process and after its conclusion, the Cake Pte. Ltd. team responded to the reported issues with swift action and comprehensive mitigation strategies.

In conclusion, the application architecture had some weaknesses in its design and architecture, which were addressed by Cake Pte. Ltd early on after the reporting from Cure53. Typically widespread issues such as XSS, SQLi, and to a large extent ACL controls seem to be under control thanks to the correct usage of well-known frameworks, which contributes to the positive impression gained on the whole. However, Cure53 strongly recommends initiating a comprehensive code audit for future assessments to detect even the most deeply-entrenched framework weaknesses.

This positive impression has been confirmed with the subsequent stages of fix verification. Cure53 can confirm that all relevant findings received due attention and should be considered resolved. For fix verification purposes, Cure53 had access to the detailed fix descriptions and screenshots highlighting the code and configuration changes, the information was presented in a very structured way and enabled Cure53 to perform a refreshingly efficient review process.

Cure53 would like to thank U-Zyn Chua, Arif Khan, Daniel Lo, Asyraf Norafandi, Ben Zumbrunn, and Steven Kearns from the Cake Pte. Ltd. team for their excellent project coordination, support and assistance, both before and during this assignment.