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 PayTec TMS Solution Web UI & API , Management Summary, 02.2025

Cure53, Dr.-Ing. M. Heiderich, Dipl.-Ing. A. Inführ, E. Foudil, H. Jaiswal, M. Pedhapati

Cure53, a Berlin-based IT security consulting firm, has been contracted to conduct a penetration test and source code audit of the PayTec TMS solution, with a focus on its frontend aspects and UI, as well as its backend components and API endpoints.

The assignment originated from a contact between PayTec AG and Cure53 in November 2024. The test execution was scheduled for CW06, corresponding to early February 2025. A total of thirteen person-days were invested to achieve the expected coverage, with a team of five senior testers managing all phases of the project.

The work was split into two separate work packages (WPs), defined as:

- **WP1**: White-box pen.-tests & code audits against PayTec TMS solution frontend
- **WP2**: White-box pen.-tests & code audits against PayTec TMS backend & API

To enable a thorough assessment, the testing team was equipped with a full suite of resources, encompassing source code, URLs, test credentials, and all other required access, aligning with a white-box methodology.

In late January 2025, specifically during CW05, the groundwork was laid to ensure Cure53's testing phase commenced without a hitch. A dedicated, shared Slack channel was established as the central communication point, effectively merging the teams from PayTec and Cure53. This platform became the primary space for collaboration, with all involved parties participating. The clarity of the scope and thorough preparation resulted in a remarkably smooth communication flow, with questions being minimal and easily resolved.

The testing itself unfolded without any significant roadblocks, and Cure53 provided consistent updates, shared their findings, and even offered live reporting for a selection of requested findings through the established Slack channel.

Cure53's assessment, which achieved good coverage across the defined scope items, resulted in the identification of eighteen security-related findings. Of these eighteen findings, eight were classified as security vulnerabilities, representing potential points of exploitation. The remaining ten were categorized as general weaknesses, which, while present, pose a lower risk of actual exploitation. The overall number of findings is considered to be a higher amount than expected, which is a matter of concern

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

Identified Vulnerabilities

- PYT-01-001 WP1: Multiple reflected XSS via AddItem (High) **Fixed**
- PYT-01-002 WP1: Reflected XSS via RequestedPath parameter (Medium) **Fixed**
- PYT-01-006 OOS: SQL injection via installation ID (High) **Fixed**
- PYT-01-007 WP2: Missing authorization check in multiple Terminal methods (High) **Fixed**
- PYT-01-009 WP2: SQL injection in OLE DB Excel connection (High) **Fixed**
- PYT-01-011 WP2: IDOR to modify report jobs (High) **Fixed**
- PYT-01-012 WP2: Shared event logs disclosing sensitive information (Medium) **Fixed**
- PYT-01-013 WP2: IDOR to modify default brand (High) **Fixed**

Building upon the above listed vulnerabilities, Cure53 also identified ten general weaknesses that, at the time of testing, presented no exploitable security impact. All of these weaknesses were classified with an Info severity rating. Demonstrating a proactive approach to security enhancements, the PayTec team has already remediated four of these identified weaknesses.

The security assessment uncovered common vulnerabilities inherent in older codebases, specifically related to inconsistent application of SQL and Access Control List (ACL) security mechanisms. Given that several of these vulnerabilities were classified as High severity, Cure53 strongly recommended an immediate investigation into their underlying causes. It is imperative not only to address these issues promptly to mitigate potential risks, but also to leverage them as valuable learning opportunities for future development practices.

Furthermore, the implementation of robust code checks is advised to prevent their recurrence. To ensure a comprehensive understanding of the system's security posture and identify any potentially more complex issues, a more extensive future assessment is also recommended.

PayTec demonstrated a proactive approach to security by swiftly implementing Cure53's recommendations. The development team initiated the resolution of all identified vulnerabilities, as well as a selection of general weaknesses shortly after the completion of the security assessment. This rapid response underscores their commitment to continuous improvement and ensuring a safe user experience for the solution. Cure53 was provided with detailed information regarding the implemented fixes and was able to verify and confirm their efficacy, as documented in the list of findings provided above.

Cure53 would like to thank Thomas Seiler from the PayTec AG team for his excellent project coordination, support and assistance, both before and during this assignment.