Magnolia International Ltd.

Pentest Magnolia Core 6.4

Version:	v1.0
Project Number:	90620
Date of Delivery:	December 19th, 2025

Compass Security Schweiz AG, Werkstrasse 20, CH-8640 Rapperswil
T +41 58 510 36 00, team.csch@compass-security.com, www.compass-security.com

Executive Summary

In September 2025, Compass Security Schweiz AG (Compass) conducted a penetration test of Magnolia Core 6.4. In October/November 2025 a reassessment was conducted of previously identified weaknesses. This document is intended to provide a high-level summary of the assessment results. Further details have been reported to Magnolia in a separate document.

Scope

The targets in scope are listed in the following table:

Target	Date	Effort
Manual Hacking Web Application	01.09.2025 – 05.09.2025	10 PD
Recheck of previously identified weaknesses	13.10.2025 – 15.10.2025 19.11.2025 – 19.11.2025	2.5 PD

The statements made in this document are only applicable to the exact dates listed above.

Procedures

The web application was tested from the perspective of an anonymous user as well as with multiple user accounts with varying permission levels. The testing focused on identifying issues such as misconfigurations, injection vulnerabilities, and weaknesses in user authentication and authorization, as well as other security risks.

Both manual and automated testing methods were employed.

Weakness Rating

Compass groups the findings into four categories: low, medium, high and critical. The ratings are based on their intrinsic technical properties and are not a risk score. Other factors such as a threat actor's motivation or financial loss incurred by a successful exploitation of a vulnerability have not necessarily been considered.

Results

During the security assessments no critical or high-rated vulnerabilities could be found.

Multiple medium and low rated weaknesses were correctly remediated between both the initial assessment in September 2025 and the Rechecks performed in October and November 2025. However, certain issues remain that decrease the overall resilience of the application against common attacks. It is still possible to manipulate certain aspects of the AI queries allowing the user to bypass which models are used. Furthermore, it is still possible to upload arbitrary files, which when downloaded could present a risk for other users or for the security of the application.

While the low-rated issues do not pose a directly exploitable threat, they still have a negative impact on the overall security posture of the application and should therefore be remediated in a future release.

About

Compass Security Schweiz AG is a Swiss IT security company specializing in providing tailored high-quality attack simulations, security assessments and forensic investigations to customers. Founded in 1999, Compass has over 25 years of experience working on national and international projects with Fortune 500 companies, small and medium-sized companies, as well as with start-ups operating in the financial, medical, industrial, and pharmaceutical industries. The diverse training and specializations of our security analysts, as well as close cooperation with leading Swiss universities, ensure that our analysts are always informed about the latest developments in the security industry.