

GCP MT Penetration Test Report - February 2025

Report generated on Feb 18 2025

Prepared for Databricks by Cobalt. This report is for informational purposes, not for any other purpose, and may only be shared with third-parties by Databricks. Cobalt disclaims all liability to any third-party arising from this report. Usage of this report by shall be subject to Cobalt's terms, available at <https://cobalt.io/terms/>.

Targets

https://7068289608840589.9.gcp.databricks.com/

| Test period | Status |
|-----------------------------|--------|
| Jan 31, 2025 Feb 14, 2025 | Final |

Test performed by

-  Shashank Shashank Lead
-  Shpend Kurtishaj Pentester
-  Brad Turner Pentester

Executive Summary

Cobalt conducted a pentest of the GCP MT application and API to assess its risk posture and identify security issues that could negatively affect Databricks's data, systems, or reputation. The scope of the assessment covered GCP MT and included credentials for various levels of privilege within the scope. A Cobalt pentest team of 3 conducted this engagement between Jan 31, 2025 and Feb 14, 2025.

The web application pentest was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the [Open Web Application Security Project \(OWASP\) Top 10](#). The assessment also included a review of security controls and requirements listed in the [OWASP Application Security Verification Standard \(ASVS\)](#).

The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis.

During this engagement, Cobalt's testers reported their findings and rated them based on the following severities:

| | <div><div></div>CRITICAL</div> | <div><div></div>HIGH</div> | <div><div></div>MEDIUM</div> | <div><div></div>LOW</div> | <div><div></div>INFO</div> |
|----------|--------------------------------|----------------------------|------------------------------|---------------------------|----------------------------|
| Open | 0 | 0 | 0 | 6 | 1 |
| Resolved | 0 | 0 | 0 | 0 | 0 |
| Total | 0 | 0 | 0 | 6 | 1 |

Approach

The engagement was done according to industry best practices. The following outlines the process from start to finish.

Pre Engagement

- Scoping
- Customer documentation
- Access

Engagement

- Reconnaissance
- Tool assisted assessment
- Manual assessment
- Vulnerability identification and/or exploitation
- Risk analysis
- Reporting

Post Engagement

- Prioritized remediation
- Recommendations
- Retesting (if applicable)

Risk Factors

Each finding is assigned two factors to measure its risk. Factors are measured on a scale of 1 (very low) through 5 (very high).

Impact

This indicates the finding's effect on technical and business operations. It covers aspects such as the confidentiality, integrity, and availability of data or systems; and financial or reputational loss.

Likelihood

This indicates the finding's potential for exploitation. It takes into account aspects such as skill level required of an attacker and relative ease of exploitation.

Severity Definitions

When our pentesters find vulnerabilities, they use the standard [OWASP Risk Rating Methodology](#), and then classify them into one of the following risk levels, based on their business impact and likelihood: $\text{risk} = \text{impact} * \text{likelihood}$

● CRITICAL

Includes vulnerabilities that require immediate attention. Risk score of 25.

● HIGH

Impacts the security of your application/platform/hardware, including supported systems. Includes high probability vulnerabilities with a high business impact. Risk score range: 16 through 24.

● MEDIUM

Includes vulnerabilities that are: medium risk, medium impact; low risk, high impact; high risk, low impact. Risk score range: 5 through 15.

● LOW

Specifies common vulnerabilities with minimal impact. Risk score range: 2 through 4.

● INFORMATIONAL

Notes vulnerabilities of minimal risk to your business. Risk score of 1.

Terms

PLEASE NOTE: It is impossible to test networks, information systems, and people for every potential security vulnerability. This report does not form a guarantee that your assets/targets are secured from any and all threats. All assessments performed, and their results, are only from the point-of-view of Cobalt, at the time of the engagement. Cobalt is unable to ensure or guarantee that your assets/targets are or will be completely safe from every form of attack now or in the future. With the ever-changing environment of information technology, any assessment performed by Cobalt will necessarily exclude vulnerabilities in software or systems that are unknown at the time of the engagement. For a full list of terms governing the services of Cobalt, this report, and the usage thereof, please consult the Terms of your Agreement with Cobalt or www.cobalt.io/terms.