



AWS MT Penetration Test Report - March 2024

TARGET(S)

<https://dbc-baab306e-ba03.staging.cloud.databricks.com/>

TEST PERIOD

Mar 4, 2024 → Mar 18, 2024

STATUS

Final

Contents

Executive Summary	2
Methodology	3
Pre Engagement 1 Week	3
Penetration Testing 2~3 Weeks	3
Post Engagement On-demand	3
Risk Factors	4
Severity Definitions	4

Executive Summary

Cobalt conducted a pentest of the AWS MT application and external network 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 AWS MT and included credentials for various levels of privilege within the scope. A Cobalt pentest team of 3 conducted this engagement between Mar 4, 2024 and Mar 18, 2024.

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 external testing was a combination of manual and automated assessments of the external infrastructure, which included testing various services and applications present on each system for known vulnerabilities and security weaknesses within the [Common Vulnerabilities and Exposures \(CVE\)](#) databases. The Cobalt team conducted this penetration test following recommended industry best practices to test the various security controls. The pentesters relied on tools to guide the first wave of testing, followed by manual testing to provide an accurate and in-depth analysis.

During testing, Cobalt's pentesters tested for vulnerabilities and rated them based on the following categories:

Critical	High	Medium	Low	Informational
0	0	0	4	5

Methodology

The test was done according to penetration testing best practices. The flow from start to finish is listed below.

Pre Engagement

- Scoping
- Customer documentation
- Information discovery

Penetration Testing

- Tool assisted assessment
- Manual assessment
- Exploitation
- Risk analysis
- Reporting

Post Engagement

- Prioritized remediation
- Best practice support
- Retesting

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:

```
risk = impact * 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.

Info

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