AWS AI Security Agent

Penetration Test Report

Belinaonline

26 February 2026

Table of Contents

Report Filters Applied **3**

Executive Summary **4**

Scope **6**

Methodology **7**

Findings (0) **8**

Detailed Findings **9**

Report Filters Applied

This report includes the following filters:

Risk levels:

Confidence:

Status:

Risk types:

Task status

Note: Filters apply only to the Findings section and the Tasks Executed table in Methodology. Executive Summary and Scope sections show the complete penetration test. For full unfiltered results, access the console.

Executive Summary

The security assessment of cloud.belinaonline.com identified one confirmed security finding rated as LOW severity. A CloudFront Web Application Firewall (WAF) bypass vulnerability was discovered, where the WAF fails to normalize UTF-8 overlong encoding sequences before applying path traversal security rules. While this misconfiguration allows requests to bypass WAF protections (changing HTTP 403 responses to HTTP 200), no actual exploitation was achieved as backend security controls properly prevented unauthorized file access. All bypassed requests returned empty responses, indicating the vulnerability represents a defense-in-depth failure at the WAF layer rather than a critical path traversal vulnerability. Two additional findings were assessed as false positives: a standard URL path normalization behavior misidentified as path traversal, and innerHTML usage in static HTML attributes without any user-controllable input vector.

The target application is a public static website hosted on Amazon S3 behind CloudFront CDN, consisting primarily of HTML pages, CSS files, images, and JavaScript assets including a 3CX Live Chat widget. Testing expanded from the initial root endpoint to discover eight total endpoints, including several SOAP-related paths and standard website resources. All content is intentionally publicly accessible with no directory-based access controls implemented. The assessment was conducted against a fully public infrastructure with no authentication mechanisms, and testing was limited to the CloudFront/S3 architecture boundaries. The total assessment yielded three findings: one confirmed LOW severity security misconfiguration and two false positives that were thoroughly analyzed and dismissed.

Note: This Executive Summary is based on all findings and is not affected by report filters.

Understanding Finding Metrics

Agent confidence level: Indicates AWS Security Agent's certainty that a finding represents a genuine security vulnerability. High confidence findings have been verified and confirmed through successful exploitation. Medium and low confidence findings may require additional manual validation.

Severity levels:

Critical Requires immediate action; exploitation could lead to system compromise.

High Requires prompt attention; exploitation could result in significant security impact.

Medium Should be addressed in a reasonable timeframe; contributes to overall security risk.

Low Can be addressed as part of regular maintenance; minimal immediate risk.

Informational For informational purposes; minimal to no immediate risk.

Risk score: A numerical assessment combining the severity of the vulnerability with the likelihood of exploitation using Common Vulnerability Scoring System (CVSS) metrics. Higher scores indicate findings that should be prioritized for remediation. Risk scores are calculated using CVSS v3.1 (Common Vulnerability Scoring System version 3.1).

Finding status: Tracks the remediation workflow state. Active findings require review. Mark findings as Resolved when fixed, Accepted when risk is acknowledged, or False Positive when determined to be incorrect. Incomplete findings require additional investigation.

Scope

The following domains were in scope for the penetration test:

- https://cloud.belinaonline.com

Methodology

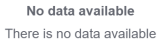
This penetration test was conducted using AWS Security Agent, which deploys specialized AI agents through a four-phase approach: Preflight (connectivity validation), Static Analysis (code and configuration review), Penetration Testing (runtime vulnerability exploitation), and Finalizing (validation and reporting). The agent analyzes application context from source code and documentation to identify vulnerabilities through tailored multi-step attack scenarios.

Testing Approach

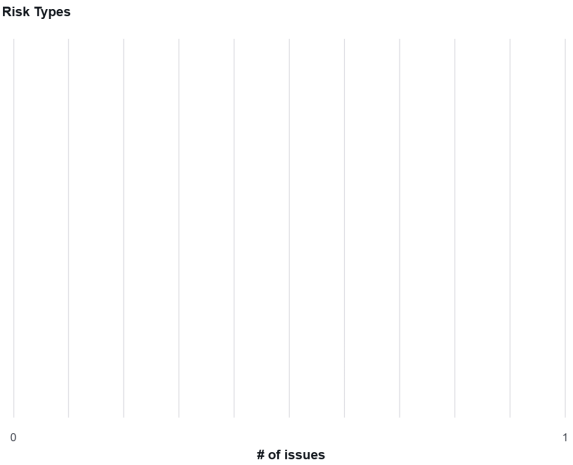
AWS Security Agent validates findings through proof-based exploitation, providing reproducible attack paths with step-by-step evidence. Each finding includes CVSS v3.1 severity assessment, confidence rating based on validation success, and detailed reproduction steps. The testing methodology follows industry-standard attack patterns while adapting to application-specific context.

Findings (0)

Severity Distribution



Risk Types



Finding	Severity	Status