Security Assessment Report

Generated: 2026-02-03T07:09:15.136056Z

Scope: Uploaded Files Analysis

Executive Summary

Here is the executive summary:

This security assessment report provides an analysis of uploaded files to identify potential vulnerabilities and risks. The scope of this assessment focused solely on uploaded files, providing a comprehensive view of the organization's file upload practices. Overall, our findings indicate a moderate risk posture, with 2 high-severity, 1 medium-severity, and 2 low-severity issues identified.

The majority of these findings are categorized as high severity, highlighting the need for immediate attention to mitigate potential security breaches. Notably, there is a significant gap between the number of high- and low-severity findings, emphasizing the importance of prioritizing remediation efforts.

While this report provides valuable insights into the organization's file upload practices, it is essential that analysts review these findings in detail to develop targeted mitigation strategies. A thorough analysis will enable the organization to effectively address the identified vulnerabilities and minimize potential risks.

Next steps should focus on addressing the high-severity findings first, followed by a comprehensive review of all findings to ensure a robust security posture.

Scope & Methodology

This assessment employed a deterministic rule-based scanning approach combined with AI-assisted analysis.

Detection Method:
• Pattern-based rule engine for vulnerability detection
• Evidence collection with exact file and line references
• Confidence scoring based on rule metadata and evidence completeness

Analysis Method:
• Local LLM (Ollama) for explanation and remediation suggestions
• Analyst review for final severity assessment
• Evidence-based validation of all findings

All findings include exact locations and evidence snippets for verification.

Findings

VULN-001: Hardcoded password detected

Severity: High
Confidence: 0.66
Category: Credentials

Affected Files:
- `01_harcoded_credentials.txt`

Locations:
- `01_harcoded_credentials.txt`

Evidence:
`
username=admin
password=SuperSecret123
host=prod-db.internal
`

VULN-002: Debug mode enabled

Severity: Low
Confidence: 0.62
Category: Debug

Affected Files:
- `02_debug_logging.conf`

Locations:
- `02_debug_logging.conf`

Evidence:
`
service.name=payment-gateway
debug=true
log.level=INFO
`

VULN-003: Hardcoded password detected

Severity: High
Confidence: 0.66
Category: Credentials

Affected Files:
- `04_mixed_signals.log`

Locations:
- `04_mixed_signals.log`

Evidence:
`
2026-01-07 10:01:22 INFO Starting service

debug=true
connecting with password=admin123
`

VULN-004: Exposed administrative or database port

Severity: Medium
Confidence: 0.55
Category: Network

Affected Files:
• `04_mixed_signals.log`

Locations:
• `04_mixed_signals.log`

Evidence:
`
2026-01-07 10:01:22 INFO Starting service
debug=true
connecting with password=admin123
`

VULN-005: Debug mode enabled

Severity: Low
Confidence: 0.62
Category: Debug

Affected Files:
• `04_mixed_signals.log`

Locations:
• `04_mixed_signals.log`

Evidence:
`
2026-01-07 10:01:22 INFO Starting service
debug=true
connecting with password=admin123
`

Risk Overview

Risk Overview
==

Total Active Findings: 5

High Severity (2 findings):
Requires immediate attention. These findings pose significant security risks and should be remediated as a priority.

Medium Severity (1 findings):
Should be addressed in the near term. These findings indicate potential security concerns that should be evaluated in context.

Low Severity (2 findings):
May be addressed as resources permit. These findings represent lower-risk issues or hygiene improvements.