

# Security Assessment Report

\*\*Generated:\*\* 2026-02-09T10:30:40.519243Z

\*\*Scope:\*\* Uploaded Files Analysis

## Executive Summary

This security assessment identified 5 active vulnerability findings in Uploaded Files Analysis.

Severity Distribution:

- High Severity: 2 findings
- Medium Severity: 1 findings
- Low Severity: 2 findings

Findings include evidence-based detections with specific file locations and remediation suggestions. All findings should be reviewed by a security analyst for contextual risk assessment.

## 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.