Precursor

# Security Assessment Report

## 9fin LTD

## Web Application Security Assessment

Version:
2026-11-17 17:04:17

CREST

www.precursorsecurity.com

# 1. Management Summary

Precursor Security performed a web application security assessment against the 9fin LTD assets, defined within the Scope of Engagement. The purpose of the assessment was to identify security vulnerabilities which could impact the security of the 9fin LTD assets resulting in the compromise of information, accounts and the system itself.

## Vulnerability Summary

A total of 22 findings were identified, 7 of which were resolved. The following table details the severity categories for each identified finding:

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| No findings | No findings | 3 findings | 7 findings | 5 findings |

Table 1.1: Finding counts by severity.

## Business Risk

The findings of the assessment present a medium security threat to the 9fin LTD assets. The original assessment identified several significant security issues, a number of which have since been remediated following the retest.

Unauthorised users could enumerate the categories of private documentation held for individual companies through the separately provisioned private-content model. Although the retrieval of encrypted document contents was subsequently remediated, the ability to identify what private materials exist for a given company remains unresolved and could assist targeted reconnaissance against specific clients.

The AI assistant exhibited insufficient guardrails and could be induced to perform tasks beyond its intended remit as a credit-analysis tool, including generating arbitrary code and rendering user-supplied images. Two of the three conditions required for automated data exfiltration through the assistant were already present: the ingestion and summarisation of untrusted document content, and the ability to render externally hosted image URLs. Access to sensitive user data, the third condition, was not yet present at the time of testing.

Following the retest, seven findings were confirmed as remediated. Denial-of-Service protections were implemented on the Legal Exports endpoint, and rate limiting was introduced on the chatbot endpoint to reduce the risk of denial-of-wallet attacks. The Markdown Injection vulnerability in the AI assistant output was resolved. Both username enumeration vulnerabilities, on the login portal and the forgotten password portal, were remediated. Broken Object Level Authorisation on the Locked Document Download endpoint and the Broken Access Control subscription tier bypass were also confirmed as resolved.

# 2. Summary of Findings

| # | Title | Status | Severity |
|---|---|---|---|
| 024 | Denial of Service: Legals Export | ✔ Resolved | HIGH (7.5) |
| 020 | Broken Access Control: Subscription Tier Bypass | ✔ Resolved | MEDIUM (6.5) |
| 022 | Broken Access Control: Paywall Bypass | ✘ Unresolved | MEDIUM (6.5) |
| 007 | Lack of Multi-Factor Authentication (MFA) | ✘ Unresolved | MEDIUM (5.6) |
| 005 | Broken Object Level Authorisation: Locked Document Download | ✔ Resolved | MEDIUM (5.3) |
| 018 | Broken Access Control: Private Document Categories | ✘ Unresolved | MEDIUM (5.3) |
| 025 | Lack of Rate Limiting | ✔ Resolved | MEDIUM (5.3) |
| 014 | Username Enumeration: Forgotten Password Portal | ✔ Resolved | MEDIUM (5) |
| 015 | Username Enumeration: Login Portal | ✔ Resolved | MEDIUM (5) |
| 023 | Information Disclosure: Internal Service Hostname | ✘ Unresolved | LOW (3.7) |
| 004 | CSV Injection | ✘ Unresolved | LOW (3.5) |
| 003 | Documents Contain Metadata | ✘ Unresolved | LOW (3.1) |
| 006 | AI Chatbot: Guardrail Bypass | ✘ Unresolved | LOW (3.1) |
| 013 | Absent Content Security Policy | ✘ Unresolved | LOW (3.1) |
| 021 | Pagination Bypass: Bulk Transaction Exposure | ✘ Unresolved | LOW (3.1) |
| 010 | Missing Security Headers: Referrer-Policy | ✘ Unresolved | LOW (2.8) |
| 002 | Improper Output: Markdown Injection | ✔ Resolved | LOW (2.6) |

| # | Title | Status | Severity |
|---|---|---|---|
| 009 | Information Disclosure: HTTP Response Headers | ✗ Unresolved | INFO (0) |
| 016 | 2/3 Factors of the AI Lethal Trifecta | ☑ Partially Resolved | INFO (0) |
| 017 | AI Chatbot: System Prompt Disclosure | ✗ Unresolved | INFO (0) |
| 019 | Deprecated Header: X-XSS-Protection | ✗ Unresolved | INFO (0) |
| 026 | Insecure Direct Object Reference: Sequential Integer Identifiers | ✗ Unresolved | INFO (0) |

Table 2.1: Findings ordered by severity.