SECURITY ASSESSMENT REPORT

iamneo / examly Platform

manipal969.examly.io · admin.manipal969.examly.io

Prepared by: Ariet Jha

Date: April, 2026

Severity	Count
CRITICAL	6
HIGH	5
MEDIUM	5
INFO	4

1. Executive Summary

A security test was conducted on the iamneo/examly platform as deployed for [redacted]manipal969.examly.io). Testing was performed using passive reconnaissance, client-side analysis, and authenticated API probing. No destructive actions were taken, and no data was modified or exfiltrated.

The assessment revealed a significant number of high and critical severity vulnerabilities, several of which are platform-wide and affect every institution hosted on the iamneo/examly SaaS infrastructure — not just [redacted]. Most critically, production secrets including an [redacted]. These findings warrant immediate remediation and responsible disclosure to iamneo's security team.

Scope

Target	Description
manipal969.examly.io	Student exam/lab portal
admin.manipal969.examly.io	Admin management panel
api.examly.io	Backend API (tested indirectly)
examly-push.firebaseio.com	Firebase RTDB (tested)

2. Findings Summary

ID	Title	Severity	CVSS
F-01	[redacted]	CRITICAL	9.8
F-02	[redacted]	CRITICAL	9.5
F-03	[redacted]	CRITICAL	9.1
F-04	[redacted]	CRITICAL	8.8
F-05	[redacted]	CRITICAL	8.6
F-06	[redacted]	CRITICAL	8.4
F-07	[redacted]	HIGH	7.8
F-08	[redacted]	HIGH	7.5
F-09	[redacted]	HIGH	7.2
F-10	[redacted]	HIGH	6.5
F-11	[redacted]	HIGH	6.8
F-12	[redacted]	MEDIUM	5.9
F-13	[redacted]	MEDIUM	5.5
F-14	[redacted]	MEDIUM	4.8
F-15	[redacted]	MEDIUM	4.3
F-16	[redacted]	MEDIUM	4.1
F-17	[redacted]	INFO	N/A
F-18	robots.txt Allows Full Indexing	INFO	N/A
F-19	Wildcard TLS Cert *.examly.io — Shared Risk Surface	INFO	N/A
F-20	Microsoft Clarity Behavioral Tracking on Exam Platform	INFO	N/A

3. Detailed Findings

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4. Informational Findings

ID	Finding	Note
F-17	Platform is iamneo/examly SaaS, not Manipal-built	Confirmed via console log: 'ORg setted --> iamneo-production'. Findings affect all iamneo clients.
F-18	robots.txt allows full indexing (Disallow: empty)	Entire platform content is permitted for search engine indexing.
F-19	Wildcard TLS cert *.examly.io used across all subdomains	Certificate compromise would affect all institutions simultaneously.
F-20	Microsoft Clarity behavioral analytics active on exam platform	Session recording and heatmap data collected during exams.

5. Remediation Priority

The following remediation actions should be treated as immediate priorities given the severity of the exposed credentials and the platform-wide impact of these findings:

Priority	Action	Findings
P0 — Immediate	[redacted]	
P0 — Immediate	[redacted]	F-04
P1 — This Sprint	[redacted]	F-01 through F-09
P1 — This Sprint	[redacted]	F-05, F-11
P2 — Next Sprint	[redacted]	F-07
P2 — Next Sprint	[redacted]	F-13
P2 — Next Sprint	[redacted]	F-12
P3 — Backlog	[redacted]	

6. Methodology

This assessment was conducted using a grey-box approach with a valid student account on the platform. Testing was entirely non-destructive — no data was modified, deleted, or exfiltrated. All findings were identified through passive observation, client-side analysis, and limited authenticated API probing.

Phase	Techniques Used	Tools
Reconnaissance	Passive fingerprinting, technology detection, subdomain enumeration	Wappalyzer, subfinder, nmap, whatweb
Client-Side Analysis	JS bundle review, localStorage/sessionStorage inspection, JWT decoding	Browser DevTools, jwt.io
API Analysis	Network traffic inspection, endpoint mapping, header analysis	Browser DevTools Network tab, Burp Suite
Authentication Testing	JWT manipulation, Firebase API probing, user enumeration	curl, jwt.io
Directory Enumeration	Web path discovery on student and admin subdomains	dirsearch