

Security test report: Eko Fresh (fictional)

DMILZE EdTech practice file · Cybersecurity Basics · Week 7. Eko Fresh, its staff and its systems are invented. This is a sample of what a professional test report looks like, for learners to read and act on.

1. Executive summary

The overall risk to Eko Fresh is **high**. The most urgent problem is a customer database backup that anyone could download from the website (F-01). Four further high-risk issues (F-02 to F-05) would each let an outsider reach business systems or staff email. Most fixes are low cost and can be done within two weeks.

2. Scope and permission

Item	Detail
Authorised by	Managing Director, signed rules of engagement dated 2 March
In scope	www.ekofresh.example website, Ikeja branch office network, staff email settings
Out of scope	Payment provider systems, POS vendor cloud, staff personal devices, denial of service, social engineering
Test window	3 to 7 March, 09:00 to 17:00
Contacts	IT lead (day to day), Managing Director (escalation)

3. Method (summary)

Asset discovery and vulnerability scanning of in-scope systems, manual review of website and network configuration, and a check of email security settings. Testing stopped at proof that a weakness existed; no data was changed or deleted. Copies of the exposed data were deleted at the end of testing.

4. Findings

ID	Finding	Severity
F-01	Customer database backup file downloadable from the public website	Critical
F-02	Router admin page reachable from the internet with the factory password	High
F-03	Guest Wi-Fi on the same network as POS terminals and the file server	High
F-04	No multi-factor authentication on staff email	High
F-05	Website content system three years out of date	High
F-06	Stock app login sent over plain HTTP	Medium
F-07	One admin account shared by four staff	Medium
F-08	Error pages show software names and versions	Low

F-01: Customer database backup file downloadable from the public website **[Critical]**

What we found: A file named backup.zip in the website's main folder could be downloaded by anyone. It contained a copy of the customer database (names, phone numbers, delivery addresses).

Why it matters: Customer personal data exposed; likely a reportable breach under the NDPA.

Recommended fix: Remove the file now. Keep backups off the web server. Check web logs to see if anyone else downloaded it. Get legal advice on notification.

F-02: Router admin page reachable from the internet with the factory password **[High]**

What we found: The office router's admin page at the Ikeja branch answered from outside the network and accepted the default login printed on the device.

Why it matters: Anyone could change network settings, redirect traffic or lock staff out.

Recommended fix: Change the admin password, turn off remote admin, update router firmware.

F-03: Guest Wi-Fi on the same network as POS terminals and the file server [High]

What we found: A laptop on the guest Wi-Fi could see the POS terminals and the shared drive.

Why it matters: A customer's infected phone or a visitor could reach business systems.

Recommended fix: Put guests on a separate network that only reaches the internet.

F-04: No multi-factor authentication on staff email [High]

What we found: All 14 staff mailboxes use passwords only. Two staff passwords appear in public breach lists.

Why it matters: Phishing or reused passwords lead straight to email takeover and invoice fraud.

Recommended fix: Turn on app-based MFA for every mailbox; reset the two exposed passwords first.

F-05: Website content system three years out of date [High]

What we found: The online shop runs a content management version with several publicly known security flaws, and two out-of-date plugins.

Why it matters: Attackers routinely look for these versions; the site could be taken over.

Recommended fix: Update the system and plugins; remove unused plugins; turn on automatic updates.

F-06: Stock app login sent over plain HTTP [Medium]

What we found: The internal stock app login page does not use HTTPS, so passwords cross the network unencrypted.

Why it matters: Anyone on the same network could read staff passwords.

Recommended fix: Enable HTTPS on the stock app; change the passwords that were used.

F-07: One admin account shared by four staff [Medium]

What we found: The accounts system has a single 'admin' login known to four people.

Why it matters: No way to tell who made a change; ex-staff may still know the password.

Recommended fix: Give each person their own account with only the access they need; disable the shared one.

F-08: Error pages show software names and versions [Low]

What we found: Website error pages show the web server and language versions.

Why it matters: Helps an attacker pick known weaknesses.

Recommended fix: Turn off detailed error messages in production.

5. Positive observations

The main website uses HTTPS with a valid certificate. Laptops have disk encryption turned on. Staff reported a suspicious email to IT during the test window.

6. Next steps

Eko Fresh should agree a fix plan with owners and dates, then book a retest of every Critical and High finding.