Sri Lanka Institute of Information Technology

Cyber Security Assignment (2025)

Cryptographic Failures

Bug Bounty Report- 10

IT23363366

TABLE OF CONTENT

1. Title

Report Title: Cryptographic Failures
Reported By: Raahim Mahmooth
Platform: responsibly disclose
Tested On: topjobs.lk

2. Scope & Objective

This assessment examined how topjobs.lk protects sensitive information through cryptographic means. We reviewed the site's TLS/SSL configuration, the algorithms and protocols in use, and any evidence of encryption for data stored on the server. In parallel, we noted related account-management observations—specifically around registration and login—that touch on broken access control, so they are included here for awareness.

3. Enumeration and Reconnaissance

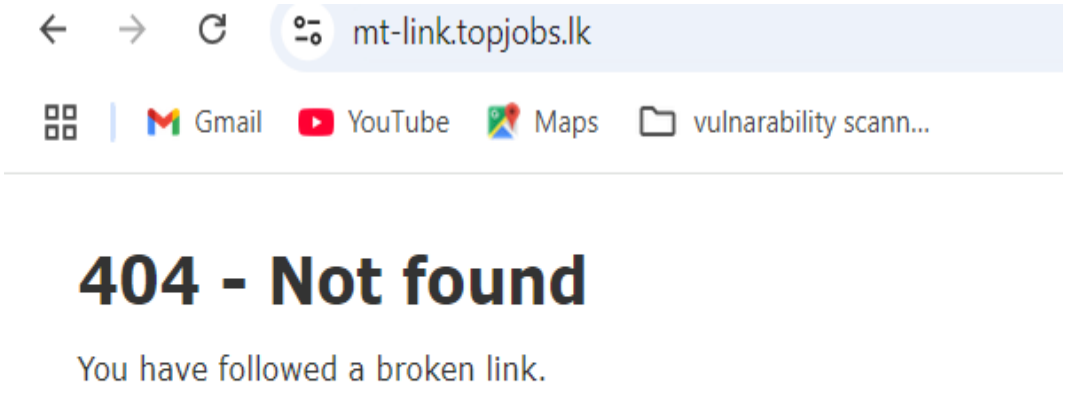
3.1 Tools Used

- **whois** for domain registration details
- **Sublist3r** for subdomain enumeration
- **Shodan** for exposed service discovery
- **SSL Labs** for TLS/SSL grading
- **Nikto** for web server scanning
- **Gobuster** for directory enumeration
- **sqlmap**

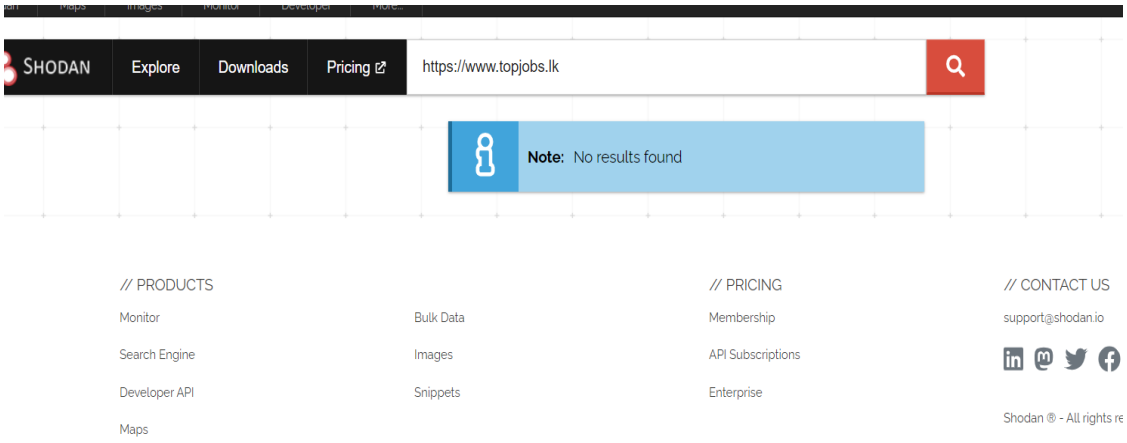
3.2 Steps Taken

Domain Lookup: *Retrieved registration and name-server information.*

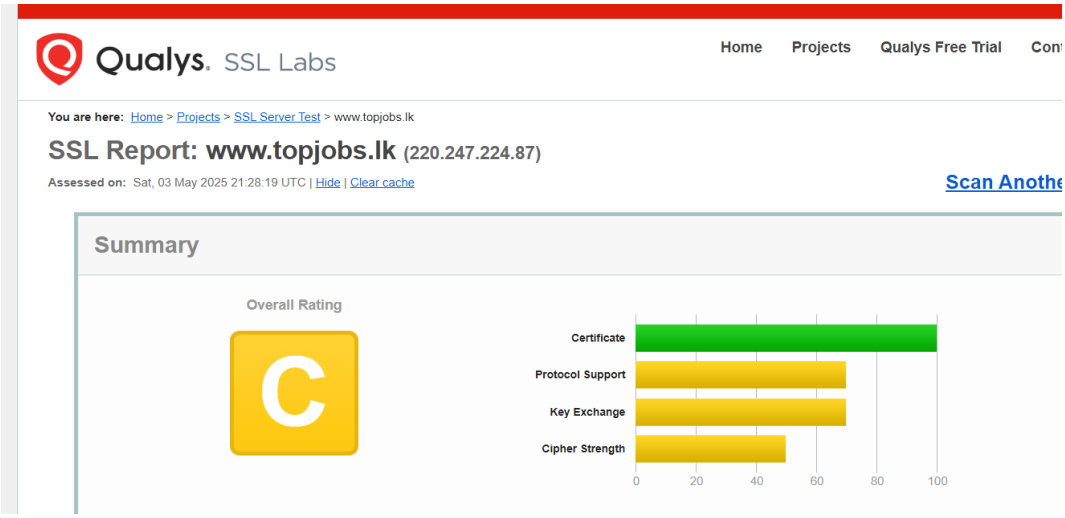
Subdomain Enumeration: *Found two subdomains via Sublist3r.*



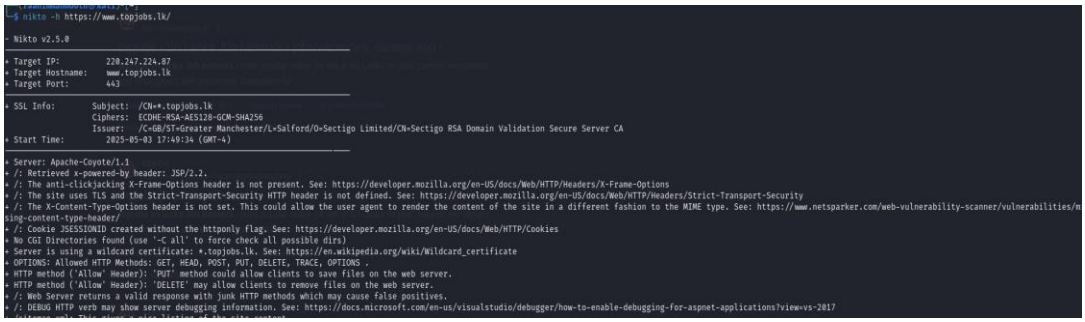
Shodan Search: *No additional exposed services located.*



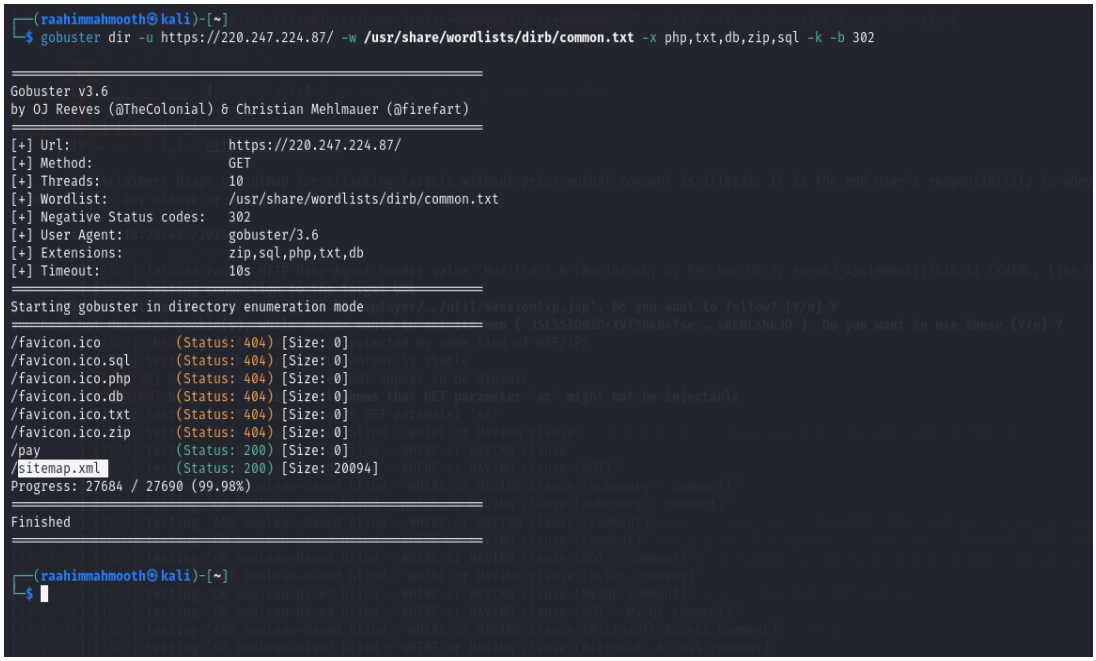
TLS/SSL Analysis: *SSL Labs graded the configuration as "C," indicating support for deprecated protocols (TLS 1.0/1.1) and weak cipher suites.*



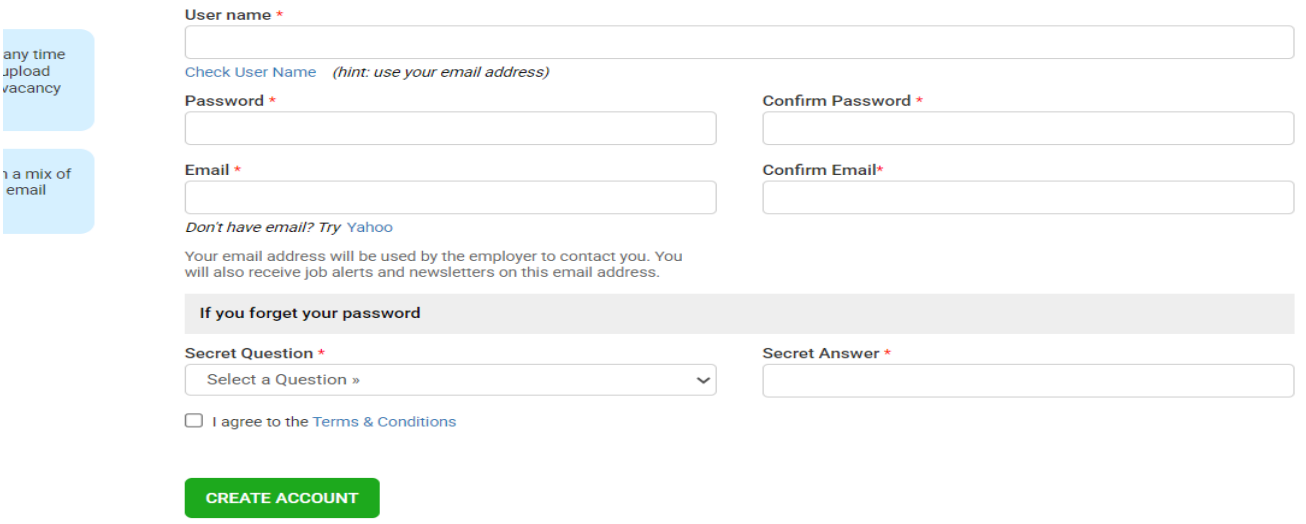
Server Scan: *Nikto scan did not identified critical SSL/TLS issues. No HTTP Strict Transport Security (HSTS) header is enforced*



Directory Enumeration: Gobuster revealed no hidden directories.



Manual Review of Authentication: *Observed account-management weaknesses (broken access control), noted below.*



4. Vulnerability Description

Cryptographic Failures (OWASP A02:2021):

- TLS configuration permits outdated protocol versions (1.0, 1.1) and weak ciphers (e.g. RC4).
- No HTTP Strict Transport Security (HSTS) header is enforced.
- No evidence of strong encryption for sensitive data at rest.

Broken Access Control (OWASP A01:2021) *(not primary scope but observed)*:

- Registration allows multiple accounts with the same email but different usernames.
- No email-verification step permits unverified accounts.
- Knowledge of a username alone allows login-style access flows that could be abused for impersonation.

5. Affected Component

- **TLS/SSL Configuration** on the web server
- **Employer Endpoint:** `https://www.topjobs.lk/employer/home.jsp?ac=0000000431&ec=0000000566`
- **Registration Logic** (duplicate-email, no verification)

6. Impact Assessment

Cryptographic Risks:

Because the server accepts TLS 1.0/1.1 and weak ciphers, an attacker positioned to intercept traffic could force a downgrade and decrypt sensitive information, including session tokens or user credentials. The absence of HSTS makes such downgrade attacks easier to execute. On the server side, any data stored without robust encryption (for example, user credentials or personal profiles) would be exposed in clear or weakly hashed form if the database were ever compromised.

Broken Access Control Risks:

The registration and login design flaws exacerbate these risks by allowing unverified or duplicate accounts and by enabling login flows without confirmed ownership of an email address. Together, these weaknesses could lead to account takeover, unauthorized data access, and further exploitation of the system.

Together, these issues can lead to account takeover, data leakage, and broader system compromise.

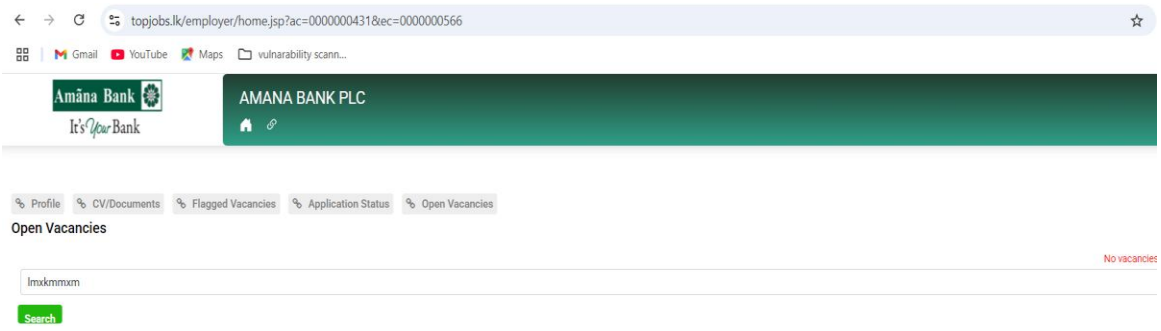
7. Proof of Concept (PoC)

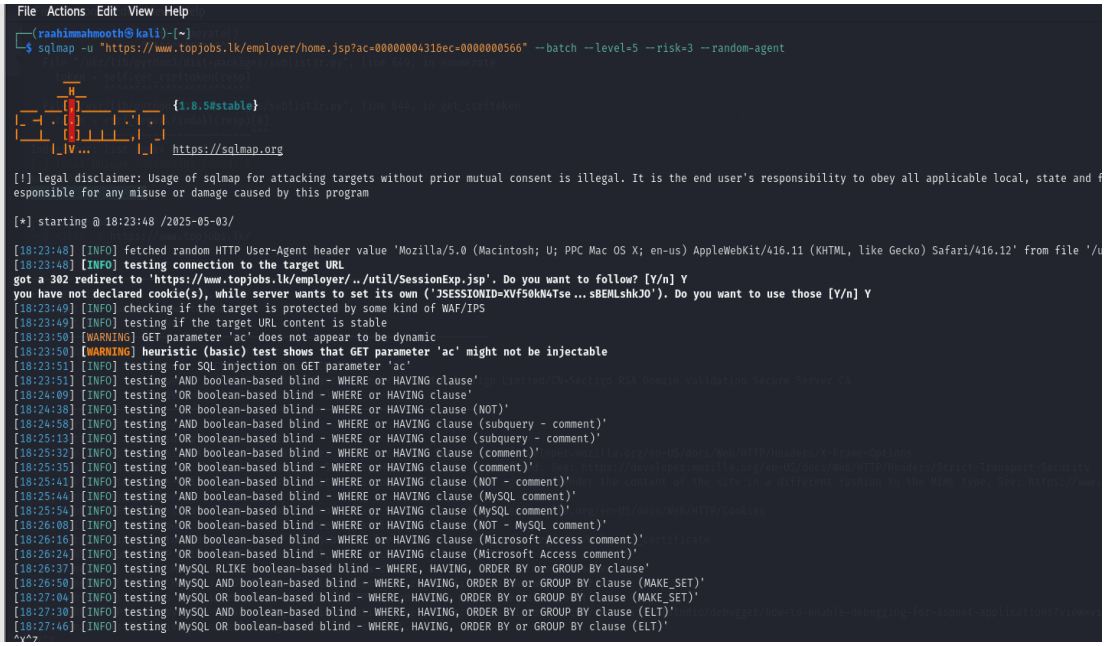
SSL Labs Report:

- Grade: C
- TLS 1.0/1.1 enabled, weak cipher suites accepted, no HSTS.

Manual Parameter Inspection and as part of responsible testing, the URL was tested with ***`sqlmap`***.

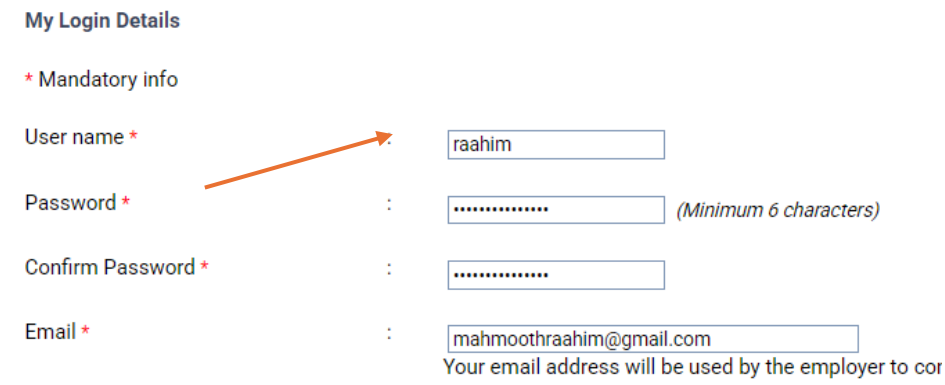
- Employer endpoint parameters (`ac`, `ec`) passed without integrity protections.

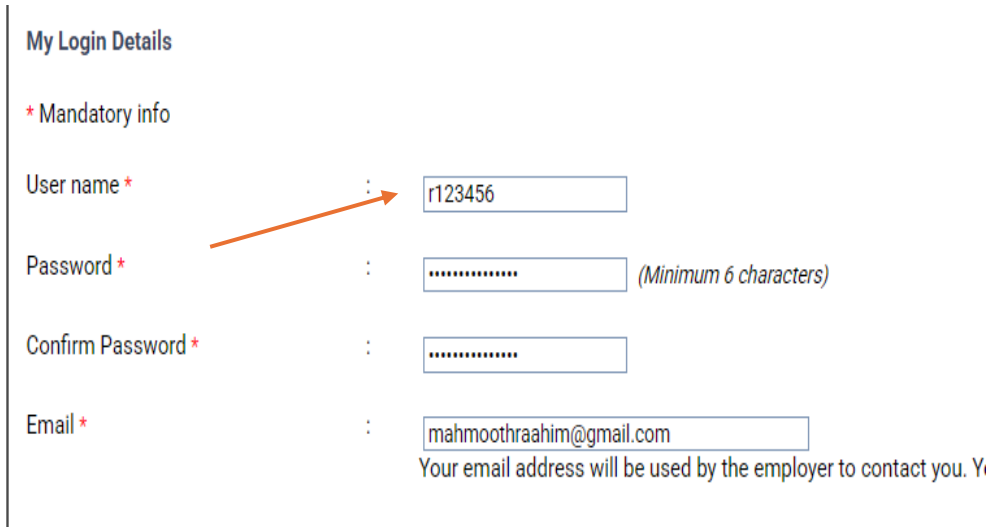




Registration Testing:

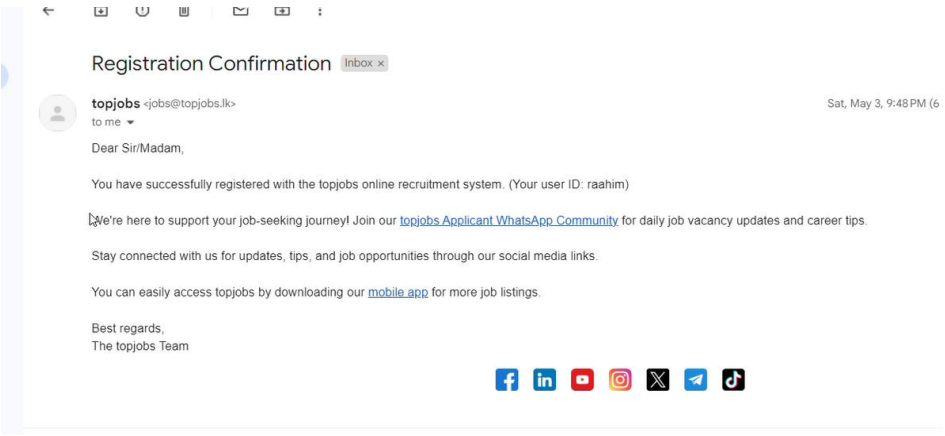
- Created two accounts using the **same email but different** usernames both succeeded without email verification.





Login Without Verification:

- Logging in with a known username triggers application flows even if the **email was never verified**.



- Created a account for one of my friend **without verification of email(with her permission)**

My CV/Document(s)

Document shown to	Document	Uploaded Time	View
-	-	-	-

My Common Profile

Your Common Profile is the base for profiles customised for each employer. Changes to your Common Profile will apply to all customised employer profiles. e.g. Updating your work experience, Perma

Create My Common Profile

My Login Details

* Mandatory info

User name * : hana_saleed

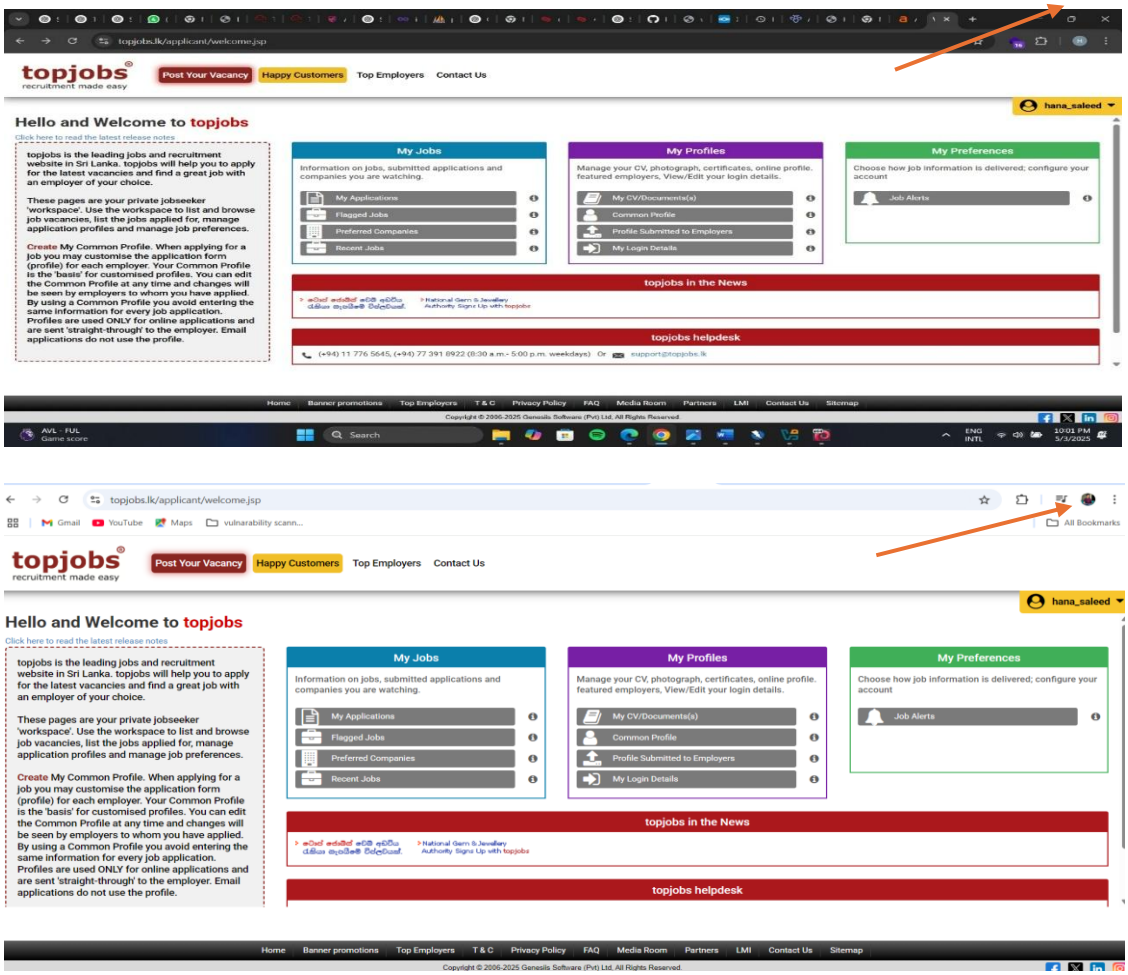
Password * : •••••••••• *(Minimum 6 characters)*

Confirm Password * : ••••••••••

Email * : hazure2312@gmail.com

Your email address will be used by the employer to contact you. You will also receive job alerts and newsletters on this email address.

***Concurrent Access**: No session restrictions; the same account can be used simultaneously on multiple devices.*



8. Proposed Mitigation

- **Harden TLS:** Disable TLS 1.0/1.1, permit only TLS 1.2+ with forward-secret ciphers, and enable HSTS.
- **Encrypt Data at Rest:** Use AES-256 (or stronger) with secure key management.
- **Integrity Protection:** Sign or MAC critical query parameters to prevent tampering.
- **Email Verification:** Enforce email confirmation before account activation.
- **Unique-Email Enforcement:** Prevent registration of multiple accounts with the same email.

9. Conclusion

Topjobs.lk exhibits **medium** cryptographic weaknesses and **critica**l broken access control issues. Strengthening TLS, encrypting stored data, and tightening **registration/login logic** will significantly improve overall security and protect user data from interception, tampering, and unauthorized access.

10. References

- OWASP A02:2021 – Cryptographic Failures
- OWASP A01:2021 – Broken Access Control