

Sri Lanka Institute of Information Technology



Cyber Security Assignment (2025)
Cryptographic Failures

Bug Bounty Report- 10
IT23363366

TABLE OF CONTENT

Title	3
Scope & Objective	3
Enumeration and Reconnaissance.....	3
Tools Used	3
Steps Taken	4
Vulnerability Description	7
Affected Component	7
Impact Assessment	7
Proof of Concept (PoC)	8
Proposed Mitigation	12
Conclusion	12
References	12

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.

```
File Actions Edit View Help
(raahimmahmooth@kali)~$ nslookup topjobs.lk
Server: 192.168.127.2
Address: 192.168.127.2#53

Non-authoritative answer:
Name: topjobs.lk
Address: 220.247.224.87
;; communications error to 192.168.127.2#53: timed out

(raahimmahmooth@kali)~$ whois topjob.lk
connect: Connection refused

(raahimmahmooth@kali)~$ whois https://www.topjobs.lk/
No whois server is known for this kind of object.

(raahimmahmooth@kali)~$ whois www.topjobs.lk
connect: Connection refused

(raahimmahmooth@kali)~$ whois 220.247.224.87

% [whois.apnic.net]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html
% Information related to '220.247.224.0 - 220.247.224.255'
% Abuse contact for '220.247.224.0 - 220.247.224.255' is 'abuse@slt.lk'

inetnum: 220.247.224.0 - 220.247.224.255
netname: SLTIDC-SLT-LK
descr: INTERNET DATA CENTER - SRI LANKA TELECOM
descr: DATA CENTER
descr: COLOMBO
country: LK
admin-c: AE70-AP
tech-c: AE70-AP
abuse-c: AL164-AP
status: ASSIGNED NON-PORTABLE
mnt-by: MNT-SLT-LK
mnt-irt: IRT-LKTELECOM-LK
last-modified: 2021-01-12T03:04:01Z
source: APNIC
```

Subdomain Enumeration: Found two subdomains via Sublist3r.

```
(raahimmahmooth@kali)~$ sublist3r -d topjobs.lk

Google
SUBLIST3R
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for topjobs.lk
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in Threatcrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Error: SSL certificate probably now is blocking our requests
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.12/multiprocessing/process.py", line 314, in _bootstrap
    self.run()
  File "/usr/lib/python3.12/multiprocessing/process.py", line 269, in run
    domain_list = self.enumerate()
  File "/usr/lib/python3.12/multiprocessing/process.py", line 649, in enumerate
    token = self.get_csrf_token(resp)
  File "/usr/lib/python3.12/multiprocessing/process.py", line 644, in get_csrf_token
    token = csrf_regex.findall(resp)[0]
IndexError: list index out of range
[-] Total Unique Subdomains Found: 2
mt-link.topjobs.lk
www.topjobs.lk

(raahimmahmooth@kali)~$
```

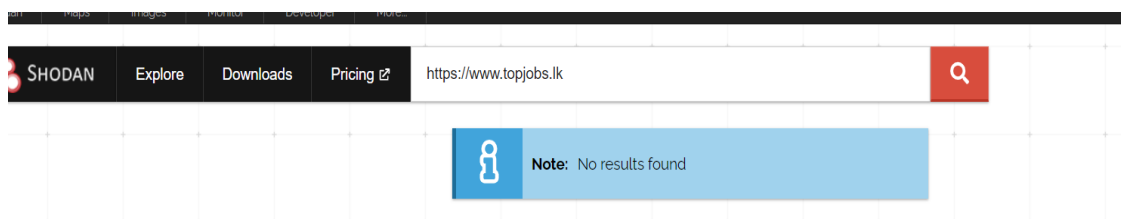
← → ↻ 🔍 mt-link.topjobs.lk

🗄️ | 📧 Gmail 📺 YouTube 📍 Maps 📁 vulnerability scann...

404 - Not found

You have followed a broken link.

Shodan Search: *No additional exposed services located.*



// PRODUCTS

Monitor

Search Engine

Developer API

Maps

Bulk Data

Images

Snippets

// PRICING

Membership

API Subscriptions

Enterprise

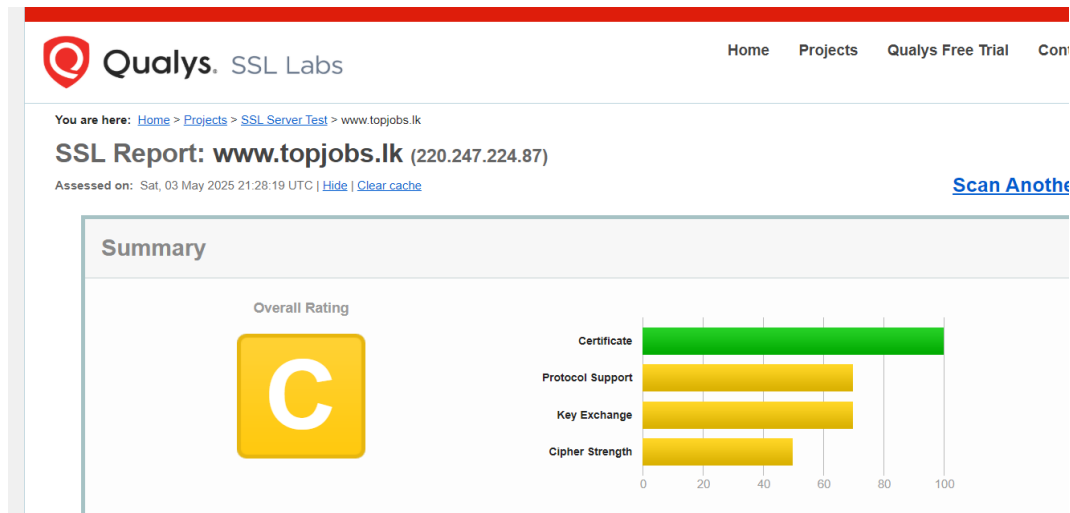
// CONTACT US

support@shodan.io



Shodan © - All rights reserved

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

```
nikto -h https://www.topjobs.lk/
- Nikto v2.5.0

+ Target IP: 220.247.224.87
+ Target Hostname: www.topjobs.lk
+ Target Port: 443

+ SSL Info: Subject: /CN=*.topjobs.lk
+ Ciphers: ECDHE-RSA-AES128-GCM-SHA256
+ Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo RSA Domain Validation Secure Server CA
+ Start Time: 2025-05-03 17:49:34 (GMT+4)

+ Server: Apache/2.4.18
+ /: Retrieved x-powered-by header: 3SP/2.2.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie JSESSIONID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI directories found (use '-C all' to force check all possible dirs)
+ Server is using a wildcard certificate: *.topjobs.lk. See: https://en.wikipedia.org/wiki/Wildcard_certificate
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
+ HTTP method ('Allow' header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' header): 'DELETE' may allow clients to remove files on the web server.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.microsoft.com/en-us/visualstudio/debugger/how-to-enable-debugging-for-aspnet-applications?view=vs-2017
```

Directory Enumeration: Gobuster revealed no hidden directories.

```
(raahimhath@kali)-[~]
$ gobuster dir -u https://220.247.224.87/ -w /usr/share/wordlists/dirb/common.txt -x php,txt,db,zip,sql -k -b 302

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@fireart)

[+] Url: https://220.247.224.87/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 302
[+] User Agent: gobuster/3.6
[+] Extensions: zip,sql,php,txt,db
[+] Timeout: 10s

Starting gobuster in directory enumeration mode
+-----+-----+-----+-----+-----+-----+
+ /favicon.ico (Status: 404) [Size: 0]
+ /favicon.ico.sql (Status: 404) [Size: 0]
+ /favicon.ico.php (Status: 404) [Size: 0]
+ /favicon.ico.db (Status: 404) [Size: 0]
+ /favicon.ico.txt (Status: 404) [Size: 0]
+ /favicon.ico.zip (Status: 404) [Size: 0]
+ /pay (Status: 200) [Size: 0]
+ /sitemap.xml (Status: 200) [Size: 20094]
Progress: 27684 / 27690 (99.98%)

Finished

(raahimhath@kali)-[~]
```

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

any time
upload
vacancy

1 a mix of
email

User name *

Check User Name (hint: use your email address)

Password *

Confirm Password *

Email *

Confirm Email *

Don't have email? Try [Yahoo](#)

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

If you forget your password

Secret Question *

Select a Question »

Secret Answer *

☐ I agree to the [Terms & Conditions](#)

CREATE ACCOUNT

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.



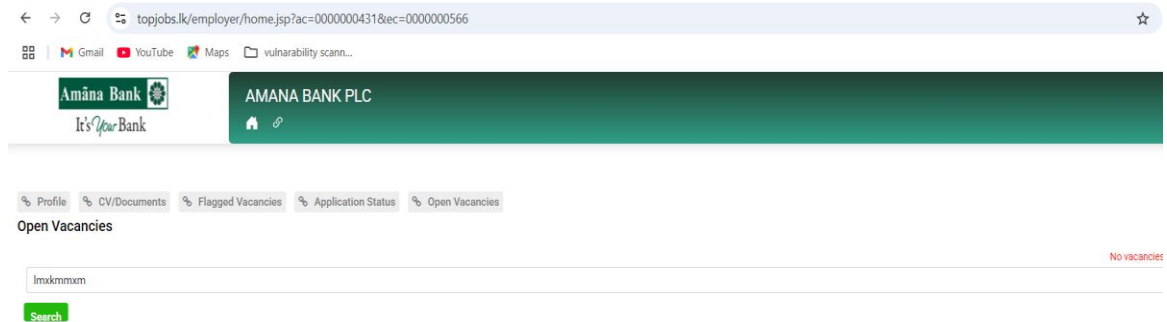
The screenshot displays an SSL Labs report interface. The 'Protocols' section shows TLS 1.3, 1.2, 1.1, and 1.0 as 'Yes', while SSL 3 and 2 are 'No'. The 'Cipher Suites' section is expanded for TLS 1.2, listing 16 suites, all marked as 'WEAK'. The bottom of the image shows the beginning of the TLS 1.1 section.

Protocols	
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites	
# TLS 1.2 (server has no preference)	
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	WEAK 112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 1024 bits FS WEAK 112
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH sec571r1 (eq. 15360 bits RSA) FS WEAK 112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK 128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits FS WEAK 128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH sec571r1 (eq. 15360 bits RSA) FS WEAK 128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK 128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 1024 bits FS WEAK 128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH sec571r1 (eq. 15360 bits RSA) FS WEAK 128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK 128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 1024 bits FS WEAK 128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH sec571r1 (eq. 15360 bits RSA) FS WEAK 128
# TLS 1.1 (server has no preference)	

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

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



```
File Actions Edit View Help
[raahimamhooth@kali:~]
$ sqlmap -u "https://www.topjobs.lk/employer/home.jsp?ac=000000431&ec=000000566" --batch --level=5 --risk=3 --random-agent

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws.
[*] starting @ 18:23:48 /2025-05-03/

[18:23:48] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/416.11 (KHTML, like Gecko) Safari/416.12' from file '/usr/share/sqlmap/user-agents/ie6.0sp1.txt'
[18:23:48] [INFO] testing connection to the target URL
got a 302 redirect to 'https://www.topjobs.lk/employer/./util/SessionExp.jsp'. Do you want to follow? [Y/n] Y
you have not declared cookie(s), while server wants to set its own ('JSESSIONID=XVF50kU4Tse...sBEMLshAJO'). Do you want to use those [Y/n] Y
[18:23:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[18:23:49] [INFO] testing if the target URL content is stable
[18:23:50] [WARNING] GET parameter 'ac' does not appear to be dynamic
[18:23:50] [WARNING] heuristic (basic) test shows that GET parameter 'ac' might not be injectable
[18:23:51] [INFO] testing for SQL injection on GET parameter 'ac'
[18:23:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:24:09] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[18:24:38] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[18:24:58] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[18:25:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[18:25:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[18:25:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[18:25:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[18:25:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[18:25:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[18:25:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[18:25:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[18:25:13] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[18:25:13] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[18:25:13] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[18:25:13] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[18:25:13] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[18:25:13] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
```

Registration Testing:

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

My Login Details

* Mandatory info

User name * : raahim

Password * : (Minimum 6 characters)

Confirm Password * :

Email * : mahmoothraahim@gmail.com
Your email address will be used by the employer to cor

My Login Details

* Mandatory info

User name * : r123456

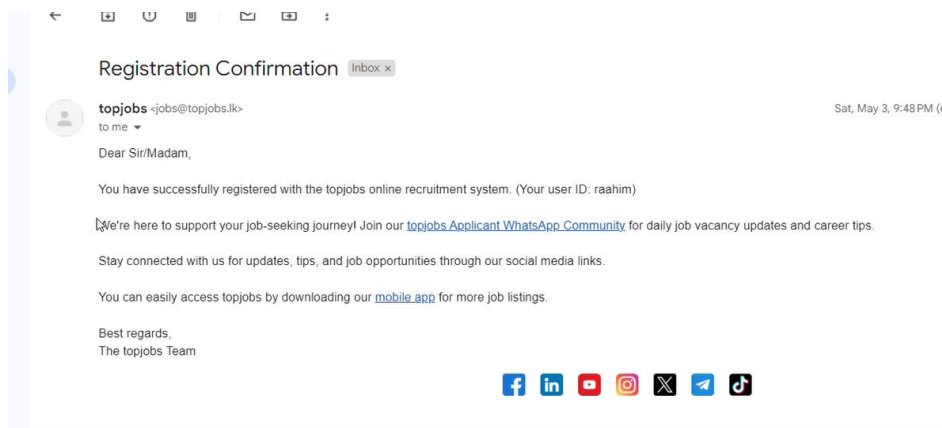
Password * : (Minimum 6 characters)

Confirm Password * :

Email * : mahmoothraahim@gmail.com
Your email address will be used by the employer to contact you. Y

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

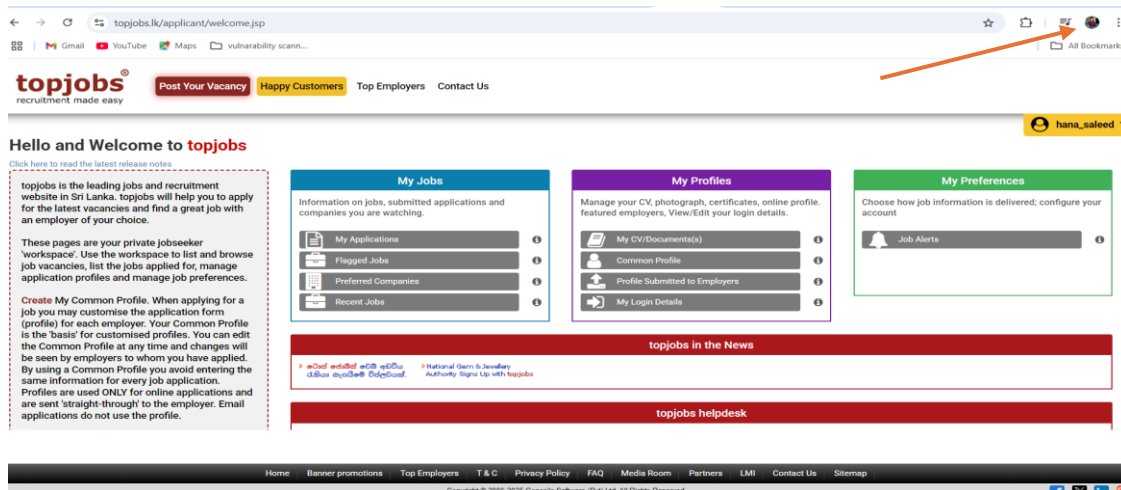
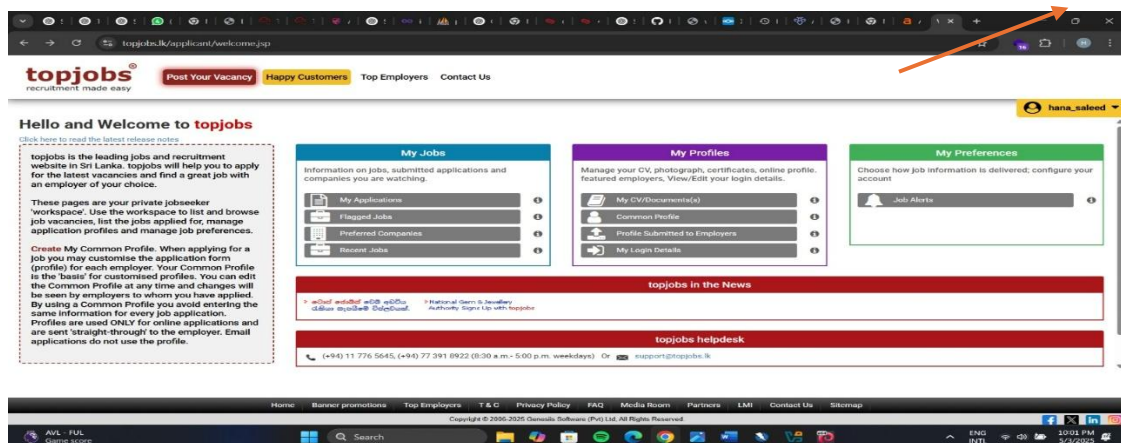
User name * :

Password * : (Minimum 6 characters)

Confirm Password * :

Email * :
 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 **critical** 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](#)