

QuantumShield Report

Target: <https://islamiacollege.edu.in>

Risk Level: LOW

LOW RISK — No Shor-vulnerable algorithms detected

Component Analysis:

- TLS 1.3 — Modern

Recommended Fixes:

Sample Kyber Code (Key Exchange):

```
from oqs import KeyEncapsulation

kem = KeyEncapsulation("Kyber512")
public_key = kem.generate_keypair()
ciphertext, shared_secret = kem.encap_secret(public_key)
# Use shared_secret for symmetric encryption (AES-256)
```

Sample Dilithium Code (Signature):

```
from oqs import Signature

sig = Signature("Dilithium2")
public_key = sig.generate_keypair()
message = b"Hello quantum-safe world"
signature = sig.sign(message)
# Verify: sig.verify(message, signature)
```

Generated by QuantumShield — Prepare for the quantum era