QuantumShield Report

Target: https://iust.ac.in
Risk Level: POST QUANTUM CRYPTOGRAPHY
POST QUANTUM CRYPTOGRAPHY RISK — Shor-vulnerable components detected

Component Analysis:

• Certificate signature: ECC (ECDSA) — Shor-vulnerable
• Certificate signature: RSA — Shor-vulnerable
• Key exchange: Classical ECC (X25519/ECDH) — Shor-vulnerable
• TLS < 1.3 — Outdated

Recommended Fixes:

• Replace ECC signature with Dilithium (ML-DSA)
• Replace RSA signature with Dilithium (ML-DSA)
• Replace key exchange with Kyber/ML-KEM hybrid
• Upgrade to TLS 1.3

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