QuantumShield Report

Target: https://google.com
Risk Level: LONG TERM POST QUANTUM CRYPTOGRAPHY
LONG TERM POST QUANTUM CRYPTOGRAPHY RISK — Shor-vulnerable components detected

Component Analysis:

• Certificate signature: ECC (ECDSA) — Shor-vulnerable
• Certificate signature: RSA — Shor-vulnerable
• Key exchange: Hybrid PQC (Kyber/ML-KEM) — Quantum-safe
• TLS 1.3 — Modern

Recommended Fixes:

• Replace ECC signature with Dilithium (ML-DSA)
• Replace RSA signature with Dilithium (ML-DSA)
• Key exchange already quantum-safe — keep it!

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