What Works / What's Next

WHAT WORKS

End-to-End Functionality

The system successfully provides a complete, working vertical slice:

- HTTPS server running inside Docker
- Secure image upload workflow: client → HTTPS → validation → storage → retrieval
- Filename sanitization to prevent traversal
- MIME-type checking to block invalid or malicious uploads
- Dedicated restricted /photos storage directory
- Server runs as a non-root user inside the container
- Automated demo (make demo) verifying the flow end-to-end

Testing and CI

- Unit tests covering core utilities (sanitization, MIME detection)
- Integration tests validating upload behavior
- GitHub Actions CI builds, tests, and uploads coverage
- Coverage generated via gcov

Observability and Evidence

- Logging of server operations
- Metrics exported in JSON
- Evidence stored in artifacts/release/

Security Enhancements Implemented

- HTTPS-only communication
- Non-root container execution
- Input and filename sanitization
- Minimal storage permissions

WHAT DIDN'T MAKE IT INTO THIS RELEASE

PF Firewall Rules for DDoS Mitigation

PF is not supported on Linux/WSL/Docker environments. Future work may include application rate limiting or nftables.

chroot() for Additional Isolation

Chroot requires root privileges and Docker already provides filesystem isolation, so it was not implemented.

WHAT'S NEXT

Additional Hardening

- Add rate limiting

Expanded Evaluation

- Larger datasets
- Performance and latency tests
- Reject-case analysis

Documentation and User Experience

- Final architecture diagrams
- More troubleshooting detail