COMP.SEC.300
Exercise Work Presentation
Symmetric Searchable Encryption

Anmol Arora

anmol.arora@tuni.fi

Overview

- Enable secure keyword search over encrypted data
- Python (Flask), SQLite, HTML/CSS
- Deployed with Docker

Key Features:

- Upload plaintext files via web UI
- Encrypt files and store securely
- Keyword search over encrypted content
- Fast and privacy-preserving query handling

Security Focus

- No plaintext storage of sensitive data
- Key derived from client's IP for demo purposes
- AES-CFB encryption with random IV
- Same file upload prevented using content based hash
- File size limit 1Mb
- Only TXT files allowed
- Secure_filename used to prevent upload vulnerabilities

Vulnerability scanning

- SONAR code coverage – 1 Code smell, 0 bugs, 0 vulns
- Trivy Filesystem + Docker image scan – No CRITICAL or HIGH vulnerability
- Docker scout via DockerHub – No CRITICAL or HIGH vulnerability (26 Low)
- DAST-OWASP ZAP – Pass 55, Fail 0

Manual Testing and Fixes

- Possible to upload same file again and again – Content based hash
- No check if request comes from specified user – CSRFProtect
- Insecure filename or filename with '..' or '//' – secure_filename utility
- SQL injection in search section – Static queries run on database, user input not embedded in queries
- Corrupt db with huge file upload – 1Mb size limit on upload
- Upload more than one file at once – Form allows one file at a time only

Demo / Questions?