🔒 Security Policy - TruthLens

Supported Versions

Version	Supported
1.x.x	:white_check_mark:
< 1.0	:x:

Reporting a Vulnerability

If you discover a security vulnerability, please report it by emailing:
102012dl@gmail.com

Please include:
- Description of the vulnerability
- Steps to reproduce
- Potential impact
- Suggested fix (if any)

Security Measures

1. Authentication & Authorization

- JWT-based authentication
- bcrypt password hashing
- Rate limiting on auth endpoints
- Session management with Redis

2. Input Validation

- Pydantic models for request validation
- SQL injection prevention via SQLAlchemy ORM
- XSS prevention with input sanitization
- CSRF protection

3. API Security

- API key authentication
- Rate limiting (per IP, per user)
- Request size limits
- CORS configuration

4. Data Protection

- HTTPS/TLS encryption
- Sensitive data encryption at rest
- PII anonymization in logs

- GDPR compliance

5. Infrastructure Security

- Non-root Docker containers
- Secrets management (env vars)
- Container vulnerability scanning
- Network isolation

6. Monitoring & Logging

- Security event logging
- Anomaly detection
- Audit trails
- Incident response procedures

Security Headers

```
SECURITY_HEADERS = {
    "X-Content-Type-Options": "nosniff",
    "X-Frame-Options": "DENY",
    "X-XSS-Protection": "1; mode=block",
    "Strict-Transport-Security": "max-age=31536000; includeSubDomains",
    "Content-Security-Policy": "default-src 'self'",
    "Referrer-Policy": "strict-origin-when-cross-origin"
}
```

Dependency Security

- Regular dependency updates
- Automated vulnerability scanning (Snyk, Dependabot)
- License compliance checking

Compliance

- GDPR (General Data Protection Regulation)
- OWASP Top 10 mitigations
- SOC 2 Type II (planned)