**URL Scanner Project Structure**

**url\_scanner/**

**├── app/**

**│ ├── \_\_init\_\_.py**

**│ ├── main.py done✅ # FastAPI application entry point**

**│ ├── config.py done✅ # Configuration settings**

**│ ├── database.py done✅ # Database connection and models**

**│ ├── auth.py done✅ # Authentication and authorization**

**│ ├── models/**

**│ │ ├── \_\_init\_\_.py**

**│ │ ├── user.py done✅ # User model**

**│ │ ├── scan.py done✅ # Scan task model**

**│ │ └── vulnerability.py done✅ # Vulnerability model**

**│ ├── scanners/**

**│ │ ├── \_\_init\_\_.py**

**│ │ ├── base.py # Base scanner class**

**│ │ ├── http\_client.py done✅ # HTTP client with security features**

**│ │ ├── owasp/**

**│ │ │ ├── \_\_init\_\_.py**

**│ │ │ ├── a01\_broken\_access.py**

**│ │ │ ├── a02\_crypto\_failures.py**

**│ │ │ ├── a03\_injection.py**

**│ │ │ ├── a04\_insecure\_design.py**

**│ │ │ ├── a05\_security\_misconfig.py**

**│ │ │ ├── a06\_vulnerable\_components.py**

**│ │ │ ├── a07\_auth\_failures.py**

**│ │ │ ├── a08\_integrity\_failures.py**

**│ │ │ ├── a09\_logging\_monitoring.py**

**│ │ │ └── a10\_ssrf.py**

**│ │ └── scanner\_engine.py done ✅# Main scanner orchestrator**

**│ ├── api/**

**│ │ ├── \_\_init\_\_.py**

**│ │ ├── auth.py # Authentication endpoints**

**│ │ ├── scans.py # Scan management endpoints**

**│ │ └── users.py # User management endpoints**

**│ ├── services/**

**│ │ ├── \_\_init\_\_.py**

**│ │ ├── ptaas\_manager.py # PTaaS service management**

**│ │ ├── report\_generator.py # Report generation**

**│ │ └── notification.py # Notification service**

**│ └── utils/**

**│ ├── \_\_init\_\_.py**

**│ ├── rate\_limiter.py # Rate limiting utilities**

**│ ├── validators.py done✅ # URL and input validation**

**│ └── helpers.py # General helper functions**

**├── tests/**

**│ ├── \_\_init\_\_.py**

**│ ├── test\_scanners.py**

**│ ├── test\_api.py**

**│ └── test\_auth.py**

**├── docker/**

**│ ├── Dockerfile**

**│ └── docker-compose.yml**

**├── deployment/**

**│ ├── k8s/**

**│ │ ├── deployment.yaml**

**│ │ ├── service.yaml**

**│ │ └── ingress.yaml**

**│ └── monitoring/**

**│ ├── prometheus.yml**

**│ └── grafana-dashboard.json**

**├── requirements.txt**

**├── .env.example**

**├── .gitignore**

**├── README.md**

**└── run.py # Local development runner**

**Key Components Overview**

**Core Features**

* **FastAPI-based REST API with async support**
* **PostgreSQL database with SQLAlchemy ORM**
* **JWT authentication with role-based access**
* **Modular OWASP Top 10 scanners**
* **PTaaS subscription management**
* **Comprehensive reporting system**
* **Rate limiting and security controls**
* **Docker containerization**
* **Kubernetes deployment ready**

**Scanner Modules**

**Each OWASP category has a dedicated scanner implementing:**

* **Static analysis techniques**
* **Payload testing**
* **Pattern recognition**
* **Vulnerability classification**
* **Evidence collection**

**API Endpoints**

* **/api/v1/auth/\* - Authentication management**
* **/api/v1/scans/\* - Scan operations**
* **/api/v1/users/\* - User management**