Security Backend Engineer Roadmap (Beginner → Job-Ready)

Phase 0 — Mindset & Foundations (Month 0–1)

- Programming basics (Python)
- Git & CLI
- Linux basics
- HTTP & networking fundamentals

Mini-projects:

- Simple Flask “Hello World” API
- Push to GitHub

Phase 1 — Backend Skills (Month 1–3)

- Flask or FastAPI
- SQL & NoSQL (Postgres, MongoDB)
- ORM (SQLAlchemy)
- JWT auth & session management
- API routing & versioning
- Docker basics

Mini-projects:

- User auth system (login/register/roles)
- CRUD REST API
- Dockerized Flask app

Phase 2 — Security Fundamentals (Month 3–4)

- OWASP Top 10 (Injection, Auth, Sensitive Data)
- Input validation (Pydantic/Marshmallow)
- Password hashing (bcrypt, Argon2)
- CORS, CSRF, rate limiting
- HTTPS & TLS
- Secure config & secrets management

Mini-projects:

- Harden Flask API (JWT + RBAC + input validation)
- HTTPS via NGINX + Certbot

- Rate limiting & logging

Phase 3 — Server & Infrastructure (Month 4–6)

- Linux server hardening (SSH keys, firewall, permissions)
- NGINX reverse proxy
- Docker + Docker Compose
- Postgres + Redis in Docker
- CI/CD basics (GitHub Actions)

Mini-projects:

- Full backend stack (Flask + Postgres + Redis + NGINX)
- Hardened server (fail2ban, SSH keys, firewall rules)
- Deploy stack locally or on AWS EC2

Phase 4 — Cloud & Monitoring (Month 6–8)

- AWS EC2, VPC, Security Groups
- IAM (least privilege)
- Cloud logging / monitoring (CloudWatch, ELK)
- S3 & secure storage
- Automating deployment pipelines

Mini-projects:

- Deploy secure backend stack on AWS
- Lock down IAM roles & VPC
- Monitoring & logging setup

Phase 5 — Attack Your Own Apps & Servers (Month 8–10)

- Nmap, Nikto, Gobuster
- BurpSuite basics
- SQL injection, XSS, JWT tampering
- Directory traversal, broken auth
- Patch & document vulnerabilities

Mini-projects:

- Scan own servers & APIs
- Exploit & fix vulnerabilities
- “Attack → fix” reports

Phase 6 — Advanced Security + DevSecOps (Month 10–12)

- Automated CI/CD scans (dependency & container scanning)
- Docker security & hardened images
- Static & dynamic analysis (SAST / DAST)
- Threat modeling & secure coding
- Logging & alerting

Mini-projects:

- Secure CI/CD pipeline
- Harden Docker images
- Threat model Flask API

Phase 7 — Portfolio & Job Prep (Month 12–15)

- Full secure backend projects (Flask + DB + Redis + NGINX + CI/CD)
- Hardened cloud server deployment
- Vulnerability reports & documentation
- Logging dashboards

Optional Certs:

- Security+
- eJPT
- AWS Developer / Security Specialty

Phase 8 — Apply for Jobs (Month 15+)

Target Roles:

- Junior/Security Backend Engineer
- Junior DevSecOps
- Application Security Engineer (backend)
- Cloud Security Engineer

Pro Tips:

- Emphasize “I built secure backend servers from scratch”
- Show “attack → fix” writeups
- Strong GitHub + LinkedIn presence
- Know OWASP Top 10 cold