AJAY ANANDAN

+91 7358300538 · ajayanandan072007@gmail.com · Chennai, Tamil Nadu
linkedin.com/in/ajayanandan747 · github.com/AjayAnandan07

PROFESSIONAL SUMMARY

Offensive-security-focused B.Sc. Computer Science student who built a production-grade C2 framework with AES-128 encryption and anti-sandbox evasion at internship, trained a 164K-email phishing detection model achieving 97.97% accuracy, and solved 31 CTF challenges across Web Exploitation and Forensics covering SQLi, SSTI, IDOR, and rate-limit bypass. Combines hands-on red-team depth with Python-driven secure development — seeking roles in penetration testing, security engineering, or vulnerability research.

EDUCATION

B.Sc. Computer Science

Prince Shri Venkateshwara Arts and Science College, Chennai · 2024 – 2027 · CGPA: 8.09 / 10 · Expected Graduation: April 2027

INTERNSHIP EXPERIENCE

Cyber Security Intern — Femtosoft Technologies

Dec 12, 2025 – Jan 12, 2026 · On-site, Chennai

› Designed and built NightShade, an encrypted C2 framework (AES-128) for authorized offensive security research — implementing anti-sandbox detection via RAM/CPU/process fingerprinting, Windows registry persistence, and stealth self-sanitization modules.

› Researched real-world red-team attack techniques including payload evasion, process injection, and forensic countermeasures to document defenses against advanced persistent threats.

› Implemented modular architecture separating C2 server, agent, and encryption layer — enabling controlled lab testing of attacker TTPs without live deployment risk.

Cyber Security Intern — Thiranex

Jun 1, 2026 – Jul 1, 2026 · Remote · All projects: github.com/AjayAnandan07

› Built a production-grade secure login system (Flask + Argon2 + SQLAlchemy) with CSRF protection, brute-force rate limiting, account lockout, and Blueprint-based modular architecture — deployable with zero known injection or session vulnerabilities.

› Trained a phishing email detection model (Random Forest + TF-IDF) on 164,000+ emails achieving 97.97% accuracy — extracting URL patterns, sender metadata, and header anomalies for classification.

› Developed a port and vulnerability scanner integrating the NVD API to cross-reference detected software versions against live CVE feeds — generating structured PDF assessment reports via FPDF2.

› Built a password strength analyzer with entropy scoring, complexity enforcement, and breach-database reuse prevention — reducing weak credential risk at the point of account creation.

PROJECTS

NightShade — Offensive Security Research Tool Private Repository

Python, Flask, AES-128, Cryptography, pynput, mss

› Built encrypted C2 framework using AES-128 for authorized red-team lab research — simulating real attacker infrastructure in isolated environments.

› Implemented anti-sandbox evasion using RAM, CPU, and process-count fingerprinting to detect analysis environments before payload execution.

› Developed persistence (Windows registry), stealth execution, and self-sanitization modules — documenting each technique alongside its detection and mitigation.

RedChain-Kit — Automated Red Team Recon & Reporting github.com/AjayAnandan07/RedChain-Kit

Python, subprocess, nuclei, subfinder, httpx, katana, Flask, SQLite, FPDF2

› Built full kill-chain recon pipeline: subdomain discovery (subfinder + amass) → live host probing (httpx) → endpoint crawling (katana) → nuclei vulnerability scanning — single CLI command.

› Implemented regex-based exploit hint classifier flagging SQLi, IDOR, open redirect, path traversal, and exposed admin endpoints for manual follow-up testing.

› Generated dual-format output (PDF + HackerOne-ready Markdown) with CVSS severity scoring; Flask dashboard with SQLite history tracks attack surface changes over time.

Secure Login System github.com/AjayAnandan07/Secure-Login-System
Python, Flask, SQLAlchemy, Argon2, Flask-WTF, SQLite, Flask-Migrate

› Implemented Argon2id password hashing — memory-hard algorithm resistant to GPU and ASIC brute-force attacks.
› Eliminated SQL injection risk via parameterized queries through SQLAlchemy ORM; added CSRF tokens on all state-changing forms.
› Enforced brute-force protection with per-IP rate limiting, temporary account lockout, and secure cookie flags (HttpOnly, Secure, SameSite).

Phishing Email Detection Model github.com/AjayAnandan07/Phishing-Email-Detection-Model
Python, Scikit-learn, Pandas, TF-IDF, Random Forest

› Trained Random Forest classifier on 164,000+ emails achieving 97.97% accuracy — outperforming baseline Naive Bayes by 4.2 percentage points.
› Engineered features from URL patterns, keyword frequency (TF-IDF), sender domain reputation, and email header anomalies.
› Evaluated with confusion matrix, precision/recall/F1 — achieving 98.1% precision to minimize false positives in production.

Vulnerability Scanner github.com/AjayAnandan07/Vulnerability-Scanner
Python, Socket, Requests, NVD API, FPDF2

› Scanned targets for open ports and weak configurations — cross-referenced findings against NVD API CVEs; generated client-ready PDF reports with CVSS severity tiers.

Password Strength Analyzer github.com/AjayAnandan07/Password-Strength-Analyzer
Python, JavaScript, HTML/CSS

› Scored passwords using Shannon entropy, complexity checks, and pattern detection; integrated database layer to prevent credential reuse attacks.

CTF & COMPETITIONS

picoCTF picoGym — Web Exploitation & Forensics · 2026 · github.com/AjayAnandan07/CTF-Writeups

› Solved 31 challenges (23 Easy, 7 Medium, 1 Hard) across Web Exploitation and Forensics — all documented with full methodology in public writeup repository.
› Web Exploitation techniques: IDOR, PostgreSQL SQLi, SSTI → RCE, file upload bypass, rate-limit bypass via X-Forwarded-For spoofing, session hijacking, credential stuffing, SQLMap-based injection, authentication bypass, 2FA bypass, robots.txt recon, hash-based access control bypass, and HTTP header inspection.
› Forensics techniques: binary digit analysis, file corruption recovery, steganography (hidden in plain sight), registry-based artifact analysis, and disk image forensics (DISKO 1).
› Automated multi-step attacks using Python (requests, socket, hashlib) — demonstrating scripted recon and exploitation capability across challenge categories.

TECHNICAL SKILLS

Security Tools	Burp Suite, Metasploit, Nmap, Wireshark, Netcat, FFUF, nuclei, subfinder, httpx, katana
Languages	Python (primary), JavaScript, Java, HTML/CSS, Bash
Frameworks	Flask, FastAPI, SQLAlchemy, Flask-WTF, Scikit-learn, React
Security Concepts	Penetration Testing, Red Teaming, SIEM, IAM, Threat Intelligence, OSINT, Incident Response, Vulnerability Assessment
Networking	TCP/IP, Network Security, DNS, HTTP/S, Linux
Databases & Tools	SQLite, Git, GitHub, REST APIs, NVD API, FPDF2

CERTIFICATIONS & VIRTUAL INTERNSHIPS

› IBM — Cybersecurity Fundamentals (Dec 2025)
› IBM — Getting Started with Threat Intelligence and Hunting (Dec 2025)
› IBM — Getting Started with Cybersecurity (Dec 2025)
› Mastercard — Cybersecurity Job Simulation via Forage (Jun 2026)
› TCS — Cybersecurity Analyst Job Simulation via Forage (Jun 2026)