Praneesh R V

praneeshrv404@gmail.com • +91-6374028342 • PraneeshRV • LinkedIn • Team Hunter

SUMMARY

Cybersecurity undergraduate at Amrita Vishwa Vidyapeetham, focused on VAPT and agentic AI red teaming. Researching LLM exploitation techniques at TIFAC CORE and building AI-assisted security tooling. Competes with Team Hunter, a CTFtime Top-10 India team, and has organized and built CTF infrastructure for 200+ participants.

EDUCATION

Amrita Vishwa Vidyapeetham — **Coimbatore, India**
B.Tech in Computer Science – Cybersecurity | CGPA: 7.71 — *2023 – 2027*

Sishya School — **Hosur, India**
Class XII | 87% — *2023*

EXPERIENCE

AI Developer Intern — **Apr 2026 – Present**
Joy IT Solutions – Remote

- Building a recruitment agent platform with **C#, .NET, Azure DevOps, Azure Document Intelligence, and Azure OpenAI**.
- Implemented document ingestion and OCR flow for PDF/DOCX/image resumes, including raw text extraction, fallback OCR behavior, folder lifecycle handling, idempotency, and raw data lake writes.
- Integrated **Azure OpenAI GPT-4o** parsing to transform unstructured resume text into structured candidate profile JSON using canonical mapping and schema-driven processing.
- Added curated profile transformation for skills, experience, education, certifications, and languages, with tests for duplicate handling, optional sections, and parquet/data lake output.
- Worked with **Azure Key Vault-backed secrets**, bearer-token API testing, Azure Boards user stories, sprint tasks, PR-style development, and Swagger-based debugging.
- Working on browser-extension authentication and backend communication using **Azure B2C, OAuth 2.0 Authorization Code + PKCE, MSAL, access tokens, scopes, redirect URIs, and bearer-token API calls**.

Research Intern – AI Red Teaming — **2026**
Securin Research – TIFAC CORE in Cybersecurity, Amrita Vishwa Vidyapeetham

- Researched agentic AI red teaming across **MCP, A2A, memory poisoning, tool misuse, goal hijacking, JWT abuse, agent-card trust chains, and multi-agent orchestration risks**.
- Built OpenTelemetry/OpenInference proof-of-concepts for tracing LLM agent workflows using **LangChain, Jaeger, Arize Phoenix, and GPT-backed agents**.
- Contributed merged PRs to **Granzion Labs**, adding four attack scenarios: token forgery, agent-card forgery, orchestrator task queue poisoning, and delegation-loop abuse.

Core Organizer & Lead Infrastructure Engineer — **Dec 2025**
L3m0nCTF 2025 – Amrita Vishwa Vidyapeetham

- Operated **GCP**-hosted CTF infrastructure for a 24-hour onsite CTF with around **200 participants**.
- Customized and deployed **CTFd**, including the **Stargaze theme**, challenge imports, live scoring, submissions, and event operations.
- Managed Dockerized challenge packaging and authored challenges across **Web, OSINT, Forensics, and AI Security**.
- Designed AI security challenges covering shared-memory poisoning, prompt injection, JSON injection, and confused-deputy behavior in agent-to-agent workflows.

Competitive CTF Player — **2024 – Present**
Team Hunter – CTFtime Top-10 India Team

- Competed in **50+ national and international CTF competitions** across OSINT, forensics, web exploitation, crypto, and misc.
- Analyze artifacts, logs, source code, network traces, and web applications under time pressure to identify vulnerabilities and solve challenges.

PROJECTS

RedCalibur — **Python, FastAPI, Next.js, LLMs**

- Building an AI-assisted red teaming toolkit for reconnaissance, enumeration, vulnerability analysis, exploit research, and report generation.
- Integrated API-driven tooling and LLM-assisted analysis to automate repetitive VAPT and OSINT workflows for authorized security testing.

Agentic AI Security CTF Challenges — **Node.js, React, Docker, LLM Agents**

- Built AI-security CTF challenges covering prompt injection, shared-memory poisoning, JSON injection, confused-deputy behavior, and multi-agent trust-boundary failures.
- Designed Dockerized challenge environments with backend APIs, agent workflows, player-facing interfaces, and reproducible solve paths.

Personal Portfolio Website — **Next.js, TypeScript, React Three Fiber, Vercel**

- Built a production portfolio site with a cybersecurity-themed interactive 3D archive, custom UI sections for projects, skills, experience, certifications, CTF work, and resume access.
- Implemented SEO and production-readiness features including metadata, sitemap, robots, manifest, Open Graph/Twitter images, JSON-LD structured data, WebGL fallback, reduced-motion handling, and Vercel Analytics.

ACHIEVEMENTS

H7CTF 2025 — **SRMIST Chennai**

Finalist – Team Hunter — *2025*

- Qualified for onsite finals from a **2,500+ participant, 500+ team** online qualifier and secured **14th out of 30 finalist teams**.

KICTF – Yugam 2026 — **Kumaraguru Institutions**

Top-8 Finish and Best Write-up Winner — *2026*

- Placed in the top 8 and received best write-up recognition in a national CTF with **50+ teams** and **170+ participants**.

TECHNICAL SKILLS

Security:	Web Exploitation, Digital Forensics, OSINT, Cryptography, VAPT, CTF Challenge Design, Vulnerability Assessment
AI Security:	Agentic AI Red Teaming, Prompt Injection, Tool Misuse, MCP/A2A Security, LLM Tracing, OpenTelemetry, LLM Prompt Design
Cloud & IAM:	Azure DevOps, Azure Key Vault, Azure B2C, OAuth 2.0, PKCE, JWT, RBAC Concepts, Access Tokens, App Registrations
Tools:	Burp Suite, Wireshark, Metasploit, Docker, CTFd, Swagger, Git, Linux, Google Cloud Platform
Programming & Scripting:	Python, C#, JavaScript, TypeScript, Bash, REST APIs, JSON Mapping
Frameworks & Platforms:	.NET, FastAPI, Next.js, React, Azure Blob Storage, ADLS Gen2, Parquet Pipelines, Dockerized APIs

CERTIFICATIONS

- **PJPT** – Practical Junior Penetration Tester, TCM Security *(In Progress)*
- **Ethical Hacker** – Cisco • **NSE 1 & 2** – Fortinet • **Google Cybersecurity Professional Certificate** – Coursera

LANGUAGES & INTERESTS

Languages: Tamil (Native), English (Fluent), Hindi (Intermediate)
Interests: CTFs, Agentic AI, Linux Tooling, Arch Linux Ricing