AY

Aayush Yadav

Second-Year Undergraduate, Bennett University

Major: Computer Science Engineering | **Specialization:** Cybersecurity

aayushyadav.dev@gmail.com
linkedin.com/in/aayush-yadav-477028370
+91-7607102398
github.com/maverickaayush

Education

Year	Qualification	School / Institution
2025 – 2029 (Exp.)	B.Tech, Computer Science Engineering (Cybersecurity)	Bennett University
2024	XII (Intermediate)	Nalanda Academy
2022	X (Matriculation)	KV IIT Kanpur

Achievements & Recognition

- Reported **25 vulnerabilities** across ISRO (9), Meshery (2), Appwrite (2), Kickbacks.ai (2), DoIT (1), and Vercel/ESA via HackerOne and Intigriti (9, closed as duplicates of earlier reports); two Kickbacks.ai findings vendor-validated, one with a $100 reward.
- Ranked **Top 5% globally** on TryHackMe (Sapphire league, 124-day streak), including hands-on practice with CVE-2024-21413 (Moniker Link).
- ONUS, an open-source AI-assisted VAPT platform, is listed in OWASP's **Vulnerability Scanning Tools** directory.
- Selected for HackPrinceton Fall 2026.

Work Experience

Cybersecurity Project Intern
Jun '26 – Jul '26

Indian Institute of Technology, Kanpur (Computer Centre)

- Independently designed and built ONUS, a security-scanning platform, as a supervised two-month project under the Computer Centre's Chief Computer Engineer; later open-sourced it (see Projects).

Founder & CEO
Jul '25 – Present

Clinkl

- Lead a student-run team building an AI-powered adtech marketplace; designed the frontend and directed its launch.

Positions of Responsibility

Deputy Minister, Digital Infrastructure
Aug '26 – Present

SCSET Student Cabinet, Bennett University

- Direct digital-infrastructure initiatives for the student-led body overseeing all 24 technical clubs and chapters at Bennett University.

Technical Skills

Embedded & Bluetooth: BlueZ, HCI/L2CAP/RFCOMM/AVDTP/SDP/GATT, Ghidra (ARM/Thumb & Pi32v2), static firmware unpacking/analysis, UART/I2C/SPI exposure, Wireshark

Languages & Tools: C, Python, Kotlin, Bash, Java, TypeScript/JavaScript, SQL, Git/GitHub, Docker, GitHub Actions CI

Systems: Linux, Android (rooted/AOSP-level debugging), kernel-level Bluetooth bring-up

Security Tooling: OWASP ZAP, Nikto, Nuclei, Nmap, Burp Suite, CVSS v3.1

Relevant Courses

Microprocessors and Computer Architecture
Linux and Shell Programming
Data Structures using C++
Database Management Systems
Probability and Statistics

Key Projects

Bluetooth Earbud Firmware | Security Research
2026

Independent research · Ghidra, REA, JADX, Python · JieLi AC710N & BES2300 platforms

- Performed offline static analysis of 8 commercial TWS-earbud firmware images across two embedded Bluetooth SoC families; wrote a custom unpacker for one proprietary container format and imported application code into Ghidra for ARM/Thumb and vendor-DSP disassembly.
- Traced AVDTP, RFCOMM, SDP, and SPP protocol-handler code paths and identified several in-image memory-safety conditions (incl. a heap-overwrite from an undersized SPP event); explicitly flagged as confirmed application-code behavior, not demonstrated remote exploits, since no device was flashed and no live radio traffic was sent.
- Cross-checked companion Android app code (JADX) to map BLE/GATT transport and OTA handling; corroborated two findings with a second independent static-analysis pass.

M30 | Bluetooth Security Lab
Oct '26

Personal Project · github.com/maverickaayush/m30-security-lab · Kotlin, Python, C, Bash, BlueZ, Linux kernel

- Built a bounded-experiment lab on an owned Samsung phone (Android app plus Linux fixtures) to study standalone Bluetooth/HCI access, with hard caps on every test (e.g. scans stop at 30s or 500 records).
- Brought up a supervised Linux HCI path through the phone's SCSC Bluetooth controller (research kernel); validated LE scan and L2CAP echo across 3 Android-to-Linux-to-Android handoffs, incl. an instrumented 100/100 echo run confirmed by a second phone's HCI log.
- Traced a missing RFCOMM protocol to a commented-out kernel Makefile entry and analysed the vendor HAL in Ghidra, keeping an evidence ledger labelling each claim observed, inferred, or unsupported.

ONUS | AI-Assisted VAPT Platform
Jun '26 – Jul '26

Personal Project · github.com/maverickaayush/ONUS · FastAPI, PostgreSQL, Celery/Redis, Next.js, Docker, Ollama

- Architected a self-hosted, air-gapped VAPT platform running 8 parallel scanning modules against one normalized finding schema, with a deterministic CVSS v3.1 scoring engine covering 73 finding types verified across 690 pytest tests for byte-identical repeat scans.
- Designed a three-tier confidence stage (confirmed/probable/unverified), keeping AI-generated remediation prose fully isolated from scoring logic; migrated production to Oracle Cloud ARM64 behind a hardened Caddy reverse proxy with TLS.

Valsec | Network Compliance Auditor

Personal Project · github.com/maverickaayush/Valsec · FastAPI, PostgreSQL, Celery/Redis, Next.js, Docker

- Normalized Cisco IOS/IOS-XE, Juniper JunOS, and Fortinet FortiOS configs into one schema evaluated against CIS, NIST SP 800-53, DISA STIG, and ISO/IEC 27001, with authenticated CDP/LLDP discovery validated on real hardware (OpenWrt router, Cirotech appliance).

Open Source

Contributor, Meshery
CNCF project

github.com/meshery/meshery

- Contribute to Meshery's server, backend, and CI pipelines; Meshery is a cloud native management plane.
- Reported 2 security vulnerabilities to the project.