

Piyush Satyarthi

Cybersecurity | Web Application Security | Backend Development

casetted.work@gmail.com | github.com/PiyushSatyarthi | linkedin.com/in/piyush-satyarthi-257b53443

SUMMARY

BCA (Cybersecurity) student at Sharda University seeking junior penetration testing, VAPT internship, or web application security roles. Conducts independent web security research focused on access control, authentication, and business logic weaknesses, supported by Python and Bash reconnaissance automation. Built and deployed ZeroDay Care, a self-hosted cybersecurity training platform that runs sandboxed per-student vulnerable labs. Builds backend services (FastAPI, Flask, Express, MongoDB), configures Linux servers (Nginx, UFW, TLS), and develops AI retrieval applications.

EDUCATION

Sharda University

2025 – 2028

Bachelor of Computer Applications (BCA), Specialization in Cybersecurity

INDEPENDENT SECURITY RESEARCH

Web Application Security Research

Self-initiated

Independent study; not part of an employment, client engagement, or bug bounty program

- Observed Broken Object Level Authorization (BOLA/IDOR) issues on multiple websites that exposed other customers' email addresses and order histories (OWASP API1:2023, Broken Access Control).
- Observed business-logic and authentication weaknesses: price tampering caused by insufficient server-side validation, authentication bypass to protected functionality, and account takeover through referral-code functionality.
- Followed a reconnaissance workflow of subdomain enumeration, live-host discovery, and endpoint and parameter discovery, then manually validated automated scan output (Burp Suite, ffuf, Nuclei, Subfinder, httpx).
- Wrote Python and Bash scripts to automate reconnaissance and result collection. Affected sites and technical details are intentionally omitted.

TECHNICAL SKILLS

Hands-on (used in projects or research)

Web & API Security	Access-control testing (IDOR/BOLA), authentication and session logic testing, business-logic testing, REST API request analysis, parameter manipulation
Reconnaissance	Subdomain enumeration, live-host discovery, endpoint and parameter discovery with Subfinder, Amass, httpx, ffuf, Gobuster, Nuclei
Security Tooling	Burp Suite (Proxy, Repeater, Intruder, Decoder), cURL, Kali Linux, Python and Bash automation
Programming	Python, JavaScript, TypeScript, Bash, SQL; also C, C++, C#, HTML, CSS
Backend & Web	FastAPI, Flask, Node.js, Express, Uvicorn, REST APIs, Prisma, React, Vite, Streamlit
Data Stores	PostgreSQL, MongoDB, SQLite, Redis, Supabase, ChromaDB
Linux & Infrastructure	Ubuntu server administration, Nginx reverse proxy, Docker, gVisor, Cloudflare DNS, UFW, TLS/HTTPS, systemd, Microsoft Azure, Google Cloud, DigitalOcean, Git, GitHub
AI / ML	TensorFlow, Keras, CNNs, Ollama, SentenceTransformers, RAG and vector search, Random Forest, QSVM
Embedded	Arduino UNO R4 WiFi, ESP32; MQ-2, DHT22, PIR, and HC-SR04 sensors

Familiarity (studied, limited practical use)

Vulnerability Classes	SQL and NoSQL injection, XSS, SSRF, CSRF, CORS misconfiguration, file-upload flaws, cache poisoning, host-header attacks, race conditions, OAuth and JWT security, static Android analysis (APKTool, JADX)
------------------------------	--

Currently learning

Focus Areas	eJPT certification preparation, Active Directory, Kerberos and NTLM, Windows and Linux privilege escalation, cloud security assessment
--------------------	--

PROJECTS

ZeroDay Care: Self-Hosted Cybersecurity Training Platform

Next.js, FastAPI, PostgreSQL, Docker, gVisor

Personal project; live at zerodaycare.casotted.dev

- Built a CTF-style training platform where each student receives a private, disposable vulnerable lab: a Next.js and TypeScript frontend, a FastAPI, SQLAlchemy, PostgreSQL, and Redis backend, and a Docker lab orchestration service.
- Authored and integrated 26 challenges across SQL injection, XSS, CSRF, command injection, broken access control, authentication flaws, and cryptography, including headless-browser “victim” labs for client-side attacks.
- Issued per-student, per-lab HMAC-derived flags so flags cannot be shared; labs are reachable only by their owner through an authenticating Nginx wildcard HTTPS proxy using single-use tickets.
- Hardened every lab container (non-root, read-only filesystem, all capabilities dropped, no-new-privileges, PID and memory limits) with iptables egress blocking and gVisor kernel sandboxing; verified isolation with automated checks.
- Secured the application with Argon2id password hashing, double-submit CSRF protection with origin checks, and per-account and per-IP rate limiting; covered with automated backend, frontend, and exploit tests.
- Deployed on a Microsoft Azure Ubuntu VM with Let’s Encrypt TLS, systemd services, and daily database backups with a tested restore procedure.

Web Authentication and Licensing System

Flask, Express, Prisma, SQLite, MongoDB

- Implemented token-based licensing with hardware-ID (HWID) bound authorization, administrative token revocation, and HWID reset.
- Applied HMAC request-signing concepts, CORS restrictions, and endpoint rate limiting.
- Deployed behind Nginx and Cloudflare with UFW firewall rules, TLS, and reduced network exposure of the database.

University Attendance and Marks Management System

React, Vite, TypeScript, Express, Supabase

- Built a full-stack application with role-based access for admin, faculty, student, and parent users.

AI Study Bot

Python, Ollama, Nomic embeddings, MongoDB

- Built a Telegram bot that retrieves academic material from arXiv, Semantic Scholar, and DOAB and summarizes it with a local LLM using embedding-based retrieval and vector search.
- Deployed on an Ubuntu VPS with Uvicorn behind an Nginx reverse proxy.

QuantumMed: Hybrid Quantum-Classical Heart Disease Detection

Smart India Hackathon 2026

Team Lead, six members

- Led development of a hybrid quantum-classical machine learning platform. QSVM experiment accuracy improved from 55.74% to 81.97% across iterations, with results framed against classical baselines.

Offline AI Survival Assistant

Python, SentenceTransformers, ChromaDB

- Built an offline-first retrieval-augmented assistant with local LLM inference, semantic retrieval over reference material, and routing via GraphHopper and OpenStreetMap data.

Other Projects

- **ASL Recognition:** CNN image classifier trained with TensorFlow and Keras.
- **Instagram Chat Analyzer:** Streamlit app for parsing and visualizing exported conversation data.
- **IoT Prototypes:** Arduino UNO R4 WiFi and ESP32 builds with gas, temperature and humidity, motion, and ultrasonic sensors.

ACADEMIC PROJECTS AND PRESENTATIONS

- Heart disease prediction using the Random Forest algorithm: coursework research paper prepared in IEEE conference format, co-authored with N. Dhar.
- Presentations (coursework): Cybercrime and the Information Technology Act, 2000; Generative vs. Discriminative AI Models.