Harshdeep Athawale

athawaleharshdeep@gmail.com | linkedin.com/in/harshdeepathawale | github.com/HarshdeepAthawale | https://harshdeepathawale.in/

Education

Thapar Institute of Engineering & Technology — Patiala, India
B.E. in Computer Engineering — *Aug. 2024 – June. 2028*

Experience

Iris Intelligence — April. 2026 – June. 2026
Security Engineer (Internship) — *Delhi, India (Hybrid)*

- Performed **vulnerability assessments** across REST APIs, authentication flows, and the sandboxed code-execution layer, surfacing broken access control, injection, and cross-tenant data-leakage gaps and driving remediation before launch.
- Authored **SOC 2 and ISO 27001 compliance** documentation with privacy-by-design controls (data classification, encryption, retention), establishing the company's GRC baseline.
- Hardened request rate limiting and agent runtime restrictions to keep workloads isolated and abuse-resistant as the platform **securely scaled to 5K+ concurrent users**.

HackerOne — Dec. 2025 – March. 2026
Security Researcher (Part-time) — *San Francisco, CA (Remote)*

- Submitted **35+ vulnerability reports** to global programs including Goldman Sachs, Flipkart, Adobe, Netflix, Red Bull, NVIDIA, Anduril, Coca-Cola, and Superdrug – headlined by a **Critical (CVSS 9.1)** GraphQL flaw at Red Bull exposing employee PII, and an unauthenticated API exposing 892 employees PII with write access to a production database.
- Found high-impact **infra and supply-chain** bugs: remote code execution in a build pipeline, a subdomain takeover at Anduril, and exposed source maps leaking OAuth secrets at Flipkart/Myntra.
- Discovered **hardcoded OAuth secrets** leaking NHS medical data and an appointment IDOR at Superdrug, preventing potential patients data breaches

Projects

Transformer-Based WAF Pipeline | *Python, FastAPI, PyTorch* — GitHub | Jan. 2026 – Apr. 2026

- Built a reverse-proxy WAF combining sliding-window rate limiting with transformer-based request inspection, and benchmarked it against **ModSecurity with OWASP CRS v4** on 675 labeled real-world payloads, achieving a **96% detection rate vs. 46%**.
- Fine-tuned **DistilBERT** to detect 10 web attack classes, achieving **97.5% detection accuracy** across Path Traversal, SQLi, XSS, SSRF, and IDOR.
- Deployed OWASP Juice Shop, WebGoat, and DVWA behind a Docker Compose reverse-proxy gateway with per-IP rate limiting and monitor, block, and challenge enforcement before reaching the origin.

Technical Skills

Languages: Python, Bash, C++
Security Tools: Burp Suite, Nmap, Metasploit, OWASP ZAP, sqlmap, Nuclei, MobSF, Frida, JADX, Wireshark, Shodan
Frameworks & Methodologies: MITRE ATT&CK, Cyber Kill Chain, OWASP Top 10, OWASP MASVS, STRIDE Threat Modeling
Governance, Risk & Compliance: SOC 2 Type II, ISO 27001, Privacy-by-Design, Risk Assessment, Security Policy Drafting
Infra & DevOps: Docker, CI/CD, GitHub Actions, AWS, Linux, Git; PostgreSQL, SQL
Networking: OSI Model, TCP/IP, DNS, DHCP, Firewalls, IDS/IPS

Achievements

Ranked Top **1**% Worldwide on TryHackMe (India Rank #**2,052**), **300+** day streak, **230+** labs solved.
Intigriti Hall of Fame - Earned 4 severity badges: Exceptional (4×), Critical (3×), Medium (2×), and First Valid Submission.
National 1st Runner-Up at the **PSB Hackathon Series 2026** – organized by the Government of India with Central Bank of India & MNNIT Allahabad – outlasting **226 teams** to win an **INR 3,00,000** cash prize as part of Team Dhurandhar.