Harshdeep Athawale

harshdeepathawale27@gmail.com | linkedin.com/in/harshdeepathawale | github.com/HarshdeepAthawale | https://harshdeepathawale.vercel.app/

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 — *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, and Row-Level Security – 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 — *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.
- Identified **infrastructure and supply-chain risks**: an unauthenticated Artifactory access chain combined with npm dependency confusion for build-pipeline RCE, a dangling-CNAME subdomain takeover at Anduril Industries, and exposed source maps leaking OAuth credentials and 149 microservice definitions 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 AI WAF Pipeline | *Python, FastAPI, PyTorch, ONNX* — GitHub | Feb. 2026 – Present

- Built a reverse-proxy AI WAF combining Redis rate limiting, DDoS detection, bot scoring, and transformer-based request inspection, outperforming **ModSecurity OWASP CRS v4** (96% vs 46%) on 675 real-world payloads.
- Fine-tuned **DistilBERT** for 10 web attack classes, achieving **97.5% detection** on Path Traversal, XXE, SSRF, and LDAP/XPath Injection through training–inference alignment and hard-negative mining.
- Reduced inference latency by **8**× (46 ms → 6 ms p50) using ONNX Runtime and deployed as a multi-tenant FastAPI service with monitor, block, and challenge modes.

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, NGINX, Linux, Git; PostgreSQL, MongoDB, Redis, 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.