

ASHUTOSH JENA

Web & API Penetration Tester · OWASP Top 10 · Security Researcher & Blogger

+91-9827885028 | ashutosh.jena.mav.1@gmail.com | ashutosh-jena.in | LinkedIn | GitHub: MAVERICK-VF142 | Hack The Box

SUMMARY

VAPT professional with hands-on experience in Web and API penetration testing, authentication bypass, and business-logic exploitation. Identified 12+ vulnerabilities — including Account Takeover, OTP bypass, SSRF, IDOR, and rate-limit bypass — across enterprise VAPT engagements and public VDP / open-source disclosure programs, delivering PoC-based reports with CVSS v3.1 scoring — four CVEs assigned, more in progress. Active security blogger with 20+ published writeups on OWASP methodology, API security, and real-world exploitation.

SKILLS

Offensive Web & API VAPT · OWASP Top 10 & API Top 10

Tools Burp Suite · Postman · Nmap · Gobuster · sqlmap · curl · Nuclei

Other Python · Bash · Linux (Kali / Ubuntu) · CVSS v3.1 · PoC Documentation · Remediation Advisory

EXPERIENCE

VAPT Intern · Tytova Technologies

Remote | Jan 2026 – Mar 2026

- Performed Web & API VAPT on staging and production-like environments — OWASP Top 10 and API Top 10 attack classes.
- Identified 3 critical / high-severity vulnerabilities (CVSS 8.5+).
- Account Takeover via broken authentication, OTP bypass in password-reset flows, and rate-limit bypass on login endpoints.
- Delivered PoC-based reports with CVSS scoring, reproduction steps, and remediation advice — accepted without revision.

Research Intern · NIT Puducherry Karikal

May 2024 – Jul 2024

- Built a 360° video multi-object tracking system with hardware-accelerated processing and improved detection accuracy.

Technical Writer · GeeksforGeeks

Remote | Jan 2023 – Jan 2024

- Authored 15+ cybersecurity and networking articles; reviewed peer submissions for technical accuracy.

VULNERABILITY DISCLOSURE (VDP)

Open-Source & Public VDP Programs

Mar 2026 – Present

- Server-Side Request Forgery (SSRF) in PDF rendering — assigned **CVE-2026-83744** (VDB-397500).
- Broken Access Control (IDOR) — assigned **CVE-2026-83743** (VDB-397499) and **CVE-2026-86285** (VDB-399445) .
- Arbitrary file-upload vulnerability in UnoPim escalated to Remote Code Execution (RCE) — assigned **CVE-2026-82524** .
- Identified and responsibly disclosed a stored XSS vulnerability and Submitted PoC write-ups through official VDP / security.txt channels; all findings acknowledged and remediated by maintainers. *CVE assignment in progress with MITRE for the stored XSS finding.*

PROJECTS

Exploit Ledger

Feb 2026

- Professional VAPT workspace with AI-powered finding analysis (Gemini), CVSS v3.1 scoring, OWASP API Top 10 compliance tracking, multi-user RBAC, and watermarked PDF / DOCX report export with audit trails per §9.1.4 pentest standards.

Protocol

Feb 2026

- Cybersecurity identity platform consolidating CVEs, PoCs, and research into a verifiable professional profile for security practitioners.

Pi Honeypot

Dec 2023

- Low / high-interaction honeypots on Raspberry Pi capturing SSH brute-force and port-scan traffic from real attackers for threat intelligence.

EDUCATION & CERTIFICATIONS

B.Tech, Computer Science Engineering

Sambalpur University Institute of IT · Burla, India · 2021 – 2025

- Microsoft Certified: Azure Fundamentals
- Fundamentals of Red Hat Enterprise Linux
- IBM Cybersecurity Analyst
- API Security Fundamentals