HARSH SANDILYA

LinkedIn: linkedin.com/in/harshtalks **GitHub:** github.com/rooter09 **Website:** harshsandilya.vercel.app

Email: harshsandilya09@gmail.com **Phone No:** +91 7903314729 **Location:** Patna, India

SUMMARY

Hardworking and detail-oriented **Cybersecurity Analyst & Security Researcher** with expertise in **VAPT, OSINT, Red Team operations, and bug bounty hunting.** Skilled in collaborating with cross-functional teams to build secure, scalable, and innovative solutions across web applications, automation frameworks, UI/UX design, and digital platforms. Experienced in developing end-to-end security products (Web, GUI, CLI) integrating advanced reconnaissance and vulnerability assessment tools while ensuring user-centric design and optimized performance. **Strong technical foundation in Development, UI coupled with proven experience in SEO and digital marketing strategies to drive visibility and growth.** Recognized for blending security, development, design, and marketing expertise to deliver impactful, multi-domain technology solutions.

EDUCATION

- **AMITY UNIVERSITY PATNA**   **Aug 2022 – Present**
  B.Tech in Computer Science Engineering, CGPA - 8

SKILLS

- **Languages:** C, Java, Python, JavaScript, SQL, Bash, Shell
- **CyberSecurity Tools:** BurpSuite, Nessus Scanner, WireShark, NMAP, Metasploit. OSINT, Sqlmap, SET Kit, Autopsy, Netcat, Jhon the Ripper, Masscan, Nikto, Maltego, Builtwith, Wappalyzer MobSF.
- **Cybersecurity Skills & Roles:** SQL Injection, XSS Scripting, Penetration Tester, CTF Player, Security Researcher, Threat Analyst, OSINT Investigations, Security Auditor, OWASP ZAP, Bug Bounty Hunter, VAPT, Red Team Specialist, Digital Forensics Analyst, Cybersecurity Consultant, IAM Developer.
- **Web Development:** WordPress, Shopify, MERN Stack, Next.Js, Tailwind CSS.
- **Design & Marketing Tools:** Canva, Photoshop, Illustrator, SEMrush, HubSpot, Zoho, Yoast, Brevo, Meta Suite, MailChimp, GMB, GSC.
- **Soft Skills:** Leadership, Public Speaking, Teamwork, Initiative Skills, Communication Skills, Cross Functional Team, Management.

PROJECTS

1. ReconRay – Advanced Reconnaissance Toolkit   **Web:** Link, ↗ **GitHub**: (Link) ↗

- **Built ReconRay Framework (Web + GUI + CLI)** – Developed a Next.js + FastAPI web app, PyQt5 GUI, and CLI interface with dynamic tool execution, PDF export, custom payloads, and real-time logs.
- **Integrated 15+ Recon, VAPT & OSINT Tools** – Unified scanners for SQLi, XSS, CORS, CVEs, Subdomains, Ports, JS endpoints, Directory brute force, WHOIS, Email/Phone extraction, and more into one extensible platform.
- **Optimized Scanning & Orchestration** – Implemented tool_function_map for dynamic backend routing, minimized runtime while ensuring payload effectiveness, and enabled "Full Scan Mode" with multi-tool orchestration under 5 minutes.
- **User-Centric Controls & Accessibility** – Delivered dynamic front-end controls (start/stop scan, payload management, result export), intuitive offline GUI, flexible CLI, and live demo at **reconray.vercel.app**.

2. CyberRakshak - Awareness Platform on Cybercrimes   **Link** ↗

- Developed a **Next.Js** project for the awareness on cybercrimes.
- Used Radix UI, TypeScript and Tailwind CSS for best user experiences.

3. Password Generator with Strength Checker and Encrypted Storage   **Link** ↗

- **Developed** a Python-based password generator with **customizable, secure password creation** and **strength validation**.
- Integrated encrypted storage using **cryptography.fernet** to securely store generated passwords.

4. Steganography Tool   **Web:** Link, ↗ **GitHub:** Link ↗

- Developed a tool to securely embed and extract hidden messages in images and audio files using **Least Significant Bit (LSB) techniques.**
- **Supports PNG, JPG, and WAV files**, enabling users to embed messages and save modified files.
- Integrated a user-friendly interface with **PySimpleGUI** for seamless user interaction.

5. Malware Analysis Sandbox

- Developed a **Python tool** to simulate and monitor malware behavior, tracking file system changes, registry modifications, and network activity.
- Enabled early threat detection and analysis of suspicious files using libraries: **watchdog, pywin32, and scapy.**

6. Keylogger Tool

- Developed **an ethical keylogger in Python** to capture and store keystrokes locally with a **24-hour self-destruct mechanism.**
- Features include **stealth mode, secure log management, and automatic log deletion using pynput, time, and os.**

7. Website Development   **Link** ↗

- Developed and delivered 50+ websites using WordPress, ensuring responsive design and user-friendly interfaces.
- Specialized in Shopify e-commerce websites, optimizing user experience and business growth.

8. Graphics / UI Designing   **Link** ↗

- Designed visually appealing graphics for social media, websites, and digital platforms to enhance brand presence and engagement.
- Created custom designs for marketing campaigns, product branding, and digital media projects.

NOTABLE VULNERABILITIES REPORTED

1. Critical Cryptographic Flaws - Fireblocks
- Identified **ECDSA flaws** in Fireblocks' MPC-lib enabling **replay attacks, quorum bypass, and signature forgery** using malformed scalars.
- Submitted a Gold Standard Safe Harbor report with full PoC, output logs, and cryptographic CWE analysis, demonstrating risks of transaction replay, unauthorized signing, and protocol downgrade.
- Findings acknowledged on HackerOne, showcasing expertise in MPC security, ECDSA internals, and protocol misconfiguration detection.

2. JWT Security Research - Porsche
- Discovered **RS256 and HS256 JWT signing key misconfigurations** in Porsche's authentication system, enabling payload tampering and alg:none bypass attacks; submitted a full PoC demonstrating account takeover and privilege escalation.
- Submitted findings under HackerOne program with complete PoC, request/response logs, and methodology; report acknowledged and tracked, showcasing expertise in JWT security, algorithm attacks, and key mismanagement detection.

3. Wildcard CORS Misconfiguration – Recreation.gov
- Identified a **Wildcard CORS misconfiguration** on Recreation.gov allowing cross-origin access with cookies, highlighting potential credential/data leakage if Access-Control-Allow-Credentials: true is implemented.
- Submitted a Gold Standard Safe Harbor report with full curl-based PoC, HTTP response analysis, and risk evaluation (CWE-284).
- Report acknowledged and tracked via HackerOne, demonstrating expertise in HTTP protocol behavior, browser Same-Origin Policy, and secure misconfiguration detection.

EXPERIENCE

1. Tymor Technologies - CyberSecurity Specialist and Software Developer (Full-Time) **Sept 2025- Present**
- **Cybersecurity & Risk Management:** Conducting daily security audits on company and client websites to detect vulnerabilities, ensure compliance, and reduce security risks.
- **Software Development:** Developing secure, high-performance web applications and internal tools using the latest technologies to enhance business efficiency and digital transformation.

2. CLEVERHEX - Security Analyst (Contract), Web Dev (Part-TIme) **July 2024 - Sept 2025**
- **Cybersecurity & Risk Management:** Executed VAPT, audits, and threat analysis; reducing risks by 80% and ensuring 100% security compliance.
- **OSINT & Security Research:** Detected data leaks and insider threats using open-source intelligence to protect critical assets.
- **Innovation & Leadership:** Built 20+ websites and led Microsoft-backed EagleEyeAI, delivering tech-driven products with cross-functional teams.

2. Purezza Technologies - Head of Operations & Digital Solutions (Contract) **Jan 2023 – Jan 2025**
- Project Management: Delivered 100+ projects across dev, marketing, and client services—on time and within scope.
- Team Leadership: Led cross-functional teams, mentored members, and implemented modern tools and workflows.
- Web Development: Built 50+ WordPress sites and 10+ Shopify stores with a focus on speed, security, and UX.
- Design & Branding: Created 1500+ assets, including 20+ logos and 10+ UI/UX prototypes to elevate brand identity.
- Digital Marketing: Drove SEO, social media, and email campaigns—generated 100+ leads and boosted visibility.
- Cybersecurity: Performed VAPT and audits to safeguard digital assets for both company and clients.

3. Bug Hunting - HackerOne, BugCrowd **Jan 2024 – Present**
- CTF & Ethical Hacking: Gained hands-on expertise in web exploitation, OSINT, cryptography, reverse engineering, and detection of logic flaws, misconfigurations, and client-side security weaknesses.
- Bug Bounty & Disclosure: Reported multiple vulnerabilities via HackerOne under Gold Standard Safe Harbor, strengthening real-world application security.
- Technical Skills: Demonstrated proficiency in HTTP request manipulation, PoC creation, and security reporting (CWE/CVSS), with focus on IDOR, CORS, XSS, subdomain takeover, and access control flaws.

INTERNSHIPS

- **Graphics Design Specialist** – Clinical AI Assistance Jan 2024 – Feb 2024
- **Head Of Department(Graphics Design)** – Nyaysahay Foundation Aug 2024 - Sept 2023
- **Visual Designer** – Time Line Investment Aug 2023 – Nov 2023
- **Website Developer** – Lush Association Mar 2023 – Aug 2023
- **Digital Marketing & Graphics** – De Castro Group Mar 2023 – Aug 2023
- **Social Entrepreneurship** – Humari Pahchan Mar 2023 – Aug 2023

AWARDS & HONORS

- **Amity University Patna:** 1st Prize – Pitch Battle (EagleEyeAI), 2nd Prize – Engineering Day Conclave, Best Tech Member – AMIPHORIA 2024.
- **Purezza Technologies: Letter of Recommendation**, Certificate of Appreciation, Best Intern of the Month (×3), Best Emerging Intern (×2), Cash Prize Winner, Featured on Wall of Fame.
- **Clinical AI Assistance:** Best Intern of the Month.

EXTRA CURRICULAR ACTIVITES

- **Training & Mentorship:** Trained 1000+ students (Cybersecurity, Web Development, Graphics, Digital Marketing) at Amity; mentored 800+ students/professionals at Purezza.
- **Leadership & Event Management:** Organized **HACKIT** (Amity's first hackathon); managed 3 technical clubs (Amikriti, Amikicks, Amikoders), driving cross-domain collaboration.
- **HR & Talent Acquisition:** Supported recruitment & onboarding processes at Purezza Technologies.
- **Tata Cybersecurity Job Simulation (Forage, 2025):** Gained IAM expertise, delivered security documentation & presentations aligned with consulting practices.

CERTIFICATIONS

- **Cybersecurity:**
  - **Cisco** (Intro, Network Defense, Threat Management),
  - **TryHackMe** – Linux Fundamentals,
  - **My OSINT Training** – Intro to OSINT,
  - **LinkedIn** – Microsoft Copilot for Security,
  - **ComproAvi** – Offensive Hacking Unfolded & Pentesting Resources.
- **Design & Marketing:**
  - **Canva** – Graphic Design Essentials,
  - **Google Ads** (Measurement Certification).
- **Other Tech:**
  - **C Language** – LearnTube,
  - **Postman API Days -** NIT Patna,
  - **Ethical Hacking & Cyber Security** – Celesta IIT Patna (×2).