Pratham Gupta

Phoenix, Arizona | *929-461-9230* | *pratham.gupta@nyu.edu* | *Personal Website* | *Linkedin/PrathamGuptaaa* | *Github/PrathamGupta*

Professional Summary

Cybersecurity professional with a **Master's from NYU** and hands-on experience in security engineering, penetration testing, and enterprise security controls. Proven ability to develop and implement security tools, automate workflows, and support compliance with **ISO 27001 and NIST**. Skilled in **Cloud Security** and **DevSecOps**, with a strong track record of reducing risk and improving system resilience. **Effective communicator and collaborator**, consistently delivering results in diverse team environments. Actively pursuing opportunities to leverage advanced technical and security expertise in dynamic organizations.

Education

New York University, Tandon School of Engineering *August 2023 – May 2025*
Master of Science | Cybersecurity | GPA: 4.00
Recipient of Scholarship and Academic Excellence Award

IIIT, Delhi *August 2018 – May 2022*
Bachelor of Tech | Computer Science and Engineering | GPA: 3.5
Recipient of Dean's List Award

Experience

IT Security Administrator | ***XpertDox*** *Jun 2025 – Present*

- Set up and integrated **Secrets Manager** to ensure secure application credential management and enhance automation workflows.
- Administered **Google Admin Console** for user and group management, while enforcing enterprise-wide security policies and access controls.
- Developed and launched **phishing awareness** campaigns, enabling employee threat reporting and improving organizational security posture.
- Identified and remediated **critical vulnerabilities** through penetration testing and contributed to ongoing system hardening efforts.
- Configured, secured, and managed Linux machines and endpoints using **MDM/RMM** solutions to maintain **compliance and device security**.
- Implemented robust **web access controls,** established endpoint management procedures, and enforced a single browser policy.
- Enabled and managed Chrome Enterprise Policies across the organization, ensuring secure and consistent browser usage.
- Reviewed and updated **firewall rules**, strengthening the network perimeter and overall security.
- Developed secure **Google Cloud APIs**, and managed service accounts and encryption keys to support cloud security.
- Maintained detailed **technical documentation**, facilitating collaboration and process improvement within the IT and security teams.

Cybersecurity Intern | ***Protiviti*** *May 2024 – September 2024*

- Developed a Python-based **DNS Resolver tool** to automate the resolution of subdomains and IP addresses, enhancing vulnerability assessments and supporting advanced offensive security research.
- Engineered an Active IP Finder tool to automate the identification and reporting of active IPs within subdomains, streamlining **reconnaissance** and exporting actionable insights for analysis.
- Conducted **penetration tests** on multiple systems, uncovering and documenting 10+ vulnerabilities, and delivering detailed remediation plans that reduced overall risk exposure by 50%.
- Collaborated with security teams to update technical documentation and reporting processes, improving team knowledge and audit readiness.
- Utilized Excel automation to facilitate **vulnerability tracking** and prioritize remediation efforts across diverse network environments.
- Supported **incident response** efforts by providing rapid reconnaissance data and vulnerability intelligence, enabling swift mitigation actions.
- Engaged in ongoing knowledge transfer with team members, sharing findings from vulnerability assessments and tool development to uplift **offensive security** capabilities.

GenAI Intern | ***SymphonyAI*** *May 2024 – July 2024*

- Automated complex script execution workflows by dynamically altering variables, consolidating retailer-specific scripts into a unified modular framework, and reducing redundancy while **improving operational efficiency by 40%**.
- Built and maintained interactive dashboards and reporting tools to visualize **key performance indicators (KPIs)** and metrics, enhancing accessibility and supporting data-driven decision-making for stakeholders.
- Collaborated with cross-functional teams to design, deploy, and optimize **AI-driven solutions**, accelerating data processing **speed by 5x** and significantly improving overall system performance.
- Streamlined data integration from multiple sources, ensuring consistent data quality for analytics and reporting initiatives across departments.
- Provided ongoing support, **bug fixes**, and documentation for systems, ensuring long-term **scalability** and ease of use for end-users.
- Engaged in regular knowledge-sharing sessions with team members to communicate solution architecture and best practices, fostering a culture of continuous improvement and innovation.

Software Developer | ***PayTM*** *May 2022 – August 2023*

- Secured multi-platform payment systems by implementing **PCI DSS-compliant** 3D Secure payment solutions, mitigating **potential financial losses of $30M** and significantly reducing transaction fraud.
- Developed and optimized transaction flows across payment platforms, **increasing efficiency by 50%** through secure wrapper integration and API hardening techniques to safeguard sensitive user data.
- Identified and **resolved vulnerabilities** in token-based payment methods, eliminating exploits such as replay attacks and enhancing the overall security of the payment gateway.

- Designed, built, and maintained distributed systems using **Kafka, Spring Boot, and sharding mechanisms** to ensure high availability, scalability, and robust transaction handling for millions of users.
- Conducted **routine security audits** and code reviews to proactively identify weaknesses and ensure compliance with industry standards and internal security guidelines.
- Collaborated with cross-functional engineering and security teams to integrate real-time monitoring and alerting for transaction anomalies and **potential security breaches**.
- Authored and maintained comprehensive technical documentation, supporting knowledge transfer, troubleshooting, and audit preparedness.
- Assisted in incident response for **payment security** events by rapidly analyzing logs, identifying root causes, and implementing targeted **remediations to prevent recurrence**.

Projects

LintAid: Seamless Linter Integration | *Python, Npm, CLI, OpenSSF, OWASP* *Spring 2024*

- Developed a **CLI tool in Python** and npm that automates linter integration for multiple languages, ensuring consistent code quality and compliance with security standards.
- Integrated popular **security-focused linters** (e.g., Bandit for Python, ESLint with security plugins for JavaScript) to help detect vulnerabilities and enforce secure coding practices.
- Streamlined onboarding and configuration through modular setup, simplifying implementation across varied codebases and improving developer adoption.
- Facilitated adoption of **OpenSSF and OWASP guidelines**, enabling automated detection of insecure code patterns during CI/CD workflows.

Real-Time Forex Arbitrage and Price Prediction System | *Python, Apache Spark, Airflow, Flask, Looker Studio* *Spring 2024*

- Developed a distributed forex trading platform using Apache Spark for arbitrage detection and integrated robust authentication mechanisms to ensure secure transaction processing.
- Utilized a bi-directional LSTM model for real-time price prediction, implementing data validation and input sanitization to prevent injection or data manipulation risks.
- Integrated Flask APIs and automated secure data ingestion with Airflow, ensuring encryption of data in transit and deploying dashboards in Looker Studio with role-based access controls.
- Prioritized secure coding methodologies and regular vulnerability assessments throughout the platform's development to protect sensitive financial data.

OpenTelemetry Security Assessment | *Git, OpenSSF, OWASP, Threat Modelling* *Fall 2023*

- Conducted a comprehensive security assessment for the **OpenSSF OpenTelemetry** project, evaluating architecture and codebase for potential risks and exposures.
- Performed detailed **threat modeling** to identify, analyze, and prioritize security risks, producing actionable recommendations based on **OWASP and OpenSSF** best practices.
- Analyzed project requirements and deliverables from a security perspective, providing clear insights to improve the project's security posture.
- Authored an assessment report that was peer-reviewed and **successfully merged** into the official OpenSSF repository, contributing to the project's open-source security standards.

CineVerse – Movie Discovery & Social Platform | *Git, Django, React, REST APIs, PostgreSQL* *Fall 2023*

- Built a full-stack social movie discovery platform leveraging Django, React, and PostgreSQL, implementing user authentication, password hashing, and secure session management.
- Integrated external RESTful APIs with proper authentication, HTTPS enforcement, and data caching, and **containerized using Docker Compose** to isolate services and enhance deployment security.
- Designed secure user data storage and access controls to prevent unauthorized data exposure and **cross-site scripting (XSS) attacks**.
- Conducted regular code reviews and employed automated security tests to identify and remediate vulnerabilities in both backend and frontend components.

DESy: Decentralized Education System | *Hyperledger Fabric, Node.js, REST APIs, GoLang, Python* *May 2022*

- **Led a team** to build a blockchain-powered academic platform using Hyperledger Fabric, enabling cryptographically verifiable course credentialing and secure multi-institution transcript sharing.
- Developed and audited smart contracts in Go, ensuring security against common vulnerabilities like reentrancy and access control flaws.
- Built Node.js backend services with **strong authentication**, role-based access, and data encryption for all sensitive student and academic records.
- Collaborated with **government stakeholders** to align smart contract logic with national education data privacy standards and compliance frameworks.

Technical Skills

Languages :Python, C, C++, Java, JavaScript, Go, SQL, Bash
Tools :NinjaOne, BitDefender, Barracuda, AWS (Secret Manager, IAM), Google Admin, Google Cloud, Azure, GitHub Actions
Security : Kali Linux, Burp Suite, Metasploit, Nessus, Splunk, OpenVAS, Palo Alto, SQLMap, OpenSSL, Libgcrypt
Networking : Packet Analysis (Wireshark, tcpdump), Secure Protocols (SSH, TLS/SSL)
Compliance and Frameworks : Sprinto, ISO 27001, OWASP, NIST, PCI DSS
DevSecOps : Docker, Kubernetes, SonarQube, Jenkins
Key Concepts :Cryptography, Network Security, Penetration Testing, Vulnerability Analysis, Application Security, Operating Systems
Certifications :Cybersecurity & IoT Certification, Machine Learning Certification