SHUBH GUPTA

Security Automation & Scripting Engineer

gshubh270@gmail.com
linkedin.com/in/shubhgupta19
quietcod.github.io/Shubh-Gupta

PROFILE

Security Automation & Scripting Engineer with hands-on experience building Python and PowerShell automation for vulnerability intelligence, system configuration, and security workflows. Experienced with Windows/Linux environments and CVE research, with a focus on reliable, repeatable automation that supports human decision-making.

SKILLS

- **Languages** Python, PowerShell, Bash
- **Frameworks** Django, REST APIs, Automation Pipelines
- **Tools** Git, GitHub, Nmap, Wireshark, Metasploit
- **Platforms** Windows, Linux
- **Security Operations** CVE Analysis, Vulnerability Monitoring, Alert Tuning

EXPERIENCE

Security Automation & Scripting Intern
Sunrise Computers — Jaipur, Rajasthan | Jul 2025 – Present

- Automated Windows system configuration, optimization, and reporting workflows using PowerShell, improving consistency and reducing manual setup effort.
- Developed a Python-based CVE monitoring and email alert system to track newly published vulnerabilities relevant to internal software and infrastructure.
- Built automation scripts to collect system logs, process security data, and export structured reports to Google Sheets for internal analysis.
- Contributed to internal CRM feature updates and bug fixes using PHP, researching solutions and applying rapid learning to deliver functional improvements.

Data Analysis with Python Intern
Amnex Infotechnologies — Remote | Jun 2024 – Sep 2024

- Processed, cleaned, and transformed datasets using Python and Pandas to support automation and reporting workflows.
- Created Python scripts to automate recurring data analysis tasks, improving reporting efficiency and consistency.
- Used Git for version control, debugging, and iterative improvement of automation scripts.

Junior Python Developer
Marktine Technology Solutions — Jaipur, Rajasthan | May 2023 – Jul 2023

- Supported backend development using Django, contributing to API functionality and internal automation features.
- Worked with MySQL and Django ORM to manage structured data and improve database interactions.
- Debugged and refactored backend components to enhance performance, reliability, and maintainability.

PROJECTS

CVE Notification & Intelligence System

- Built a Python-based system to track new CVEs, enrich data, reduce alert noise, and send contextual email alerts.

Windows Automation Suite

- Developed a PowerShell toolkit to automate Windows setup, configuration, and safe optimization with guardrails.

PROJECTS — TECHNICAL DETAILS

CVE Notification & Intelligence System (Python)

- Designed a stateful automation pipeline to ingest CVE data from public APIs
- Implemented deduplication, enrichment, and severity-based filtering
- Reduced alert noise by surfacing only relevant, contextualized vulnerabilities
- Integrated email alerts for timely vulnerability awareness
- Implemented state tracking to prevent duplicate alerts and reduce notification fatigue
- Persisted CVE metadata locally to enable idempotent execution and historical comparison

Windows Automation Toolkit (PowerShell)

- Built modular PowerShell scripts for Windows setup, optimization, and reporting
- Automated application installation, configuration, and system data collection
- Designed scripts with guardrails to avoid unsafe OS modifications
- Included dry-run and controlled execution patterns to minimize configuration risk
- Structured scripts modularly to allow selective execution and safer reuse across systems

---

SECURITY AUTOMATION & SYSTEM DESIGN

- Authored in-depth technical articles on security automation failures in production environments
- Documented system design tradeoffs related to alert fatigue, blast radius, and automation guardrails
- Researched and analyzed CVE intelligence pipelines and responsible remediation workflows
- Focused on human-in-the-loop security automation and operational risk reduction
- Applied system-design principles to balance automation speed with operational safety

---

SECURITY OPERATIONS & AUTOMATION PRACTICES

- Designed automation with explicit guardrails to limit blast radius and prevent unsafe execution
- Prioritized information-first workflows before automated remediation
- Emphasized repeatability, observability, and explainability in security tooling
- Evaluated automation failure modes and incorporated safe defaults
- Designed automation to fail safely by default and require explicit intent for destructive actions

---

EDUCATION

B.Tech - Computer Engineering

Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune | 2021 - 2025

CERTIFICATIONS

EC Council

- Certified Ethical Hacker (CEH)
- Open Source Intelligence
- Network Defense Essentials (NDE)

Google

- Foundations of Cybersecurity
- Automate Cybersecurity Tasks with Python

IBM

- Introduction to Cybersecurity tools and Cyber Attacks

The Linux Foundation

- Linux for Developers
