Ayush Gupta

Security Researcher

Nagpur, Maharashtra, India | +91 77210 47701 | ayushgupta02655@gmail.com | linkedin.com/in/ayushg18

Hands-on experience in cybersecurity, penetration testing (VAPT), and vulnerability assessment through independent research, labs, and real-world security testing. Skilled in identifying security vulnerabilities, ethical hacking, and securing web applications against cyber threats. Proficient in network security, web application security, and exploit development using industry-standard tools and frameworks.

EDUCATION

- **B. Tech Computer Engineering:** 2020-2024, St. Vincent Pallotti College of Engineering & Technology | **CGPA – 7.8**
- **Higher Secondary Education:** 2018-2020, Prerna Jr. College, Nagpur | Percentage – 63.85.
- **Secondary School Education:** 2018, Charisma English Convent, Nagpur | Percentage – 81.20.

TECHNICAL SKILLS

- **Cybersecurity & InfoSec:** VAPT, Threat Detection, Security Monitoring, Incident Response, Threat Hunting, OSINT, Malware Analysis, Risk Management
- **Programming Language & Scripting:** Python, C, Java, Shell Script.
- **Operating Systems:** Linux (Kali, Ubuntu), Windows
- **Security Tools:** Burp Suite, Metasploit, OWASP ZAP, Wireshark, Nmap, Nessus, Splunk, Ghidra, Snort, OpenVAS, SIEM, IDS/IPS, Firewalls
- **Supporting Skills:** Project Management, Collaboration & Team Work, Problem-Solving, Documentation.

WORK EXPERIENCE

- **Security Researcher |** Freelancing, Nagpur. (Remote) July 2023 - Present
  - Reported 5**+ HIGH-severity vulnerabilities**, including critical authentication bypass, privilege escalation, and API security flaws, enabling security teams to deploy patches that mitigated 50% of potential attack vectors.
  - Developed **custom scripts** in Python and Bash to automate security testing, reconnaissance, and exploit development, increasing efficiency in penetration testing workflows.
  - Created detailed vulnerability reports, including proof-of-concept **(PoC)** exploits, risk assessments, and remediation recommendations, to assist developers and security engineers in fixing security flaws.
  - Conducted comprehensive ethical hacking assessments on web applications, utilizing tools like Burp Suite, Nmap, OWASP ZAP, SQLmap, and Nikto to uncover security vulnerabilities.
  - Performed manual and automated penetration testing to identify risks such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and Broken Authentication.
- **Cyber Security Analyst Intern |** IWM Cyber Sec Pvt. Ltd, Nagpur. (On-Site) Jan 2024 - Apr 2024
  - Conducted a comprehensive threat analysis by leveraging security tools, network monitoring techniques, and threat intelligence sources to detect and respond to emerging cyber threats effectively.
  - Conducted penetration testing on various models and performed continuous security monitoring as a cybersecurity engineer.
  - Contributed to web security projects by analyzing web applications, testing for vulnerabilities, and implementing security measures to enhance resilience against attacks.
- **Cybersecurity Researcher Intern |** Cyber3ra, Nagpur. (Remote) May 2023 - Aug 2023
  - Acquired proficiency in security tools like Metasploit and Wireshark, detecting and analyzing threats with a 90% success rate, supported by extensive research on emerging cyber threats and attack vectors.
  - Conducted in-depth security research on emerging cyber threats, attack vectors, and exploitation techniques to strengthen cybersecurity defenses.
  - Assisted in penetration testing (VAPT) engagements, identifying and documenting security flaws in web applications, APIs, and network infrastructures.
- **Team Lead |** Phoenix Cybersecurity Club, Nagpur. (On-Site) Oct 2021- Jan 2024
  - Led end-to-end cybersecurity projects, optimizing network security processes and strengthening system defenses.
  - Mentored and trained junior cybersecurity enthusiasts, fostering hands-on experience in ethical hacking, incident response, and penetration testing.
  - Restructured communication flow across 4 departments within the forensics and penetration testing teams, improving collaboration and efficiency.

CERTIFICATIONS

- **Threat Intelligence Analyst** | ARCx
  - Certified ARCx Threat Intelligence Analyst with expertise in cyber threat analysis, risk assessment, and incident response. Skilled in tracking cyber threats, analyzing attack patterns, and leveraging intelligence frameworks to enhance security posture.
  - Threat Intelligence & Analysis – Cyber Kill Chain, MITRE ATT&CK
    ✔ Incident Response & Digital Forensics – Malware Analysis, Threat Hunting, SIEM Monitoring
    ✔ Security Tools & Techniques – Wireshark, Splunk, Threat Intelligence Platforms
    ✔ Vulnerability & Risk Management – OSINT, Threat Modeling, Attack Surface Reduction
    ✔ Network & Cloud Security – IDS/IPS, Zero Trust, Cloud Threat Intelligence
- **Practical Ethical Hacking** | TCM Security
  - TCM Security Certified cybersecurity professional with hands-on experience in penetration testing, vulnerability assessment, and offensive security. Skilled in network and web application security. Proficient in ethical hacking methodologies, red teaming, and security hardening to enhance cybersecurity defenses.
    ✔ Certified in Practical Ethical Hacking – TCM Security with hands-on cybersecurity experience.
    ✔ Skilled in penetration testing, red teaming, and ethical hacking methodologies.
    ✔ Knowledge of OWASP Top 10, MITRE ATT&CK, and exploit development.
    ✔ Experience with reconnaissance, exploitation, privilege escalation, and post-exploitation techniques.
- **API Penetration Testing** | APIsec University
  - Certified in API Penetration Testing (APIsec University) with expertise in securing APIs, identifying vulnerabilities, and preventing exploitation in modern applications. Skilled performing automated and manual security testing, and implementing secure API development practices.
    ✔ API Security & Testing – OWASP API Security Top 10, Authentication & Authorization (OAuth, JWT)
    ✔ Penetration Testing & Vulnerability Assessment – API Fuzzing, Broken Object, Rate Limiting Bypass
    ✔ Security Tools & Techniques – Postman, Burp Suite, OWASP ZAP, SQLmap, JWT.io
    ✔ Threat Detection & Exploit Development – API Reconnaissance, SSRF, Injection Attacks (SQLi, XML, GraphQL)
    ✔ Cloud & Web Security – Securing REST & GraphQL APIs, Container Security (Docker, Kubernetes)

PROJECT

- **Face Recognition System | YOLOv5, OpenCV, Git, Linux, Python** (GitHub Repo)
  - Key Responsibilities - Data Gathering, Model Training, Data Set Handling, Model Integration, Implementing branching strategies for managing **Dev, Test, Prod** Environment
  - Developed a real-time face recognition model utilizing **YOLOv5** to automate attendance marking in academic settings.
  - Designed and optimized **Python-based** algorithms to improve face detection accuracy and recognition performance. Integrated **OpenCV** for image processing and real-time tracking. Conducted model training on **Google Colab**, utilizing datasets from **Kaggle** and **Roboflow**.
  - Implemented the system on **Windows** and **Linux**, employing **Git, GitHub,** and **GitBash** for version control and source code management.
- **Packet Sniffer Tool | Scapy, Wireshark, Python, Git, Linux**
  - Developed a custom packet sniffer using **Scapy** and Python to capture and analyze real-time network traffic.
  - Integrated Wireshark for enhanced **protocol analysis** and visualization of captured packets.
  - Implemented filters for TCP, UDP, ICMP, and HTTP/S packets to detect anomalies and **potential security threats.**
  - Designed the tool for **cross-platform compatibility**, tested on both Windows and Linux environments.
- **reconDomain | Bash, Git, Linux**
  - Developed an automated reconnaissance tool to streamline **domain enumeration** and subdomain discovery.
  - Integrated multiple open-source **OSINT tools** for efficient data collection.
  - Utilized Python and Bash scripting for automation, reducing manual **reconnaissance workload**.

ACHIEVEMENTS

- Recognized in the **Hall of Fame** by the following companies for exceptional bug-finding skills: **Zoho**, Immutable, Gusto, Octopus, Sophos, Pantheon.
- **Research Paper** on Packet Sniffer Cyber Security Tool | | ISSN: 2278-6848 – Published a research paper on network packet sniffing methodologies, analyzing data traffic to enhance cybersecurity insights and threat detection.