**Gaurav Bhatia**

Mumbai, India | [bhatiagaurav1211@gmail.com](mailto:bhatiagaurav1211@gmail.com) | [linkedin.com/in/gaurav-bhatia-bb290916a](https://linkedin.com/in/gaurav-bhatia-bb290916a) | [hackerone.com/gaurav-bhatia](https://hackerone.com/gaurav-bhatia)

**SUMMARY**

**Cyber Security Researcher** with 3+ years of hands-on experience in **VAPT**, **bug validation**, and **security automation**. Currently working as a **Security Researcher** at **Microsoft**, focusing on **bug triage, security research, and process automation** to enhance internal security workflows and reduce turnaround time.

Previously at **Oracle Financial Software Services**, where I identified vulnerabilities in internal banking software, validated client-reported bugs, supported developers in secure remediation, and automated security scans using **Jenkins and CloudLab** for efficient reporting.

Specialized in **web/mobile/API/cloud security**, skilled in tools like **Burp Suite, Metasploit, Wireshark**, and fluent in **Python** and **Shell scripting**. Strong foundation in **OWASP, NIST, and ASVS** frameworks. I believe in **automating repetitive tasks** and focusing on **smart work over hard work**.

**Published author** in reputed journals, winner of the **Sainya Ranakshetram (Indian Army) Hackathon**, and participant in the **CCTNS Cyber Challenge**. Earned **multiple bug bounties and Hall of Fame mentions** from **Google (3x), Microsoft (4x), Palo Alto, Adobe**, and more via **HackerOne and Immunefi**. Credited with **multiple CVEs** for critical vulnerabilities in open-source and enterprise software.

**SKILLS**

**Operating Systems:** Windows, Linux – (Kali Linux, Parrot)

**Programming:** Python, Shell.

**Software tools:** Burpsuite, Postman, Mobsf, Frida, Objection, SQLMap, Metasploit, Wireshark, ZAP

**Framework:** OWASP, NIST ASVS.

**Pentest:** Web Application, Mobile Application (Android), API, Automotive, Cloud Security

**WORK EXPERIENCE**

**Microsoft Security Response Centre(MSRC) JULY 2025 – PRESENT**

*Security Researcher*

1. Triaged and validated security bug reports, collaborating with product teams to ensure accurate prioritization and remediation.
2. Conducted in-depth security research to identify potential threats and emerging attack vectors impacting Microsoft products.
3. Developed and implemented small-scale automation scripts to optimize repetitive tasks in the bug triage and research workflow.
4. Assisted in analysing root causes of vulnerabilities and provided actionable recommendations to strengthen product security.
5. Collaborated with cross-functional teams to ensure security issues were resolved efficiently and aligned with Microsoft’s security standards.
6. Improved internal workflows by reducing manual effort and accelerating turnaround time for security issue handling

**Oracle Financial Software Services JUNE 2024 – JULY 2025**

*Associate Application Developer (Product Security)*

1. Conduct security assessments and identify vulnerabilities in internal banking applications.
2. Validate and triage client-reported bugs, working closely with development teams to ensure timely and effective remediation.
3. Provide actionable mitigation strategies and assist developers in implementing secure coding practices.
4. Automated security scanning workflows using **Jenkins** and **CloudLab**, enabling scheduled scans and automatic report distribution.
5. Contributed to improving internal security posture by streamlining manual processes and reducing turnaround time.
6. Focused on **task automation and smart workflows** to enhance productivity and reduce repetitive effort.

**99ideas Infotech Services December 2021 – January 2022**

*Security Analyst*

1. Performed **web application penetration testing** to identify and report security vulnerabilities.
2. Prepared detailed **proof-of-concepts (POCs)** and **vulnerability reports** for internal assessments.
3. Collaborated with the development team to suggest effective **mitigation strategies** for discovered issues.
4. Conducted in-depth research on common and emerging vulnerabilities to support internal security awareness.
5. Created comprehensive documentation covering vulnerability types, impact analysis, and remediation steps.

**CERTIFICATION**

Oracle Cloud Infrastructure Security 2021 Certified Associate February 2022

eLearnSecurity Certified Professional Penetration Tester (Ecpptv2) January 2023

**PUBLISHED CVE**

1. **CVE-2024-6577 (PyTorch)** – Identified insecure reference to an unclaimed S3 bucket in a script, potentially exposing data or allowing unauthorized access.
2. **CVE-2024-1682 (Python Software Foundation)** – Discovered use of an externally claimed S3 bucket in documentation, risking data leakage or malicious hosting.
3. **CVE-2023-6017 (H2O.ai)** – Reported takeover risk due to reference to a non-existent S3 bucket, enabling potential abuse or phishing.
4. **CVE-2022-3497 & CVE-2022-3519 (Open Source)** – Found **stored XSS vulnerabilities** in open-source web applications leading to potential session hijacking or script injection.

**BUG BOUNTY**

**Hall of Fame**: **3x** Google , **4x** Microsoft , Palo Alto, MPL, Adobe

**Hackerone**: **4x** Reddit (**Top 25** Worldwide), BitGo (**Top 15** Wordlwide), **2x** Ubiquiti, **2x** AmazonVRP, EPAM, Cosmos, Elastic, Brave, Crowdstrike, Sony, Linode, General Services America(GSA) , Datastax, Lumos-Labs(Lumosity), LaunchDarkly, WorldCoin, Mendix, Kraden, Slack

**Immunefi**: Moonbeam, Nodle, Boson-Protocol, Polygon , Gnosis-Chain,

**Appreciation Letter**: AWS Security, FileCoin

**EDUCATION**

**Thadomal Shahani Engineering College June 2024**

Bachelors in Information Technology

**PROJECTS**

**Vulneralysis:**  
It is a combination of tools combined together to automate the task of vulnerability assessment.  
**Unsecured and Secured coding of Python Pickle:**The project shows how an unsecured code of python pickle is written and exploited to achieve remote code execution and also it shows proper way of coding in python pickle to make the applications secure from the dangerous attacks.  
**Imagestegano:**  
It is a tool for Image steganography where people can encrypt and decrypt the sensitive data behind the image.