Atharav Hedage

San Francisco, CA | atharavhedage55@gmail.com | +1(404)-884-2841 | **LinkedIn** | **GitHub**

Security Engineer with experience across threat detection/response, vulnerability research, and security automation (Meta, ExtraHop, EY); M.S. (GPA 4.0); $13.8K bug bounties.

EDUCATION

Georgia Institute of Technology, Atlanta, GA ***Aug 2022 to Dec 2023***
M.S in Cybersecurity (Specialization: Information Security) GPA: ***4.0/4.0***
- **100% scholarship + assistantship**: supported CTF/Malware/Crypto/Web-Sec labs (testing + tutoring).

University of Pune ***Aug 2018 to May 2022***
Bachelor of Technology in Electronics and Computer Engineering CGPA: ***9.61/10***

SKILLS & CERTIFICATIONS

Certifications: eLearnSecurity eJPT | AWS SAA | AWS Security Specialty | ISC2 CC | IBM Sec Analyst
Detection/IR: threat hunting, incident response support, alert triage, log/telemetry analysis, MITRE ATT&CK
Vuln/AppSec: Vulnerability research, web/API testing (OWASP), vulnerability management
Automation/Data: Python, SQL (Presto), APIs (REST/gRPC), Git workflows
Tools and Technologies: Burp Suite, Nessus, Nmap, Metasploit, AWS, Ghidra/GDB

PROFESSIONAL EXPERIENCE

Meta : ***Security Engineer*** ***Oct 2024 to Present***
- Tracked **eCrime / nation-state** threat actors and **ORB** infrastructure targeting Meta; translated TTPs into detections and response guidance.
- Supported **live nation-state IR events** (from scoping to legal remediation), delivering real-time intel, threat analysis, and on-call investigation support.
- Partnered with internal teams (especially Red Team and Endpoint Protection Team) to run **adversary emulation** and strengthen monitoring coverage; identified telemetry gaps and drove detection improvements.
- Led **TTP-driven threat hunts** mapped to MITRE ATT&CK; translated adversary behaviors into durable detection opportunities and actionable playbooks/runbooks.
- Designed, implemented, and maintained an **RMM abuse control system** (tracking, detection, and prevention), improving visibility into RMM activity and strengthening protections against tooling misuse.
- Drove rapid tuning for emerging threats and infection trends to keep detections current.

Extrahop : ***Security Engineer*** ***May 2024 to Oct 2024***
- **Simulated** 20+ critical CVEs to derive network + application indicators, then shipped detection logic and validation test cases. Produced clear, **engineering-ready write-ups** to support faster triage and response.
- Mapped AD and remote tooling abuse to MITRE ATT&CK and created repeatable detection content + briefings.

Ernst & Young : ***Cybersecurity Consultant Intern*** ***Jun 2023 to Jul 2023***
- Developed Python connector drivers for a **PAM platform** using **gRPC/REST/SOAP,** integrating with Cisco FTD/IOS, ServiceNow, and MongoDB Atlas. Contributing to OWASP-aligned cloud hardening guardrails in AWS.
- Customized Power BI dashboards and API/SQL queries to meet client reporting requirements.
- Managers remark - "*We expected the ServiceNow task to take 7 weeks, but he completed it in ~4 days*"

Tech Mahindra : ***Cybersecurity Analyst Intern*** ***Sep 2021 to Mar 2022***
- Identified Log4Shell (Log4j) exposure, validated impact, and escalated remediation guidance; recognized with **Internship Excellence Award** (top 1/37).
- Built a **GCP** security testing environment with centralized log/metrics monitoring (**Elastic**/**Kibana**) and executed Nessus compliance scans to surface and report control gaps.

Bluefire-Redteam : ***Cyber Security Analyst Intern*** ***May 2021 to Jun 2021***
- Triaged security findings, documented Proof-of-Concepts and hardening guidance for clients.
- Contributed to designing security questionnaires and pen-testing checklist for Web-App, API, and Cloud.

HONORS & AWARDS

- Acknowledged with a **total bounty** worth **$13,800 for Bug Bounty Hunting** on Bugcrowd and Hackerone.
- Acknowledged with **reward worth $5,000** and allotted CVE (**CVE-2021-39628**) by Google for reporting a high severity (Priority- P2, Severity- S2) android security flaw, vulnerability released in Android Security Bulletin.
- 4-star silver badge achiever at HackerRank & secured **17th position among 1800** participants in VishwaCTF21.
- Conducted cybersecurity engagement with 9 corporate organizations, **delivered cyber-awareness seminars**.
- Freelanced a **personal Security Assessment project** with the college's Education Mgmt. Software vendor.

PROJECT EXPERIENCE

Empirical Study of Malware in Nulled WordPress Plugins *-Python, PHP, Regex, AST* ***Jan 2023 to May 2023***
- Conducted **empirical study on malware in nulled WordPress** plugin marketplaces and identified **1,851 malicious plugins out of 4,271**. Developed Kratos, an automated framework, to detect malicious behaviors in plugin code using regex-based and Abstract Syntax Tree (AST) signatures. (Paper publication in progress)

Secure Shared Cloud Storage and Communication *-Python (Flask), OpenSSL, CA, AES, RSA* ***Aug 2020 to Mar 2021***
- Developed a **Secure Cloud Storage Framework** with distributed systems security. Utilized certificates, mutual authentication, and encrypted communication channels to enable secure document storage, retrieval, and access control for multiple users, ensuring data integrity and confidentiality.

RESEARCH EXPERIENCE (PATENT & PUBLICATIONS)

Patent/Publications: Co-applicant patent (**"A Security System and Method for Cloud IoT Interface"↗**);
IEEE ICIPTM 2022 co-author for "End-to-End Security in Cloud Systems" ↗.