MUNI NITISH KUMAR **YADDALA**

Security Engineer | Vulnerability Management | Application & Cloud Security
Seattle, WA • +1-404-451-4193 • nitish.yaddala@gmail.com • linkedin.com/in/nitish-yaddala

SUMMARY

- Security Engineer specializing in application, cloud, and offensive security, with experience identifying 100+ vulnerabilities across distributed AWS services.
- Validates threat models, verifies architectural controls, and performs web and API exploitation to confirm real-world impact.
- Builds Python automation for endpoint discovery and TLS/SSL configuration analysis to support scalable security assessments.
- Partners closely with engineering teams to translate exploit scenarios into clear, engineering-ready remediation guidance.

EDUCATION & CERTIFICATIONS

Georgia Institute of Technology — MS Cybersecurity (Information Security) 2022–2023
SRM Institute of Science & Technology — B.Tech in Computer Science Engineering 2018–2022
Certifications: CEH • CND • CC (ISC2)

PROFESSIONAL EXPERIENCE

Bureau Veritas | Amazon AWS Security Assessments Mar 2024 – Present
Security Engineer

- Performed penetration testing across **35 AWS services**, identifying **100+ vulnerabilities** (**20+ high severity**) across web, API, console, and distributed cloud workloads using Burp Suite Pro, Nmap, ScoutSuite, and Python automation.
- Validated Amazon-defined threat models and MTCs, exercising IAM boundary checks, access-control rules, and S3 exposure paths to verify architectural controls and security requirements were implemented as designed.
- Built **AWSPorter**, a Python/Nmap automation tool for large-scale endpoint discovery and TLS/SSL configuration and certificate-chain evaluation using testssl.sh and OpenSSL.
- Identified AuthN/AuthZ bypasses, logic flaws, and cloud configuration weaknesses through targeted Web and API testing supported by custom fuzzers and intercepting proxies.
- Authored structured security test plans and engineering-ready reports with CWE mappings, CVSS scoring, and remediation guidance; collaborated with service teams to evaluate exploitability and accelerate remediation timelines across release cycles.

HP Inc. Feb 2022 – Jul 2022
Cybersecurity Engineer

- Executed penetration testing of 6 web apps, uncovering **20+ critical vulnerabilities**, including AuthN/AuthZ bypass, SQLi, XSS, XXE, and race conditions.
- Correlated Veracode SAST with manual DAST findings and standardized reporting via CVSS/CWE to reduce developer triage effort.
- Automated TLS/SSL assessments using Python + OpenSSL to standardize certificate-chain validation across services.
- Delivered structured testing updates to engineering teams to clarify exploitability and prioritize remediation.

PROJECTS

System Call Telemetry & Anomaly Detection – Python, Linux Kernel
Implemented Linux syscall hooks capturing parameters across **21 syscalls** to gain runtime visibility into process behavior. Built a Python analysis framework trained on benign syscall sequences to flag anomalous execution patterns, demonstrating feasibility and noise tradeoffs of syscall-level behavioral detection.

Binary Exploitation & Payload Automation – Ghidra, Python
Reversed and exploited memory-corruption vulnerabilities by identifying vulnerable code paths, calculating offsets, and crafting controlled payloads. Automated exploitation workflows using Python (**pwntools**) to validate exploit reliability & confirm real-world exploitability.

Honeypot+ Service Emulation Framework – Python, Snort
Developed a lightweight honeypot emulating **30 network services** to observe attacker reconnaissance and exploitation behavior. Integrated Snort-based detection and centralized logging to enable attack-surface visibility with minimal resource overhead.

SKILLS

Offensive Security: Web & API Exploitation • Authorization(AuthZ) & Authentication(AuthN) Bypass • Request Tampering • API Enumeration • SSRF • XSS • Injection • Business Logic Flaws
Secure Engineering & SDLC: Threat Modeling • Architectural Control Validation • Security Requirements Review • Vulnerability Triage & Prioritization • Pre-release Security Assessments • Engineering & Remediation Coordination
Cloud Security: AWS Service Security Assessments • IAM Boundary & Permission Validation • Network Boundary Analysis • Cloud Workload Reconnaissance
Tools: Burp Suite Pro • Nmap • Semgrep • ScoutSuite • Linux (Kali, Ubuntu, ParrotOS) • Custom Python Tooling & Fuzzers
Standards: OWASP Top 10 • CWE • CVSS • MITRE ATT&CK
Languages: Python • C • C++ • Bash • JavaScript