Abhishek Reddy

Saarbrücken, Germany | +49 1625922595
abhishek.ramesh@cispa.de | linkedin.com/in/r-abhishek-reddy | lordprime | Portfolio

Professional Summary

M.Sc. Cybersecurity student and Research Assistant at CISPA with technical & practical foundation in **Web Security**, **AI Agent Vulnerabilities**, and **Machine Learning**. Currently leading novel research on Service Worker-mediated Web Cache Deception (SW-WCD) and the first systematic security evaluation of Autonomous Coding Agents (Intent-Driven Autonomous Development). Proficient in building complex simulation infrastructures (Docker/Nginx/Playwright), statistical analysis (R), and auditing AI-generated software using eBPF and stateful fuzzing. Experienced in debugging complex Python pipelines and deploying ML models.

Technical Skills

Web & Offensive Security: VAPT, System exploitation, Privilege escalation, Proof of concept development, Client-side vulnerability assessment, Browser and extension testing, CDN Architecture (Nginx/Varnish/Cloudflare), OWASP Top 10.
Security Operations: Splunk, Wireshark, Autopsy, MITRE ATT&CK, ITIL Framework, ISO 27001, Security Audits, Risk Assessment.
Cloud & DevSecOps: AWS Security fundamentals, Azure SIEM/SOAR, Infrastructure as Code (Terraform), Container security (Docker, Kubernetes), CI/CD Security concepts, Misconfiguration analysis.
Programming: Python (automation, security tooling, agent workflows), Bash/Shell Scripting, JavaScript/Node.j, C++
ML & Tools: PyTorch, TensorFlow, Autoencoders, RL, LLMs (Claude Code), HuggingFace, RunPod, Langchain, VectorDatabases, Docker, Kubernetes.
AI Security: Attacks : (Prompt Injetion, Jailbreaking, Data Poisoning, Membership Inference attack. Defense : (Input Sanitization (Guardrails), Adversarial Training, Robustness Verification.)
AI & Security Automation: AI-assisted security workflows, Integration with LLMs (Claude, GPT, Llama), agent-based automation.
Database & Data Handling: SQLite3, PostgreSQL, JSON-based data modeling, dataset preprocessing for security and ML pipelines.
Productivity Ecosystem: Workspace (Script automation, Data Studio reporting), Jira (Agile workflow management), Documentation (GitHub, Markdown), Communication (Slack, Teams, LaTeX).

Professional Experience

CISPA – Helmholtz Center for Information Security — Saarbrücken, Germany
Research Assistant (Web & AI Security) — *Sep 2025 – Present*

- **SW-WCD Research:** Developed `SW-WCD-RESEARCH`, a controlled prototype to study Service Worker-mediated Web Cache Deception. Architected a simulation environment using Nginx (CDN logic) and Express (Origin) to test path sculpting and header manipulation payloads.
- **Infrastructure Automation:** Implemented a Playwright-based test suite for cross-browser validation and an R-based statistical engine to compute attack success rates and time-to-cache metrics.
- **AI Agent Security (IDAD):** Leading the Vibecoding Security Gap study, benchmarking Agent-Native IDEs vs. CLI Agents. Designing the `XYZ Bench` framework to evaluate 275 development tasks for hallucinated dependencies, logic optimization bypasses, and security vulnerabilities.
- **Vulnerability Discovery:** Uncovering novel Verification Gap, risks where autonomous agents report successful tests on vulnerable code, specifically in context poisoning and legacy pattern propagation & identifying Security Vuln.

Hackers4u — Remote
Penetration Testing Intern — *Sep 2023 – Oct 2023*

- Executed black-box penetration tests on web applications, identifying critical vulnerabilities (SQLi, XSS, IDOR).
- Automated network enumeration using Nmap and Nessus APIs, reducing manual scanning time by 40%.
- Documented findings in markdown reports for technical and non-technical stakeholders.

CybersecuredIndia — Bangalore, India
Cybersecurity & Digital Forensics Intern — *Dec 2022 – Feb 2023*

- Analyzed malware behavior logs using Python to detect obfuscation patterns.
- Conducted forensic investigations preserving chain-of-custody; reconstructed attack timelines using Registry and Prefetch artifacts.
- Translated findings into actionable risk mitigation plans.

Virtual Testing Foundation — Remote
Information Security Administrator Intern — *Sep 2022 – Nov 2022*

- Mapped adversary behaviors to controls using MITRE ATT&CK to identify gaps.
- Assisted in drafting Information Security and Acceptable Use Policies (ISP/AUP).

Key Projects & Research

SW-WCD-RESEARCH: Web Cache Deception Prototype | *Docker, Nginx, Playwright, R, JS, SQL* Research
- Engineered a complete research testbed to evaluate how Service Workers influence WCD behaviors in CDN-backed architectures.
- Implemented Node.js anomaly detectors to log rewritten URLs and cache indicators.
- Developed attack payloads (e.g., t1-path-sculpting.js) to bypass standard CDN cache armor.
- Designed PostgreSQL schema for trial data storage and statistical power analysis.

The Vibecoding Security Gap (IDAD Evaluation) | *Python, eBPF, Gemini 3.5, Claude Code* Research
- Building `XYZ Bench` to compare Agent-Native IDEs vs. CLI agents across 275 software tasks.
- Measuring hallucinated dependencies and context poisoning rates in autonomous coding.
- Using eBPF to monitor insecure execution patterns in agent-generated code.

Protocol Fuzzing | *Python, Fandango, SMTP, Redis-like Protocol* Course Project
- Designed a stateful Fandango IO grammar for a Redis-like key-value store, enabling valid command sequences (SET/GET/UPDATE) with response validation.
- Simulated an SMTP man-in-the-middle attack by hijacking authenticated sessions to send spoofed emails without hardcoded credentials.
- Used derivation tree constraints and prefix-aware tracking to enforce protocol correctness during fuzzing.

HACKBOT: AI-Powered Automated Exploit Engine | *Python, Meta-Llama 3, RunPod, RAG* GitHub
- Local LLM interface with RAG to query CVE databases without hallucinations.
- Deployed on RunPod with latency/resource optimization.
- Integrated static analysis for auto-generated vulnerability reports.

API-Based NMAP Dashboard | *Python, Flask, REST API* GitHub
- Full-stack dashboard for managing and visualizing Nmap scans.
- Enabled real-time asset visibility and centralized reporting.

Publications

Autoencoder-Driven Machine Learning for Advance Cybersecurity Malware Detection
FMDB Transactions on Sustainable Intelligent Networks, Vol. 1, No. 4, pp. 252–264, 2024.
DOI: 10.69888/FTSIN.2024.000292
Developed an autoencoder-based AI model to detect and classify malware from the EMBER dataset.

Docker Based Decentralized Vulnerability Assessment with Port Scanning
FMDB Transactions on Sustainable Intelligent Networks, 2024.
DOI: 10.69888/FTSIN.2024.000290
Integrated GPT-3 and Docker for efficient, distributed vulnerability scanning in decentralized systems.

API-based Network Scanning, Mapana
In: *Proceedings of National Conference on Emerging Trends in Computer Science*, 2024.
ISBN: 978-93-95830-43-0
Built a Python-Flask API for dynamic Nmap scan profiling and centralized dashboard monitoring.

Enhancing Fog Computing Through Data Center Expansion
SIJSS-UGC Journal (ISSN: 0972–8945), 2023.
Proposed a load-balancing algorithm improving IoT scalability by 40% via distributed resource optimization.

Certifications

Certified Ethical Hacker (CEH v12) — EC-Council
Certified Network Defender (CND v2) — EC-Council
IBM: Python for Data Science — IBM
IBM: Cybersecurity Analyst — IBM
Practical Penetration Testing — TCM Security