Athul Prakash NJ

Security Analyst (VAPT)

Kerala
+91 8921511945
athulprakashnj@gmail.com
https://linktr.ee/psychoSherlock

Summary

Security enthusiast with hands-on experience in **VAPT, application security, and exploit development** across web, mobile, and cloud environments. Skilled in discovering and validating **critical vulnerabilities**, building **security automation**, and delivering **high-quality assessment reports**. Actively engaged in **bug bounty programs, CVE research, and competitive CTFs**, with strong interest in offensive security and continuous learning.

Education

Muthoot Institute Of Technology And Science
BTech Computer Science & Cyber Security
October 2023 - Present

Certifications

Certified AppSec Practitioner (CAP)
The SecOps Group
March, 2024
secops.group

Awards

Top 8 Asia/Oceania Kaspersky{CTF}
Kaspersky
September 2025

1st place in HackAtArch
GEC Thrissur and TinkerHub
March 2025

1st Place in Intercollege CTF
MITS
March 2024

1st in National Level Hackathon
IEEE SB MITS
January 2025

References

Embibe - Hall Of Fame
Bug Bounty Experience
https://www.embibe.com/in-en/vulnerability-...

Hackerone Profile
Bug Bounty Experience
https://hackerone.com/psychosherlock

Rajat Moury
CEO, Apnisec
rajat.moury@apnisec.com

Skills & Tools

Ethical Hacking

networking, exploit, development, cloud, android, linux

VAPT

linux, windows, security, server, web application, burpsuite, sql injection, idor, xss, ssti, ssrf, csrf, buisness logic, frida, nmap

Python & JavaScript

Automation, Selenium, Web Scraping, Flask, FastApi, React, React Native, Vite, NextJs

Cloud & Orchestration

docker, kubernetes, vagrant, fail2ban, falco, scp, tailscale, openvpn, redis, mongodb

Experience

Apnisec — **June 2025 - September 2025**
Security Analyst (VAPT) — Remote
apnisec.com

- Performed **end-to-end VAPT** across **15+ client environments**, assessing **100+ assets per client** including web apps, subdomains, Android apps, and production infrastructure.
- Conducted **asset discovery and attack surface mapping**, identifying exposed services, misconfigurations, and weak trust boundaries.
- Identified and exploited **critical vulnerabilities** including **Account Takeovers (ATO), Authentication & Authorization Bypass, IDOR, Business Logic flaws, Cryptographic Bypass, and XSS**.
- Authored **client-facing security assessment reports** with clear reproduction steps, impact analysis, and remediation guidance, ensuring actionable findings.
- Built **automation scripts** for detecting asset misconfigurations and exposed endpoints; participated in **CERT-In empanelment-style labs** involving reverse engineering and low-level analysis.

VDP Programs — **Jan 2023 - Present**
Bug Bounty Hunter — India

- Reported **high-impact vulnerabilities** including **Account Takeover (ATO), Business Logic flaws, Authentication & Authorization Bypass, IDOR, Rate Limiting issues, and Reflected XSS** across multiple public and private programs.
- Gained **root access to scammer infrastructure and cloud assets** during investigation; performed **responsible disclosure and assisted Kerala Police**.
- Reported **Open Redirection** in a **Next.js application** under a private bug bounty program.

Fetlla — **Jun 2023 - Present**
Security Engineer and Developer — Kerala
fetlla.com

- Developed **custom Nuclei templates** to automate detection of **vulnerable WordPress plugins** and common misconfigurations.
- Published **multiple CVE exploits on Exploit-DB**, leveraging **reverse engineering and offensive testing techniques**.
- Built **5+ Boot2Root CTF labs** using **Docker & Vagrant**, featuring real-world vulnerabilities such as **SSRF, IDOR, and XSS**, and provided **technical mentorship** within the security community.

MITS — **Oct 2023 - Present**
Tech Lead — Kerala
mgmits.ac.in

- Led **authorized security assessments** of campus infrastructure, including exploitation of **Hikvision CVE-2017-7921**, privilege escalation, and coordinated remediation with authorities.
- Served as **Tech Lead** for **ACM & MITS Cyber Security Club**, designing CTF labs and managing **infrastructure, orchestration, and deployment** for events.
- Built and maintained CTF environments using **Docker, AWS, GCP, Oracle Cloud, and Redis**, ensuring scalability and reliability.

Publications

WP Statistics - Time based SQL injection — **February 2022**
Exploit DB
https://www.exploit-db.com/exploits/51711

Attacking Home Routers: The ROM-0 Vulnerability [With Exploit] — **April 2023**
Medium
https://medium.com/@psychoSherlock

Choosing your exploits — **July 2023**
Medium
https://medium.com/@psychoSherlock

Projects

Exploits Developed & Published
exploit-db.com/exploits/51711

CVE-2022-25148 and CVE-2022-25149. Exploit for WP Statistics Plugin <= 13.1.5 ip & current_page_id - Time based SQL injection (Unauthenticated).

exploit, cve, SQL, injection

CTF Boxes

Designed multiple vulnerable Linux labs featuring IDORs, JWT issues, LLM security issues, RCE and privilege escalation, used for hands-on security training and CTFs. Published on Tryhackme, and private CTF competitions

CTF Labs
github.com/psychoSherlock/labs/

Created various levels of labs for CTF's such as Web, Android and Cloud

Managed And Orchestred CTF Infra

During various CTF conductions I've Managed, Orchestred, and Secured multiple cloud environments including AWS, GCP, Oracle. Ensuring flow through CI/CD, Docker environments, IDS using Falco, IPS using fail2ban etc