Reetik Rajan

Security Engineer

A versatile and detail-oriented security engineer with 3+ years of experience, build from scratch expertise in **Blockchain and DevSecOps Security Engineering**, and system architecture. Proficient in Solidity, EVM, Bitcoin and APIs, with a track record of safeguarding assets, leading audits, and optimizing secure infrastructure for **high-growth startups and environments**.

r4reetik@gmail.com

+91 7701857692

New Delhi, India

linkedin.com/in/r4reetik

@r4reetik

SKILLS

Security Engineering | Automated Testing Expertise | Exceptional Critical Thinking | Meticulous Attention to Detail

EVM & Bitcoin Understanding | Building Systems from Scratch | Product Enhancement for Resources

SPEAKER

Twitter(X) Spaces - AMA (07/2024)
Garden Finance & Tail of Bits
https://x.com/r4reetik/status/1816334955414171712

Blockchain Bytes (02/2024)
Blockchained India
https://x.com/r4reetik/status/1758370177870413860

WORK EXPERIENCE

Security Engineer
Zupee

04/2025 - Present   *Gurugram, India*

Impact / Responsibility

- Architected and deployed **AWS Network Firewall** across 16 VPCs, establishing **100% egress traffic** visibility to enable proactive threat blocking.
- Hardened the **Kubernetes (EKS)** security posture by implementing container vulnerability scanning and generating Software Bill of Materials (**SBOM**s) with Syft.
- Re-engineered a **Zero Trust** Network Access (ZTNA) framework across cloud and on-premise infrastructure, enforcing full SSL inspection without exceptions.
- Automated security alert analysis, **reducing manual triage time by 70%** and improving the efficiency of the incident response process.
- Engineered a centralized **SIEM** by integrating **13 security sources**, including Akamai (WAF), SentinelOne (EDR), Wiz (CNAPP), and AWS services.
- Spearheaded a **PII discovery initiative**, mapping sensitive data across 770+ cloud resources to enforce least privilege and minimize data breach blast radius.
- Managed infrastructure and application secrets using **AWS Secrets Manager**, preventing hardcoded credentials and centralizing sensitive data management.
- Fortified web applications against OWASP Top 10 threats by implementing and tuning Akamai **WAF** and **Site Shield** configurations.
- Developed **CSPM** automation to continuously monitor the AWS environment, instantly flagging misconfigurations and newly exposed internet-facing resources. Including the findings from **GuradDuty**, **Cloudtrail**, **AWS Config** and **Security Hub**.
- Implemented **Teleport** for fully audited pod/node access and enforcing EKS micro-segmentation to isolate containerized workloads.

WORK EXPERIENCE

Lead Security Engineer
Catalog

02/2024 - 02/2025   *Hyderabad, India*

Impact / Responsibility

- Designed a secure fund management system using **air-gapped devices** and **multi-sig wallets**, minimizing risks.
- Automated bug tracking services to ensure **zero recurrence** of known vulnerabilities.
- Open-sourced six GitHub repositories adhering to security best practices, increasing industry credibility.
- Established monthly red teaming sessions, identifying over **20 improvement** opportunities.
- Integrated **agile security** practices into development workflows, reducing feature deployment delays by 70%.
- Launched a bug bounty program, maintaining a resolution **SLA of just 2 hours** per submission.
- Implemented chaos engineering tools to assess system limitations and inter-service dependencies.
- Reduced AWS **server costs** for development environments by **25x** through strategic resource optimization.
- Authored a risk-based threat model, approved by C-suite executives, focusing on "no fund loss" and "meeting external commitments".

Product Security Analyst
Catalog

08/2022 - 02/2024   *Hyderabad, India*

Impact / Responsibility

- Engineered a **kill switch** for services, enabling system shutdown within 30 seconds to prevent exploitation during critical incidents.
- Discovered and mitigated 2 attack vectors and **1 critical** vulnerability during internal smart contract audits.
- Coordinated with **PeckShield** for external audits, ensuring timely information exchange and report delivery.
- Implemented **Wazuh** as SIEM for alerting and monitoring, enhancing visibility into computation and transaction behaviors.
- Investigated and resolved a critical miscalculation issue, saving **$120,000** worth of assets.
- Reduced backend latency by **80%** through AWS VPC optimization, improving system availability.
- Conducted load testing on a proprietary L2 blockchain with **10,001 nodes**, monitored using **Prometheus** and **Grafana**.
- Facilitated secure fund withdrawal plans post-Ren shutdown, ensuring **zero asset loss**.
- Spearheaded four months of R&D, demonstrating rapid learning and delivering POCs on emerging technologies.
- Took over DevSecOps responsibilities, integrating security into development workflows after the departure of the DevOps lead.

Product Security Analyst (Continued...)
Catalog

Impact / Responsibility

- Introduced "shift-left" security practices, embedding security in the development lifecycle for a new product, Garden Finance. This reduced pre-production security **audit time to three days**.
- Performed an internal audit of cross-chain **Smart Contracts**, **Bitcoin scripts**, and Web2 integrations, identifying two writable SQL injections and **eight fund-loss vulnerabilities**.
- Built CI/CD pipelines with approval mechanisms, leveraging AWS IAM and Secrets Manager for **secure deployments**.
- Implemented **Sentry** and AWS **CloudWatch** for advanced log management and debugging.
- Managed end-to-end external audits with **Trail of Bits**, delivering comprehensive technical and game-theoretical insights.
- Developed Discord bots for **anomaly detection**, resource monitoring, and DEX flow alerts, strengthening operational oversight.
- Explored Apache **Kafka** for blockchain monitoring with partial success.
- Set up custom **SonarQube** workflows in **GitHub Actions** for automated code quality checks.
- Improved system-wide latency by **10x** using AWS API Gateway.

WORK EXPERIENCE

Application Security Intern
Catalog

01/2022 - 07/2022   *Hyderabad, India*

Impact / Responsibility

- Mapped the entire system architecture and business logic. Documented all actors and flows in **diagrams**, making the system accessible even for non-technical stakeholders. This enhanced team understanding and accelerated onboarding at the early **startup** stage.
- Achieved 99% statement and 100% branch test coverage for EVM Smart Contracts using **Hardhat**, **Chai**, and **Mocha**.
- **Optimized gas** usage by 7% through Solidity updates after identifying inefficiencies during testing.
- Conducted security analysis with **Slither** and **Mythril**, addressing optimization-level findings.
- Implemented **six** additional security headers and patched XXS and CSRF vulnerabilities, fortifying frontend security.
- Conducted API security testing based on the **OWASP** checklist. Discovered and resolved **three critical vulnerabilities** in APIs.
- Redesigned backend **input validation** processes to enforce type safety and eliminate runtime errors across all system entry points.
- Developed a CLI-based transaction **troubleshooter** to improve support efficiency by reducing response time.

Security Practitioner Intern
Azure Skynet

04/2018 - 06/2018   *Delhi NCR, India*

Impact / Responsibility

- Conducted internal and external **network penetration testing**, identifying vulnerabilities in network configurations and protocols.
- Performed system audits to uncover weaknesses in **endpoint security**, privilege management, and access control mechanisms.
- Evaluated security tools and techniques for real-time threat detection and mitigation.
- Documented findings and recommendations in **detailed reports**, aiding stakeholders in understanding security gaps and remediation steps.

CERTIFICATES

CEH (02/2021 - 02/2024)
Certified Ethical Hacker (CEH) is a core training program for an information security professional by EC-Council.

OSINT (05/2021)
Open-Source Intelligence (OSINT) is a methodology for collecting, analyzing and making decisions about publicly available data by TCM Security.

AWS CCP (11/2022 - 11/2025)
The AWS Certified Cloud Practitioner offers a foundational understanding of AWS Cloud concepts, services, and terminology.

CONSULTANT EXPERIENCE

Mindler
Web2 Services and APIs - Penetration Testing

08/2023 - 02/2020

Accomplishment

- Secure implementation of their **payment gateway** and enhancements in managing account data - **PII**.

SAFU
Smart Contract Audits

02/2023

Accomplishment

- An **audit report** was submitted detailing **seven findings** and their respective solutions.

CONSULTANT EXPERIENCE

Dr. Code
Responsible and Secure use of AI

10/2024 - Present

Accomplishment
- Enhance **product** robustness and prevent unexpected behaviors by mitigating **prompt injections**.

PERSONAL PROJECTS

BixMix - Zero Knowledge Bitcoin bridge (12/2024)
- A zero knowledge bitcoin bridge using citrea's tech.
- Won ETHIndia 2K24.

DPI - Decentralised Payment Interface (12/2022)
- DPI (yes, it's inspired from UPI) stands for decentralized payment interface, it is a non-custodial payment interface for on chain payments.
- **Won** $2,000 at ETHIndia 2K22.
- https://github.com/r4reetik/dpi/

zkRizz (12/2023)
- The Web3 dating platform that uses zero knowledge proofs to verify identity and match users.
- **Won** $1,250 at ETHIndia 2K23.
- https://github.com/r4reetik/zk-rizz/

Kademlia p2p (01/2023)
- Implementation of Kademlia research paper in Golang for chatting platform.
- https://github.com/r4reetik/kademlia-p2p/

Debloat Android (07/2022)
- Remove system apps from your android device with a UI for non-tech people.
- https://github.com/r4reetik/debloat-android-archive/

EDUCATION

Bachelor of Technology - Computer Science Engineering
Echelon Institute of Technology

08/2018 - 07/2022   *8.022 CGPA*