Rootconf 2025 Workshop: Detecting Supply Chain Attacks at Runtime with eBPF

Rohit Kumar (@rohitcoder)

Who am I?

- Handle - @rohitcoder (LinkedIn, Github, Medium)
- Product Security Engineer @ Groww
- Top 20 Security Researcher at Meta Bug Bounty since last 5 years
- Maintaining multiple open-source Security projects
- Building Source Code Security tools day and night for years.

Why Runtime Security?

- Static tools look at code, not behavior.
- Most attacks execute only in CI/CD or production — post-build.
- Runtime = observe real behavior: file reads, shell spawns, exfiltration.