Shoeb Patel

APPLICATION SECURITY ENGINEER

London, UK

patelshoeb4@gmail.com | shoebpatel.com | github.com/shoebpate1 | linkedin.com/in/iamshoebpatel

Work Experience

Amazon

Oct. 2022 - Present, London, UK

SECURITY ENGINEER II, CORPORATE TECHNOLOGY

July 2025 - Present

- Application security engineer for Amazon's corporate technology org (HR, Finance, Legal), running threat modelling, design and code review, and pentesting for new web apps, APIs, and AI products, covering prompt injection, MCP attack surface, and authorisation architecture for agents.
- Moved security review into the pull request by building a multi-agent workflow and the org-wide detection ruleset behind it, baselining each repo then flagging new issues and broken invariants on every change, and cut review time from a month to a week.
- Owned security for an internal legal AI platform, finding a confused deputy flaw where the agent queried with its own privileges instead of the caller's, exposing the full case corpus.
- Owned security for Amazon's identity provider consolidation, finding a cross-tenant authorisation flaw where a user permitted on one tenant could reach another, fixed before company-wide rollout.
- Led bot abuse mitigation for Amazon's public hiring portal, where automated schedule booking fed a resale market charging candidates up to $2,000, mapping all endpoints and abuser personas to replace two years of point fixes with one layered, measurable strategy along with metrics that define success.
- Built the security training for the org's apprentice engineers, taking them from how the web works to spotting vulnerabilities on their own, now the standard course for every new apprentice.

SECURITY ENGINEER II, AWS

Oct. 2022 - July 2025

- Application security owner for AWS networking services (VPC, Elastic Load Balancing, Transit Gateway, VPC Lattice, CloudWAN), running threat modelling, architecture and code review, and pentesting across a portfolio serving 2000+ engineers.
- Owned a full-scope security assessment of Transit Gateway, mapping an undocumented architecture end to end and surfacing 53 issues through pentesting.
- Influenced early-stage design of high-scale distributed systems, negotiating security trade-offs with service teams and leadership, and uncovering critical flaws in production APIs that had been vulnerable since launch.
- Uncovered RCE deep in AWS internal infrastructure, in a component deployed across thousands of internal services.

Flipkart

Bangalore, India

SENIOR SECURITY ENGINEER

Oct. 2019 - Sept. 2022

- Application security owner for Seller and Support platform teams, running threat models, architecture reviews and code reviews across web apps, microservices, the Kubernetes platform and mobile applications.
- Designed the vulnerability feedback loop, using each reported bug for RCA, variant analysis, a centralised fix, a permanent detection query in the scanning suite, and developer training material, so the same class could not recur.
- Deployed CodeQL SAST across the top 50 repositories, uncovering 10+ critical and 100+ valid issues, and led the triage programme.
- Ran the private invite-only bug bounty programme, owning triage through to patch verification, and started an internal red team with the same model, personally finding issues worth $30,000 in bounty value.
- Developed and hosted CTF competitions twice yearly, built from real vulnerabilities found on Flipkart assets.
- Promoted from Security Engineer to Senior Security Engineer in Aug. 2021.

BrowserStack

Mumbai, India

SECURITY ENGINEER

Jun. 2019 - Oct. 2019

- Among the first hires on a new security team, building application security from scratch including the company's first asset inventory, threat modelling and review process, and red team testing of production applications.
- Built an in-house system that continuously monitored public sources for leaked BrowserStack source code and credentials.
- Deployed Wazuh as the team's first detection capability, covering AWS control-plane, network and application-layer events.

Google

Remote

STUDENT DEVELOPER, GSOC 18 & MENTOR, GSOC 19

Apr. 2018 - Jun. 2019

- Selected for Google Summer of Code to extend OWASP Juice Shop, OWASP's flagship deliberately-vulnerable application, used worldwide for security training and CTFs.
- Built 11 security challenges covering SSTI, SSRF, NoSQL injection, mass assignment, HTTP parameter pollution, XSSi, race conditions and a Zip-Slip dependency flaw, each backed by working e-commerce features in Node.js and AngularJS with unit, integration and E2E tests. Project report.
- Returned as a GSoC mentor in 2019, guiding selected students through challenge design, secure implementation and upstream contribution.

CVEs & Blogs

2022 [Security Tooling] **Automata: automation platform for recon and continuous leak monitoring**

2022 [AppSec] **How Flipkart Reacts to Security Vulnerabilities**

2021 [Security Research] **CVE-2021-32817 *Collision* - The Secret Parameter, LFR, and RCE in NodeJS Apps**

2021 [Security Research] **CVE-2021-22255 - SSRF Vulnerability in BaseRow**

Bug Bounty & Open Source

NOTABLE COMPANIES SECURED (30+ TOTAL)

• Google • Amazon Web Services • U.S. Department of Defense • GitHub Security Lab (CodeQL) • Oracle • Intel • MasterCard

• 100% of reports accepted as valid, holding the maximum Signal rating on HackerOne and BugCrowd

OPEN SOURCE CONTRIBUTIONS

• Metasploit • OWASP Zaproxy • OWASP Juice Shop • Subfinder • Reconnoitre • NoSQLMap • GitDump • freeCodeCamp

Skills

Security

• Threat Modelling • Web/API/Mobile Testing • Secure Code Review • LLM & Agent Security • Cloud Security • Bug Bounty

Programming

• Python • JavaScript / Node.js | Code review: Java • TypeScript • C/C++

Platforms, Tools & Frameworks

• Claude Code • Kubernetes • AWS • Containers • Burp Suite • Caido • CodeQL

Community

2019 - 2021 **UnderDawgs**, Founder & Captain, CTF team (CTFtime) *India*

June 2020 **BSides Ahmedabad**, CTF Organizer & Challenge Writer *India*

Education

NIT Goa (National Institute of Technology) *Goa, India*

B.TECH. IN COMPUTER SCIENCE AND ENGINEERING, CGPA 8.53/10 *July 2015 - Apr. 2019*