Dear Hiring Team,

I am writing to apply for the Security Engineer role at Geico because I want to help evolve offensive security at scale within an organization that balances user trust, regulatory pressure, and product velocity. My background in hands-on penetration testing, secure backend development, and building automated vulnerability workflows positions me to deliver measurable security and compliance outcomes for Geico.

At Zenith Bank and in personal projects, I led large tactical assessments across web, API, and cloud targets using Burp Suite, SQLMap, Metasploit and custom Python/PowerShell scripts, discovering 15+ vulnerabilities and producing prioritized remediation plans aligned to OWASP Top 10. I've built automation to ingest and normalize security findings, integrating OWASP and NIST guidance to support PCI DSS readiness and executive risk reporting—work that directly mirrors Geico's need for scalable penetration testing and regulatory alignment.

I'm experienced with attack-path development and red/purple teaming concepts, and I've developed tooling (Go, Python) for host discovery, protocol fingerprinting, and exploitation workflows that improve speed and reproducibility of assessments. I coach engineers through secure design and testing practices, translating technical findings into clear business risk decisions—an ability I'll bring to collaborate with Blue Teams, Threat Intel, and leadership at Geico.

I'm excited by the opportunity to design advanced threat emulation scenarios and build automated offensive capabilities that reduce risk and improve compliance posture. I welcome the chance to discuss how my blend of offensive skill, automation-first mindset, and compliance-focused experience can help strengthen Geico's security program.

Sincerely,
Osayemwenre Sam Jegbefumwen
jegbefumwenosayemwenre@gmail.com
+1 (323) 946-1946