Brett Bergin

Email: brettberginbc@yahoo.com | **Phone:** (408) 300-3210 | **Location:** Bakersfield, CA
GitHub: https://github.com/brettbergin/ | **GPG:** 5A35 BE3F 200D 3389 EB4D 8F9A 1354 C7F6 593D 4B54

Professional Summary

Senior application security engineer with 10+ years developing and operationalizing comprehensive security programs for enterprise organizations. Proven expertise in vulnerability management, penetration testing, security automation, and DevSecOps at scale. Strong technical background in cloud security, risk assessment, security architecture, and distributed systems with a track record of implementing Zero Trust security solutions supporting millions of users. Experienced in compliance frameworks including GDPR, SOX, and PCI-DSS. Active developer of AI-powered security tools and Model Context Protocol (MCP) servers for enhanced productivity in red team operations, network security monitoring, and security automation workflows.

Key Achievements

- Designed OAuth-based identity solution supporting 10+ million users
- Built automated vulnerability management program with comprehensive reporting and distribution
- Deployed vulnerability scanning infrastructure covering 500,000+ compute endpoints in OpenStack environment
- Implemented Splunk-based security analytics platform for web traffic analysis
- Developed IoT network forensics solution for traffic pattern anomaly detection and protocol analysis
- Created automated network traffic capture system with deep packet inspection integration
- Architected vulnerability tracking solution mapping security issues to system owners across enterprise

Core Competencies

Application Security	Vulnerability Management	Security Operations
Threat Modeling	Penetration Testing	Threat Detection
Security Automation	Risk Assessment	Incident Response
SAST/DAST/IAST	Network Forensics	SIEM/SOAR
DevSecOps	Compliance Management	Threat Hunting

Open Source Projects

Project	Description
adversary-mcp-server	Model Context Protocol server for adversarial security testing and red team operations
pihole-mcp-server	MCP integration server for Pi-hole DNS filtering and network security monitoring
ChatGPTCodeScanner	AI-powered static analysis tool using ChatGPT, Python & Flask

CalGEMDataIngest	Data pipeline for California Department of Conservation using Python & Jupyter
SystemStatsAPI	System telemetry collection and API service in Python & Flask
DisableMySSH	AWS security automation to disable SSH access from 0.0.0.0/0
DisableMySSH-Infra	Terraform infrastructure automation for DisableMySSH

Technical Skills

Security Tools: Burp Suite Professional, Metasploit Framework, OWASP ZAP, SQLMap, Nmap, Bettercap, MITMProxy, TCPDump
SIEM/Analytics: Splunk, ELK Stack, SOAR platforms
Cloud Security: AWS Security Hub, AWS GuardDuty, Azure Security Center, Cloud Security Posture Management
Platforms: Kali Linux, AWS, Azure, OpenStack, Docker, Kubernetes
Languages: Python, SQL, Bash, JavaScript, PowerShell
Frameworks: Flask, Terraform, Ansible, Jenkins
Security Testing: SAST, DAST, IAST, Static Code Analysis, Dynamic Analysis
Compliance: ISO 27001, NIST Cybersecurity Framework, PCI-DSS, GDPR, SOX
Specializations: Zero Trust Architecture, DevSecOps, IAM, Multi-Factor Authentication, Risk Assessment, Security Architecture, Threat Hunting, Incident Response, Security Governance

Work Experience

Senior Application Security Engineer

OnePay - Remote
September 2024 - Present

- Lead application security initiatives for fintech payment processing platform serving financial APIs
- Implement PCI-DSS compliance controls and security frameworks for payment card data protection
- Design and deploy DevSecOps practices with security testing automation in CI/CD pipelines

Senior Application Security Engineer

Cisco Systems Inc. / Meraki - Remote
April 2022 - September 2024

- Implemented SAST/DAST tools with CI/CD integration for enhanced vulnerability detection across cloud infrastructure
- Designed and deployed Zero Trust security controls and multi-factor authentication frameworks
- Led red team exercises and penetration testing initiatives for cloud infrastructure and APIs

Information Security Engineer

Mode Analytics - Remote
January 2020 - February 2022

- Developed company-wide threat model identifying attack vectors and OWASP Top 10 threat scenarios
- Managed penetration testing and bug bounty programs with validation and remediation workflows

- Created automated security review process with SAST/DAST integration and SLA reporting

Director, Application & Product Security

Ring.com - Remote
April 2018 - November 2019

- Established application and offensive security teams through strategic hiring and vendor partnerships
- Developed penetration testing program for consumer IoT products and cloud services
- Created managed bug bounty strategy for secure product launches

Senior Manager, Information Security

Ring.com - Remote
January 2017 - April 2018

- Built comprehensive security operations framework and integrated security assessments into release cycles
- Developed automated SAST solution with CI/CD pipeline integration
- Designed custom risk ranking methodology combining SLA requirements and CVSS scoring

MTS 1, Data Science Engineer – Security Data Science

eBay Inc. - Remote
March 2016 - January 2017

- Created executive dashboards and actionable reports for threat and risk exposure analysis
- Developed risk and threat data models to assess financial, legal, and brand impact scenarios
- Built data aggregation pipelines for predictive security breach impact modeling

MTS 1, Information Security Engineer – Vulnerability Management

eBay Inc. - San Jose, CA
November 2014 - March 2016

- Designed high-performance vulnerability scanning architecture covering 500,000+ endpoints with concurrent processing
- Created automated patch management integration for security patch deployment
- Developed risk ranking algorithms to prioritize vulnerability remediation efforts

Information Security Engineer 3 – Application Security

eBay Inc. - San Jose, CA
December 2012 - November 2014

- Developed penetration testing methodologies and conducted assessments on mobile applications and web services
- Created security policies and remediation procedures for operational teams
- Integrated security assessments into software development lifecycle processes

References

Robert Meives | Senior Manager, Engineering | Charter Communications
San Luis Obispo, CA | (805) 305-8853 | Rob.Meives@chartercom.com

Lance Harris | Chief Information Security Officer | Esurance
San Francisco, CA | mr.lance.harris@gmail.com

Steve Pace | Senior Vice President, Global Sales | Core Security Technologies
Boston, MA | (626) 200-5124 | space@coresecurity.com