Behrad Taher

McLean, VA | behradtaher@gmail.com | https://behradtaher.dev | https://linkedin.com/in/behradtaher

Senior Security Engineer with 7+ years securing cloud-native web applications and distributed systems through offensive security, security platform engineering, and automation. Proven record of discovering critical vulnerabilities, building widely adopted security products, and influencing organization-wide security decisions.

EXPERIENCE

Senior Security Engineer - Amazon (June 2022 - Present)

- Executed 26 penetration testing engagements across web applications, APIs, and cloud infrastructure, identifying 100+ vulnerabilities (12 critical, 30 high) including RCE, SQLi, SSTI, XXE, SSRF, and authentication bypass
- Led 4-month emergent penetration test of healthcare platform directed by CISO; identified 59 findings (9 Critical, 10 High) across 2,400+ APIs including Account Takeover, RCE, and SQLi that influenced strategic deprecation decisions
- Conducted security research initiative discovering 14 RCE vulnerabilities across Ruby-on-Rails applications through systematic analysis of code injection, SSTI, reflection, and insecure deserialization patterns
- Architected full-stack reporting platform (Python/Flask, AWS Lambda, DynamoDB) managing 5,900+ pentests and 8,000+ findings; replaced 3P tool saving $200k/year achieving 100% user satisfaction and 10 hours saved per pentest
- Designed AI-assisted reporting interface using AWS Bedrock with document aggregation pipeline consolidating architecture diagrams, historical findings, and security reviews; achieved 95% adoption across 369 users with 11,500+ AI-assisted content generations
- Evaluated AI-powered security testing tools (black-box DAST, code-aware DAST, LLM-assisted code analysis); assessed effectiveness at identifying business logic vulnerabilities and complex vulnerability chains versus traditional methods
- Engineered internal automation platform (CDK, Lambda, EventBridge) with self-service deployment framework and shared Python library abstracting AWS auth and 3P integrations; adopted across 40+ tools/automations saving 2,550 hours annually
- Established org-wide tooling governance and penetration testing reporting standards; defined tool lifecycle management, severity frameworks, and quality bar across 36 tools and 7 teams

Application Security Engineer - Hyperscience (March 2021 - May 2022)

- Performed threat modeling, code reviews, and penetration testing across 6 major product releases for ML-powered document processing platform
- Built automated DAST scanning pipelines using OWASP ZAP, Ansible, Terraform and GitLab CI; implemented and configured AWS SecurityHub, Inspector, GuardDuty, and WAF, triaging 1,000+ findings
- Hardened application security controls including CSP, SRI, and secrets management for SaaS launch on EKS
- Created secure coding training for engineering teams; published security advisories and addressed customer inquiries

Security Engineer - Verizon (June 2018 - March 2021)

- Led engineering and scaling of enterprise Nessus deployment (20+ scanners across 10+ datacenters and AWS networks) targeting ~100,000 assets; increased scan frequency by 300% and coverage by 50%
- Integrated vulnerability scanning into AWS build process, terminating vulnerable instances pre-deployment; integrated with Splunk, CyberArk for downstream automation
- Conducted web application security testing of PCI environments and Bug Bounty program targets
- Provided security assessments of golden images deployed to ~50,000 servers monthly

EDUCATION & CREDENTIALS

George Mason University, Volgenau School of Engineering - Fairfax, VA

- **M.S.** Applied Information Technology, Cybersecurity (2020)
- **B.S.** Applied Information Technology, Information Security (2018)

OSWE | **OSWA** | **OSCP** | **OSWP** | **SSCP** | **AWS Security Specialty** | **AWS Solutions Architect Associate** | **CCSK**
CVE-2021-43481 - Discovered SQL Injection vulnerability in WebTareas 2.4p3