Kayvon Karimi

Folsom, CA 95630 | cyberbykayvon@gmail.com | cyberbykayvon.com | LinkedIn | GitHub

Professional Statement

Cybersecurity professional (MS Cybersecurity Engineering, Dec 2025) transitioning from full-stack development to Application Security with 6+ years of secure coding experience. Completed 320-hour intensive pre-apprenticeship gaining hands-on expertise in penetration testing, vulnerability assessment, and OWASP Top 10 controls. Built 100+ production websites with security-first architecture and developed a full-stack security analytics platform. Focused on securing web applications, APIs, and cloud infrastructure while bridging development and security teams.

Skills

Technical Skills: Network & Web Application Exploitation • Penetration Testing • Vulnerability Assessment • Server Hardening • Incident Response • Packet Analysis • Traffic Decryption • Bash/Python Scripting • Linux/Windows Administration • API Security & Rate Limiting • CORS Configuration • Session Management & Fingerprinting • Threat Modeling • System Forensics

Security Tools & Technologies: Burp Suite • OWASP ZAP • Nmap • Metasploit • SQLmap • FFUF • Gobuster • Nikto • Wireshark • Nessus • OpenVAS • Wazuh • Splunk • Snort • Security Onion • ELK Stack • Hashcat • John the Ripper • Aircrack-ng • Airmon-ng

Web Development & Application Security: FastAPI • React • Flask • SQLAlchemy • REST APIs • JavaScript • HTML/CSS • PHP • MySQL • PostgreSQL • Vite • Axios • OpenSSL • Apache2 HTTPS • PKI/TLS/SSL • X.509 • Certificate Authority Configuration • WordPress Hardening • Input Sanitization • Parameterized Queries • Django • JSON Web Tokens • Browser Dev Tools

Infrastructure & Cloud: AWS (EC2/S3/IAM/Security Groups) • Azure • Docker • Kubernetes • Active Directory • Windows Server • VirtualBox • Pi-hole • WireGuard • Railway • Vercel • iptables • Terraform • Nginx Reverse Proxy

Frameworks, Standards & Compliance: OWASP Top 10 • NIST 800-53 • MITRE ATT&CK • CIS Benchmarks • ISO 27001 • SOC 2 • CVE/CVSS • DISA STIGs • Zero Trust Architecture • CIS Controls v8 • NIST SP 800-260

Education

University of San Diego **Dec 2025**

Master of Science, Cybersecurity Engineering (GPA: 4.00) *San Diego, CA*

•**Achievements:** Capstone in enterprise security hardening and remediation

Texas A&M University **May 2012**

Bachelor of Arts, Psychology, Minor in Business Administration (GPA: 3.4) *College Station, TX*

•**Achievements:** Men's D1 tennis team

Certifications & Training

- **CompTIA Security +:** Expected December 2025
- **OverTheWire Natas Wargames:** July 2025
  *Web application security challenges covering SQL injection, XSS, authentication bypass, and command injection.
- **Cyber Proud Cybersecurity Pre-Apprenticeship (320 hours):** May 2025
  *Completed a 16-week intensive training in security fundamentals, cryptography, cloud security, and web security.
  *Developed proficiency in Windows/Linux, Active Directory, PowerShell, AWS, Docker, Kubernetes; hands-on with pentesting, vulnerability assessment, SIEM, IDS/IPS.
- **TryHackMe:** February 2025 - Present
  *Hands-on cybersecurity labs covering network security, penetration testing, vulnerability assessment, and incident response.
- **Harvard: VPAL Cybersecurity - Managing Risk in the Information Age:** August 2023
- **Google Foundations of Cybersecurity:** July 2023

Cyber Security Projects

GhostTrack – Security Analytics Platform | Capstone Project * | GitHub **Oct 2025 – Current**

Independent Project

- Developed full-stack security analytics platform using React, FastAPI, PostgreSQL with behavioral bot detection, threat intelligence, and real-time session tracking.

- Built RESTful API with SQLAlchemy ORM for event ingestion, analytics aggregation, device fingerprinting, and deterministic visitor identification.

WordPress Security Infrastructure Hardening | Report **Oct 2025 - Nov 2025**
Cyber Proud
- Detected 5 threat actors; deployed defense-in-depth architecture (IDS/IPS/WAF) with geographic blocking of 5M+ malicious IPs.
- Hardened Apache with security headers (CSP, HSTS, X-Frame-Options); deployed Wordfence WAF blocking 47 attacks in 24 hours.

Security Hardening & Vulnerability Remediation | YouTube **Aug 2025 - Nov 2025**
Design World
- Remediated 35 critical vulnerabilities including EternalBlue/SMBv1 across 8-host environment; disabled RDP, hardened Active Directory, modernized SSL/TLS, enabled host firewalls; validated via Nessus achieving 0 exploitable findings.
- Produced comprehensive security report with NIST/CIS-aligned remediation procedures, before/after metrics, and Zero Trust architecture recommendations.

Internal Penetration Test | Active Directory & Network Exploitation | Report **Sep 2025 - Oct 2025**
Design World
- Exploited SMBv1 (MS17-010/EternalBlue) for RCE and lateral movement across segmented enterprise hosts.
- Identified weak SSL/TLS ciphers (SWEET32, RC4) and recommended cryptographic hardening for Active Directory environment.

Web Application Vulnerability Assessment | eCommerce Platform | Report **Aug 2025 - Sep 2025**
Court Crate
- Performed reconnaissance and enumeration using Nmap (SYN stealth scans, service version detection) and Tenable Nessus, identifying 26 vulnerabilities across 2 severity tiers (0 critical, 2 medium).
- Mapped findings to OWASP Top 10 with CVSS risk ratings and delivered executive/developer remediation reports.

VPN Client Monitoring with Wazuh SIEM | AWS Cloud Deployment | Report **June 2025 - Jul 2025**
University of San Diego
- Provisioned and configured AWS EC2 instance to deploy a secure, cloud-based VPN infrastructure using Pi-hole for DNS-level ad/tracker blocking and PiVPN (WireGuard) for encrypted remote access.
- Integrated Wazuh SIEM/XDR to enable centralized log aggregation, correlation rules, and alerting mechanisms for VPN client activity.

Wireless Traffic Capture & WPA2 Cracking | Capstone Project * | YouTube **Feb 2025 - Apr 2025**
Cyber Proud
- Captured and decrypted 5,000+ WPA2-encrypted 802.11 frames using monitor mode and aircrack-ng to crack weak Wifi passwords.
- Analyzed over 5,000 decrypted traffic in Wireshark, exposing DNS, TLS, ARP, SSDP, LLMNR metadata and endpoint behavior.

Professional Experience

Court Crate | *Security Project Manager* **Oct 2019 – Present**
Remote
- Built and managed a secure e-commerce platform with WordPress hardening, user authentication, HTTPS/TLS, and uptime SLAs.
- Implemented web application security controls, including SSL/TLS enforcement, plugin audits, and regular vulnerability patching to protect user data and maintain platform resilience.

Broadstone Sports Club | *Operations & Technology Specialist (Part-Time)* **May 2023 – Present**
Folsom, CA
- Manage client database, scheduling systems, and payment processing with data privacy and security best practices.
- Develop training programs and operational processes, ensuring compliance with organizational policies and procedures.

Tri-Force Marketing | *Web Developer* **Feb 2015 - May 2021**
Dallas, TX
- Developed 100+ full-stack websites (HTML5, CSS3, JavaScript, PHP, MySQL) with secure form handling, authentication, and server-side validation.
- Implemented input sanitization and parameterized queries to prevent XSS, CSRF, and SQL injection per OWASP Top 10.
- Configured SSL/TLS, access controls, and log analysis to strengthen deployment security and operational monitoring.