Kevin
Guarnes

Vancouver, WA
(503)927-3237
kevinguarnes@gmail.com
linkedin.com/kevinguarnes
github.com/kevinguarnes
kevinguarnes.github.io

EXPERIENCE SUMMARY

● Transitioning from a successful leadership role in hospitality management to a thriving career in cybersecurity, leveraging strong analytical and problem-solving abilities.
● Recently graduated from an intensive cybersecurity bootcamp, gaining hands-on expertise in full-stack development, threat detection, and data protection.
● Demonstrated leadership and a track record of maintaining high standards of service and operational security in fast-paced environments.
● Highly adaptable, bringing a unique cross-functional skill set and the ability to solve complex cybersecurity challenges with a fresh perspective.

SKILLS SUMMARY

Programming/Development:	Phyton, C#, JavaScript, HTML/CSS, SQL, Bash/Shell Scripting, Secure Software Development, Containerization (Docker), Data Protection and Encryption, Cloud Security and Database Management.
Frameworks/Libraries:	JQuery, React, Angular.
Database:	SQL, Microsoft SQL, Oracle Database, MongoDB,
IDEs:	Visual Studio Code (VS Code)
Project Management:	Azure DevOps
Version Control:	GitHub
Non-Technical:	Interpersonal Skills, Problem-Solving Skills, Adaptability and Flexibility, Customer Service, Emotional Intelligence

WORK EXPERIENCE

Restaurant and Bar Manager
Salty's on the Columbia, Portland, OR | May 2021 - Present

- Monitored beverage preparation and presentation quality, established performance and customer service standards, organized training programs, resolved personnel issues.

Banquet Captain
LifeWorks Restaurant Group @ Nike WHQ, Beaverton, OR | February 2014 - September 2020

- Assigned work schedules and ensured timely service delivery, trained workers in procedures and company policies, resolved customer complaints, maintained cleanliness.

Restaurant and Bar Manager
Ivories Jazz Lounge and Restaurant, Portland, OR | November 2011 - March 2014

- Trained workers in food preparation, service, and safety, supervised bar and dining activities, estimated food and beverage needs.

Cybersecurity Analyst (Intern/Student Live Project)
Prosper IT Consulting, Portland, OR | September 2024

- Conducted offensive and defensive security tasks, including executing SQL injections to bypass login authentication, performing brute force attacks to reset admin passwords, exploiting CAPTCHA vulnerabilities using Burp Suite, and analyzing malware-infected network traffic with Wireshark, identifying malicious files, domains, and remediation strategies.

Kevin
Guarnes

Vancouver, WA
(503)927-3237
kevinguarnes@gmail.com
linkedin.com/kevinguarnes
github.com/kevinguarnes
kevinguarnes.github.io

EDUCATION & TRAINING

Certification in Cyber Security | The Tech Academy | April 2024 – September 2024

- Completed a comprehensive Cyber Security & Full-Stack Development Bootcamp, gaining hands-on experience in full-stack web development (HTML, CSS, JavaScript, SQL, Java, Swift) and cyber security, including network security, VPNs, threat detection, ethical hacking, software/mobile app security, database protection, and end-user security awareness.

Student Live Project | The Tech Academy | September 2024

As part of a hands-on cybersecurity project, I successfully executed various offensive and defensive security tasks using industry-standard tools like Burp Suite and Wireshark. My responsibilities spanned from identifying and exploiting vulnerabilities in web applications to conducting thorough network traffic analysis for malware infections.

Key Responsibilities:

- **Offensive Security:**
  - Bypassed login authentication mechanisms (both admin and user accounts) by leveraging **SQL Injection** techniques on the OWASP Juice Shop platform, successfully gaining unauthorized access to sensitive accounts.
  - Conducted a **brute force attack** using Burp Suite to discover admin credentials and reset the password on a compromised account.
  - Exploited weak CAPTCHA mechanisms by flooding the system with multiple HTTP requests, effectively bypassing its security with **CAPTCHA flood attack** tactics.
- **Defensive Security:**
  - Utilized **Wireshark** to analyze malware-related network traffic, identifying malicious files and associated IP addresses, MAC addresses, and hostnames.
  - Detected and documented malware types such as **Trojan.Qbot/Qakbot** by extracting and analyzing **SHA256 hashes** using VirusTotal and similar platforms.
  - Investigated **malware traffic** on compromised systems, tracing infections to suspicious domains and proposing remediation strategies like endpoint security and user awareness training.

Tools and Technologies:

- **Burp Suite**: For executing SQL injections, brute force attacks, and CAPTCHA exploitation.
- **Wireshark**: For network traffic analysis and malware detection.
- **VirusTotal**: For verifying malware hashes and understanding threat levels.

Results:

- Demonstrated the ability to find and exploit critical vulnerabilities in web applications, improving awareness of the need for robust input validation and password protection.
- Identified and mitigated malware infections by analyzing traffic data and implementing strong security recommendations, such as rate-limiting, strong CAPTCHA systems, and network monitoring.