Business Goose Resume v0.2

Seattle, WA (646)884-2886 business@goose.art goose.business

Technical analyst with **6 years** experience in ***web application security***, ***data science***, and ***IT management***. Strong foundations in network security, Linux internals, and DevOps practices.

Skills

Application Security: Burp Suite, OWASP ZAP, OWASP Top 10, Threat Modeling, Wireshark, nmap, Metasploit, sqlmap, radare2, Ghidra
Development: AWS (IAM, CloudWatch, CloudTrail, CodeDeploy/CodePipeline), Docker, Kubernetes, GCP, Terraform
Programming Languages: R, Python, Bash, Java, C, Node.js, SQL

Experience

Macmillan Learning | New York, NY
Data Management Specialist Aug 2016 - Jan 2019
Key Skills: Python, R, Microsoft Excel, Google Sheets. Salesforce, SQL, PowerBI
- Designed pipeline systems to ensure database data was quickly integrated into Salesforce CRM.
- Maintained and managed large spreadsheets and databases in Excel, Google Sheets, and an Oracle SQL database.
- Developed automated cleanup system for millions of malformed address records, saving thousands
- Built dashboards in R that ingested company data and visualized metrics.

Search on Dora | Remote
Data Operations Lead Mar 2022 - Oct 2024
Key Technologies: Kubernetes, AWS (S3, DynamoDB, Aurora, CloudWatch, EC2, EKS), Python, GitHub, GCP
- Developed and **maintained more than 20 Python and Bash tools** managing data upkeep and updates.
- **Managed Kubernetes cluster** controlling upkeep of up to 8 deployments.
- Oversaw **multi-cloud migration** between Amazon Web Services and Google Cloud Platform.
- Documented and developed mitigation strategies for security vulnerabilities disclosed to the development team.
- Coordinated acquisition and management of various datapoints used to improve search.
- Led terabytes of data-scraping and pipelining projects between AWS S3, DynamoDB, and Aurora.

Security Innovation | Seattle, WA
Security Engineer Aug 2021 - Mar 2022
Key Technologies: Burp Suite, AWS, OWASP ZAP, Python, Bash, Java, JavaScript, Python, Linux, JTAG, ScoutSuite
- **Manually penetration tested 20+ web applications** using Burp Suite, ZAP, and custom Python and Bash tooling.
- **Audited AWS account security** using manual and automated techniques for best practices and privilege escalation risks.
- Performed code reviews on dozens of applications in Java, JavaScript, and Python.
- Wrote and presented vulnerability reports to multiple stakeholders after security assessments.
- Reviewed and expanded on threat models created for pre-launch services.
- Developed and presented mitigation plans for significant web security vulnerabilities (XSS, CSRF, SSRF).
- Communicated security vulnerabilities found through testing to various high-level stakeholders at client companies.

Security Engineering Intern May 2019 - Aug 2021

- Utilized Burp Suite, Postman, and OWASP ZAP, among other tools to assess the security posture of numerous client services.
- Assessed the security of 12 hardware and software products, involving OS testing in Linux, code review, and application security testing.
- Assisted security engineers in reporting and presenting security issues found during the course of testing.
- Developed hardware exploits to reveal issues with the security of Unix-based hardware products.

IC2 CISSP Training | Online Mar 2025 - July 2025

- Preparing to take **CISSP** exam in August to be certified in managing information security systems.
- Developing familiarity with compliance frameworks, secure development systems, and cloud security best practices.

Rochester Institute of Technology | Rochester, NY Aug 2017 - May 2021

BS Computer and Information Systems Security | *Minor in Criminal Justice* | *4 Yrs Dean's List* | *3.78 GPA*

- Competed on Blue Team in five Red Team/Blue Team competitions as part of RITSec. Awarded 2nd place in two.
- Developed key skills in Network Security, Intrusion Detection/Prevention, malware analysis, Incident Response, and Forensic Analysis. Maintained dual focus on legal compliance and offensive security.

Projects

Bluetooth Research Paper **- Security Innovation**

Key Technologies: Wireshark, Python, Linux Internals,

- Two months long research project examining security vulnerabilities in common bluetooth products and protocols.
- Built custom software to exploit vulnerabilities in improperly configured Bluetooth and BLE devices
- Explored security of encryption used in various Bluetooth devices, as well as possible attack vectors against them.

Capstone Election Security Assessment - **Rochester Institute of Technology**: University News Article

Key Technologies: Linux Internals, Binary Exploitation, Radare2, Network Security, HID Protocols

- Conducted rigorous tests of production hardware and software security, resulting in a number of significant findings.
- Uncovered vulnerabilities in the HID daemon, credential management, and binary security.
- Leveraged Linux expertise to gain privilege escalation through use of privileged system binaries.
- Delivered thorough report of all vulnerabilities found in LaTeX format.
- Established a professional relationship between RIT and ES&S, coordinated creation of RIT Election Security Labs.
- Recipient of "Top Capstone Project of the Year" award within major.