**Andrew C. Bell**

Application Security Consultant **|** <https://andrewbydesign.com/>

(Remote) FL **|** **a****ndrew.bell@andrewbydesign.com**

I am an IT Security professional with 9+ years of experience in the domains of Application, Network and Cloud Security, with a focus on web and software security assurance. I have performed various secure design reviews, threat modeling, and white box penetration tests of web applications/services, as well as maintained various network security devices ranging from WAFs, web app/server security scanners (SAST/DAST solutions), static source code scanners, SIEMs, and IDS/IPSs. Additionally, my work has given me opportunities to better explore systems and service development and I have published/contributed to several homegrown in-house applications and tools which promote and enforce a continuous Secure Development Lifecycle (SDLC).

I am interested in job roles which will allow me to sharpen and extend my development skills, knowledge and problem solving to deliver on effective security solutions which can greatly empower application software developers with the resources and information necessary to build and maintain secure software. I want to help free up Security Engineering efforts to tackle the most interesting problems requiring humans and let automation help with the rest.

**TECHNICAL SKILLS**

* **SECURITY TOOLS**: PortSwigger Burp, Tenable Nessus, Netsparker, Rapid7 AppSpider, Rapid7 Metasploit, nmap, nikto, hping3, sqlmap, OWASP ZAP, OWASP O-Saft, ScoutSuite, HP Fortify, Synopsys Coverity, Checkmarx, Veracode, Arachni, Brakeman, Bandit, IBM SIEM, Sourcefire IDS/IPS, Cisco ASA, F5 BIGIP, F5 ASM,
* **OPERATING SYSTEMS:** Windows XP/7/Server2003/Server2008/Server2012/8/10, Linux Debian/Ubuntu/Red Hat, Kali Linux, BackTrack Linux, BSD (Free/Net), CiscoIOS, VMWare, Mac OS X 10.13+
* **NETWORKING & PROTOCOLS:** HTTP/(1.1, 2), HTTPS(SSL/TLS), SSH, DNS, BOOTP/DHCP, TCP/IP, SMTP, POP3, IMAPv4, SNMPv3, ARP, RARP, VLANs, RIPv2, STP, NAT, IPv4 Subnetting, Wireshark, tcpdump, curl
* **DEVELOPMENT & COLLABORATION:** notepad++, vim, PyCharm, MySQL, MSSQL, Fiddler, Postman, Git, Heroku, gunicorn, IIS, various Apache Software Foundation products, WordPress, Splunk, Elasticsearch/Kibana, Syslog-ng, Redis, OpenStack Swift, IntelliJ, Atom, iTerm2, Media Wiki, XWiki, Quip, Quiver, Slack, Basic Machine Learning (ML), Amazon Chime, SDLC, CI/CD
* **PROGRAMMING/SCRIPTING LANGUAGES**: Python (2.7/3.6+), Python Machine Learning (numpy, pandas, scipy), Perl, Bash, Ruby, C++, Powershell, JavaScript, Java 8+, Abstract Syntax Trees (JavaParser), Regular Expressions, SQL, HiveQL, NoSQL
* **AMAZON WEB SERVICES:** S3, EC2, Route53, AWS RDS, IAM, AWS Auth Sigv4, VPC, AWS Code Services, Mechanical Turk, EC2 Systems Manager, EMR, AWS CloudFormation, AWS Lambda, KMS, Amazon ElasticSearch Service, API Gateway, Step Functions, CodeGuru, SageMaker, DynamoDB
* **SECURITY TESTING:** XSS, CSRF, Broken Access Control (IDOR), Injection issues (SQL/Command/NoSQL/etc), Path Traversal, Remote File Inclusion, SSRF, SSTI, Cache Poisoning, CSP, CORS, sandboxing (iframes/jails), Open Redirect, Broken/Weak Cryptography, XXE

**PROFESSIONAL EXPERIENCE**

**VERACODE INC. (Remote) FL**

*Application Security Consultant June 2022 – Present*

* Lead consultation sessions and assist developers with understanding the behavior and results generated by the Veracode SAST, DAST, and SCA analyzers. Serve as a security SME for developers and provide them tailored, experienced recommendations on how to best respond to and address the security issues raised in their scan reports.
* Lead mentorship engagements where I developed partnerships with customer application security engineering + policy contacts. Provided the teams with proactive guidance on how they can maximize the quality of their static scans and best resolve + reduce reported flaws.

**AMAZON.COM, INC. Seattle, WA – (Remote) FL**

*Security Engineer I April 2018 – April 2019*

*Security Engineer II May 2019 - February 2022*

* Worked as part of a specialized Security Scanners team to develop scanner rulesets to report security weaknesses and vulnerabilities present in static source code files hosted in internal source control repositories, as well as backend metadata stores. Scanner rules were written using combination of regular expressions, HiveQL queries and JavaParser Abstract Syntax Tree (AST) methods. Have written around 15 unique scanner rules reporting on High security impact weaknesses in code/metadata. Detections written were ranked and benchmarked against latest OWASP Top 10 and CWE Top 25 issues.
* Led and developed on comprehensive in-house detections for the following static analysis issues: hardcoded secrets of all types and broken service access control. Secrets checked for included generic passwords, database passwords, private (RSA) keys, and AWS keys, among others.
* Collaborated with a partner dedicated InfoSec Software Engineering team to run our developed rules at scale and cut risk tickets to code owners as part of SDLC. Proposed at least 3 key feature enhancements and bug fixes wherever I identified gaps in the framework. Mentored other team members on how to effectively build new SAST rules in our environment.
* Tested and performed regular audits of scanner ruleset performance to identify and eliminate/minimize False Positive (FP) rates in the rules. Overall, developed scanner rules have had between 5-10% FP rate relative to total number of security risks reported. Compiled and maintained strict insightful documentation regarding scanner framework behavior and mitigation actions for each rule which developers should take to properly respond and address scanner risks.
* Collaborated with Scanners team on team-wide project evaluating 3 third-party secure static source code analyzers for use in auditing internal code repos at scale. Analyzers were Fortify, Coverity, Checkmarx. Led on duty to assess scanners performance against C/C++ source code. Partnered with selected C/C++ development teams to rate tools and put together a security engineer use case and customer experience evaluation doc for running these scanners as part of SDLC. Performed subsequent evals of Coverity against Java/Python code for Top 25 CWE coverage. Later I performed similar evaluation against semgrep and semmle.
* Collaborated with Scanners team on team-wide project to develop and deploy an internal dynamic scanner framework to report on high impact web app security issues to the Amazon Retail site. Led on and developed dynamic scanner checks for insecure CSP configurations in running web applications, as well as researching and designing a proposal rule for finding IDOR issues.
* Wrote and contributed new rule plugins for internal running AWS CodeGuru service which can detect Top 25 CWE security weaknesses in Java and Python source code developed at Amazon. Led development of rules reporting on OS command injection and hardcoded secrets issues. Documented the internals of how CodeGuru operates as a runbook reference for rest of team seeking to develop and release their own rules. Led on team-wide effort to evaluate CodeGuru security rules written by AWS security engineers for onboarding in our scanning environment.
* Used Machine Learning to prototype improvements to our dynamic scanner framework by putting together an automated solution to discover and determine ownership of Amazon managed URL endpoints
* Participated in team on-call/primary rotation, responding to urgent secure design questions, deep dive design consultations, and risk assessments. Contributed and maintained a central team runbook of on-call duties to ease handling of similar, frequent consultation requests.

**AMAZON WEB SERVICES INC. Seattle, WA**

*Application Security Engineer July 2016 – April 2018*

* Partnered with AWS software development teams to review service designs and threat models, both from the ground up as new products and as iterative enhancements. Served as a security SME to help teams identify attacker threats/risks and prioritize appropriate remediation strategies to manage uncovered risks. Led on security design reviews relevant to the AWS re:Invent 2017 conference.
* Contributed to content of our team’s internal AppSec Knowledge Base for AWS developer teams to reference and consume during service design, implementation, and release phases.
* Defined pen test engagements and test scoping points based upon service threat models. Partnered with external pen test vendors to drive consensus on risk assessment and prioritization of uncovered pen test vulnerabilities.
* Utilized homegrown SAST tools as well as open-source security tools (e.g. Scout2, now ScoutSuite) to scan and audit service AWS account configurations and service source code files.
* Obtained high level design exposure to some key AWS services involved in the build, release, deployment, and management of applications built inside AWS.
* Participated in team on-call/primary rotation and wrote custom scripts in Python to automate repetitive review triage tasks.

**FACTSET RESEARCH SYSTEMS INC. Norwalk, CT** *Security Assurance Engineer June 2013 - January 2016*

* Performed several tens of white-box penetration tests of web applications, services, systems, networks and other in- house developed FactSet products, thoroughly and comprehensively testing each for weaknesses according to OWASP and MITRE CWE classifications and testing methodologies. Possess some exposure pen testing a few mobile based web applications for iOS.
* Worked with FactSet Software Engineers to prioritize and confirm remediation of security bugs and issues uncovered from product penetration tests with 100% of high/critical severity bugs getting remediated within six weeks of the test’s conclusion.
* Served as team’s lead engineer in configuring and maintaining F5 Web Application Firewall running on top of F5 BIGIP Load Balancer. Led the effort to create new policies and created comprehensive policies/procedures on analyzing WAF log events to determine legitimate security threats from client false positive, as well as document procedures for deploying new WAF policies. Served as part of regular on-call rotation for responding to events generated by WAF.
* Maintaining and making enhancements to our team web application security scanners and the infrastructure/framework that they run on. Ran 20+ Internet facing Web applications through this framework to catch any low hanging security vulnerabilities introduced into the code after initial penetration tests, using the internal staging/QA instances of these apps.
* Worked with team to develop an internal web application for hosting internal team notes, workflows, and processes using the Python/Flask/SQLAlchemy framework.
* Led the development of new REST APIs written in Python which would allow software engineers to confirm security of their web services through automated, ad-hoc security scanning (using backend web security scanners). Worked with QA and Developer Services to integrate these new APIs as part of the Continuous Integration and Delivery cycle.
* Served as a software security SME for the software engineering audience. Created two online software security presentations on Authentication/Authorization and Cross Origin Resource Sharing (CORS). Wrote and contributed to several internal wiki pages regarding software and system security best practices.
* Performed basic patching and systems security maintenance for various internal servers and devices within FactSet's Internal and DMZ networks using Nessus. Against newly reported zero-days (e.g. Heartbleed), production systems and network devices were patched/hardened within 2-5 days of the zero day's disclosure.

**MIT LINCOLN LABORATORY Lexington, MA**

*IT Network Engineer Intern June 2012 - August 2012*

* Assisted in setting up a test network environment for emulating the Laboratory's real time WANs via a WAN emulator to perform simulated file/data transfers. Network tests included optimizing WAN bandwidth and introduced external factors such as latency, jitter, and bit corruption.
* Investigated the usage of a network intrusion detection system using the open- source product Snort on same testbed.
* Assisted in the IT systems management for my group and other divisions using the Laboratory's own personal databases.

**UNITED LIGHTING SALES Riviera Beach, FL**

*IT Part-Time Network Support June 2011 - August 2011*

* Assisted with setting up a new computer network for the company (infrastructure, server/client relationship, etc.). First exposure to IT consulting with helping fellow sales employees with their computer issues.

**EDUCATION AND TRAINING**

**SANS SEC588: Cloud Penetration Testing Virtual Location**

*Certificate of Completion March 2021*

**SANS SEC660:** **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking**

*Certificate of Completion* **Virtual Location** *July 2020*

**Developing on AWS Virtual Location**

*Certificate of Completion April 2020*

**SANS SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques San Jose, CA**

*Certificate of Completion August 2019*

**SANS SEC460: Enterprise Threat and Vulnerability Assessment San Francisco, CA**

*Certificate of Completion August 2018*

**Architecting on AWS Seattle, WA**

*Certificate of Completion September 2017*

**ROCHESTER INSTITUTE OF TECHNOLOGY Rochester, NY**

*Bachelor of Science in Information Security and Forensics September 2010 – December 2013*

* **GPA (PFOS): 3.9/4.0**

**COURSES**

Cyber Self-Defense, Intro to Unix/Linux Seminar, Problem Solving Intro to CS,

Computer System Fundamentals, Cryptography and Authentication, Intro to Programming, Programming with Classes, Network Fundamentals, Info Security Policy, Ethics in IT, Scripting in PERL, Intro to Routing & Switching, Platform Independent Client/Server Programming, Intro to Computer Malware, Applications of Wireless Networks, Network Services, System Administration I, Intro to Database and Data Modeling, Wireless Ad-hoc and Sensor Networks, Network and System Security Audit

**PALM BEACH STATE COLLEGE**  **Palm Beach Gardens, FL**

*Dual Enrollment General Education August 2009 - May 2010*

**CERTIFICATIONS**

**Certified Ethical Hacker v9 *Certified June 29, 2016 – June 29, 2019***