FARHAN JIVA

Cumming, GA 30041 – 404-954-0674 – me@jiva.io – https://jiva.io/ – https://github.com/jiva

Objective

- To obtain a position in the realm of computer-security research/software development which utilizes and advances my skill set.

Education

- **University of Georgia—**Athens, GA
  Master of Computer Science
  - GPA: 4.0
  - **Thesis topic:** Addressing the Shortcomings of Black-box Web Vulnerability Scanners
  - Graduation Date: May, 2012
- **University of Georgia—**Athens, GA
  Bachelor of Computer Science
  - GPA: 3.49
  - Graduation Date: August, 2009

Experience

- **Vexigent, LLC—**Remote, USA
  Founder/Independent Security Researcher/Contractor: July 2023–present
  - Android Malware Reverse Engineering:
    - Proficient in reverse-engineering Android applications (APKs) using static and dynamic analysis techniques
    - Experienced in utilizing disassemblers (e.g., Ghidra, Binary Ninja) and decompilers (e.g., jadx, apktool) for code analysis
    - Skilled in identifying and analyzing obfuscation techniques, anti-debugging mechanisms, and other anti-reversing methods
    - Adept at performing dynamic analysis using emulators, sandboxes, and instrumentation frameworks (e.g., Frida)
    - Capable of extracting and decoding Android application resources, including manifest files, DEX bytecode, and native libraries
    - Experienced in analyzing network traffic and protocols used by malicious applications for command-and-control (C&C, C2) communication
    - Proficient in identifying and analyzing Android permissions, sensitive API usage, and potential security vulnerabilities
    - Skilled in developing custom scripts and tools for automating malware analysis and detection processes
    - Familiar with industry-standard malware analysis tools and platforms (e.g., VirusTotal, Hybrid Analysis, MalwareBazaar)
  - Custom, full-stack web development in Python/Flask hosted on Google Cloud.
- **Connector Team, Atomic Financial—**Remote, USA
  Staff Reverse Engineer: March 2022–June 2023
  - Perform extensive reverse engineering of Android mobile applications to discover and explore undocumented APIs.
  - Reverse engineer signature generation algorithms and be able to generate signed requests to secured back-end APIs.
  - Perform bot detection mitigation techniques when faced with challenges such as request throttling, device fingerprinting, captcha mitigation, etc.
  - Contribute JavaScript/TypeScript code to the Atomic SDK which implements work leveraged from reverse engineering efforts.
  - Be proficient at reverse engineering tools such as Frida, Objection, Bytecode-viewer, Jadx, Apktool, Burp, Ghidra.

  - Provide support and mentorship to junior-level engineers when issues related to reverse engineering arise.

- **Services, Praetorian—**Remote, USA
  Lead Product Security Engineer: October 2021–February 2022
  - Lead challenging engagements that assess the security of modern and complex product stacks.
  - Perform offensive security testing and threat modeling against a wide range of technology stacks, such as:
    - ASP.NET web applications
    - Node.js web applications
    - Infrastructure and applications for a leading cryptocurrency financial company
    - Embedded operating systems for hardware security appliances of a top player in the cybersecurity industry
  - Leverage tools such as Burp, sqlmap, Ghidra, and custom python scripts to assist with security testing.
  - Work with customers, provide subject matter expertise, and leave their security better than when we found it.
  - Optimize existing product offerings, update methodologies and deliverables, and help grow the skills-ets of the team.
- **Security Team, Mailchimp—**Atlanta, GA
  Senior Penetration Tester: November 2017–October 2021
  - Collaborate with Mailchimp's Product, Engineering, and Operations teams to review code manually and identify possible security risks.
  - Develop and execute a penetration testing plan for each new release.
  - Provide coding/technical recommendations and remedies.
  - Spend hours trying to break the Mailchimp app and other in-house developed services.
  - Develop new and contribute to existing in-house tools to assist the Security team with various efforts.
  - Review and validate vulnerabilities reported via responsible disclosure program.
- **Vulnerability and Exposure Research Team (VERT), Tripwire—**Alpharetta, GA
  Software Engineer II: March 2015–November 2017
  - Develop Python-based rules for Tripwire's IP360 vulnerability scanner that are used to detect the latest vulnerabilities and security weaknesses.
  - Perform code reviews on code written by other members of VERT to ensure high quality and reliability.
  - Conduct weekly regression tests on newly developed code to verify continued functionality.
  - Personally developed and integrated Docker-scanning abilities into IP360, enabling Tripwire to become the leader in container security-scanning technology.
  - Contribute to the development of internally-used tools written in a variety of languages such as Python, PHP, JavaScript, while interfacing with relational databases such as Postgres.
- **Vulnerability and Exposure Research Team (VERT), Tripwire—**Alpharetta, GA
  Security Research Engineer: September 2014–March 2015
  - Research and develop algorithms for newly disclosed software vulnerabilities.
  - Deploy and configure a wide range of operating systems, databases, and applications for research purposes.
  - Expand Tripwire IP360 to detect new vulnerabilities and security weaknesses.
  - Contribute to the Tripwire State of Security blog.
- **Coalfire LABS, Coalfire Systems—**Alpharetta, GA
  Security Consultant: March 2014–September 2014
  - Perform remote and onsite security consulting, including internal/external network penetration testing, web application penetration testing, and red team engagements.
  - Perform white-box style testing on custom Java applications while suggesting secure coding practices.
  - Evaluate the security of REST APIs while providing feedback on potential security issues.

  - Create custom reports for presentation to clients.

- **Security Operations Center, Dell SecureWorks—**Atlanta, GA
  Senior Network Security Analyst: August 2012–February 2014
  - Perform accurate and precise real-time analysis and correlation of logs/alerts from a multitude of client devices.
  - Analyze and assess security incidents and escalate to client resources or appropriate internal teams for additional assistance.
  - Handle clients requests and questions received via phone, e-mail, or an internal ticketing system in a timely and detail-oriented fashion in order to resolve a multitude of information security related situations.
  - Interact with, configure, and troubleshoot network intrusion detection devices and other security systems via proprietary and commercial consoles, both local and remote.
  - Develop Python-based tools and scripts to improve the workflow of real-time analysis.

- **Office of Information Security - Security Operations Center, University of Georgia—**Athens, GA
  Web Application Penetration Tester: June 2011–June 2012
  - Perform in-depth black-box pentests on web applications hosted on the campus network.
  - Assist web developers with ways to securely patch and mitigate security vulnerabilities.
  - Give occasional security awareness talks on a variety of web-related vulnerabilities and live penetration demos.

- **Office of Information Security - Security Operations Center, University of Georgia—**Athens, GA
  Student worker: March 2010–June 2011
  - Identify and remediate botnet activity on the campus network.
  - Develop tools and scripts to improve the security of information on the campus network.
  - Perform forensic analysis and deep packet inspection for special-case malware infections.

- **University of Georgia Computer Science Department—**Athens, GA
  Teaching assistant: August 2011–May 2012
  - TA for Unix Systems Programming, Computer Networking, Computer Architecture and Organization.
  - Design course-related projects.
  - Provide assistance to students with course-related needs.

- **University of Georgia Computer Science Department—**Athens, GA
  Research assistant: January 2010–August 2011
  - Conduct technical paper/grant proposal reviews, collect and analyze data.
  - Maintain the internal computer network for the Network Systems Security Lab and the Hacklab.
  - Setup and maintain lab equipment to assist professors and students with special course-related projects.

Skills

- **Operating Systems:** Linux (Ubuntu, Debian, Fedora, Red Hat), UNIX (BSD), OS X, MacOS, Windows XP/Vista/7
- **Programming Languages:**
  - AJAX, Bash, C, C++, Go, HTML/CSS, Java, JavaScript, PHP, Python, SQL
- **Tools and Systems:**
  - **APIs:** REST, SOAP
  - **Assembly:** ARM, Intel x86/x64, MSP430, MIPS
  - **Cloud:** Amazon AWS, Azure, DigitalOcean, Google Cloud Platform (GCP), Heroku, Linode, OpenShift, OpenStack
  - **Containers:** Docker
  - **Databases:** MySQL, Postgres, SQLite, SQLAlchemy
  - **Forensics:** Foremost, Scalpel, Sleuth Kit/Autopsy, Volatility

  - **Fuzzing:** american fuzzy lop (AFL)
  - **Hardware:** Arduino, ESP32, HackRF, JTAGulator, Logic Analyzers (Saleae), Proxmark, Ubertooth, WiFi Pineapple
  - **IDS/IPS:** AlienVault OSSIM, FireEye, McAfee IntruShield
  - **Mobile:** Frida, Objection, Bytecode-Viewer, Jadx, Apktool, YASNAC
  - **Networking:** Dpkt, Ettercap, Iptables, Kismet, Libpcap, Nmap, Scapy, Tcpdump, Twisted, Wireshark
  - **Reverse Engineering:** Binary Ninja, GDB, Ghidra, IDA Pro, OllyDbg, Radare2
  - **Security:** Aircrack, Cain and Abel, John the Ripper, L0phtCrack, Metasploit, Nessus, Nexpose, Sqlmap
  - **Version control:** Git, Perforce, Subversion
  - **Virtualization:** Parallels, VirtualBox, VMware
  - **Web:** Apache, Bottle.py, Burp Suite, Django, Flask, Gunicorn, Nginx, WSGI
  - **Wireless:** Zigbee, Z-Wave

Projects

- **Thesis research**
  - Proposed a method for crawling a web application in a DOM-context, implemented a JavaScript-based web-crawler as a Google Chrome extension, outperformed many others on the market.
  - Proposed a method for detecting blind SQL injection (using behavior analysis), as well as a proof-of-concept implementation in Python.
  - Wrote a tool in Python to facilitate the exploitation of blind MySQL injection using an efficient bit shifting method.

- **Course projects**
  - **Directed study:** Created a web-based framework called *Hack The Planet* along with several security-related challenges which can be used to host Capture the Flag style events.
  - **Game programming:** Wrote a Pacman clone using C++ and LibSDL for Windows.
  - **Databases:** Implemented a database management system with a B+ tree index from scratch using Java.
  - **Computer security:** Prepared a web-based scoreboard and a security-related challenge-delivery system in PHP which was used by the students throughout the semester.
  - **Computer/networks attacks and defenses:** Evaluated the performance of Tcpdump on a variety of modern operating systems.
  - **Machine Learning:** Worked on a project using the *Weka* framework to detect and classify web robots using passive request headers.
  - **Advanced Distributed Systems:** Wrote a web-based management system for OpenStack in Python.

- **Other**
  - Launched a popular free image hosting service which assists in collecting research-related data.
  - Started a project dubbed *Bprobe* which is a web analytics engine that is aimed at providing web site owners with in-depth information regarding their user base.

Achievements and Activities

- Organized and hosted the OpenCTF contest at DEFCON 30, which included creating a custom CTF scoreboard platform and several CTF challenges.
- Former member of Hacklab @ UGA which is a group of computer-security enthusiasts that have weekly meetings to discuss current topics in the area of information security.
- Active member of the CTF team *disekt*; competed and performed in a number of well-known Capture the Flag events.
- Competed in the 2012 Codegate Final CTF round in Seoul, South Korea.
- **CTF accomplishments:**

– **Event:** 2013 Defcon 21 Quals	**Rank:** 31st/414
– **Event:** 2012 Defcon 20 Quals	**Rank:** 17th/303

- **Event:** PPP's pCTF 2012 **Rank:** 12th/243
- **Event:** Codegate 2012 YUT Quals **Rank:** 9th/182
- **Event:** 2012 Ghost in the Shellcode Finals **Rank:** 14th/96
- **Event:** 2012 Mozilla CTF **Rank:** 12th/119
- **Event:** CSAW CTF 2011 **Rank:** 11th/207
- **Event:** Hack.lu CTF 2011 **Rank:** 10th/43
- **Event:** 2011 Open CTF @ Defcon 19 **Rank:** 2nd/37
- **Event:** 2011 SiBCTF Quals **Rank:** 6th/37
- **Event:** 2011 Defcon 19 Quals **Rank:** 31st/280
- **Event:** PPP's pCTF 2011 **Rank:** 8th/431
- **Event:** Codegate 2011 YUT Quals **Rank:** 4th/178
- **Event:** PAraDOx CONference 2011 CTF **Rank:** 2nd/337
- **Event:** iCTF 2010 **Rank:** 28th
- **Event:** ISEC 2010 **Rank:** 8th
- **Event:** iCTF 2009 **Rank:** 25th