**Creative Junior full stack developer with experience**  **Phone: (410) 693-2722**

**in front end and backend software development with Email:** [**Email**](mailto:kate.c.soliven@gmail.com)

**a willingness to learn new technologies; as well as LinkedIn:** [**ksoliven**](http://www.linkedin.com/in/ksoliven)

**learn on the fly. GitHub:** [**ksoliven**](https://github.com/ksoliven)

**Website:** [**Portfolio**](https://katedevdc.com/)

**Location: Northern Virginia**

**Key skills**

**Front End: Databases:**

* Angular, AngularJS, Bootstrap
* CSS3, ES6, jQuery, AJAX
* Html5, RESTful API
* ReactJS, Typescript
* SocketIO, Mongoose
* SQL, SQLite, MongoDB, SQL Server 2019
* CRUD
* ORM, EF Core

**Back End:**

* .net framework
* net MVC
* C#, Express.js, LINQ

**Devops:**

* GitHub
* Azure Dev Ops, AWS
* Nodejs
* Python **SDLC**:
* Django, Flask
* Agile and waterfall

**Work history:**

**Zekiah Technologies Inc.** 02/2020 - Present

* Developing an application using an Angular frontend and a .NET backend in an Agile process
* Using Swagger to generate Restful API routes
* Establish connections between multiple datasets in SQL Server 2019
* Using Entity Framework Core (EF Core) for Object Relational Mapping
* Using Azure DevOps and Git for Source Code control
* Unit testing using Jest and Xunit
* Using RabbitMQ for Data Ingest services
* Migrating data to S3 Object storage
* Leveraging Data Search and Analytics using ElasticSearch and Kibana (for observability, indexing, and template searches)
* Utilizing Cloud Computing Software with AWS and OpenShift

**Resident developer at Coding Dojo** 05/2019 – 08/2019

* Developed and deployed web apps from back-end to the front-end
* Engineered RESTful routes, CRUD operations (using Model View Controller), and API integration
* Established connections between multiple datasets in SQL and NoSQL (MongoDB)
* Deployed web applications using Ubuntu, NGINX, and Amazon Web Services using security protocols (PEM)
* Used GitHub for source code control
* Tested web applications repeatedly for vulnerabilities (i.e. JavaScript analyzer, SQL Injection) using Grabber

and/or free open sourced programs

**Freelance Headhunter**  10/2016-04/2019

* Matched candidates to potential employers based upon their education, skill set, and experience. Used LinkedIn, Indeed, career builder, and various job-hunting websites.

**Analyst/Developer at the Boeing Company**  06/2009 -12/2010

* Worked in an Agile development team on a 40-million-dollar project for Supplier Quality Systems. Developed a supplier quality system for Boeing Commercial Airlines and Boeing Defense Systems.
  + Data conversion with system owners and previous developers (legacy code to C#/Java)
  + Testing through code reviews, security professionals (software encryption, Sidewinder/enterprise firewalls, and tunneling protocols), and system developers
  + Planning with business analysts, internal/external suppliers, utilized SharePoint for overall project management flow, and change requests (bugs, logic errors, or vulnerabilities)
  + Executions through 2-week sprints in developing prototype builds to be presented to the Vice Presidents of Boeing Commercial Airlines and Boeing Defense Systems.
* Wrote interface control documentation and Enterprise resource diagrams for external and internal customers
* Scribed for the bi-weekly meetings with the Vice President of Supplier Quality. Conducted lunch and learns to identify new technologies (security tunneling schemas, implementing AJAX, and using Adobe Flex) that would be used in new system.
* Wrote Visual Basic Scripts for Shop Floor Control for the C-17 program to identify which data was obsolete or vulnerable (due to legacy code). Communicated with System Managers and customers for system retirement.
* Learned how to make use of Desktop Service Requests with an outside vendor (i.e. Dell). Requests consisted of matching hardware to customer (i.e. engineers receiving engineering laptops), specialized electronic devices, change in location of vendors, hardware and software issues, and network outages. Completed requests via phone and email with the customer. If a request was not completed, requests were manually modified within the system.

**Java Teacher assistant at George Mason University** 01/2006 -05/2006

* Evaluated student programs for syntax and logic errors.

**Volunteer:**

**Volunteer Junior Web Developer** 10/2019 – Present

* Working on the PWCSEPTA website to revamp the UI
  + Must be responsive
  + Color-blind friendly (WIP)
  + Register new members and take in to account member fees instead of a manual email (WIP)
  + Currently developing a UI with WordPress to accommodate ease of use for members

**Freelance Quality Assurance** 01/2011 – 09/2016

* Identified glitches and errors in software programs and evaluated fixes
* Performed server stress testing
* Conducted functional tests (graphical or logical based) and identified vulnerabilities

**EDUCATION:**

**Coding Dojo**  05/2019 – 08/2019

* A 14-week bootcamp to become a full stack developer
* Learned multiple technologies such as: HTML, CSS, JavaScript, Angular, Nodejs, MongoDB, C#, SQL, SQLite, Razor, Python, Flask, Django, jQuery, and AJAX.
* Triple Black Belt in Python, C#, and MEAN

**George Mason University**  09/2014 – 12/2014

* Certified ethical hacker course
* Learned network and software methodologies to protect systems from external and internal threats.
  + Kali-Linux with in-built penetration tools:
    - launched denial of service attacks against vulnerable websites and systems
    - used Armitage (Metasploit GUI) to visualize targets and recommend what exploits to

utilize (scripting or networks)

* + - eavesdropped (wrote phishing scripts in Python to scan email inboxes) on

communications to conduct man-in-the-middle-attacks

* + - performed SQL injection attacks against databases
    - used Wireshark to analyze packets to identify vulnerabilities on a network
    - detected and cracked using Aircrack-ng to penetrate Local Area Networks (LANs)
    - applied the Burp suite to test out Web application security
      * HTTP Proxy: interception, inspection and modification of the raw traffic passing in both directions
      * Vulnerability: automated vulnerability scans
      * Intruder: perform automated attacks on web applications; can be modified via an algorithm for precise results; detects SQL injection, cross-site scripting, and etc.
      * Spider: mapping an entire application’s content and functionality
      * Repeater: manually test out an application (modify request to server, resend, and observe the results)
      * Decoder: transforms data from its hashed state to its canonical form and recognizing the encoding applied
      * Comparer: compare data and identify any differences
      * Extender: to help load any modules for pen testing or to apply third-party code
      * Sequencer: test out application’s session tokens for possible vulnerabilities
    - OWASP ZAP (Zed-Attack-Proxy)
      * Intercepting proxy server
      * Tested traditional and AJAX web crawler (spider) to map out content and functionality
      * Active and passive scanning for vulnerable systems
      * Smart card and session vulnerabilities using scripting languages or 3rd party software
    - utilized John the Ripper password cracking tool by conducting dictionary and brute force

attacks using text-string samples (identified in a word list) and comparing against the

input hash

* Developed social engineering skills by researching intended targets via LinkedIn, social media profiles, or corporate websites

**Dale Carnegie strategic communications** 01/2010 – 05/2010

* Strategic communications course
* Taught how to conduct, lead, and present in meetings.

**Carnegie Mellon University**  08/2009 – 12/2009

* System engineering course
* Learned how to apply Agile development methodologies to various projects.
* Learned how to break down systems systematically for System Retirement.

**George Mason University**  08/2004- 05/2008

* Bachelors of Science in Decision Science and Management Information Systems with a minor in Information Technology.
* Completed 120 credit hours.
* Learned system engineering, system design using, system analysis, web design, network security, network analysis, and project management methodologies.
* Graduated Cum-laude

References:

William Goode ([Link](https://www.linkedin.com/in/wgoode3/))

Nina Ramiscal ([Link](https://www.linkedin.com/in/nina-ramiscal-b09b384/))