



# ALEXANDER WINKLER

 [awinkler.dev](https://github.com/awinkler)

 [Alexwinkler1@icloud.com](mailto:Alexwinkler1@icloud.com)

 [linkedin.com/in/alexwinklerr](https://www.linkedin.com/in/alexwinklerr)

## Education

---

### Georgia Institute of Technology

Jan. 2026 – Dec. 2027

*Masters of Computer Science*

### Eastern Florida State

May. 2021 – Aug. 2025

*Bachelors of Applied Science in Software Development*

Melbourne, FL

- Degree GPA 4.0

## Experience

---

### Police Officer

Jan. 2022 – Jan. 2023

*City of Rockledge*

Rockledge, FL

- Clearly conveyed information during high-pressure situations, ensuring accurate decision-making and precise reporting.

### Teaching Assistant

Jan. 2025 – May 2025

*Android App Development*

Melbourne, FL

- Assisted with eight Android projects, helping both students achieve final grades of A through consistent technical guidance.

## Projects

---

### Zillow Algorithmic Security Research | *SQL, Python, NextJS* [Link](#)

- Discovered and exploited critical vulnerabilities in Zillow's ranking algorithm by reverse-engineering the "Hot Home" feature
- Artificially inflated engagement metrics, increasing a property's views from **2 to 450+** and generating **400 synthetic likes**, successfully triggering the "Hot Home" tag.
- Leveraged custom OSINT tools to harvest and generate **2,000+ validated email addresses** from underground forums, achieving **98 success rate** in account creation without triggering fraud detection

### Amazon Employee Exposure Engine | *Amazon RDS, Vercel, Next.js, FastAPI, Python, SQLite,* [Link](#)

- Identified compromised data affecting thousands of senior and executive level Amazon employees, directly prompting a **AWS** security response.
- Engineered a scalable **full-stack** application on Vercel using **Next.js** and **FastAPI**, enabling real-time querying of a breach database containing email addresses and phone numbers for over 1.2 million Amazon employees
- Implemented a fully serverless backend using Python and SQLite to handle over **10.2 million** records with zero infrastructure maintenance, reducing operational overhead, then revamped by integrating **Amazon RDS** using MySQL.

### Threat Actor OSINT Harvester | *Python, SQLite* [Link](#)

- Achieved **95%** accuracy scraping 1,000+ pages at 50 pages/min, extracting **10,000+** PII records (emails, SSNs, phone numbers) from high-risk forums like Doxbin and SwatKitty
- Built a custom Python session handler that dynamically rotated authentication cookies to bypass **Cloudflare BIC** anti-bot protections, enabling uninterrupted data collection
- Used BeautifulSoup to parse and normalize data into a SQLite database, enabling efficient querying and threat actor activity analysis

### Weather Satellite | *Python, React, Javascript, Git Pages, HTML/CSS* [Link](#)

- Fulfilled the positions of **PM** and **Tech Lead** by managing a team of 3 developers and guiding from initial requirements to debugging.
- Redesigned a Python/Tkinter desktop app into a scalable React.js frontend with **OpenWeather API** integration and full mobile compatibility.

## Technical Skills

---

**Languages:** Python, Java, C++, HTML/CSS, JavaScript, SQL, Kotlin

**Developer Tools:** VS Code, Eclipse, Google Cloud Platform, Android Studio, NetBeans, SQLite, MongoDB, Git

**Technologies/Frameworks:** Vercel, GitHub, React, React.js