

# Samer Takieldin

[stakield@gmu.edu](mailto:stakield@gmu.edu)

[GoSamer.com](http://GoSamer.com)

## EDUCATION

---

**George Mason University** Fairfax, Virginia

Graduated May 2022

- Bachelor of Science in Information Technology with a concentration in Information Security with 3.63 GPA.  
Minor in Business Administration

## TECHNICAL SKILLS

---

**Certifications:** Security +, AWS Cloud Practitioner expected 04/2023

**Programming Languages:** Python, SQL, HTML/CSS, Bash, YAML, JSON, PHP

**Operating Systems:** Kali Linux, MacOS, Ubuntu, Windows, Hypervisors/virtualization

**Applications:** Acunetix, AirCrack-ng, Akamai, AWS, Azure DevOps, BurpSuite, DivvyCloud, Kubernetes, nmap, Prisma, QRadar, TFS (CI/CD), Metasploit, Microsoft Sentinel, Nessus, VeraCode, WireShark

## RELEVANT EXPERIENCE

---

**CoStar Group** Washington DC

*Associate Security Engineer- Cloud Security*

June 2022- Current

- AWS security admins working on investigating incidents through GuardDuty/CloudTrail and analyzing IAM permissions through roles with least privilege in mind
- Co-founder of AppSec division to scan web applications through Acunetix, verify using BurpSuite, and report vulnerabilities for remediation
- Using Akamai WAF to verify, deny, and tarpit malicious traffic while creating custom rules
- Creating detections in Prisma to alert us during incidents of containers in Kubernetes clusters that have anomalous activity
- Using Microsoft Sentinel to Query logs from alerts, created workbooks for reporting to senior management

**Apple** McLean, Virginia

*Technical Expert*

February 2017-June 2022

- Provided friendly and insightful advice to clients with various concerns while maintaining customer trust and provide lasting relationships.
- Collaborate with teammates to create innovative solutions for issues in a fast-paced environment.

**INOVA Health System** Sterling, Virginia

*Cyber Engineer Intern*

January 2020- May 2020

- Worked on identifying active threats on networks using IBM QRadar, Splunk, Wireshark, and Cylance to monitor, detect, and resolve vulnerabilities. Also identified current application threats that are being implemented from different vendors. Maintained security controls and operations in accordance with industry standards (NIST)

## PROJECTS

---

**Personal Website**

- Used HUGO, an open-source project I contributed to, for an interactive resume hostname that is written in Golang
- CTF**
- Organized/participated in event to create a solution for severe weather reporting including sensors and reporting back to main controller

**Senior Capstone Project**

- Created/hosted a web application using a LAMP stack, on an AWS EC2 Ubuntu instance with no security controls. Then spun up a Kali Linux machine that attacked the LAMP stack machine. Showing the POC and what is capable, I then enabled UFW, limited access to the SQL table, implemented STIG secure coding best practices, and with each security enhancement, I delivered the benefits in a document