Yusuf Hegazy

Nasr City, Cairo, Egypt

📞 +201010588770 ✉ yusuf@hegz.io in linkedin.com/in/yusufhegazy ⊙ github.com/hegzploit

⌂ hegz.io

EDUCATION

Egyptian Academy for Engineering and Advanced Technology (EAEAT)   July 2018 – 2023
Bachelor of Electronics and Communication Engineering   *Cairo, Egypt*

Al-Farouk School   2005 - 2018
Primary, Preparatory and Secondary Education   *Cairo, Egypt*

EXPERIENCE/PROJECTS

Penetration Tester — Part-Time @ Spark Engineering Consultants   December 2022 - Present
- Perform penetration tests on embedded/IoT devices.
- Mobile reverse engineering and penetration testing.
- Web and network penetration testing.

Cybersecurity Education | *YouTube, Davinci Resolve, Photoshop*   April 2020 - Present
- A series of videos on low-level security was produced, It involved memory corruption and buffer overflow attacks and their exploitation.
- A talk was given introducing buffer overflow to the masses, It included a crash course on x86 assembly and memory inner workings, It was edited and uploaded on YouTube for archiving purposes.

CTF Player and Author | *Pwn, Reverse Engineering*   July 2020 - Present
- Active player on pwn.college, almost done with my yellow belt.
- Competed and ranked with my team (locally ranked #1 on CTFTime) in a number of virtual and on-site CTFs.
- Organized and developed hardware & pwn CTF challenges for multiple events (OSC-AUC CTF, IEEE-GUC CTF, 0xL4ugh CTF '22, ...).

Dell Hackathon '23   March 2023
- Won third place in the hackathon before getting disqualified for our out-of-the-box solutions (psst... I wrote a blog post about it, check it out!)
- I was responsible for the cybersecurity portion of the competition as well as the otherwordly performance optimization that got us third place in a breeze (again check out my blog post for more info!)

Multi-modal analysis of articulation disorders | *Grad. Project, AI, Transformers, LSTM, Data collection & labeling*   June 2023
- We developed a multi-modal system that classifies and analyzes children with articulation disorders through images and audio. (once again, I have a blog post about this)
- I was responsible for the audio pipeline where I developed and deployed a system that utilizes a fine-tuned version of the whisper transformer model to generate a report of the articulation errors (letter substitution, insertion or deletion)
- An earlier version of the audio pipeline I developed was using a trained LSTM network with a purposely built dataset that we labeled, results were inferior to the newer transformers approach.

FOSS | *Python Requests, bs4, httpx, multithreading, multiprocessing*   2018 - Present
- Wrote different scrapers for automating my life
- scraper for local electronic component prices, ⊙ hegzploit/bgneh
- scraper for collecting a dataset of public student grades for data analysis experiments, ⊙ hegzploit/bazooka
- scraper for unfollowing FB pages to clean my profile, ⊙ hegzploit/ZNFS
- scraper that crawls my college's CMS for new assignment, ⊙ hegzploit/lazy-chicken

EXTRACURRICULAR ACTIVITY

Arrow Team   **May 2019 – Present**
Student Team Captain   *Cairo, Egypt*
- Collaborated and lead a team of talented individuals toward the manufacturing of electric vehicles to compete in various national and international student competitions (Shell Eco Marathon, EVER and others)

- Designed the vehicle's HMI using communication protocols and data acquisition of the multiple sensors in the vehicle.

- Assisted in designing and deploying the vehicle's wiring systems.

EAEAT Cybersecurity Circle   **March 2022 – Present**
Founder   *Cairo, Egypt*
- Formed a community of cybersecurity enthusiasts with a goal of introducing them to security.
- Participated together in multiple CTFs and hosted multiple sessions where a lot of basic concepts were established.

SKILLS

Languages: **Python**, **C**, **Assembly**, Bash, Matlab, OCaml, Rust, LaTeX, JSON, awk
Tools: Vim, tmux, GDB, Git, GNU Coreutils, KiCad, Proteus, Logisim, IDA, Ghidra
Technologies/Frameworks: Linux, SSH, HTTP, MQTT, Flask, Docker, Pandas

Yusuf Hegazy
☐ *+201010588770*
✉ *yusuf@hegz.io*

July 3, 2023

Hi!

I'm an Electronics and Communication Engineering student nearing graduation, I believe that my passion for cybersecurity, experience in embedded systems, and dedication to learning and growth would make me an ideal candidate.

Over the past three years, I have honed my cybersecurity skills by participating in Capture The Flag (CTF) competitions with my team in my spare time. We are currently ranked 1 nationally on CTFTime. In addition to my cybersecurity pursuits, I have actively engaged in extracurricular activities, such as leading my university's racing team in manufacturing and competing in local and global events, including the Shell Eco Marathon. I was also an embedded and wiring team member prior to my work as a team captain.

Currently, I work part-time as a penetration tester at a security integrator company. While I enjoy my current role, I am eager to transition into security research, particularly focusing on low-level hardware security.

I am confident that my background and skills make me a great fit for a role in automotive security, for the following two reasons:

First, my academic studies have given me a strong foundation in embedded systems and their programming. I am proficient in using microcontrollers such as Arduino, ESP8266, and Raspberry Pi, along with their interfacing and communication protocols. Additionally, I have experience in PCB design, having used KiCad multiple times for my projects.

Second, I have gained experience in both software and hardware security. In software security, I have focused on binary exploitation and successfully solved numerous CTF challenges in this area. I have also started creating educational YouTube videos on these topics in my free time, as I am passionate about teaching and sharing knowledge. I am comfortable using disassemblers, decompilers, and debuggers on the Linux operating system, which I use daily.

In hardware security, my knowledge extends to side-channel attacks, fault injection, firmware analysis, and reverse engineering.

Thanks in advance!

Yusuf Hegazy