

Momolly

Master's student in Cyber Defense at [REDACTED].
Seeking an internship in Offensive Cybersecurity.

+33 [REDACTED]
[REDACTED]@[REDACTED].[REDACTED]
Paris [REDACTED]

Profile:

Passionate about the political, strategic, and technical aspects of cyberspace, I actively train for challenges related to attacks through CTFs and Bug Bounties.

My Master's program at [REDACTED] enables me to develop a profile that combines technical skills with an understanding of governance, thanks to the involvement of professionals primarily working [REDACTED]. They share their expertise and provide high-quality pedagogy, particularly in the fields of cryptography, risk analysis and management with EBIOS RM, network security, as well as the geopolitical issues related to cybersecurity. This training effectively prepares me for the OSCP certification that I am targeting.

After participating in remediation follow-ups and conducting compromise indicator research, I actively engaged in meetings, providing daily updates to my superiors on the latest developments in cybersecurity and contributing to the implementation of new detection rules. Aware of the defensive challenges in cybersecurity, my ambition now is to actively contribute to security audits within a Red Team environment as part of an internship.

Professional Experience:

Internship at [REDACTED] SOC / [REDACTED]

From April 1st to July 31st, 2023

Defined detection strategies for critical IT systems of [REDACTED]. Processed alerts and participated in remediation operation management.

Internship [REDACTED] / [REDACTED]

From October 3rd, 2022, to March 28th, 2023.

Research and development for an NFT generation system (Ethereum blockchain) implemented on the e-commerce platform of a luxury brand.

Education:

- > Master's in Cyber Defense at [REDACTED] (ongoing)
- > Bachelor's in Information Technology from [REDACTED]
- > High School Diploma in Industrial Sciences and Technologies, specializing in Systems Engineering and Digital

Liens externes

Github: <https://github.com/Momollax>



Technical Skills

Cyber Tools and Expertise

As part of CTFs and Bug Bounty, I have learned to use reconnaissance scripts such as Burp, nmap, FFuF, Katana, as well as scripts I developed myself to, for example, identify forgotten API keys in scripts or HTML.

During these exercises, I've searched for vulnerabilities such as XSS, CSRF, LFI, RCE, and SQL injections. I've also learned to find PoCs, CVEs, Odays, as well as various channels for information and knowledge sharing.

I conduct open-source research using various dorking methods, data leaks, Shodan, and the Wayback Machine

During my internship at [REDACTED] SOC, I gained skills in using Splunk. I implemented detection rules, alerting the SOC in case of C2 beaconing or excessive volume, and worked with Windows EventID logs. I also created dashboards, conducted forensic searches, and wrote compromise reports for [REDACTED].

Programming Languages:



I use Python daily for automation projects, PoCs, and custom scripts. During my training at Epitech, I acquired skills in C, C++, Go, and Bash

Management and Collaboration Tool:



Languages

- > French (native)
- > English (B2)

Hobbies

- > Sports:
Volleyball, Voile, Kitesurf, Plongée
- > Personal Projects
- > Osint