From curiosity to critical bugs: Interview with Marc-Oliver Munz (c1phy)

BY ELEANOR BARLOW · FEBRUARY 26, 2026

Security is built by people. At Intigriti, we don't just help organizations stay secure; we shine a light on the ethical hackers making a difference. Through our Hacker Spotlight series, we celebrate the talent, curiosity, and impact of the community driving safer digital experiences worldwide.

We recently spoke with Marc-Oliver Munz, an ethical hacker from Germany with a global reach. In this Q&A, learn about his story, his adventures in cybersecurity, what trends he is seeing in the industry, and the importance of curiosity to drive real-world impact.

How did you get started with bug bounty hunting?

I got started with bug bounty hunting at the beginning of the COVID pandemic. During that time, I was on short-term work, which gave me the opportunity to really dive into the topic. Before that, I had spent a lot of time on platforms like HackTheBox, but I honestly didn't even know that bug bounty programs existed. Once I discovered bug bounty hunting, everything came together: the technical skills I had already built and the extra time I suddenly had allowed me to fully commit and get started.

What positive impact has bug bounty had on your life?

Bug bounty has had a huge positive impact on my life, especially in terms of learning and knowledge. I learn something new almost every day and stay constantly up to date with new vulnerabilities and attack techniques.

Since I'm also responsible for security in my day job, as Head of IT Security, I can directly apply what I learn through bug bounty hunting in a professional environment.

On top of that, I have met amazing people through live hacking events. The exchange, collaboration, and mutual support within the community are incredibly valuable to me and, most importantly, it's a lot of fun.

How much time, on average, do you give per week to hunting for vulnerabilities?

On average, I spend about one hour per day during the week hunting for vulnerabilities, and usually another 2–4 hours over the weekend. Over time, I've also built some automation to handle repetitive tasks, which helps me save time and focus more on manual testing and deeper analysis.

How do you see the industry growing as a whole, and what makes ethical hacking attractive for both researchers and companies?

I see a clear trend toward SaaS and web applications, often built as complex multi-tenant systems.

- From a hacker's perspective, these environments are extremely interesting and challenging to test.
- For companies, bug bounty is an attractive model because they only pay for real, valid vulnerabilities.

At the same time, crowd-sourced security testing is highly efficient and often uncovers issues that traditional audits might miss.

- For researchers, the industry offers continuous learning, real-world impact, and the opportunity to work on modern, large-scale systems.

How would you describe the "hacker mindset" in your own words?

For me, the hacker mindset means staying curious at all times. It's about constantly asking, "Why does this work this way?" and "What happens if I try something different?"

It also means not accepting things at face value, but always exploring systems deeper and thinking creatively about unintended behavior.

Keeping information anonymous, what's the most interesting vulnerability you've found and why?

There are many interesting findings, but the most exciting ones are definitely remote code execution vulnerabilities. One of my favourite findings this year was a privilege escalation on a virtual Windows machine. I was able to move laterally and gain administrator access on another VPS as well. Seeing how a small weakness could lead to full system compromise was both fascinating and very rewarding.

What would you recommend to researchers considering a career in bug bounty hunting?

Don't give up too quickly. It took me about three months to find my first valid vulnerability, and many beginners quit far too early. I strongly recommend focusing on one CMS or one or two vulnerability types instead of trying to find everything at once. A focused approach is much more effective and helps you build real expertise faster.

Building a community where hackers thrive

We want to extend a huge thank you to Marc-Oliver for sharing his journey and invaluable insights with our community. His story combines curiosity, persistence, and a passion for learning to achieve remarkable goals.

Stories like these are a reminder that behind every vulnerability report is a dedicated individual solving complex problems and making the digital world safer for everyone.

At Intigriti, along with our mission to keep companies safe, we have a mission to create a community where hackers can thrive, grow their skills, and achieve great things.

Contact the team today to learn more.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.