From the first bug to financial independence: How bug bounty hunting shaped Isira's path

BY JENNIFER CHANEY · JANUARY 12, 2026

At Intigriti, we're proud of our mission: helping companies safeguard their digital assets and protect their customers in a world where cyber threats are constantly evolving. But beyond security, we're equally passionate about empowering ethical hackers, providing them with opportunities to learn, grow, and make a meaningful impact with their skills.

We recently spoke with Isira, an ethical hacker from Sri Lanka who joined our platform at just 16 years old. Through dedication, curiosity, and hard work, bug bounty hunting has transformed his career and personal life, allowing him to achieve milestones by the young age of just 21. His experience is a powerful testament to the impact of bug bounty programs and the opportunities they create.

Read on to learn how he got started in bug bounty, tips for others looking to pursue bug hunting, how he defines the 'hacker mindset', and more.

Q&A with Isira

What positive impact has bug bounty had on your life?

I grew up in Sri Lanka in a middle-class family with very limited opportunities. The mainstream school system is highly competitive and often covers material that isn't directly useful for many careers, so it wastes a lot of time for students who want a different path. Bug bounties changed that for me. I started earning at 16, which allowed me to skip AL examinations and become financially independent, I never had to ask my parents for money again. That income paid for my private university education at NSBM, which saved me years I would have otherwise spent following the traditional route. Since then, I've:

- Worked with companies across multiple countries
- Discovered 700+ vulnerabilities through bug bounty programs
- Completed 20+ professional penetration tests
- Balanced bug hunting and pentesting with university, volunteer events, and study

By 18, I bought my first car, and by 21, I bought my first house. I also graduated with First Class Honours in Computer Security from the University of Plymouth via NSBM, which I'm proud of because I did it while actively hunting and doing pentests.

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

While I was studying I wasn't always consistent, but when I had free time I spent roughly 20–30 hours per week hunting vulnerabilities.

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

The industry has a bright future.

For researchers:

- You get to test a wide range of real-world applications owned by global companies.
- The work is rewarding financially and intellectually, and it supports freelance and remote lifestyles.
- You face varied technologies and real-world attack surfaces, which is the best way to learn, hands-on testing beats theoretical study.

For companies:

- Programs let organizations test their assets with many skilled people at a relatively low cost.
- Different researchers bring different approaches and backgrounds, so the aggregate coverage is far stronger than relying on a single tester.
- Bug bounty programs are an efficient and scalable way to tap external talent and improve security posture.

Overall, the model aligns incentives: researchers get paid for findings, companies get diverse testing, and the ecosystem improves as both sides learn from each other.

What's the most interesting vulnerability you've found and why?

I'll anonymize the details, but one of the most interesting cases stands out because it combined persistence, creativity, and several techniques:

- I first suspected the issue around 1–2 AM and worked until 8:37 AM to get a simple pingback through a strict WAF. That confirmed an XXE vector, but RCE was not immediately achievable.
- After a short break, I continued and was able to read parts of /etc/passwd as a proof of concept. Triage initially rated it as High, which underplayed the exploitation effort. I kept going.
- Later that day, I found an XML config file containing credentials and a related API endpoint that had no public references. I tracked down a server-side JAR, decompiled it with JADX, and discovered parameters that allowed command execution.

- Ultimately, I achieved RCE. The process required WAF bypasses, XXE exploitation, binary discovery and decompilation, and careful, low-impact testing to avoid affecting availability. I enjoyed this one because it felt like solving a CTF: multiple steps across layers, piecing together small leads into a full exploit chain.

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

The hacker mindset is curiosity plus persistence. It’s about asking “why does this behave this way?” and then methodically probing the system until you understand the underlying logic. Hackers think in failure modes: they look for assumptions developers made and craft tests that violate those assumptions. They are patient, detail-oriented, and willing to iterate on small signals until those signals reveal a real issue.

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

- Start with programming: build and break things. Focus on web stack fundamentals like PHP, Node.js, and how databases work.
- Learn SQL and common database behaviors. Understanding how data is stored and queried is essential.
- Master client-side technologies: HTML, JavaScript, cookies, websockets, postMessage, and Content Security Policy. These are where many modern bugs live.
- Practice with CTFs and labs. Always ask why the application was vulnerable and model the vulnerable logic in your head.
- Begin with VDPs (vulnerability disclosure programs). They are less crowded and great for experience. Once you’re comfortable with real-world sites and apps, move to public bug bounty programs.
- Be consistent and thorough. Even top hunters miss low-hanging bugs. Don’t rely solely on automated tools, automation often causes duplicate reports. Learn manual hunting techniques and use free resources like PortSwigger’s Web Security Academy and Intigriti’s Hackademy.
- When you get into the industry, don’t chase money at first, it will burn you out quickly. Instead, focus on gaining experience and finding valid vulnerabilities. Remember, even duplicate reports prove you’ve identified a real issue.

Building a community where hackers thrive

We want to extend a huge thank you to Isira for sharing his incredible journey and invaluable insights with our community. His story is a perfect example of the hacker mindset, combining curiosity, persistence, and a passion for learning to achieve remarkable goals. Stories like Isira's 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.

AUTHOR

Jennifer Chaney

Head of Marketing, Intigriti

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com