Bug Business #6 – Get to know Robin, Intigriti's Top Hacker in Q1

BY ANNA HAMMOND · JULY 14, 2020 · LAST UPDATED ON MARCH 6, 2025

Bug Business is a series of interviews in which experts from the bug bounty industry shine their light on bug types and trends.

This interview features Robin who won the first place in our leaderboard in the first quarter of 2020. He gracefully took a break from an already busy life to answer our questions on this cool feat.

Hi Robin! Can you tell us a bit about yourself, who you are and how you got into bug bounty hunting?

Hey, I'm Robin. I'm 20 years old and I live close to Ghent, Belgium. I recently got my bachelor's degree in Computer Science at Ghent University and will be studying for a master's degree next. In my free time I enjoy reading about technology and playing table tennis. I got into programming back when I was 13 and taught myself how to program in Java using some YouTube videos. I used this Java knowledge to build plugins for games, mostly for fun. Later on I experimented with HTML, PHP and SQL to develop very basic websites. I didn't really focus on the security aspects of developing software until the end of high school. I poked around at the student portal that our school was using and found some vulnerabilities using techniques I found in some online articles. I wrote up a report and sent an e-mail to the company. A few days later I had a call with their CEO and they awarded a €50 giftcard as a token of appreciation.

Back then bug bounty wasn't as popular and there weren't as many programs to hack on, so I stopped for a little while. I started to pick up bug bounty again about one year ago. The space had matured a lot since I last looked so I got back to work. I accidentally found a pretty nice vulnerability on a responsible disclosure program and it was accepted pretty quickly. From there on, I received a private invite to a brand new private program, on which I soon found some other vulnerabilities and got my first bounty. This got the ball rolling and I realised that it's definitely possible to earn some nice bounties for reporting bugs. Since that day, I've been actively bug hunting and never stopped.

So, what does your life look like now? Do you do bug bounty full-time or as a hobby, and how does it fit into your life?

Bug bounty for me is mostly a hobby. As a university student, I don't have a lot of free time and have to spend most of my time visiting lectures and working on assignments.
When I hunt, it's usually late at night during the week or sometime during the day on the weekend.

Besides these activities, I also maintain multiple other software projects and websites, which also take up a lot of my time.

How do you approach a target? Do you follow a pre-defined methodology? And would you recommend testing few functionalities for all possible bugs, few bug classes across all endpoints, or anything else?

I don't really have a good pre-defined way to approach a target. When a new bug bounty program pops up, I try to look at as much of the scope as possible in a short amount of time. This allows me to quickly assess what kind of developers have been working on this, which software stack they use and how hardened the target already is. On these new programs, I can usually find some low hanging fruits pretty quickly. If I like the way the team responds to these first reports, I will dive deeper into the application.

I would personally recommend trying all endpoints for a few bug classes to start off. This shouldn't take too much time and will let you decide which endpoints you should return to to test some more complex bugs on.

Does recon play an important part in your bug hunting? And how does it look like for you?

I don't hunt often on programs that have a huge wildcard scope, so recon is not that important for me. If there is a wildcard scope, I usually run a subdomain scan and a quick wordlist for folders and files on these hosts. I'm working on building some tools that would make it easier for me to map out the assets on some of these larger programs. I don't think that you need an extensive recon strategy in order to be successful in bug bounty, but it does help for certain types of programs.

Do you have any favourite bug classes or types of targets that you focus on the most, and why?

I love bugs that take advantage of weird browser tricks which the average web developer doesn't expect, such as Cross-site WebSocket hijacking, CORS issues by abusing 'force-cache', CSRF through converted content types and Cross-Site Search (XS-Search) attacks. If you're familiar with these tricks, you can easily spot them when going over a target and with a nice proof of concept, they can definitely have a lot of impact. You can also very frequently spot these vulnerabilities on new programs.

After I look for these vulnerabilities, I usually focus on the backend. Most IDOR vulnerabilities are very obvious and usually have a high impact. I also try to look for cache poisoning on every host I see, as it's easy for a developer to misconfigure it.

What was the most interesting bug you found (or your favourite)?

On a web portal of a certain bug bounty program, I created an account with the username 'admin'. It turns out this username hadn't been taken yet and the user somehow got additional permissions because of the username. I wonder what the developers were thinking when they added this feature.

A lot of people are curious to know about the tools other bug hunters use. So, what does your arsenal look like? Which types of tools do you rely on, how do you choose them and which would be your favourites?

My main tool is Burp Suite because it does almost everything I need. It's an amazing product and I have it open almost non-stop. On top of that, I frequently use Turbo Intruder, a free tool developed by James Kettle. It lets me easily work out certain attacks and test for race conditions using Python scripts.
For recon I use dirsearch and amass, that's pretty much it.

Besides the existing tools, I frequently use Python scripts to make it easier for triagers to reproduce a bug. This is really useful for the types of bugs where reproducing it would normally be a hassle. I would recommend any hunter to practice basic programming, as it will really helps you to think about how a feature might be implemented behind the screens.

What advice would you give your past self about bug hunting?

I would advise myself to see bug hunting as a business and try to maximise your ROI. In this case your time is your investment and bounties are your reward. In the beginning, I didn't focus enough on the actual business impact of my reports. I did find a lot of bugs, but the bounties I received were very small. Later on, I focused more on assessing what the actual impact is of a vulnerability, which would indicate whether it's worth my time to investigate it more.

One thing that can help keep track of everything is taking good notes. Do you use any note-taking apps or knowledge management system?

In all honesty, I barely take notes. If I discover something interesting that I need to investigate later, I usually write some keywords on a post-it. If a program has a very wide scope, I might write down a few things in Markdown if I see something special. I aspire to improve my strategy by taking more notes, which should help me if I revisit an old target.

I personally believe that bug bounty requires working on technical skills as much as personal skills. This includes managing emotions, accepting duplicates or "failure", overcoming any personal fears and doubts... So, do you have any last advice on dealing with this non-technical side of bug bounties?

One thing bug bounty has definitely made me learn is patience. I used to underestimate the time a company needs to properly assess a vulnerability, especially if they don't have a dedicated security team. I used to be very annoyed if I didn't get a response within a few days, but I have learned to appreciate the process. Especially on Intigriti, I know that the team cares about the hackers and will make sure that we're not left in the dark. This means that I don't have to spend my time worrying about a response to my report.

I luckily don't have to deal with duplicates very often, for me it just means that I was on the right track, but that I had to be faster.

What are you still aspiring to as a hacker? In other words, do you have any learning goals, monetary goals or collaboration wishes?

I aspire to make my bug hunting efforts and rewards a bit more consistent. I often go through a few days of very intense bug hunting and then I do almost nothing for the next few days. This is not really healthy in the long-term, so I want to change my strategy a little bit.
Besides that, I also want to focus a bit more on certain vulnerability classes that I have not looked into enough, such as XXE and SQL injections.

Which hacker(s) would you give a shoutout to, whether they are a mentor or a community member?

I'm a big fan of the work that James Kettle (@albinowax) puts out. He has done some amazing technical talks about Cache Poisoning, HTTP Desync Attacks and ways to automatically detect potential vulnerabilities. I use his free tools very frequently.

I also like reading the technical writeups by @terjanq on Medium. He's very knowledgeable about weird browser quirks.

> **"Try and communicate with other hunters. Even if you're not collaborating on a specific vulnerability, sharing and receiving knowledge is one of the most important things you can do to get better"**

Have you already collaborated with other bug hunters? Can you share with us your experience, and if there is anyone you would like to collaborate with in the future?

I have done some collaboration with Kuromatae (@Kuromatae666) on a private program on Intigriti, which rendered some great results. We both have different skillsets, so it was nice to put our minds together to find some nice bugs. I don't have any specific people that I would like to collaborate with. Anyone who feels like it, can send me a private message.
I would recommend starting bug bounty hunters to try and communicate with other hunters. Even if

you're not collaborating on a specific vulnerability, sharing and receiving knowledge is one of the most important things you can do to get better.

Did bug bounty change your life? And how did Intigriti help you in your hacking journey?

Although I've only been actively doing bug bounty for almost a year, it has definitely impacted my life. I've got to talk to a lot of fascinating people that are passionate about what they do and I learned a ton of stuff. As a student, I don't really have any living expenses, so the bounties have definitely provided me with a nice financial buffer that I can use later on.

Thank you so much for this interview! Any last words?

I would like to thank everyone at Intigriti for providing such a great platform. They really care about the security researchers on their platform. I wouldn't be where I am today without Intigriti.