Meet the hacker: 0xkasper, CTF player, student, and hunter.

BY INTIGRITI · MAY 13, 2021 · LAST UPDATED ON MARCH 6, 2025

Our in-house team of security analysts won't judge reports by their author, but some researchers are known internally to put a smile on the face of our triage team. One of these researchers is 0xKasper, who as it turns out only lives a few blocks away from one of our Intigriti offices. More than enough reasons to catch him for an interview!

Hi Kasper! It's always an inspiration that a fellow countryman is successful in bug-bounty hunting. Can you tell us a bit about yourself, who you are, and how you got into bug bounty hunting?

Sure thing! I'm Kasper, a Dutch student currently doing a Master's degree in Computer Science at Ghent University in Belgium. I'm graduating soon and I will start working as a security consultant after the summer. I'm doing my thesis on Linux kernel fuzzing.

I first got into CTFs after I followed a course on cybersecurity. This sparked my interest and played almost every weekend with my team. After a few months, I found out about bug bounty and started looking around on Hackerone and later Intigriti. I submitted my first bug in August last year and I've started doing it more seriously since January.

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?

Well, bug bounty started as a hobby, but now I've been doing it more and more, so it has pretty much become a part-time or freelance job. Of course, I still prioritize my study work and I won't do any bug bounty whenever I just don't feel like doing it. But bug bounty has become an important part of my life and I enjoy it very much.

> **"Bug bounty has become an important part of my life and I enjoy it very much. "**

Now some technical questions... 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?

When I first approach a target, I will just look around and try to use the application as a normal user. I try to spot interesting functionalities that could lead to bugs, especially ones that I have found before.

I do not follow a pre-defined methodology, it always depends on what kind of target it is. However, I do always try to apply techniques from bugs that I have found before.

I would recommend mastering a few bug classes and looking for those especially. Besides that, have enough knowledge and skill to look for other types as well.

You can look for those on all endpoints while staying on the target. So I don't recommend trying to find a few bug classes across a lot of different programs. I find it a lot more lucrative to stay on a single target for a longer period of time.

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

Honestly, I do not do any recon, except for some Google dorking. For that, I like to get to know the application first and look for any specific keywords, such as API name and version, error messages, and URI patterns.

> **"But besides that, recon does not play an important part in my bug hunting."**

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

My favorite bug type is probably SQL injection. They're rare but still exist if you know where to look. For example, besides the standard injection in IDs, etc. that happen in WHERE clauses, you should also look for injection in inputs that specify column names, such as for ORDER BY and GROUP BY clauses.

I have recently started taking a liking to targets with open source applications. Before I always thought that these would be extremely hardened, but that's not true. I just love being able to set up my local instance and go nuts with it. You can modify their code, add debug logs everywhere you want, and know exactly what happens. It might take a few days to understand the application, but it's worth it and way more fun.

What does your arsenal look like? Which types of tools do you rely on, how do you choose them, and which would be your favorites?

My arsenal pretty much only consists of Burp Suite. From the extensions, I like to use Burp Collaborator for SSRF, Reflector for XSS, AutoRepeater and Autorize for IDOR/BAC, and Hackvertor. However, those extensions only help sometimes or for basic cases. The best tool is your own experience.

Besides that, I might write some Python scripts that help exploit something on a specific target. I have thought about writing tools, but I've not yet gotten around to it.

> **"The best tool is your own experience."**

Let's talk about automation. Many hackers leverage it for recon, mass-scale tests, and even automated reporting of bugs like subdomain takeovers. But others prefer to focus on logic or advanced bugs that can only be found with manual testing. Where do you stand regarding this question of automation? Do you use it, and do you think it is worth spending time on?

At the moment I solely do deep diving on targets and focus on logic/advanced bugs using manual testing. I very much prefer understanding the application and uncovering its flaws. However, I have thought about writing some tools that could automate some parts of testing, but I haven't gotten around to it yet. I do think automating your workflow is worth it.

How many hours do you spend on bug hunting every week?

At the moment I think spend 20-30 hours per week on bug hunting. It highly depends on how much study work I have in that week.

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

Stop reading and just do it. I can confidently say that most of my bug hunting skill and knowledge comes from practical experience. That doesn't mean you shouldn't read articles and write-ups, but you should read them as you go. If you think you have stumbled upon something interesting, you can look for articles and write-ups about that specific thing, apply it and see what works or not.

One huge hurdle hackers face is information overload. How do you keep up with the fast pace with which attacks and tools evolve? And what would you tell beginners who feel overwhelmed with the amount of information to learn?

There is a huge amount of information out there. I find it important to prioritize and not try to read everything there is. Sometimes if the number of open tabs with articles that I still want to read just keeps growing, I will just close them all and start fresh.

One of the best places to find new information is Twitter. I come across new write-ups of cool bugs on personal blogs. But there's also a lot of negativity there and people sharing screenshots of their top bounty payouts, so that may be discouraging and create a false image of bug-bounty. So it's important to follow the right people.

I also really like Intigriti's Bug Bytes newsletter, as well as Pentesterland's huge list of bug bounty write-ups. I do not go over those write-ups one by one, but I will check write-ups of bug types that I think might apply to my target.

For beginners, I would also suggest not reading the latest articles too much and focus on the basics first. The Web Security Academy from Portswigger is amazing and offers in-depth explanations and labs for each bug type.

What is the coolest thing you did with your bounty money?

I have not yet bought anything cool actually. I'm saving it all at the moment.

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

I want to give a shout-out to @Robin and @rekter0. We did some awesome hacking together on a program and I've learned a lot from them.

I would also like to shout out my favorite Bug Bounty content creators: @InsiderPhD, @STÖK, and @Jhaddix. Go check out their content, it helped me a lot when I was starting.

What are your expectations of bug bounty platforms, and why did you choose Intigriti?

In my opinion, the most important thing is a fair triage and Intigriti has just that. Intigriti's lightning-fast triagers are also a plus.

I have not reported any bugs on other platforms and I also don't feel the need to as I like hacking at Intigriti very much.

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

Thank you for this opportunity! If anyone has any questions or wants to collaborate, just hit me up on Twitter: @0xkasper.