Bug Business #8 – Get to know Intigriti's Top Hackers in Q2: kuromatae

BY ANNA HAMMOND · AUGUST 13, 2020 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/hacker-spotlight/bug-business-8-get-to-know-intigritis-top-hackers-in-q2-kuromatae

Bug Business is a series of interviews in which experts from the bug bounty industry shine their light on bug types and trends. Today, we sat down with Anthony (kuromatae) who came in second in our leaderboard in the 2020 second quarter.

He told us how he changed his life and is now living the Bug Bounty dream, his views on recon, how he avoids burnout, and other things.

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

Hello There!

I'm Anthony alias Kuromatae, a French guy who has multiple hobbies like cars and kitesurf.

Before doing bug bounty hunting, I did factory assembly line work. I am self-taught, hacking was a hobby for me since I was young. It took many times but I never gave up and finally reached one of my life goals that is living from my passion.

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?

I'm doing bug bounty full time, my life has totally changed since I started! Imagine doing everything you like and everything you want to do. This is what my life looks like now.

I don't see bug bounty like work but more like a game. If I want to play I can and if I don't want I'll just do something else.

The cool thing is really the possibility to play from anywhere no matter the time.

How do you approach a target? Do you follow a pre-defined methodology? Any specific approach like testing few functionalities for all possible bugs, few bug classes accross all endpoints, etc?

Well, this one really depends on the target!

First, I'll check all functionalities of the application, how it's made and what can be done in normal usage. Then, I'll start to check for hidden pages in JavaScript files.

I think the more you know the application, the better it is.

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

It's one of the most important parts of bug bounty. Recon doesn't necessarily mean doing a bruteforce of all possible subdomains in order to retrieve the xxx.yyy.zzz.sub.tld which will give you a reflected XSS.

For me, it's doing some google dorks, playing with waybackmachine, analyzing javascript files, bruteforcing dir/files, etc....

Just by doing this, you'll be surprised by what can be found!

One day, I played with an application that just had an authentication page. I found a PDF file containing the default password of users, and how usernames were made (It was a special phone number format). This PDF was giving an example phone number, I bruteforced some usernames with the default password and found plenty of users!

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

Hmmm, this one is a tricky question, I like to play with all type of bugs (except living ones).

One of my favourite is probably SQL Injection, it's really underlooked and I find them very often! There are many types of them, many people miss it because sometimes it's really hard to discover it.

Concerning targets, playing with PHP websites and APIs is really funny.

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

I have many bugs I really liked, one of them was a NoSQL Injection. It's not really a super special vulnerability but it was my first time finding it in bug bounty and, playing with the application in order to exploit it was really funny.

Another one was a vulnerability in an Android app, the funny thing is that you could send requests to another user and, by doing this, the victim had a real time modification in their Android app.

What does your arsenal look like? Do you rely on any specific type of tools, and how do you choose them?

Concerning tools, I'm working with a Windows and a Debian Server.

The first one is my main OS, I have Burp Suite, assetfinder and some other tools on it.

The second one is dedicated to automated tools (Dirsearch, waybackmachine, etc...).

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

Remember that the important part of bug bounty is learning new things, have fun and don't overdo it!

Some of the main hurdles many bug hunters face are stress, burnout and struggle with time management. As a successful full-time bug hunter, do you have any advice for hackers struggling to find a work-life balance?

Answering this question is a bit hard because not everyone works the same way.
When I first started doing full time hunting, I had multiple burnout phases.

There are multiple things to do in order to avoid this.

Personally, I work from 10AM to 5PM. Also, I often play video games and see friends in order to think about something else.

When I don't feel it, I don't work.

I think the last tip is to collaborate and find a Slack or something where you can discuss things, it's always motivating to discuss and work with people who have the same passion.

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

Unfortunately, that's also one of my main problems.

I use Notepad++ to take notes but I'm considering moving to a better tool because it's really important. I missed multiple vulnerabilities and lose track of many potential domains because I didn't have a reliable way of taking notes.

Why do you hack and what motivates you to keep on bug hunting despite any hurdles?

There are multiple reasons why I keep doing bug bounty.
One of them is the euphoria it procures when you find bugs. It also really goes well with my lifestyle.This is also a good way to learn new things while having fun!

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

There are many people I want to thank but listing all of them can't be done.
So, first I want to thanks @AdibouSec, nothing would have been possible without him.
Also, I want to thank @EdOverflow who was a great help for me to integrate the community. Lastly, I have to say a big thank you to @securinti who gave me the best opportunity in my bug bounty life.

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 collaborated with many hunters, one of them was @RobinZekerNiet and we had a lot of fun on some programs. The main reason for me to collaborate is to have a different point of view, it's also a good source of motivation.

In the future, I hope to collaborate with @quintenvi because we've been talking about this for a long time but we never had the opportunity to do so.

But, more generally, I want to collaborate with anyone who wants to!

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

The important part for me in platforms is how the reports are addressed.

At Intigriti, the triagers are from the platform and respond really fast to reports, it's really important for the hunters to have a real follow-up of reports.

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

Thanks to intigriti for the platform and the interview, if someone has questions regarding full time bug hunting, don't hesitate to reach me.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com