Get to know iQimpz, one of Intigriti's top hackers

BY ANNA HAMMOND · APRIL 12, 2021 · 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. iQimpz is a well-known researcher at Intigriti, he always sends in quality reports and is known for his IDOR's.

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

Hello! I'm Dylan Lawhon, a 20-year-old hacker, Christian, and college student living in the United States. I am attending the University of Central Arkansas (UCA), pursuing a degree in cybersecurity. I am also getting my Undergraduate Certificate in Applied Cybersecurity (ACS) at SANS Technology Institute.

When I'm not smashing bounties or doing school work, I also enjoy spending time with loved ones, working out, hiking, and researching all things offensive security!

I became interested in bug bounty hunting after watching one of STÖK's YouTube videos and seeing the good vibes of live hacking events and the bug bounty community. I had already had an understanding of a lot of the common bug types from doing CTF competitions, so I thought I would give it a shot. As soon as I had my first bug triaged, and had that amazing burst of excitement, joy, and relief that it wasn't a duplicate, I was hooked! Still to this day, I get the same feeling when my bugs are triaged.

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?

Currently, attending UCA and SANS Institute takes up a good chunk of my time so I do bug bounty as a hobby. I started bug bounty at the end of October 2020, so I am still pretty new. But it has already become a huge part of my life.

In my first 3 months of bug bounty, I hit #1 on Intigriti's 90-day leaderboard, and during that time I was spending ~80 hours a week on bug bounty on top of my other activities. Now, school is starting to take up more of my time because of all the end-of-semester projects, so I only get to spend around 40 hours a week on it.

I usually hunt early in the mornings before class, then get all my work done and go to the gym for around an hour and 30 minutes, then I hunt for the rest of the day and into the early hours of the next day.

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?

I do not have a pre-defined methodology and since every target is different my approach is always different. I'm still pretty new to bug bounty so I am still refining my methodology.

Currently, I prefer to spend a large amount of time on a single target because I can uncover more impactful bugs that have less of a chance of being duplicated. Also, this method is just more enjoyable than looking at many targets for low-hanging fruit, at least for me.

There are a few things that stay the same when I approach any target. For one, I always like to get a good understanding of the purpose of the application and how it works, before I start hunting for bugs. I also always check javascript files because it's a great place to find parameter names, hidden paths, DOM-

based XSS, information disclosure, open redirects, libraries used, and more. Early on, I also like to find out what technologies the application is using, backend and frontend. A way to do this is to use automated tools like Wappalyzer, BuiltWith, and Burp Plugins. I also make sure to do this manually by analysing response headers to different endpoints then googling the ones I have never heard of. This is a great way to find less known technologies that the automated tools will not pick up.

Regarding the second question, I have tried both testing a few functionalities for all possible bug classes and hunting for few bug classes across all endpoints. I would definitely recommend searching for many bug classes on fewer targets. For one, searching for the same bug over and over gets very boring fast. And since the main reason I do bug bounty is to learn, looking for many bug classes just makes more sense because I have more opportunities to broaden my knowledge about the different bug classes.

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

Recon is very important in my bug hunting. I will say that I don't do as much as I should though.

Since I like to stick to the main application I don't do much of the broad recon like subdomain enumeration, directory brute-forcing, acquisition enumeration, and so on. Instead, my recon consists of analysing javascript files, technology fingerprinting, parameter fuzzing, GitHub, and Google Dorking, and using the Wayback Machine to discover old API endpoints and files.

The way I do recon is constantly changing though, and I plan to focus on it more, in the future.

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

I think my "favourite" bug class even though I haven't found a ton of it, is blind XSS. You submit blind XSS payloads with no expectation for them to execute. Then at any moment, you may get an email from XSS Hunter (if that's what you are using), and your mind fills with so many questions. What program is it from? Was it a payload I sent a month ago? What endpoint did it execute on? Could it be on a third-party's website?

When it comes to targets, I prefer a target that has some kind of privilege hierarchy, a ton of places for user input, and maybe some file upload functionality!

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 is very simple. My main/favorite tools are Burp Suite and Google. I would still be a successful hunter if I only got to use these two tools. These are also probably the two most common tools so they don't need much explaining. Other than that, I use Wappalyzer and BuiltWith for technology fingerprinting. Dirsearch and the Wayback Machine for web path discovery. Amass for subdomain enumeration, then httprobe to find the active ones.

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?

So currently the majority of my hunting is manual. The extent of my automation is bash aliases for basic recon when starting on a new target, testing for s3 bucket misconfigurations, web path discovery, and other small things. Also, If I find a basic vulnerability in one subdomain and the target has many similar subdomains, I'll write a little script to test for it across all subdomains. Other than that, everything is manual.

I do think automation is very valuable and very much "worth spending time on" and I plan to do more of it in the future.

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

As mentioned in the second question, I now spend around 40 hours a week on bug bounty!

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

Two things. First, spend more time on a single target. Second, all programs still have undiscovered bugs so hunt on a program you are interested in. Whether the program has been around for 7 days or 7 years, they still have bugs.

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 an enormous amount of information out there and this can seems like an insurmountable barrier for beginners. So a lot of them get discouraged and quit. I think one of the main reasons for this is because they are too focused on the destination rather than the journey. The destination being, making those 5 digit bounties or being invited to live hacking events, but they don't understand the hundreds or thousands of hours that the bug hunter has spent grinding to get to that point. If you start to measure success based on what you are learning every day, then you are winning as long as you are trying.

So for beginners, I would recommend focusing on trying to learn something regarding bug bounty, every single day. And it doesn't matter what that is, just choose something that interests you. You will realize later on that things start to tie together, and some information that, at the time you thought was useless will often prove useful in the future.

I stay up to date in a few ways. Twitter is a must. When you follow the right people you can be updated with new tools, insightful research, new CVEs, events, writeups, and so much more. I also read as many writeups as I can get my hands on. Pentester Land's list of bug bounty writeups, Intigriti's Bug Bytes, and Hackerones Hacktivitiy are great resources. Also, STÖK's Bounty Thursday YouTube videos are a good source of information.

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

I invest or save all of my bug bounty money, so I haven't bought anything too cool yet!

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

There are a few community members and leaders that I would like to give a shout-out to. First off, @securinti because he is a very creative and innovative hacker that finds some very interesting bugs. He is also very helpful and has always answered any questions I have had about Intigriti's platform.

I would also like to give a shout-out to @stokfredrik. He is a very good content creator and hacker who puts out some great motivational and informative content. I also mentioned earlier that I became interested in bug bounty because of one of his videos!

Some other people I should mention are @TomNomNom, @NahamSec, and @samwcyo. They are all insanely talented and admirable hackers and I really appreciate all the writeups, tools, content, and tips they put out.

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

I expect that my reports are treated fairly, which has always been the case at Intigriti. I also expect that questions and reports are replied to on time, and I don't know how Intigriti does it but it seems like I get responses within 24 hours 90% of the time, and the other 10% is still very quick. I also love how much intigriti does for its hackers, whether that's kind words from triagers, swag vouchers, helpful support team members, or sponsorships for content creators. Another thing that is huge to me even though it is simple, is how everyone at Intigriti makes me feel that my efforts are appreciated.

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

I would just like to thank Intigriti for this amazing platform, and for giving me this opportunity to share some insight on my bug bounty journey! If anyone has any questions or comments just send me a DM on Twitter @iqimpz.