When fear no longer holds you back. Interview with Ryan Bonner (Roll4CombatUS)

BY ELEANOR BARLOW · AUGUST 24, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/hacker-spotlight/interview-with-ryan-bonner-aka-roll4combatus

Ryan Bonner, also known as Roll4CombatUS, is a respected Bug Bounty hunter, consultant, speaker, and Intigriti Hacker Ambassador based in the United States. In today's interview, we discuss his journey into bug hunting, his recommended tools and techniques, and share advice for hunters just getting started.

Ryan, how did you get started?

To put it frankly, I got fired from my first pentesting job. I wasn't a strong report writer, and I knew it. I also knew I had to get better at what I was doing, which at the time was a mix of things.

So, I started by Googling things like HackTheBox. My research evolved, and I gave Jason Haddix's Bug Hunters Methodology course a go. This introduced me to a way to practice beyond PortSwigger labs, and improve my skills. For about a year, I supported the community with recon. This was around 2023, before seriously getting into hunting.

Later, I met Jason at DefoCon and again at RSA. We became friends, collaborated once or twice, and the rest is history.

What was the first bug you were paid for? What challenges did you face?

My initial challenge was the fear of hacking despite my strong recon skills. I was worried about not meeting expectations. I had a genuine dread that people would expect me to be this great hacker and would hate me when they realized I wasn't at that level yet.

I had to get over this fear and just go and hack stuff. It's what everyone told me to do: to read a little bit, gain some knowledge, and try to apply it in practice.

My first bug bounty was a login over HTTP, and I received $100. It did not matter to me that it was a low-severity finding. I was the most excited person on the planet when it happened. The fact that I could get paid for finding something amazed me, and this was a highly motivating factor.

How do you choose a program to hack on, and what do you like to hunt for?

Honestly, I just look for wide-scope programs. For instance, I particularly like programs that have messages like 'anything you can prove is ours, we'll pay for' in the scope. I love any program like that because it allows me to do the things I like to do most, which is not actually hacking, but the recon. I love

proving asset ownership through elements such as favicon analysis and purchase history. I have found some cool stuff using that route.

Just give me default credentials all day. Easy to find, high ROI. But the most exciting element for me is Server-Side Request Forgery (SSRF). I don't find it often, but my heart races when I've hit something on the internal, and I get to piece it together. I get really excited about that.

Currently, I'm spending more time doing deeper client-side vulnerabilities. I'm not a world-class client-side person, but I do find plenty of client-side stuff.

With the rise of AI, has your methodology changed?

I think my methodology has gotten sharper with the help of AI because I can strengthen some areas that I don't do particularly well. For instance, I do a lot of JavaScript analysis with AI, and I would say that is an improvement in my own workflow.

But I still find the same bugs that I did before AI was a big thing. I don't have an autonomous hacking system. I mean, that's cool, but I don't want to buy four subscriptions. I would say I am using AI as an assistant, not as the workhorse.

In fact, I'm giving a talk this weekend on how I think it is very important to still become the expert and not let AI drive everything that we're doing. There is a lack of critical thinking that is becoming very apparent, and I see people who have not put in the years, time, and effort into hunting are struggling because of this.

Those just starting are like “AI says it, here it is.” But they don't know right from wrong and what the output is, leading to spam submissions.

What is your favorite tool to use?

Not including proxy tools, Gungnir is by far my favourite tool. It is a CT log scanner by Golden that pumps info directly into my Discord. It’s great. For instance, I found some vibe-coded applications that were pumped out through Gungnir on a target I was looking at, which gave me full access and full control. So, shout out to Gungnir, I love that tool.

What advice would you give to programs to do better?

I think this answer is probably universal across the industry. Clear communication with researchers is paramount. I understand it’s difficult given the sheer volume, but it would make a big difference if programs could spend a little extra time engaging with the top portion of hunters (say, the top 30% who are submitting thoughtful, non-spammy work). Being able to have a real conversation, ask a question or two, and get more context from the people running the program would be incredibly valuable.

Even something like quarterly open office hours could help. For example, programs could set aside two hours for hunters to ask questions directly to the development or security team. They could share context about architecture, tech stacks, or explain complex areas.

This kind of direct interaction doesn’t need to happen for every program, but many programs would benefit from talking more openly with the hacker community, not just the top one or two researchers. Spending a couple of hours engaging with the people helping secure your environment could lead to more meaningful findings.

Ultimately, companies want valuable reports. They don’t want issues to be missed because something is too complex or unclear. Better communication helps enable hunters, which is the whole point of bug bounty: find the bugs and get them fixed.

Are there any specific skills or habits that enabled you to be successful?

In terms of habits, my mantra is to read one thing per day. Read what other hunters have done, read write-ups, read open reports, read technical blogs. Get your mind wrapped around as much as you can and try to build daily reading into a habit. You don't have to read the most technical reports; just start to get the flow, get the idea, and go from there.

The greatest skill, which admittedly is something I failed at for a long time, is just being consistent with time and effort. Spend time on a target for three or four days. You will likely get frustrated. Don't worry, I'm right there with you. But stick with it. Be willing to spend more time because things will just happen. You'll notice things; you’ll notice patterns. I feel like everybody in cybersecurity is solid about pattern recognition, and it will click.

I personally like to set time goals rather than bug-finding goals. For instance, set 20 hours on a target to avoid frustration. And always go in with zero expectations. Once I have spent the time I believe is worth the task, I move on to something else.

If you don’t like writing up your thoughts, use things like Whispr Flow for voice note-taking during research. From those recordings, I will usually then put together flow diagrams. That’s how my mind works, through abstraction and visualizations. I need colors, visualizations, and flow diagrams. Find a method that works with how you think.

How do you balance work, personal, and bug bounty time?

Honestly, I'm the worst time manager ever. Because I say yes to everything, and then I just have to figure it out.

On an average day, I would say 8 am to 5 pm is dedicated to Penetration Testing, then 5 pm to 9 pm is spent with my partner, then 9 pm to midnight is my bug hunting and research time. But in the last couple of weeks, I haven't hacked at all. On average, I probably spend around 10 hours a week. But it’s very sporadic for me. I go into flows of heavy hunting, especially after I have found something that I am hooked on.

What advice do you have for hunters wanting to get started?

My advice is to respect each other and put some effort in before you expect effort from others. This is something that we can cultivate within the community.

Asking the right questions is so important. Well-thought-out questions that show effort will get responses from experienced hunters that will certainly support your growth.

It’s the same for me today. If someone reaches out to me and asks a well-thought-out question and shows that they've tried to do something and are not just asking me to mentor them, then I will usually respond back.

Also, don't be afraid to reach out to people you look up to. For instance, I reached out to Jason, and I think 80% of where I am today is because I reached out to somebody I looked up to. Develop those connections. Most people will reply and even help if you put the effort in.

Empowering the hacking community

Thank you, Ryan, for sharing your story and wisdom! Your journey is an incredible roadmap for industry newcomers, proving that when you play to your strengths, lean on your community, put effort in, and stay resilient, you can conquer any challenge.

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.

Contact the team today to learn more.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.