Bug Business #3 – Zseano's notes on hacking & mentoring

BY INTIGRITI · APRIL 29, 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. Sean a.k.a. Zseano defines himself as "just "another" web app hacker", but is in our opinion much more than that.

Over the past few years, Sean has been an active community member across nearly all bug bounty platforms, created his own platform to exchange bug bounty notes, organised a successful live hacking event and a handful of online mentorship sessions.

Who is the Sean between the 'Z' and the 'O'? We caught him in between hacking sessions and asked!

Hi Sean, thank you so much for taking the time to have this conversation with us.

How did you get started with bug bounty? In an earlier interview, you said most of your initial bugs were on one single program. How did that come along?

I got started with bug bounties back in 2015 when a friend showed me HackerOne and said that companies were suddenly starting to pay for security vulnerabilities. Ever since then I have focused on security and tried my best to improve my knowledge & skills. I have always had hacking knowledge before bug bounties existed.

Well if I am honest, the program was a private but a certain platform had leaked their name on a blog post so I went and found a bug, reached out to the platform to get it reported and they connected me with the team. We built a good relationship over time and they allowed me to test on all of their assets *(which are now out of scope)*. Over the years I was focused on learning exactly how their sites are put together, what old code had been left on the server etc. I had a complete mind-map of one program with lots of research.. at times it felt like I worked there with how much I knew!

You have been doing bug bounty for quite some time now – how did your approach change over the past few year?

Back in 2015 I was mainly just hunting for XSS as I fully understood what XSS was, impact that can be created and how to bypass most filters. As time went on and I was hunting deeper in sites I was just naturally finding interesting functionality that made me think differently, "What is this doing? What is going on here? Can I do anything here?". I feel like now I can sort of "guess" where bugs may be (login flows or developer consoles for example) and especially once I've spent so long learning how sites are put together I just **naturally** want to look in *javascript* files to see what's going on. I don't really focus on one bug type If I am honest, as I have a 'flow' I follow on a website.

Would you rather look at core, or score on recon?

I would rather look at the core if I'm honest. I just **know** that the company will have *something* exposed out there or there will be some open redirect on an out-of-scope domain that can be used for a chain. *Boringgg*.

I prefer looking at the companies main web application which is used by potentially thousands of users a day because this is their **main** application, so if there is any security, it should be here, and I want to test it. Plus I feel like I can get a good "idea" of how a company handles security because if I found ~5 IDOR on their main web app then I know they'll probably be vulnerable to some auth issues elsewhere (no validation of who owns input). One bug leads to many more in my opinion (especially on main production servers).

If you would start a bug bounty platform today, what are some things that you would consider, looking back at your years of experience with bug bounties ?

I think platforms have a lot of work to do still, in my opinion they are still selling company the idea that "bug bounties will solve all your problems!" and whilst yes having lots of hackers looking at your assets **will** uncover vulnerabilities, not enough companies are actually ready to deal with these reports or get things fixed, and then this causes frustration for the researcher.

I'd love to see platforms focus more on training companies and it's something I am actually beginning to focus on. Companies have welcomed hackers but now they need to absorb our knowledge and learn to replicate what we're doing.

I've seen you've recently scored some gigs in the UK as well. How would you describe the current state or views about bug bounties in the UK? Are companies more open than let's say 5 years ago?

I would say the views on ethical hacking/bug bounties is seen as very positive and a lot of UK companies run their own bug bounty programs already, however when visiting some companies I can see the same trend: they don't have a process setup to deal with these incoming bug reports. UK companies are very welcoming to working with hackers though from what I've seen, especially compared to 5+years ago.

Over the past few years, you've done an impressive amount of talks, mentorships, and even a live hacking event. What drives you to do that, especially in an industry where knowledge is money?

Ever since I started spending more time on computers & learning new things I picked up two things that have always stuck with me: Sharing is caring and information is free. I don't really think about the money because in my opinion money is the root of all evil, and money can cloud your vision. I have always had people share their knowledge and help me, so I am just passing the good will on. Humans work better TOGETHER and we can solve so many more problems from combining our thoughts & ideas together.

I also just naturally enjoy talking. I can ramble for hours and still feel like I've not done a good enough job and want to give more, so I guess a lot of my talking is just me being me.. rambling zseano.

> **"I am just naturally inspired to help others"**

What is also interesting is that most of your talks cover different subjects and you don't really "recycle" that often. How do you keep getting that inspiration? As a teacher and mentor, where and how do you learn new stuff?

I receive a lot of DMs from people requesting help so sometimes I use these questions to help build content. People will ask me the same questions I was asking all them years ago and I think to myself, "Why are they struggling? What don't they get?" and I try get into their mindset and create content to help answer their queries. Sometimes you just have to explain something in a certain way for the penny to drop. To be honest I am just naturally inspired to help others and it makes me smile so much when someone messages me, "wow i found a bug thanks to you!!". I love making others happy.

I learn my content from hacking on programs and from write-ups, especially new findings from James Kettle such as HTTP smuggling. To be honest my "learning" has never stopped and I am still to this day continuing to learn and get better at hacking

You say that you continue learning, do you see yourself moving in a certain direction? As bug bounty popularity increases, bugs become harder to find. In other articles, you note that most of this comes down to having "a unique mindset" — how did you see your mindset evolve over the past few years? How do you think it will evolve, knowing that some frameworks are implementing more security measures against the more classic attacks, like XSS?

Hopefully the direction is to becoming a better hacker! I feel like I have my "flow" of approaching a web application down to a T and I can pick any website and start testing instantly, so right now I am focusing on writing better notes and research when testing as I feel like sometimes I hack "too quickly" and miss important things. My notes have saved me in the past but I am looking to make my note taking more efficient.

To be honest I am not worried about bug bounties becoming more popular because the majority are just spraying payloads wherever they can and hoping for a lucky find. Diving deep and actually spending time on a web application is where the real bugs are. I have always been naturally curious and interested to learn how something was created, so I simply apply this thought process to a website. "What happens if I do this? I wonder if the devs thought about xyz when creating this feature".

With my mindset, I like to spot pattern and trends so if I'm looking for XSS for example and I notice a website is using new framework to protect from XSS, I will stop looking for XSS. I won't waste my time looking for a bug that won't be there and i'd instead focus on what MAY be vulnerable *(Site wide CSRF issue due to misconfigured framework?).*

I'd also do research into how they've protected from something like XSS.

> **"I find secure websites interesting because it forces you think harder "**

You say that you want to help companies avoid these mistakes and learn from your submissions. You'd argue that the less mistakes they make, the less interesting they get for you as an ethical hacker – or do you look at it from a different angle?

I find secure websites interesting because it forces you think harder, “How did they prevent against? What did the developers do?”, and it also creates opportunity to find those really interesting edge-case bugs rather than “Hey I’ve found 10 XSS, bounty pls?”. It’s almost like because you can’t find something you are forced to look and try harder, which keeps me on my toes. I do think ethical hackers can play a bigger role but this is also a tough area because even though platforms say they have 100,000+ hackers, most actually just produce noise *(sorry everyone)*. There is only a certain amount of hackers who can actually give the correct knowledge to prevent bugs however as time goes on I think we will see this increase. I think the future is bright for companies working with hackers.

Thank you so much for this interview – any last words?

HACK THE PLANET, but most important, never give up. If you want something that bad you will naturally go for it. Don’t get disheartened if you have gone weeks without a bug.. instead take a step back and look at what you’ve tried, what failed, and try figure out what is maybe going wrong for you. Good luck and happy hacking everyone.