Bug Business #9 – Get to know pudsec, Intigriti's Top Hacker in Q1 & Q2

BY ANNA HAMMOND · AUGUST 20, 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. Shaun (pudsec) won third place in our leaderboard in both the first quarter of 2020 and the second quarter.

An amazing achievement considering he is relatively new to bug bounty! So, naturally we wanted to know everything about him, his lifestyle, testing methodology, favorite tools, etc.

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

I'm 38, married with 3 kids and living in the best part of Australia at the moment. I've been working in the IT industry since high school and have worked in most fields; from building computers (we're talking jumpers and dip-switches), computer/software sales, technical support (phone & onsite), software and web development, corporate managerial/technical roles etc.

From a young age I would dismantle the home computer and attempt to build it again, epic failing along the way but a trip to the library, determination, trial and error... I would get it working again.
Then comes the tweaking, modifying system boot files, rebooting, running whatever game, seeing if there's any improvement, rinse and repeat. I shudder to know how many times I have installed DOS, Windows and Linux in my lifetime.

I only got into Bug Bounty late last year after seeing a video from @nahamsec.
Then after watching some other related videos I realised that many of the bugs he and others found are things I've discovered long ago in the past, just through curiosity, although never followed through with them from fear of getting in trouble.
So I spent some time researching as much as I could on bug types and reading as many write-ups I could find to get myself up to speed and start hunting.

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 work full time as a Linux system administrator and Python/PHP software developer. With the family, sports and work, it's hard finding spare time to hunt for bugs so it's more of a hobby at the moment, but when you find vulnerabilities it can be very addictive and hard to put down.
I'll usually hunt when I get home from work and the kids are occupied with homework, then after their bedtime try and fit and hour or so in.
But with the limited time I have to hunt these days I'm looking into ways to automate some recon while I'm away from the computer.

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 don't really have any set methodology as I'm still fairly new to the game and learning things as I go. I'll usually browse (or dork) for the low hanging fruit first, and when that's exhausted spend some more time looking elsewhere.
I've found a lot of good bugs from just fuzzing hidden/forgotten endpoints and exploiting outdated libraries etc, so after that, it will involve having a read through the website code and discovering other related assets to find anything amiss.
If I find some new information from write-ups, I'll gather as much knowledge about it and try to revisit past targets to see if I can find anything again there too.

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

Recon is pretty basic at the moment, it will involve browsing the target(s) with a browser and Burp first, checking each requests as I go. If something pops up that looks interesting I'll then focus on that or write it down for later.
I don't often sign up to the websites and just see what things I can find from a unauthenticated perspective.
I'll check out Wayback for other potential endpoints which I may have missed during browsing, and see what is still alive.
Once I'm over looking for the basic bugs then comes directory fuzzing on interesting paths, inspecting Javascript files, and looking into other subdomains which may be available then rinse and repeat.

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

I really enjoy working on targets that have an open scope, where you can potentially have hundreds of websites to play with, and testing on ones which other hunters may have never seen or even thought of. You may also find some sites will share similar code-bases thereby giving you more things to test as you move along.

I tend to stumble on a wide range of bug classes, but a simple XSS can be enough to put a smile on my face and anything other than that is a bonus.

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

This was probably one of my first ever bugs but also had a good impact.
I was browsing around on a target and discovered a private employee portal which was using Google SSO for authentication.
I tried logging in with my Gmail account but it failed stating it was an invalid domain.
I checked out the requests it had sent and could see it was actually sending my Gmail address in plain text, so I decided to try log in again but this time intercept the request and change it to

pudsec@target.com.
I ended up successfully logging into in the company client portal which gave me access to all their client data.

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?

I keep it as simple as possible these days, Burp Community and browsing around.
If I feel there might be some interesting hidden files on a path I'll fire up dirsearch and if I think an endpoint has more to offer than the parameters I've discovered, I'll run Arjun against them.
If the program has an open scope I'll attempt to find as many potential domains as possible; leveraging domain lists, dorking, etc, then check out each one manually to see if they're related and what goodies I can find.

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?

My process is very manual at the moment, but as I mentioned earlier, I'm looking at ways to automate things to do the work for me when I'm away from my computer.
My job does involve writing code to automate data collection, amongst other things, so it's just finding the time to develop what I need as a tool.
I do from time to time quickly code up something to help with the automated testing of a potential bug I've found, and some other scripts I've written have been very successful helping me get a bunch of bounties and swag from programs.

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

I think my interest in breaking things has always been there from a young age but there wasn't a platform to pursue it at the time.
So I think just learn everything and anything, keep coding, keep tinkering, keep thinking outside the box and everything you learn will come into play at one point or another.

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?

It can be very overwhelming with the vast amounts of knowledge out there for beginners, but when I started out I focused on getting to know my tools first.
I would have gone weeks without finding any bugs but with determination something will pop which makes everything worthwhile and if I ever lost motivation I would look outside the platforms and submit some bugs to OpenBugBounty which would lift my spirits and get me back on track again.

Twitter is an amazing resource for write-ups, PoCs, guides etc, there are heaps of bug hunters and researchers out there sharing vital information.
I like to read as many tweets as I can but any writeups will be added to my Pocket for later consumption, however the backlog is huge at the moment, I just need to work out the hacking/reading life balance which is tough.

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

Any bounty money goes directly to my kids education so I don't have anything cool to report there unfortunately.

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

I really like what the @thexxsrat is doing for the community, he's releasing a lot of quality bug hunting content on YouTube and also runs a popular Discord channel to help aspiring hackers get started in the industry.
When I've got some spare time I like to jump on Discord and chat along with @thexssrat and @0xatul to assist with newbie hackers in finding their first bug and pointing them in the right direction.
Anyone can join too at https://discord.gg/8rUtHj9.

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

I did try some other platforms before I discovered Intigriti, but it really felt as if my efforts weren't appreciated, and currently some of my outstanding bugs there are well over 6 months old.

When I first submitted some bugs to Intigriti, they were triaged very fast and with such positive and encouraging comments which really lifted me, especially just starting out, and it really pushed me to keep trying to find more, now knowing I was on the right track and staff were helpful and happy to answer any questions that may arise.

They're so efficient too that once I submitted a bug, which triage had validated, but they went that extra mile and tried a few other things from their end.
With their skills they ended up escalating the severity of the bug and explained their workings which helped me with improving my thought processes around certain scenarios and potentially increasing bounties!

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

Thanks to Intigriti for such an amazing platform and the triage team for just being awesome!