Bug Business #10 – Get to know Intigriti content creator PentesterLand

BY ANNA HAMMOND · AUGUST 27, 2020 · LAST UPDATED ON APRIL 4, 2025

Bug Business is a series of interviews in which experts from the bug bounty industry shine their light on bug types and trends. Mariem (PentesterLand) is the curator of our Bug Bytes newsletter. But she's also a bug hunter. We sat down with her to talk about her background and her life as a hacker and content creator.

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

Hi, I'm Mariem, a 34 years old hacker and entrepreneur living in Morocco.

I don't remember where exactly I heard of bug bounties. But here's how I got into hacking...
I initially wanted to specialise in Cryptology as I was doing a Masters degree in Cryptology and IT Security. But the "IT Security" part was so fun and fascinating that I ended up doing an internship on DNS Rebinding attacks. I fell in love with Web security, and the idea of analysing Web security mechanisms to understand how they work and subvert them.
So, I got a job as a penetration tester. And as I was rummaging through InfoSec news to stay updated, I discovered bug bounty programs and got hooked.

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 wear several hats and my situation has changed a lot in the past couple of years. To give you a short answer, I do bug bounty as a hobby. It's been about three months that I've been collaborating almost full-time with Intigriti. My day job is content creation. And I hunt for bugs whenever I find the time.

Bug bounty is a passion that has changed my life for the better. It provides me with an opportunity to learn and test my knowledge, while giving back to the community.

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 have a lot of notes and checklists for different bug types but I don't use them at first, when I'm hunting on a target.
I start with navigating the main site normally to understand its purpose. I analyse requests and responses in Burp and take notes of interesting functionalities I want to test deeper, interesting URLs, parameters, headers, endpoints in JavaScript code…
I also explore the scope and look at all the subdomains, acquisitions, technologies in use, etc. This first phase is basically reconnaissance like @Jhaddix does.

Then I focus on one thing after another. If my focus at the time is SSRF, I'll look for potentially vulnerable parameters and test them. I'll also test functionalities that are generally associated with this vulnerability like import functions. That's when the checklists come in handy, they remind me of all kinds of attacks and bypass techniques to try. Then I iterate the process over another asset or bug class.

But there isn't only one way or methodology. Focusing on a bug type is useful when you want to learn about it. Sometimes I prefer testing a sensitive functionality like e-payment, and look for all kinds of vulnerabilities and ask myself "What if?" questions.

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

I used to spend days on developing recon tools. But I figured it would take too much time working on them to provide me with an edge. And there are already so many amazing tools being released all the time.

So now I do recon in two steps. The first part is running a custom Bash script that's a wrapper around dozens of public tools. It stores the results in a different folder each time, and sends me email notifications of new findings.
The second part is manual. It's about understanding the target, building custom wordlists, fuzzing specific directories to find hidden content, etc.

My goal with recon isn't to be the first person to find some obscure asset and be the only one to test it. It's rather getting an idea of the most obvious assets, then focusing on manual testing.

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

I like focusing on bug classes that scare me the most, for the challenge. If I can get a handle on them, I can do and learn anything else. Lately, this has been OAuth misconfigurations and SSRF.
Once I have found enough of these vulnerabilities, I'll switch to a different bug class I want to master.

I am not very selective about targets. I do both public and private programs. And open scope isn't a requirement, I like the challenge of finding bugs in small scopes without relying on recon.

What does your arsenal look like? Which types of tools do you rely on, how do you choose them and which would be your favourites?

My main tool is unsurprisingly Burp Suite. Other than that, I only use open source tools. Think classics like ffuf, amass, massdns, nmap, @tomnomnom's fantastic Go scripts, etc. There is also ProjectDiscovery who are doing a fantastic job especially with nuclei.

Other than these, I often test new tools and compare how they perform, which ones are faster or yield the best results. But it's hard to keep up with the pace at which tools are being released!

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?

Like I said before, I use a Bash wrapper around public recon tools for automation and monitoring. The idea is just to save time and focus on manual testing.

I think automation of both recon and bugs exploitation at mass scale is really interesting. A lot of bug hunters are using it to identify fresh assets and test for specific bugs at scale. There has been a lot of new developments recently in terms of automation tools and APIs.
It's probably something I should work on more too but for now, I prefer focusing on tests that cannot be automated.

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

Use Time Blocks to decide in advance how many hours you'll dedicate to learning, and to actual hacking every day or week.
Stop procrastinating and "wasting" time by only reading about bug bounty and not practicing.
Believe in yourself.
Find practices like yoga and meditation that will help you relieve any anxiety and fears (even if you don't realize it, you probably have anxiety and fears that are unconsciously stopping you from reaching your potential!).
And learn to take good notes. You don't have to invent a system from scratch, just use an existing solid knowledge management system like Building a Second Brain.

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?

Information overload was an issue for me because of my past doing penetration testing. Pentesters have to be polyvalent, and be able to cover more surface than bug hunters in a short time.
So, when I started bug bounty I thought I had to learn about all vulnerability types, tools and tips at the same time.

But then I noticed that many bug hunters are successful in doing a deep dive into a single bug class. So, I've changed my learning strategy. I note down any new research and information, and only come back to it when it's the subject of my focus.

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

For a really long time, I just put all my earnings from bug hunting and work in a savings account. Then this year I wanted to treat myself for the first time. I bought a ticket to @Agarri_FR's onsite training on advanced usage of Burp Suite, and booked everything from plane tickets to hotel.
Then Covid-19 happened and the event was cancelled!

So instead, I bought a new laptop and screen, a fitness watch, and a standing desk. Since I spend most of my time working at home, these are spendings that will help me be more productive while staying healthy. Basically spending more to earn more!

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

Bug bounty is a very competitive field. So, I have tremendous gratitude for anyone who takes the time to work on an article, video or tool and share them for the sake of sharing knowledge.
A few names that come into mind are @InsiderPhD, @TomNomNom, @gwendallecoguic, @albinowax, @s0md3v, @EdOverflow, @hakluke, @stokfredrik, @Jhaddix, @securinti, @farah_hawa01, the team behind ProjectDiscovery... And of course @NahamSec who is doing a huge service to bug hunters with his interview series.

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

I was hacking on Intigriti even before our collaboration started. There are several criteria for choosing a bug bounty platform or program. For me, the main reason is simply the hacker experience.
I've used several platforms and found Intigriti's triagers the most effective and polite. There is always someone on the Slack channel to answer any questions we have, or to discuss the outcome of a report.

I also appreciate everything Intigriti has been doing for the community, like encouraging content creators, sharing bug bounty tips, AMAs, etc. It shows that the company really cares about its hacker community.

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

Thanks a lot for this interview and for everything you do for the community!