## **The Harsh Reality Behind Full Time Bug Bounty Hunting: Explained**

## 

## **My Bug Bounty Background**

I receive numerous messages each week asking how to get started with bug bounty hunting because of how active I've been in the bug bounty space. After speaking with people, it becomes clear that they have internalized the notion of bug bounty hunting as a way to get away from their monotonous lives.

While I'm all for giving advice and supporting people in achieving their goals, I believe it's also my responsibility to be completely honest and explain why this preconceived concept is a little unrealistic for a huge proportion of the population, especially those that have made a recent transition towards cybersecurity.

This blog post is not intended to discourage or demotivate you from pursuing your dreams and realizing their full potential; rather, it is a list of variables to be aware of so that you can have more realistic expectations when it comes to this topic.

I've gone ahead and written a list of crucial factors that I believe are essential in determining whether or not full-time bug bounty hunting is a realistic, or even best choice for you.

## **Not a Form of Stable Income**

Firstly, bug bounty hunting as a full-time job is just not a financially secure profession. It's a pay-for-performance system that requires you to produce tangible results in exchange for money. There is a large sense of security that comes with what you're accomplishing in other elements of life, as opposed to being continually held in opposition to one solitary variable.

I can tell you from personal experience that you can make thousands one month and barely scrape by the next due to variables beyond your control, like all of your submissions being flagged as duplicates. It's not always due to inability to find vulnerabilities. Of course, for the great majority of you, this isn't ideal since you most likely have responsibilities. I can only see this working if you have a significant financial safety net in place before making this commitment.

## **Skillset and Capability Requirements**

Secondly, the level of expertise and capacity necessary to compete with other bug bounty hunters is incredibly high. When it comes to cybersecurity, there has recently been a lot of discussion regarding the notion of gatekeeping, but I disagree with those who say that this is the case. There is a severe talent disparity in the industry, and I do not believe that a beginner should attempt to transfer into cybersecurity without first having a solid comprehension of the fundamentals.

Personally, I learned by spending months or even years researching various aspects of what is now known as cybersecurity. I went through a time when I was learning the basics. I didn't simply jump right in and start breaking stuff. It's akin to attempting to fly a jet without first knowing the controls and receiving training. Without a wide understanding of the numerous areas that make up what cybersecurity is, I feel it is difficult, if not impossible, to identify vulnerabilities.

What you will also find is that the public bug bounty programs that you will initially start on will be completely clean of most vulnerabilities because they have hundreds, if not, thousands of hackers on them and the scope seldom changes.

Speaking of scope, many bug bounty hunters now have self-contained monitoring systems in place to identify external attack surface modification and dynamic content change within hours. It's trivial to write a script that gathers all subdomains and stores them in a database, compares the values every couple of hours, and then sends a message via chat software when something new occurs.

People had this thought years ago, and I personally know of a bug bounty hunter who implemented this into his pipeline and made a lot of money in a short period of time. It's not groundbreaking, but he was one of the first to put a system in place to actually do this and act on it.

So, what I'm basically saying is that there are so many new strategies being created that keeping up with them all needs a lot of research on its own. Strong comprehension of theory is not going to enable you to become a full-time bug bounty hunter. People that are genuinely successful in this space have built their own methodology and approach, which they have been updating for years.

## **Motivation and Energy**

Thirdly, the amount of drive and energy necessary to maintain the level of consistency required in full-time bug bounty hunting is extraordinary. To be able to perform efficiently and consistently, you must have a propensity, which necessitates a tremendous amount of discipline. You may experience burnout in the first few weeks because you are taking something that is lucrative and appealing through a sense of success measured in the actual identification process, and then lowering it by measuring the result of accomplishment through the monetary reward at the end.

It's difficult to be successful at something when you're chasing it for the sake of fulfilling your responsibilities rather than your own personal success and happiness; ultimately, you'll reach a point when it's no longer enjoyable.

With regular employment or most financial streams, you can have a bad few days where you're not performing well and not much changes in terms of the overall outcome, but with full-time bug bounty hunting, every day where you're not placing proactive effort into a program is a missed opportunity to fulfill your responsibilities. You can't afford to have a rough few days, and since everyone is human, this isn't something you can plan for, hence the importance of a financial safety net.

## **Geographical Location Restraints**

Fourthly, some people's desire to work as a full-time bug hunter is hampered by demographics. Bug bounty payouts are frequently given in US dollars, which in a lot of cases provides a better return on investment because many countries have lower living costs than the UK or the US.

Take Argentina, for example, where, according to Time Doctor, the average monthly wage is $400. Full-time bug bounty hunting in Argentina would be a considerably more reasonable and realistic objective because this specific monetary value is the equivalent to less than one vulnerability payout on most bug bounty programs.

## **Personal Experience and Conclusion**

Freelancing and independent consulting have always been some of the most reliable sources of income for me in the past. Companies and organizations frequently hire freelancers or independent consultants to test new or particular web-applications over a several day period. This arrangement is optimal since a pre-set amount of money is provided at the conclusion of the assessment. The amount is also frequently greater than what I could earn working full-time as a bug bounty hunter.

So my advice to people who want to use full-time bug bounty hunting to gain more flexibility and freedom in their daily lives is to look into freelancing or independent consulting, where the outcome is guaranteed regardless of the overall quality of the result. Of course, there are issues with invoices not being paid on time, but they are trivial in comparison to what you might face with full-time bug bounty hunting when it comes to performance.