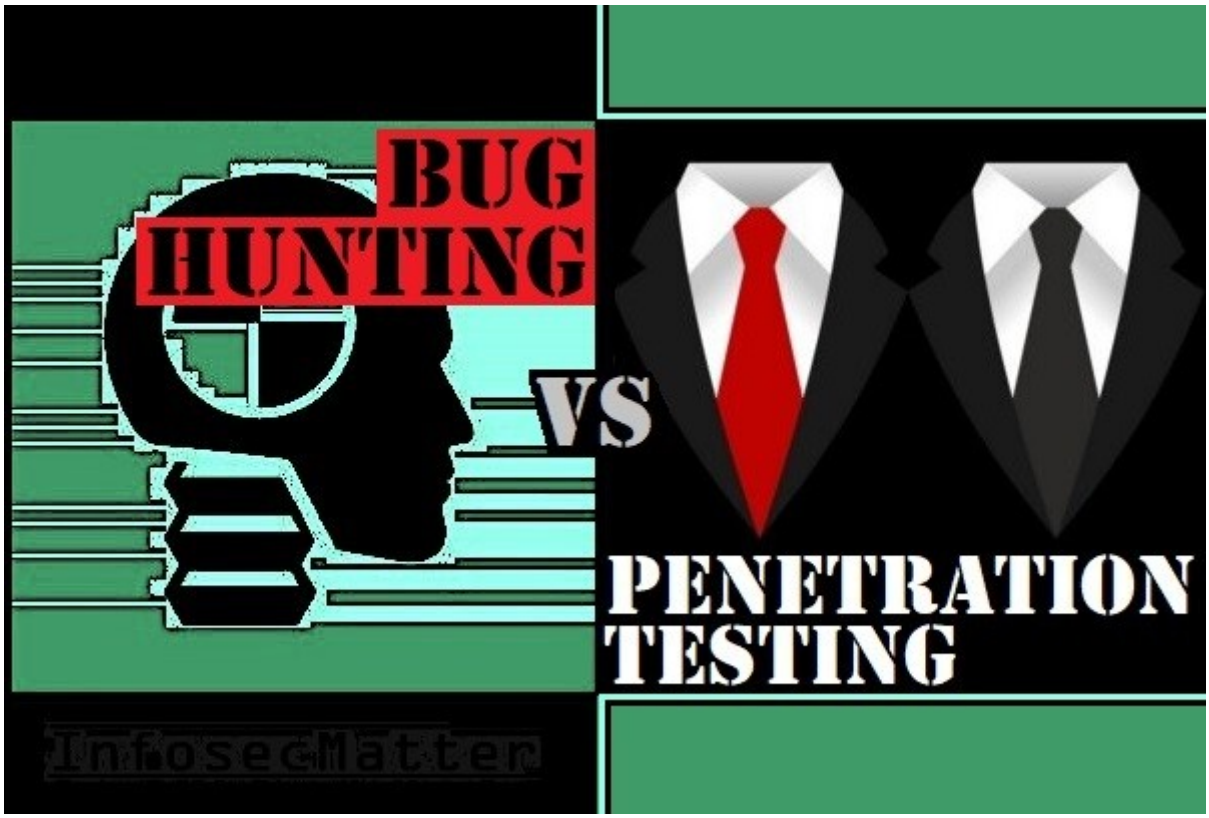
Become a Penetration Tester vs. Bug Bounty Hunter?

infosecmatter.com/become-a-penetration-tester-vs-bug-bounty-hunter

December 20, 2020



If you are looking to break into the field of offensive security and you are asking yourself whether you should aim to become a penetration tester or a bug bounty hunter, read on.

In this article we will look on the pros and cons of both career paths and lay down some of the key questions you should be asking yourself before making the choice.

Let's start on a light note.

Do you enjoy working alone?

As a penetration tester, you likely have to face your client from time to time. You also get to interact with your teammates, project managers / coordinators, your boss etc. You go to meetings, you consult things over phone, sometimes you present and do other things involving other people.

This is not the case if you are a bug hunter. As a bug hunter, you are pretty much a lone wolf. You work alone, you focus on the technicalities practically all the time. You are not bothered by anyone or anything. There is just you, your computer and the software you are trying to break.

Okay, right, there are also the triagers marking all your submissions as duplicate (joke).

Everything has its pros and cons. Although bug hunting may seem less worrisome, it also means a lot of solitude. It means less social interactions. In today's world it doesn't seem like a big deal, but on the long run this will have consequences. There will likely be detrimental effects – declining soft skills, social isolation, even loneliness.

It is prudent to not take these things lightly and try to compensate for it. We humans are social creatures and interactions with other people are crucial for our cognitive and social functions, but also for our mental health and overall happiness.

What is the value of dollar for you?

Every bug bounty program pays the same reward regardless of where you are currently living and there can be huge differences in the real purchasing power in different parts of the world. Ultimately, this can play a significant role in the decision making.

Have a look here or here to see what are some of the typical bounty earnings.

Suppose you live in a country with a strong economy such as US, Japan or any western European countries, for example. The amount of goods and services you can buy for a bug bounty reward is going to be very different in comparison to living in economically less powerful countries – e.g. some parts of Asia, Africa etc.

In some countries, the financial incentive is simply so much bigger in favor of a full-time bug bounty hunting, because getting couple hundred dollars can be a huge reward. Discovering a $30k worth critical bug on Instagram can even set you for years!

Not saying that you should be ignoring bug bounties if you are a US citizen. In fact, there are people who can make high 6 digit annual income just from bug bounty programs. Some people can even surpass $1 million, according to PCMag.com. Keep in mind, however, that those people are some of the most talented people in the world.

Do you prefer stable income?

Penetration testers who are employed as full-time employees (ethical hackers, security auditors, consultants etc.) have a steady paycheck coming every month (or week – depending on the country) to their bank account.

If you are a freelance penetration tester and you get hired on a project (e.g. as a contractor), you also have a pretty certain compensation coming to your bank account, based on your negotiated MD (man day) rate.

Now this is very different for bug bounty hunters. As a bug hunter, you never know when are you going to find something. And even if you do find a bug, it's never certain that you are going to be paid for it!

Chances are that you will find a lot of duplicates. You will also likely be stressed by companies acting unethically in regards to your findings, because some of them will do everything in their power to not pay you. It is not rare even among the biggest and most respected IT companies.

> As Microsoft have no intentions of ever paying me for all my submitted vulnerabilities I am forced to do this. Countdown starts today- then I will post them all public. MS is just trying to get time to patch them then never pay me. I have for over 100.000$ in submissions. I have not had a bounty paid for over 7 months I am in debt, my life is ruined- because I trusted that money was on the way. I am getting sick by stress, but they just ignore me. I have submitted hyper-v virtual file system escape. bitlocker full hd encryption bypass …
>
> *– Jonas L (@jonasLyk) Jul 14, 2020*

So as a bug bounty hunter, be prepared to struggle with your cash flow. If you choose this path, make sure to prepare sufficient financial cushion before you embark on this journey full-time. Reserving at least 1 year of living expenses in advance should be a reasonable minimum.

Employee benefits vs. no benefits at all

Apart from a stable income, being an employee has also many additional benefits. You've got paid vacation days, health insurance, social security, to name a few.

Working in the information security industry will typically also get you annual conference visits, trainings, certifications and other perks.

As a bug hunter, you don't have any of those things. You have to deal with everything by yourself. This of course includes making sure that your income taxes are paid on time, in according to your local government laws.

You simply have to be ready for a bit of a rocky road. As they say, with freedom comes responsibility.

Do you have certifications?

As a bug bounty hunter, you don't need to have any security certifications (e.g. OSCP, GPEN, CEH etc.). You also don't need any schools, a diploma. You don't need any resume (CV) to impress someone with on a job interview. In fact, you don't need anything except your technical skills, perseverance and your computer.

Nothing is stopping you from succeeding. Literally nothing and no one.

On the other hand, as a penetration tester you need to have certifications. Most companies expect them. They also expect you to have a nice resume and a set of skills including soft skills to make you presentable to the clients.

Have a look on what are some of the essentials penetration testing skills here. A good pentesting profile can take years to build.

Without security certifications, it is hard to break into the penetration testing and consultancy. Most hiring managers require OSCP or equivalent certification, and this is neither easy nor cheap.

How much freedom do you want?

Are you happy to work business hours (9 to 5) in an office, travel for work sometimes or do you like to work from anywhere and anytime you like?

Do you like to chose what project you will be working on, pick what you want to study or how much time you want to allocate for research?

As a penetration tester, you typically have to adhere to some rules in these regards and your choices are limited, while as a bug bounty hunter, you are the one making the rules!

As a bug bounty hunter, you can work anytime, from anywhere and focus on whatever you like. Nobody is telling you what you should do. You are your own boss, which is of course priceless.

Do you have the skills?

Now this is the crucial point. Surely, both roles require a very deep level of knowledge and technical expertise in multiple technological areas, but there are some interesting differences here.

First of all, in a professional penetration testing, the time (effort) allocated for a particular project is always limited. It is bound by the contract with the client, typically on MD rate or hourly basis, based on the projected effort estimation.

This means that as a penetration tester, you don’t have all the time in the world to spend on your target and dig in such depths as bug hunters. You typically have to adhere to a methodical approach using standardized methods, techniques and tools, in order to cover the agreed scope first. Only then you can dig deeper.

And if you don’t have sufficient time to find any critical vulnerabilities or a zero day, it is not a deal breaker for you. You are still going to get paid.

Now bug bounty hunting is completely different story. For bug hunters finding bugs is the only way to survive. They literally have no choice other than to dig and dig and dig into their target in order to find something.

This means that successful bug hunters cannot have mediocre skills, because otherwise there will be no reward for them. If they are mediocre, better hunters will surpass them and find the vulnerabilities instead.

True, you can still find a low hanging fruit sometimes in bug bounties, but the competition is fierce and growing each year (see the trend here). This really pushes the entire industry to the limits and drives the innovation (and automation) to the new heights.

For bug bounty hunters there is simply no room for mediocrity in the long run. It is a matter of pure skill and survival of the fittest, or should I say the most skillful?

What do you want to test?

From an outsider perspective, it may seem that bug bounty hunting is all about web technologies, mobile apps, little bit of a cloud infrastructure here and there and that's it, but this is just not true.

There are many different companies, organizations and projects that have an active public bug bounty program that reaches far beyond just web or mobile and which covers the whole technological ecosystems. For example:

- **Broad scope** – Apple, RedHat, IBM, OpenBSD, Microsoft, Oracle ..
- **Antivirus products** – Avira, Avast!, ESET, TrendMicro, Symantec ..
- **Security appliances** – AlienVault, PaloAlto Networks, FireEye ..
- **Network equipment** – Cisco, F5 Networks, Linksys ..
- **Chip manufacturers** – Arduino, Intel ..
- **VoIP telephony** – Asterisk ..
- **Scripting languages** – Perl, Python ..
- **Databases** – MongoDB, Firebase, Oracle ..
- **Mobile devices** – Android, Qualcomm, Nokia, HTC ..
- **Telecommunications** – AT&T, Verizon, Vodafone ..

All these have an active bug bounty program (see the full listings including scoping information here or here). You can really find various interesting projects to work on and many others are launching their bug bounty programs as well.

On the other hand, there are still some areas which are practically exclusive to penetration testers, red teams and professional consultancy firms. These areas include comprehensive security assessments such as:

- Internal network infrastructure (IT) penetration tests
- Industrial systems, SCADA and ICS (OT)
- Corporate Active Directory environments
- Configuration reviews and security auditing
- Network architecture security reviews
- Wireless penetration testing
- Physical security testing
- Social engineering

If you wish to work in these areas, you may want to focus more on the penetration testing side.

Comparison table summary

Here's a summary table pointing out the main differences between bug hunters and penetration testers in general:

	Bug bounty hunter	Penetration tester
Compensation (income)	unlimited	medium – very high
Income stability	none	very high
Competitiveness	high – very high	low – medium
Job excitement	very high	medium – very high
Freedom	very high	medium
Experience required	none	medium – high
Education required	none	medium – high
Soft skills required	none	medium
Professional certifications required	none	medium – high
Technical skills required	high – very high	high
Risk of job stress	medium – very high	low – medium

Bug bounty hunting opportunity

Through online platforms such as BugCrowd, HackerOne or Intigriti, it has never been easier to reach so many public bug bounty programs. Anyone can enroll.

All you need to do is register, look at the scope and you can start hacking with possibility of earning a solid income. How cool is that?

But before quitting your daily job and jumping on the bug bounty train full-time, better to play it safe. Try first to make it your side income, at least for several months.

See how it goes. If anything, it will at least help you sharpen your technical skills like no other thing.

Once you feel that it could be a viable source of income for you and you have accumulated sufficient financial reserves, great, go for it full-time. Keep in mind though that It is a volatile world we live in and things can change.

Looking to sharpen your ethical hacking skills?

If you would like to get into these offensive security areas, but you are just not confident enough about your technical skills yet, have a look on this article listing 25 quality CTF (Capture The Flag) websites, where you can practice ethical hacking and penetration testing techniques.

CTFs are an excellent way to improve your technical skills, for free and legally. They contain real world challenges with endless time for study and practice. This will certainly help you. I know it, because it has helped me to get my first penetration testing job!

See also list of Bug bounty tips that I'm collecting from the bug bounty hunting community on Twitter. This can help you with automation, but also for connecting to the right people.

If you liked this article and you would like more like it, please subscribe to my mailing list and follow me on Twitter and Facebook and you will get notified about new additions!

SHARE THIS

TAGS | Bug bounty | Bugcrowd | HackerOne | Intigriti | Job seeking | Penetration testing