My Journey of Bug Bounty

Ananda Dhakal   Follow

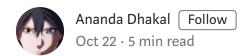Oct 22 · 5 min read

Hey, I am @dhakal_ananda from Nepal and I am back again with another writeup. This time, I want to share about my bug bounty journey. Let's dive into it already.

This all started when I was just a kid who used to play games and use facebook sometimes when I was maybe 13. I did not know that something like Bug Bounties existed until about mid-2018.

I have an elder cousin brother who knew about these things but he didn't directly tell me about bug bounties at first. He had told me that I can progress in the security field since I had an interest in HACKING-kinda things from even before. He asked me to learn about OWASP Top 10 vulnerabilities in Mutillidae. **The best thing is that he didn't give me a clue about anything. He asked me to do all the things by myself using the INTERNET.**

Well, I did not know anything about it so it took me a bit of time to set up Mutilidate and Burp Suite but I did it by myself by watching videos on YouTube. While I was confused and I could not find any solution, I would ask him for help and he would help me. But for the hacking project, all he shared was an MS-Word report of CSRF bug in Mutillidae so that I could know how to write a report. He asked me to make a similar report of Brute Force, SQLi and Reflected XSS. I was able to reproduce those bugs based on YouTube videos after some efforts but I did not know how it worked in the

real world. I learned how it worked in real-world security after some time of doing bug bounties. After doing that, I left it/(rested maybe?) for some time and after that, I got to know about bug bounties from him and I created the Hackerone account on July 30, 2018. Still, I knew nothing about security in the real world since I was just coming graduated from the virtual environment.

I still didn't know about a thing in real-world security. (*Just to let you know that I did not ask for help to anybody on twitter though*). What I did was I read the disclosed reports on Hackerone and tried to find bugs like that on other platforms☺. I read writeups and I just read and read. **I was lucky enough that I got my first valid bug in after a month**. I got even more motivated to do it and continued the journey.

I got 600+ reputations on Hackerone after some time, then I heard about BountyBash live hacking event that was being organized in Nepal. It was the first live hacking event it Nepal so I thought that I would attend the event. I went to Kathmandu and attended my first live hacking event. I met so many tech enthusiasts and really good hunters out there. I found an account takeover vulnerability but the interesting thing is that I did not

know it was an account takeover at first 😖. **Still, I got the most critical bug award in the event. I was rewarded along with** Gujjuboy10x00 as MVH and Bhavuk Jain getting the most creative bug award. @_jensec got second place in the leaderboard. *For more info regarding the event, you can go to* https://www.facebook.com/bountybash *if interested.*

So the journey in the event was also pretty good. I learned some tricks to find vulnerabilities hopefully :). Before attending this event, not even a single soul in the bug bounties world knew me. I did not have a twitter account with pretty good followers. I did not talk to anybody related to InfoSec and I was like an undercover person who just looked for bugs in Hackerone. I let out my identity after the event and it was/is really good to share things with fellow hunters.

After I came back from the event, everything is going just normal as every other bug hunters do in their daily life. I wanted to provide some suggestions to newbie bug bounty hunters and some suggestions to experienced hunters also. You can read it below.

Suggestion for newbies

1. Do not directly hunt for bugs in real-world programs. You will only end up disappointed, mostly. That's why first practice bugs in the virtual environment that don't harm anybody. **Mess things up in the virtual environment :P**

2. Trying to learn everything at once is also a bad thing. Learn about vulns one-by-one.

3. Become an expert in one bug and know enough about others also. Like, somebody is an expert in XSS while someone loves Broken Access Control and somebody could be IDORist and logical bug-finder like me. You can also be an expert in more than one though.

4. **Remember that money is not everything**. Most people getting started in bug bounties want money only. Though you can go through that approach also but it is not a healthy way because you will end up really disappointed if you don't find bugs.

5. Choose your primary target and keep hunting in that target on a daily/weekly basis. **You will have a higher chance of finding valid bugs if you keep hunting in the same program**. You can have other programs as secondary targets.

6. Gather a lot of knowledge and skillsets and then smash the target.

Some important things

1. Do not put too much pressure on yourself to find the bugs even if you don't find bugs. I also used to find only a bug in the whole month.

2. Care about your physical and mental health. Your health comes first because as you know, Health is Wealth!

3. Give time to your family also. *Without them, you will have nobody to share your joy of getting the bounties, at least for me*.

4. Sometimes, give back to the community that helped you grow. Write writeups, **not to be famous but to help others and yourself grow**.

5. Last and most important, don't forget to live your life because of bug bounties. ***Remember that you have got a life to live to the fullest.***
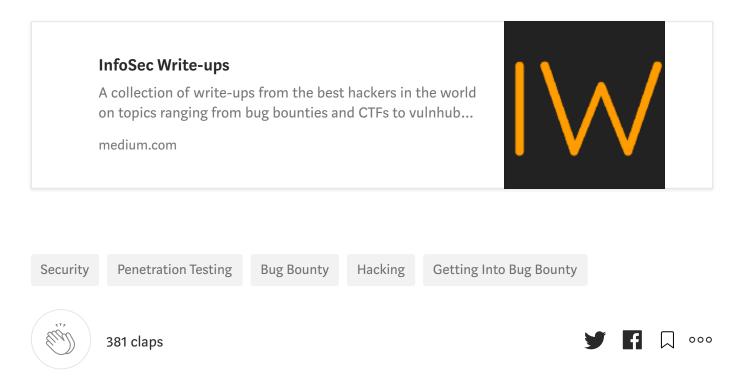
Maybe I wrote too much so that's it for today. I hope you get some motivation to do bug bounties and hope that you will be able to cope with disappointments and stress that bug bounty presents to you. See you again in next writeup.

Hackerone profile: https://hackerone.com/dhakal_ananda

Twitter profile: https://twitter.com/dhakal_ananda

. . .

Follow Infosec Write-ups for more such awesome write-ups.

InfoSec Write-ups

A collection of write-ups from the best hackers in the world
on topics ranging from bug bounties and CTFs to vulnhub...

medium.com

Security   Penetration Testing   Bug Bounty   Hacking   Getting Into Bug Bounty

381 claps

WRITTEN BY

Ananda Dhakal

Passionate about cyber security

InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Maintained by Hackrew

See responses (2)

More From Medium

Ping Power — ICMP Tunnel

Antivirus Evasion with Python
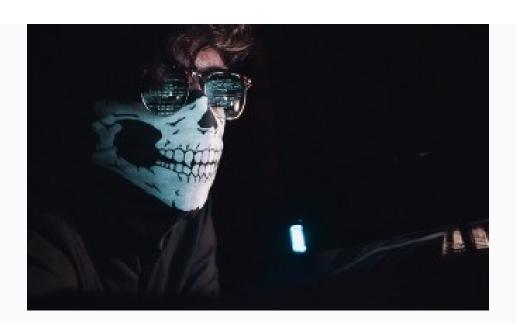
Picture Yourself Becoming a Hacker Soon (Beginner's Guide)

Abanikanda in InfoSec Write-ups

Aug 16 · 19 min read ★

685

Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade

Medium

About   Help   Legal