Meet the hacker: Get to know sumgr0, the king of subdomain takeovers.

BY ANNA HAMMOND · MAY 7, 2021 · LAST UPDATED ON MARCH 6, 2025

Intigriti researcher sumgr0 caught our eyes when he secured himself a top position in our quarterly leaderboard by honing his skills on just one program. We caught up with him for an interview to talk about his recon techniques, automation and why he enjoys using the Intigriti platform.

Hi Sumit! I'm happy we finally meet. Can you tell us a bit about yourself, who you are, and how you got into bug bounty hunting?

Hi! My name is Sumit Grover and I'm passionate about computer security, forensics, and my day job with a local Telecom Company. I came across the term *"bug bounty"* about 2 years back when I was watching a security-related video on YouTube. After that, I registered myself on all available platforms while not exactly sure of how to begin.

With some experience in vulnerability assessment and penetration testing in the past, I slowly started reading Medium articles and other blogs on bug bounty. That's when I came across the automation for Subdomain Takeovers by Hakluke. I then started using these techniques and refining them almost every day. After some time I found my first subdomain takeover and began the actual journey in bug bounty.

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 have a day job and still take time to enjoy bug bounty for learning and doing automation as a hobby. I usually spend a couple of hours a day on bug bounty while the rest of the time I spend with the family.

Now some technical questions... How do you approach a target? Do you follow a predefined methodology? And would you recommend testing few functionalities for all possible bugs, few bug classes across all endpoints, or anything else?

I sure follow a predefined methodology of enumeration via passive methods. First I try a few bug classes on all endpoints, afterwards I dig deeper into each endpoint to find more interesting things.

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

Recon surely plays a major role in my methodology. My methodology is usually to carry out basic recon. Then enumerating root domains and subdomains of the target, both vertical and horizontal. After all my enumeration I try discovering the endpoints using passive methods using wayback and gau. Then going

through the target manually by browsing the links and collecting interesting information about endpoints and functionalities.

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

I really enjoy subdomain takeovers and usually, look for wide-scope targets. As I said before, my journey in bug bounty started with subdomain takeovers after reading through Hakluke's methodology, so it surely holds a special place.

> **"My journey in bug bounty started with subdomain takeovers after reading through Hakluke's methodology."**

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?

My toolkit is usually a rough script that enumerates subdomains using various tools and methods. Post enumeration I use tools from various developers for subdomain takeover detection along with my custom scripts. My favorite tools are Findomain, Amass, Assetfinder along with gau, waybackurls, hakcrawler, and subjack.

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?

I feel automation is certainly helpful and kind of necessary. When you are new to the bug bounty game, you try doing things one step at a time and learn. After you've learned the basics and understand the workflow to discover specific bugs, you automatically tend to feel the need to automate as much as possible. I surely use automation while hunting and recommend everyone to do the same as well, however, you must create your own workflow for automation rather than blinding firing the scripts/methods of other researchers.

How many hours do you spend on bug hunting every week?

I spend at least 20 hours a week on bug hunting and learning about the topics.

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

Recon is the key, learn the process, practice, then try it and repeat.

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?

I like the old saying *"Rome wasn't built in a day".* I would like to tell the beginners to stay focused on learning and be patient when it comes to bug bounties. Do not view the success of other researchers and feel the need to achieve that in a short period of time. Learn, practice, and then analyze your position and take it slow.

> **"I like the old saying *"Rome wasn't built in a day".*"**

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

Nothing specific yet, I've only recently started.

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

@Hakluke to begin with, @Random_Robbie, @zseano, my hacker buddy and collaborator @hackingwhitehat, and to the complete #infosec community.

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

In my opinion, bug-bounty platforms have an important role in being a bridge between hackers and companies. It is really important for the triage teams to understand what the hackers are reporting before passing it to the companies. At Intigriti, I really enjoy the clear communication from the triagers. They will evaluate your report and take the right approach for both the hacker and the company. It is a great pleasure to work with them. They are knowledgeable, clear in communication, and creative (looking at the social media posts)

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

Thank you Intigriti for an amazing platform and your support towards the infosec community.