



Meet the hacker: p4fg, the Swedish master of Automation

BY INTIGRITI · JUNE 1, 2021 · LAST UPDATED ON MARCH 6, 2025

In our 'meet the hacker' series, we're taking the time to talk with Intigriti community members that have an impressive track record, an unusual methodology or have made valuable contributions to the community. This time, we're meeting up with Peter from Sweden, who goes by the handle p4fg, accompanied by his ninja-spongebob avatar.

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

Hi!

I'm Peter, 43 years old and one of the greybeards in the bug-bounty community. I'm married, have two children, and live in Sweden.

The first time I grasped the concept of bug bounties was during a presentation at the Swedish security conference "Security Fest" in Gothenburg, where Frans Rosén (@fransrosen) was presenting. It kind of got put on hold for a year or two after that, but it always remained in the back of my mind. Then I just went for it, and said: *"I will give this a year to see if I can make it"*.

The first few months were an eye-opener, this was a bit harder than I imagined. There are some, very early, reports that I'm not very proud of, but it's probably part of the learning curve!

I remember venting my frustration on Slack to my good friend STÖK (@stokfredrik) and he was super nice and just said: *"Call me"*. We had a nice long chat and I got my mind better aligned for what I needed to do next. The first year went by pretty fast and I just wanted to continue learning and hacking.

Live-hacking events are one of my biggest motivations. Getting to meet and discuss ideas with the world's top hackers is epic fun! Let us all hope the current pandemic dies down so that the live events can resume!

☰ ***"Then I just went for it, and said: "I will give this a year to see if I can make it"."***

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?

Bug bounties are currently the only thing I do. It fits in perfectly in my life, working when I want and as much (or as little) as I want/need.

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?

When I approach a single target, I first try to map out all the functionality and endpoints. What interesting things can be found? Also, I look for things that feel a bit off. I have previously worked as a software developer/architect for 20+ years and some things just *"smell"* bad. Those things are almost always interesting and rewarding.

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

Recon does play a part in my bug hunting but, manual recon is much more rewarding than automated recon. I started out writing a recon-engine that morphed into a pretty advanced automation framework which is in its third or fourth rewrite now.

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

I would not say that it is a favorite bug class (I am pretty tired of it) but I do report a lot of cross-site-scripting bugs.

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?

Most of my day-to-day work is done in or around Burp Suite.

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 do make heavy use of automation. I started building a recon-framework that morphed into an automation framework. It is mostly written in python with some node.js integrations.

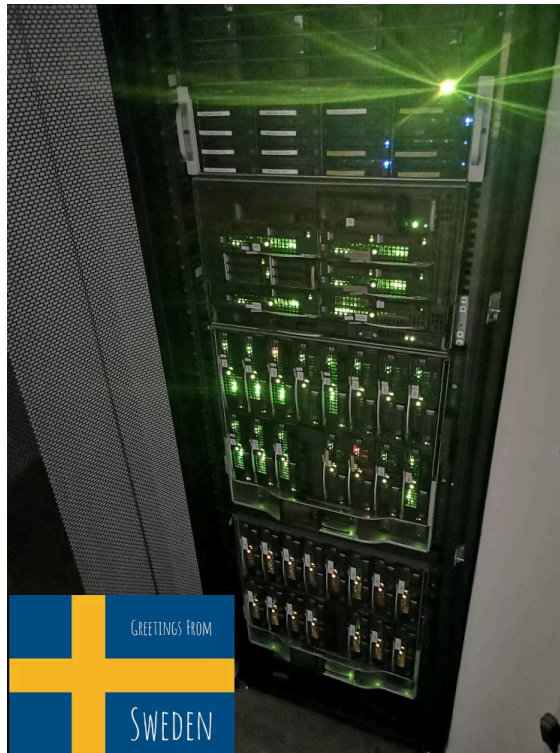
There is a twitter-quote that goes something like this:

☐ ***"if you use the same tools as everyone else, then you get the same results as everyone else!"***

I believe this to be very true, so I would encourage everyone to start building (or customizing) their own tools.

My automation framework is very much adapted to my workflow and is pretty resource-intensive. Running it in the cloud is way too expensive so the entire framework runs on blade servers that are self-hosted.

As an Intigriti-only exclusive, I have opened up the door to my server room to let the community take a sneak-peek on what is powering my automation. What you are looking at is about 40 HP blade-servers running 24/7, roaming around the internet looking for trouble.



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

I would say anything between 20 and 40 hours, depending on the targets.

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

POC || GTFO, if you cannot show a proof of concept with impact then do not send the report. Always strive to show business impact to the stakeholders:

- *WHY is this important?*
- *HOW can it hurt the business case?*

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?

For beginners, I would say: *Learn to code at least a little bit*. It will help you understand what is happening behind the scenes and will be even more important when you want to start finding more severe bugs. If you want to do anything else than basic automation it is one of the most important things to learn.

As for information overload, it is a hard one. Most things end up on Twitter, so that is probably one of my main information sources. The trick is to filter out what is important and what is not. I try to follow people with a high signal-to-noise ratio.

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

I'm currently building a swimming pool for the family, hope to get it done before the summer starts!

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

A big shout-out to STÖK ([@stokfredrik](#)) for giving me the motivation to continue in the very beginning when things were rough!

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

I do hunt on almost all major platforms, but Intigriti has more of a family feeling than the rest. Intigriti staff are always available on slack for questions and are always very helpful.

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

To anyone that is thinking about starting with bug bounties: *The best time to start is now.* Set a goal for just a few hours per week if you are new to this, but don't wait for more training or to read some more blog posts. The best education is getting your hands dirty out in the real world. Start with registering on Intigriti and check out what companies you can hack!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com