Bug Bounty Q&A #2: Isn't bug bounty only for large companies with large budgets?

BY INTIGRITI · APRIL 2, 2020 · LAST UPDATED ON MARCH 6, 2025

Bug Bounty for Business

intigriti ceo Stijn Jans answers your questions about ethical hacking and bug bounty

At intigriti, we love a good conversation. You can find us on Twitter, LinkedIn and Facebook. If the situation permits, we attend events and conferences. When the conversation turns to ethical hacking and bug bounty, some questions are commonly asked.

In this series of blog posts, we discuss these Frequently Asked Questions with our ceo Stijn Jans. Starting off, we discussed "What is ethical hacking and bug bounty?" Today's question is "Isn't bug bounty only for large companies with large budgets?". Next up, we'll be talking about "What effort does it take to set up a bug bounty program?"

If you have any questions you'd like to ask Stijn or anyone in the team, feel free to do so via hello@intigriti.com. We'll make sure every question gets answered, and if popular, we'll publish it here.

Question of The Week

Isn't bug bounty only for large companies with large budgets?

The question is legit. In the media, we read of big companies like Microsoft and Google enlisting the help of ethical hackers to test their systems and receive a reward (the bug bounty) when an issue is

found. This leads smaller companies to think that starting with bug bounty is not for them.

When we ask our ceo Stijn, his answer is clear. "The idea that ethical hacking to improve security is only for the happy few is outdated, it's no longer only for large companies with big budgets and ditto resources. Nowadays, we see companies of any size set up a customized bug bounty program. A little help and effort go a long way. "

Bug hunting: the profitable addition to classic security testing

Vulnerabilities in applications can be found in any company, regardless of size or business activity, and they can mean serious money: loss of revenue or an expensive hit on the stock exchange, a busted reputation and a lot of work to restore your business information systems. You even might get fined because you broke the law. Fortunately, there is a way to prevent this kind of expensive disaster.

Classic security testing versus. bug hunting

"These days, most companies already go through great lengths to assure the security of their applications and public environments like websites and apps", Stijn continues. "They do software security testing during development, set up software audits or arrange penetration testing and probably more. The company's management or the security department hires a professional who tests certain versions of the application to make sure that it is as secure as possible."

According to Jans, that is money well spent because it makes the application much safer, although it is not sufficient. "This approach, which we call 'classic' security testing, will miss out on a number of things. So, hoping to capture all the vulnerabilities using the classic testing methods will be to no avail; you won't find them."

> **"*"You cannot find all the vulnerabilities using classic testing methods."*"**

The explanation seems rather logical. Testing teams have limited resources and they always face pressure to speed up delivery and reduce cost. "Think about it this way: how much time can security testers spend on an application, before they must go on to the next project?"

Stijn knows from experience – after all, he used to run a pentesting company – that the security testers will check a number of times during development, have a pentest during pre-release, and then risk forgetting about it once it's in production. "Not an ideal approach, is it? Moreover, automated tools usually only see what their builders have taught them to see: well-known attack paths and vulnerabilities."

Results are key in bug hunting

Key to a bug bounty program is that you pay for the result. It is a 'nothing found, nothing paid' principle. As Stijn sees it: "Hunters spend their time looking for bugs, possibly in vain, but that's the risk they take." That's a very different story from how penetration test contractors earn their money. "Regardless of whether they find anything, you still have to pay them."

Bug bounty hunters keep looking, longer and continuously, depending on the scope and duration of the program. Time frame restrictions are limitations they don't like. Hunters do the work on their own time, regardless of the application's version. "Besides, these days, it's no longer possible for one person to

check all versions of all assets. That's why you need several hunters who all have their own specific expertise, interest and approach."

> *"Classic tools only see what their builders have taught them to see: well-known attack paths and vulnerabilities."*

The advantage of bug hunting is that it expands 'classic' secure development with many eyes, brains, and different approaches. Bug bounty programs unleash the imagination and intuition of a whole world of experts. These experts add creativity to the standard security approach. They have a very specific set of skills and knowledge that you would otherwise miss. There is always someone out there thinking of very elusive vulnerabilities. Bug hunting is the way to find that person.

"Some of the most interesting and severe vulnerabilities that are found, have nothing to do with technical expertise; they are based on thinking outside the box", says Stijn.

"Researchers can come up with ways to abuse an application based on unintended behaviour. A nice example is known as "Ticket Trick": a researcher was able to get inside the internal social media channels of a lot of organizations without actually hacking them. He only abused a logical flaw in their setup."

> *"Bug bounty hunters find the bugs other methods don't."*

Compared to the more 'classic' tools, bug bounty hunters are quite often an important source of information on more severe and unusual vulnerabilities. "Bug bounty hunters find the bugs other methods don't find", says Jans. "They go for the more exotic approach, the 'who would have thought of that?'- stuff."

Return on investment

The interesting thing about bug bounty programs is that their input can help to change or fine-tune classic security development approaches. Especially if it appears that the reported vulnerabilities could have been found with the available in-house resources. "A bug hunt report shows you a very specific problem, what it is and where it was found. You get information about real exploitable dangers. However, thanks to the bug bounty program you are warned and therefore able to prevent a serious attack."

So, does a bug bounty program render the classic secure development approach unnecessary? "Far from it, actually", Stijn explains, "but if you go about it in the right way, it provides a rich and solid return on investment."

Do you want to know more?

Our team is ready to answer all your questions about IT security testing, the intigriti platform, pricing or anything else. Click the button below and we'll get in touch.

Get in touch

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com