Computest
always on.

White paper **Security**

You should know thisbefore you set up a bug bounty programme

INTRO

They all do it: Apple, ABN AMRO, Tesla, Facebook, Google and Yahoo. They set up bug bounty programmes to track down vulnerabilities in their services using the knowledge of ethical hackers. If they find anything, the company pays the hacker a fee. Do you want to know if such a program is suitable for your company? Or do you want to know more about bug bounty programs as a supplement to your security policy? Then read on!

They all do it: Apple, ABN AMRO, Tesla, Facebook, Google and Yahoo. They set up bug bounty programmes to track down vulnerabilities in their services using the knowledge of ethical hackers. If they find anything, the company pays the hacker a fee.

It's an attractive win-win: the organisation's infrastructure becomes more secure and the hacker can earn good money, because the bigger the bug, the higher the reward. Confirmation that bug bounties are an attractive market for hackers came when Apple recently increased the maximum fee for finding significant iOS bugs to $1 million.

Apple, in turn, benefits from the expertise of a large network of ethical hackers, so helping it prevent possible security and reputational damage.

Bug bounties can indeed be an effective means of discovering weaknesses in your infrastructure. But they won't solve all your security problems. So in order to help you use a bug bounty programme effectively for your organisation, in this paper we answer the following questions:

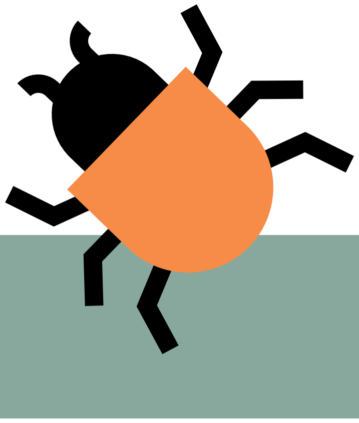


Table of contents

01 When is it a good idea to set up a bug bounty programme? page 3

02 What do you have to do before putting a bug bounty programme online? page 4

03 What should you expect if you are running a bug bounty programme, and what shouldn't you? page 5

01 When is it a good idea to set up a bug bounty programme?

We can answer this question briefly: it’s almost always a good idea to work with a bug bounty programme, provided you make sure the basic conditions are in place and you understand that it is an addition to the security efforts you are already making as an organisation.

Why bug bounties?

Because the development cycles of applications are much shorter nowadays and new releases come and go more quickly, it’s hard to always perform a security test before they go to production. The tests you perform are a snapshot, because a day later a new version may be online. In order to nevertheless maintain the focus on the security of your application in the time between different security tests, offering bug bounties can be an excellent idea.

Bug bounty as a cost-cutting measure

There are also organisations (usually smaller ones) that decide to get rid of their entire testing programmes for cost reasons and rely exclusively on bug bounty programmes for the security of their applications. However, they are forgetting an important aspect at the heart of the security tests they were previously performing: a security test is always based on a specific question. For example: can a user see paid content for free? Or, are the personal data of our users also visible to other people who log in?

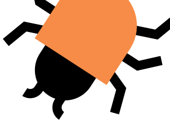
Following the execution of a security test, this question can be answered positively or negatively. This is a very different starting point than: “check to see if you can find any leaks in my application”. If you do not receive any notifications, you won’t have an answer to your security question. After all, you don’t know how many hackers have investigated your application, how thoroughly they have done so and how skilled they are. It is often forgotten that, in addition to offering bug bounties themselves, companies like Tesla and Facebook also employ hackers for security testing or hire them in. So the idea that by setting up a bug bounty programme you can stop performing security testing or outsourcing it to another company is therefore a misconception.

No confirmation that an application is secure

A notification from a hacker is also a completely different thing than a security test. You do not get a report containing validated results and the notifications you receive will be highly variable in quality. Moreover, what does the hacker do if he finds nothing and the application is secure? You will not get a report confirming this fact, simply because the hacker is not paid for positive notifications.

> “The idea that by setting up a bug bounty programme you can stop performing security testing or outsourcing it to another company is therefore a misconception.“
>
> Daan Keuper - Security Specialist at Computest

In short, if you decide to use a bug bounty programme, you should be aware that this programme should never stand alone, but should be part of your security policy.



02 Checklist

What do you have to do before putting a bug bounty programme online?

Putting a bug bounty programme online is not the hardest part. Make sure you have gone through the checklist below before launching a programme.

□ Your bug bounty programme is in fact an extension of your Responsible Disclosure policy. You offer a reward for what an ethical hacker reports via RD. So check whether your RD policy needs to be updated and whether or not the two are in line.

□ Check that you have the right expertise in-house to deal with the notifications you get from hackers. Simply setting up a programme and offering a reward is not sufficient. You will need to evaluate all the notifications you receive and provide a response.

□ Don't underestimate how much time it will take to manage the programme. It is usually agreed that an organisation will respond to a notification within 48 hours. Make sure you have resources available for this.

□ Identify and cover the risks – because you are actively inviting people to attack your applications. What will that mean for the performance of an application, for example?

□ Evaluate the arrangements you have in place with all your vendors, such as hosting parties and external software suppliers. Where does their responsibility begin and where does it end? And if a vulnerability with a particular classification is reported, how quickly should it be resolved?

□ Set the boundaries of what is to be investigated: establish which systems/vulnerabilities are excluded from bug bounty rewards.

□ Make sure you always have access to someone who can assess the business impact of the vulnerability. Some vulnerabilities can be mission-critical, but others may not need to be resolved immediately. Being able to consult security expertise quickly can give you peace of mind.

□ Define your limits: the rules set out in a responsible disclosure policy are not always read or scrupulously followed. What do you do if a hacker reports a vulnerability but also sends you your entire user database (which means he has downloaded it)?

□ Consider whether to post a document setting out the bug bounties policy on your site or register with an intermediary like HackerOne. This is a platform for hackers and organisations where firms can post bounty challenges and hackers can choose which ones they want to tackle.

□ Decide whether to post your responsible disclosure and bug bounty documents in Dutch or in English. If you post them in Dutch, your target group will be smaller but communication may well be smoother and faster. Also consider that €100 is quite a large sum in many low-wage countries. Hackers from those countries will be willing to engage in lengthy discussions with you to get hold of that reward for any notification they make (which you may consider unusable).

□ Decide on the amount of the reward you will pay for vulnerabilities. You can set up a classification system in which you link the impact of a vulnerability to the reward. HackerOne provides a guideline that assigns standard amounts to different vulnerabilities.

□ Decide whether the hacker's notification may be made public after the vulnerability is resolved. For the hacker, this is often a matter of pride and a recognition of his skills. It also demonstrates that your organisation is actively working to combat vulnerabilities and that you have an open attitude to hackers wanting to report a vulnerability.

03 What should you expect if you are running a bug bounty programme, and what shouldn't you?

Once your programme is up and running, you'll have to wait and see what hackers find and when and how they report that to you. Most organisations have high expectations of bug bounty programmes. In order to provide a realistic picture of what you should and shouldn't expect, you need to bear the following in mind:

> There is a lot of competition and the rewards vary. The chances that you'll find highly qualified hackers eager to test your applications for a €100 bounty are slim.

> " If you pay peanuts you get monkeys... "
>
> Daan Keuper - Security Specialist at Computest

> Be aware that the quality of the reports you receive can be disappointing. After all, you don't know the level of a hacker who has investigated your applications and how much time he or she has spent on them. This can mean that handling the notifications takes up a lot of your time. For instance, some hackers will send you the output of an automated tool and leave the assessment to you. There is a high probability that many of the notifications you receive will ultimately prove to be false positives.

> Be aware that there are also malicious hackers (so-called black hat hackers) whose intentions are not benign. Rather than reporting a vulnerability, they will be more inclined to exploit it. In that case, you have a problem.

> As mentioned previously, you cannot expect that simply by setting up a bug bounty programme, the security of your application will be monitored in a structured and thorough way. So be aware that security testing will also be required to evaluate the security of your applications.

More information?

If you have any questions after reading this white paper, please don't hesitate to contact the security specialists at Computest. E-mail us at **info@computest.nl** or call +31 (0)88 733 13 37.

We'll be happy to help!

Computest
always on.

info@computest.nl
+31(0)88 733 13 37
www.computest.nl

We are a team of passionate and experienced technical specialists who make sure your applications and infrastructure run at their best. We offer consultancy and training in integrated quality assurance, and provide performance, security and functional testing services. Whatever and everything we do for you is driven by our incessant need for quality, so we operate in small agile industry teams that work directly with you.