CASE STUDY

PUBLIC BUG BOUNTY PROGRAM

BLABLACAR

January 2020

BLABLACAR

What made you decide to get into Bug Bounty?

Alain Tiemblo, Web Security Lead Engineer, Blablacar.

We used to rely on "traditional" audits: vulnerability scans, penetration testing, code analysis, etc. which already allowed us to find a lot of things. Then, we started receiving messages from trolls on social networks, reporting potential vulnerabilities, without notice and without any details.
We also received some emails via customer support regarding vulnerabilities, without precise or exploitable information. These people wanted to be paid before telling more, but in the absence of any "proven" flaw, it was impossible for us to pay them.

These messages became more and more numerous, up to the point where we decided to take the Bug Bounty step, in order to channel this flow of noisy reports.

We compared different Bug Bounty platforms in Europe and **chose YesWeHack mainly for regulatory and data sovereignty reasons**. Another decision criteria was **the number of active hunters on the platform**: it doesn't make much sense to put money and energy into a Bug Bounty program if there isn't a sufficient number of hunters to effectively search for vulnerabilities.

Conversely, we integrated security.txt on our website to guide hunters to the YesWeHack platform, a Bug Bounty program being a good way to encourage Coordinated Vulnerabilities Disclosure.

Can you describe the evolution and progress of your program from the beginning?

Alain Tiemblo, Web Security Lead Engineer, Blablacar.

We launched our private program end of 2017, with an important running-in phase: when we opened, we first received many reports, then we gradually refined our program; we defined our scopes better, the type of vulnerabilities we wanted to see reported, etc.

From the beginning we received «real» and potential critical vulnerabilities, which convinced us of the relevance of the model and the effectiveness of the platform.

After a week, the number of reports started to decrease overall, but the ones that came up were more and more interesting, because the hunters "got into" our product and produced reports that were really specific to our business.

After a first month, it became more quiet, so we invited new hunters on the program to get new eyes and other skills on specific aspects of our program.
The private program also allowed our teams to learn how to managed reports, classify and qualify them, and adjust the program rules.

Seven months after the opening of the private program, we decided to switch to a public program. We were really satisfied with the quality of the interactions with the hunters during the private phase, and were therefore not worried about this transition... We just wanted more hunters on our program!

We also wished to send a strong message to the community: anyone who finds a flaw can bring it back to us! Of course, we received more reports after the switch to a public program, but it was totally manageable.

Antonin Le Faucheux, CISO, Blablacar.

Today, we are striving for quality reports on increasingly complex vulnerabilities that require more operating time for hunters, and more experienced hunter profiles.
In this context, we have notably increased the amount of our rewards for critical and high vulnerabilities. The challenge is, with the support of YesWeHack, to attract researchers who find great stuff without "exploding" our rewards budget.

What do you think are the added values of Bug Bounty compared to traditional solutions like pentest?

Antonin Le Faucheux – CISO – Blablacar.

For me, every tool has its uses. **The advantage of Bug Bounty is first of all crowdsourcing**: with an audit they have a couple consultants at your disposal, whereas with Bug Bounty, we potentially have hundreds or thousands of researchers working on our program.

BLABLACAR

Then there is continuity, 365/24/7, while a penetration testing usually takes place over a limited period of time and brings a "snapshot" at a specific moment. This continuity is critical to detect bugs as early as possible, as we update our applications very frequently.

Another key differentiator is that Bug Bounty implies an obligation of result (you pay only for what you get), while penetration testing only implies an obligation of means. This also helps to get security budgets internally: we can explain that we only pay people who find exploitable vulnerabilities, rather than pay auditors "to see" whether they will find something, without any obligation of results.

Bug Bounty is also a strong message to hackers. Many companies have long threatened to prosecute hackers who reported vulnerabilities. As a result, there is a kind of trauma among some bug hunters who find vulnerabilities and hesitate to contact the organizations concerned, for fear of being badly treated.

With our public program, we're sending this very strong message to the community: we want you to report flaws to us and for that, we give you a legal and secure framework, with a trusted third party between us to make sure everything goes well.

We want hunters to think : «I found a vulnerability on BlaBlaCar, I can be rewarded for this work legally and without taking any risks». Rather than some people ending up selling the vulnerabilities on the black market...

How do you handle bug reports internally?

Antonin Le Faucheux – CISO – Blablacar:

The security team is in charge of handling bug reports, provides a first qualification, in order to set the severity of the bug, whether it requires immediate attention or not. If the flaw is complex, we discuss about it with our team.

Once the vulnerability has been qualified internally, the dev team concerned is notified using a ticketing system provided by the YesWehack platform. This ticketing system allows us to monitor the progress of the teams in their patching process and to get back to them if needed.

We then move on to the step of checking the fix with the hunter. It's often a formality because we've usually checked ourselves, but it's always interesting to have an outside eye, and sometimes we have surprises: the hunter tells us that it's not correctly fixed!

Have you been able to observe any internal changes in your teams since you are on Bug Bounty?

Today, the security aspect is much more taken into account. In our internal training, we no longer talk about potential flaws, but we show concrete cases, flaws that have been brought to our attention as part of our program, which has a much greater impact.

How does Bug Bounty fit into your agile approach?

Bug Bounty is integrated into each team workflow via a ticketing system, the idea being that security breaches are tasks just like any other, which we assign to each team concerned with the right level of priority.

As we deliver continuously, the ability to extend our program scope in one click, and to detect things quickly on these new scopes also makes us more agile: as soon as an application is updated, we can have it tested, take the results into account, and easily set up a feedback loop.

What is the next step in your Bug Bounty strategy?

Next step is to continue to fine-tune our program to continuously improve the quality of our reports and attract better hunters.