

YES WE H/CK

 BlaBlaCar

BLABLACAR

Public Bug Bounty Program

CASE STUDY

WHY DID YOU DECIDE TO LAUNCH A BUG BOUNTY PROGRAM?

**ALAIN TIEMBLO, CHIEF WEB SECURITY ENGINEER,
BLABLACAR:**

We used to rely on 'traditional' audits, such as vulnerability scans, penetration testing, and code analysis, which exposed a lot of threats. Then, we began receiving messages from trolls on social networks, reporting potential vulnerabilities, without notice and without any detail.

We also received emails via customer support regarding vulnerabilities, with no precise or exploitable information. These people wanted payment before revealing more information, but in the absence of any 'proven' flaw, it was impossible for us to pay them.

The volume of these messages grew and grew, 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 reason for choosing YesWeHack 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, as Bug Bounty is a good way to encourage Coordinated Vulnerabilities Disclosure.



“ We chose YesWeHack mainly for regulatory and data sovereignty reasons. Another reason for choosing YesWeHack was the number of active hunters on the platform. ”

CAN YOU DESCRIBE THE EVOLUTION OF YOUR PROGRAM FROM THE BEGINNING?

ALAIN TIEMBLO:

We launched our private program in late 2017, with an important running-in phase. When we opened, we initially received many reports, then we gradually refined our program. For example, we defined our scopes more clearly, including the type of vulnerabilities we wanted to see reported.

From the outset, we received 'real' and potential critical vulnerabilities, which convinced us of the relevance of the model and the effectiveness of the platform.

After one week, the number of reports began to decrease, but the ones that came up were more and more interesting. This is because the hunters 'got into' our product and produced reports that were really specific to our business. After the first month, it became quieter, so we invited new hunters onto the program to introduce fresh eyes and other skills on specific aspects of our program.

The private program also allowed our teams to learn how to manage reports, classify and qualify them, and adjust the program rules.

Seven months after launching the private program, we switched to a public program. We were very 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 wanted 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 increased the value 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.





“After one week, the number of reports began to decrease, but the ones that came up were more and more interesting. This is because the hunters ‘got into’ our product and produced reports that were really specific to our business.”

WHAT VALUE DOES BUG BOUNTY OFFER COMPARED WITH TRADITIONAL CYBERSECURITY SOLUTIONS, SUCH AS PENETRATION TESTING?

ANTONIN LE FAUCHEUX:

The advantage of Bug Bounty is first of all crowdsourcing. With an audit, you only have a couple consultants at your disposal. With Bug Bounty, we potentially have hundreds or thousands of researchers working on our program.

Then there is 365/24/7 continuity, whereas a penetration test usually takes place over a limited period of time and only offers 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 us obtain security budgets internally: the rationale being 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 also sends a strong message to hackers. Many companies have long threatened to prosecute hackers who report 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 mistreated.

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

Ultimately, 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 MANAGE BUG REPORTS INTERNALLY?

ANTONIN LE FAUCHEUX:

The security team is in charge of handling bug reports. They provide an initial qualification, in order to set the severity of the bug, and determine whether it requires immediate attention or not. If the flaw is complex, we discuss it with our team.

Once the vulnerability has been qualified internally, the relevant dev team is notified using a ticketing system provided by the YesWeHack platform.

This ticketing system enables us to monitor the progress of the teams in their patching process and to respond to them if needed.

We then move on to check 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. We sometimes have surprises: the hunter might tell us it's not fixed correctly, for instance!

HAVE YOU OBSERVED ANY CHANGES TO YOUR TEAMS SINCE YOU BEGAN USING BUG BOUNTY?

ANTONIN LE FAUCHEUX:

The security aspect is much more important now. 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. This has a much greater impact.

“ 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 degree of priority.

HOW DOES BUG BOUNTY FIT INTO YOUR AGILE APPROACH?

ANTONIN LE FAUCHEUX:

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 degree 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'S NEXT?

ANTONIN LE FAUCHEUX:

We will fine-tune our program to continuously improve the quality of our reports and attract better hunters.

ABOUT

YES WE H/CK

Founded in 2013, YesWeHack is a Global Bug Bounty & VDP Platform.

YesWeHack offers companies an innovative approach to cybersecurity with Bug Bounty (pay-per-vulnerability discovered), connecting more than 23,000 cybersecurity experts (ethical hackers) across 170 countries with organizations to secure their exposed scopes and reporting vulnerabilities in their websites, mobile apps, infrastructure and connected devices.

YesWeHack runs private (invitation based only) programs and public programs for hundreds of organizations worldwide in compliance with the strictest European regulations.

In addition to the Bug Bounty platform, YesWeHack also offers: support in creating a Vulnerability Disclosure Policy (VDP), a learning platform for ethical hackers called Dojo and a training platform for educational institutions, YesWeHackEDU.

→ CONTACT US

→ VISIT OUR WEBSITE