openbugbounty

Non-Intrusive, Coordinated and Ethical Testing by the Community and for the Community

1,507,126 coordinated disclosures
1,208,992 fixed vulnerabilities

1,785 bug bounties with 3,602 websites
36,900 researchers, 1,588 honor badges

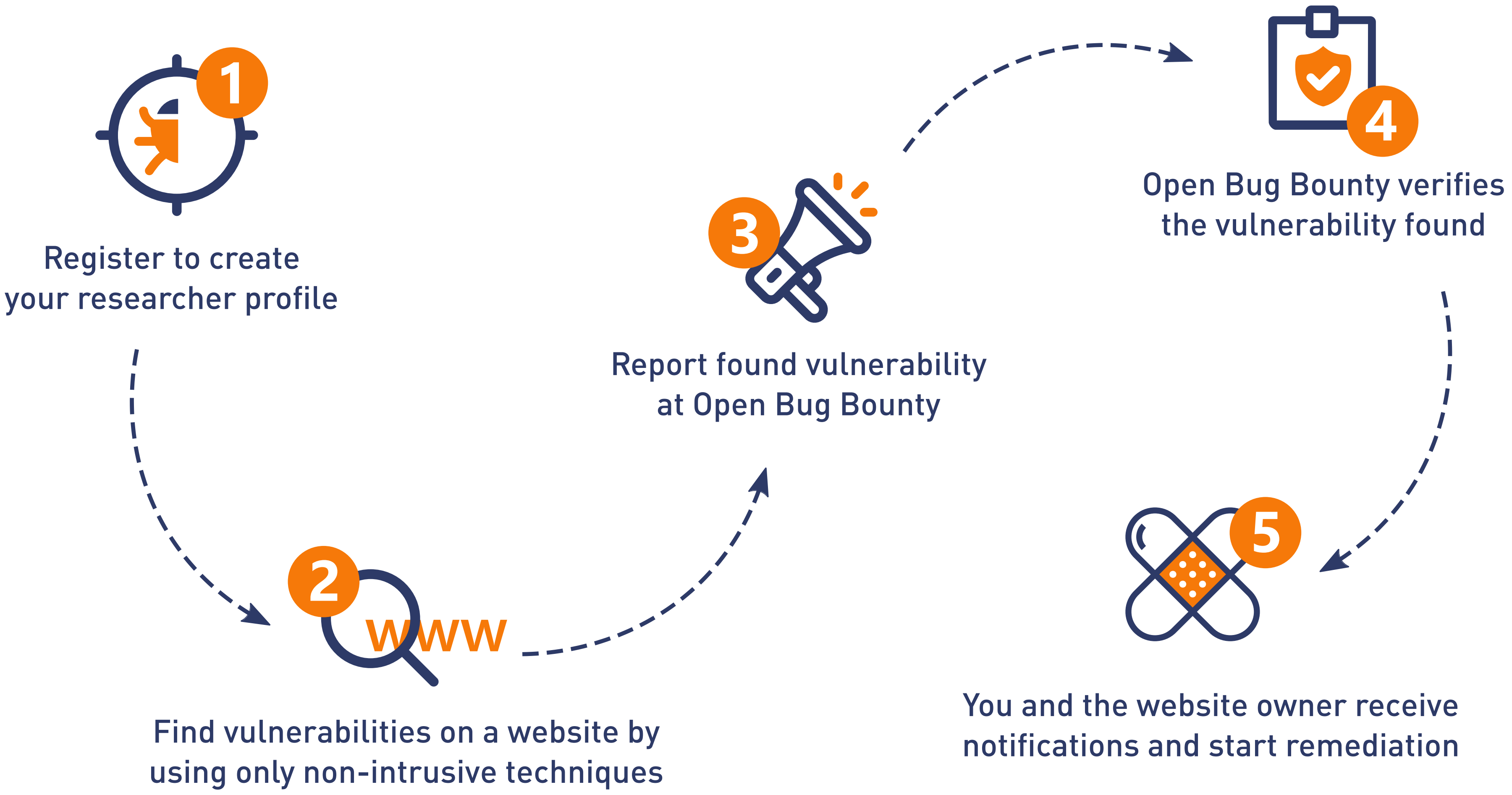
INFOSEC INSTITUTE

Open Bug Bounty named among the Top 6 Bug Bounty Programs in 2022

The Hacker News

Open Bug Bounty selected among the Top 5 Bug Bounty programs to watch by The Hacker News

Open Bug Bounty for Security Researchers



1 Register to create your researcher profile

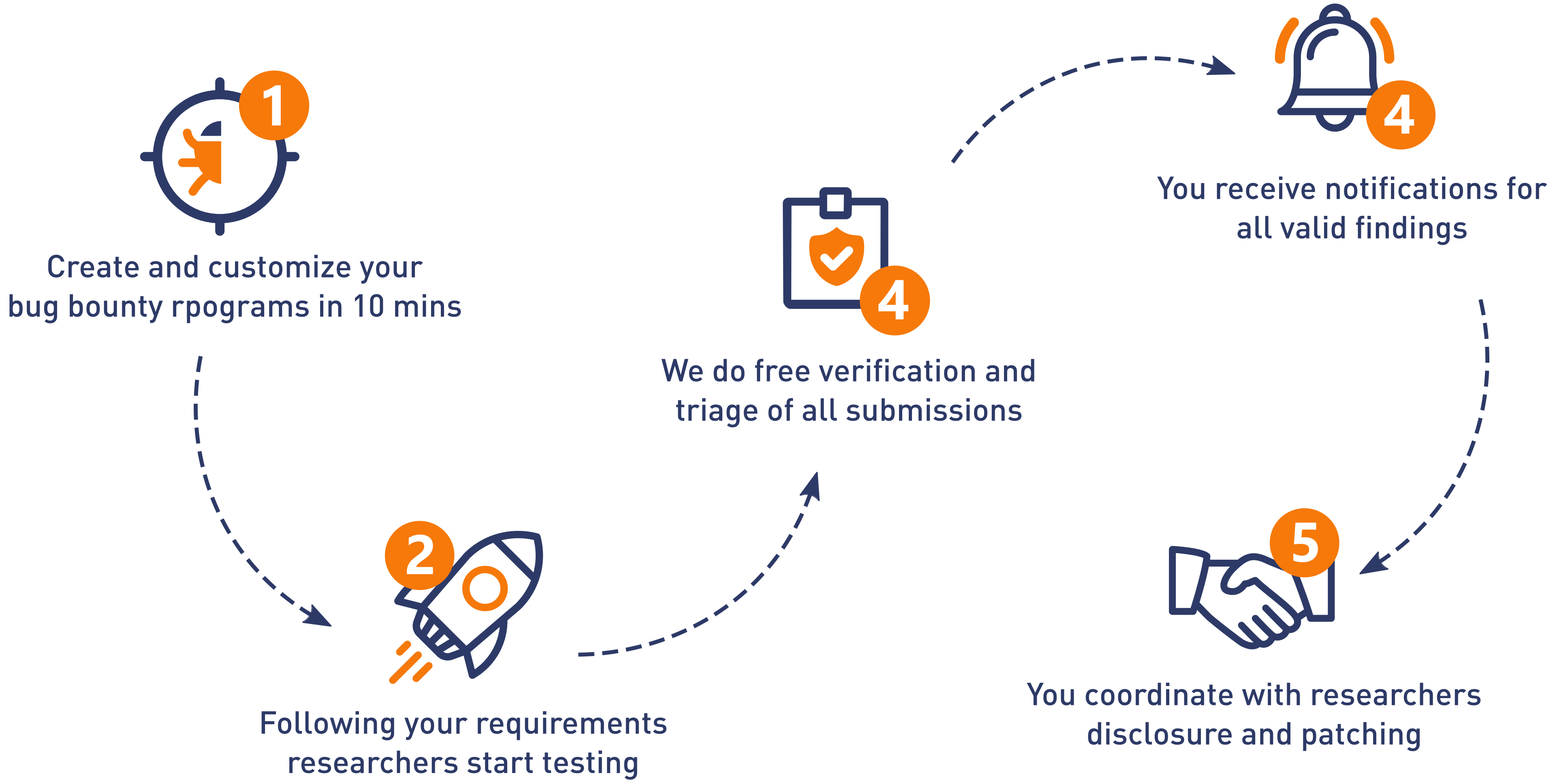
2 Find vulnerabilities on a website by using only non-intrusive techniques

3 Report found vulnerability at Open Bug Bounty

4 Open Bug Bounty verifies the vulnerability found

5 You and the website owner receive notifications and start remediation

Open Bug Bounty for Website Owners



Create and customize your
bug bounty rpograms in 10 mins

Following your requirements
researchers start testing

We do free verification and
triage of all submissions

You receive notifications for
all valid findings

You coordinate with researchers
disclosure and patching

Start Your Bug Bounty Program at Open Bug Bounty

Open Bug Bounty allows any verified website owners to run a bug bounty for their websites at no cost. The purpose of this non-profit activity is to make relations between website owners and security researchers sustainable and mutually beneficial in a long-term prospective.

Starting a bug bounty is free and open to everyone. Once logged, you can create your bug bounty program in a few minutes and get unlimited access to our security researchers. Once a vulnerability is reported, you will get instant notification to coordinate disclosure and remediation with researcher.

Open Bug Bounty does triage and verification of the submissions. However, we never intervene to the further process of your communication with the researchers, vulnerability remediation and disclosure. Once a vulnerability is verified and reported to you, our role in coordinated disclosure process is over.

For website owners, we provide vulnerability data export option to the following SDLC, DevOps and bug tracking systems:

Bugzilla

splunk>

Jira Software

mantis BUG TRACKER

About Open Bug Bounty

Open Bug Bounty's coordinated vulnerability disclosure platform allows any security researcher reporting a vulnerability on any website as long as the vulnerability is discovered without any intrusive testing techniques and is submitted following responsible disclosure guidelines.

The role of Open Bug Bounty is limited to independent verification of the submitted vulnerabilities and proper notification of website owners by all available means. Once notified, the website owner and the researcher are in direct contact to remediate the vulnerability and coordinate its disclosure.

At this and at any later stages, we never act as an intermediary between website owners and security researchers.

Coordinated and Responsible Disclosure, ISO 29147

Open Bug Bounty platform follows ISO 29147 standard's (“Information technology -- Security techniques -- Vulnerability disclosure”) guidelines of ethical and coordinated disclosure. As per the standard, Open Bug Bounty pursues the following goals of vulnerability disclosure:

- ✓ ensuring that identified vulnerabilities are addressed;
- ✓ minimizing the risk from vulnerabilities;
- ✓ providing sufficient information to evaluate risks from vulnerabilities to their systems;
- ✓ setting expectations to promote positive communication and coordination among involved parties.

As a global vulnerability disclosure Coordinator, Open Bug Bounty also serves the following non-profit roles as suggested by ISO 29147 in the vulnerability disclosure process:

- ✓ act as a trusted liaison between the involved parties (researchers and website owners);
- ✓ coordinate responsible disclosure;
- ✓ enable communication between the involved parties;
- ✓ provide a forum where experts from different organizations can collaborate.

Risk level of the submitted vulnerabilities is scored using Common Vulnerability Scoring System (CVSS).
Submitted vulnerabilities are classified by Common Weakness Enumeration (CWE).

Project History

Started by a group of independent security researchers in June 2014, Open Bug Bounty is a non-profit platform designed to connect security researchers and website owners in a transparent, respectful and mutually valuable manner. Our purpose is to make the Web a safer place for everyone’s benefit.

We have no financial or commercial interest in the project. Moreover, we pay hosting expenses and web development costs from our pocket, and spend our nights verifying new submissions.

openbugbounty

Started in 2014

Safe and Non-Intrusive Testing

We only accept Cross-Site Scripting, CSRF and some other vulnerabilities that figure among the most common web application vulnerabilities today. When reporting GDPR PII exposure, we do not store the PII but the blurred screenshot after verifying the vulnerability.

The proper process of testing for these vulnerabilities is harmless and cannot damage a website, database, server or related infrastructure. We do not accept vulnerabilities that can, or are intended to, harm a website, its data or related infrastructure.

Open Bug Bounty prohibits reporting of vulnerabilities that were detected by vulnerability scanners and other automated tools that may impact website performance or cause any other negative impact.

Bounties and Awards

A website owner can express a gratitude to a researcher for reporting vulnerability in a way s/he considers the most appropriate and proportional to the researcher's efforts and help.

We encourage website owners to say at least a “thank you” to the researcher or write a brief recommendation in the researcher’s profile. There is, however, absolutely no obligation or duty to express a gratitude in any manner. We promote positive, constructive and mutually respectful communications between website owners and security researchers.

On the platform, researchers get various honorary badges for quality of their submissions and the number of websites they helped to secure. We always encourage quality, not quantity of submissions.

Good Faith and Ethics

We have a zero tolerance policy for any unethical or unlawful activities. We always encourage the researchers to be respectful, responsive and polite, to provide website owners with all reasonable help and assistance.

If a researcher violates the enacted standards of ethics and good faith (e.g. demands something to delete a submission or refuses to share vulnerability details with the website owner), such submissions will be immediately deleted.

Researchers who violate the aforementioned rules and ethical guidelines may get suspended from the platform, up to a permanent ban. If you believe that a researcher violates the rules, please first talk to the researcher and try to resolve a possible misunderstanding. If the issue remains unresolved, please contact us.

Privacy and Security

We do not store, process or export any Personally Identifiable Information (PII) as defined in General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Connection to the website is available via HTTPS only.

Open Bug Bounty does not transfer any vulnerabilities, or vulnerability-related data, to any third-parties. For privacy reasons, we also keep no logs of any activities of website owners or security researchers.

GDPR

Terms and Conditions

Open Bug Bounty reserves the right to reject any Open Bug Bounty Program for any reason in its sole discretion.

Open Bug Bounty may terminate any Researcher's or Website Owner's access to and use of the Open Bug Bounty Platform, at Open Bug Bounty's sole discretion, at any time and without notice to the Researcher or Website Owner.

The site may contain links to third-party websites or resources. Open Bug Bounty provides these links only as a convenience and is not responsible for the content, products or services on or available from those websites or resources or links displayed on such websites. Researcher or Website Owner acknowledges sole responsibility for and assumes all risk arising from Researcher's or Website Owner's use of any third-party websites or resources.

FAQ for Security Researchers

Q: What kind of vulnerabilities can I report?

Currently, there are two different types of vulnerability reports that you can submit to the Open Bug Bounty project:

1. Vulnerabilities for a hosted bug bounty program in compliance with its specific guidelines available on the bug bounty page. Please note that some dangerous types of vulnerabilities (e.g. SQL injections or RCEs) must be sent directly to the bug bounty owner’s email available on the bug bounty page.

2. XSS and some other types of web application vulnerabilities for any websites if the vulnerabilities were detected by non-intrusive means as prescribed by our guidelines.

Q: How long does it take to verify a reported vulnerability?

We do our best to verify vulnerabilities as soon as possible, depending on the volume and other factors. However, being a non-profit project, we have limited resources and cannot provide instant verification. Usually, verification of XSS and some other uncomplicated vulnerabilities take up to 5 days. More sophisticated vulnerabilities, such as Improper Access Control, may take up to 10 days. We appreciate your patience.

FAQ for Security Researchers

Q: How do I get remunerated for reported vulnerabilities?

First, please note that, as a non-profit project, Open Bug Bounty does not pay any bounties and does not charge website owners anything for hosting their bug bounty programs and triage.

Second, for any hosted bug bounty program, the program owner shall pay security researcher directly for valid vulnerability reports made in compliance with the bug bounty guidelines available on its page. Not all bug bounty owners offer monetary payments as a remuneration, some may offer gifts or other signs of appreciation, please read bug bounty guidelines carefully.

Third, for all other vulnerability reports made in compliance with our by non-intrusive testing guidelines for website having no hosted bug bounty program, the website owners have absolutely no obligation to pay you. This is a volunteering work to make Internet a safer place, to help security researchers improving their application security testing skills, and to enhance researchers' CVs with recommendations and proven experience. To maximize the value you deliver to website owners by reporting vulnerabilities and thereby to maximize your chances to get an award, consider the following:

Do not report vulnerabilities on small, dysfunctional or abandoned websites that visibly do not care about their security.

Do offer your help in amicable and friendly manner to actually help fixing the vulnerability in polite and respectful manner.

Do not talk about remuneration before the vulnerability is actually fixed. After, you may politely ask whether the website owner wishes to give you a recommendation on your researcher's profile or express any other form of appreciation of your efforts. The less pushy and more collaborative you are, the higher your chances are to get a better reward. If you are looking for certainty of remuneration, then focus on hosted bug bounty programs.

FAQ for Security Researchers

Q: What if a hosted bug bounty owner does not pay me?

If after submitting a valid vulnerability report in compliance with a hosted bug bounty program guidelines, its owner refuses to pay you in accordance with the guidelines, please send us all the details for review. Do not send confidential or personal information. If the bug bounty owner refuses to pay you in bad faith and in violation of its own remuneration guidelines, its bug bounty program may be permanently suspended.

Q: What can I do if my vulnerability report is rejected?

Please attentively review our vulnerability submission guidelines. As per our statistics, 99.9% of rejected vulnerabilities either belong to a class of vulnerabilities that we do not accept (e.g. SQL injections or misconfigured HTTP headers) or cannot be easily reproduced. Being a non-profit project, we cannot spend our hours reading multi-page reports and trying to reproduce the vulnerability. If you are certain and confident that the submitted vulnerability is in full compliance with the guidelines, please contact us, we usually try to reply within one week.

Q: Where can I get help if I have other questions?

First, please carefully read about the Open Bug Bounty Project and then search our forum: most questions have been already answered there. If your question is general and does not contain any confidential or personal information, please always use our forum to ask it, so other users can also answer or get answers to their future questions. If after carefully reviewing the forum you still cannot get the answer, please contact us, we usually try to reply within one week.

FAQ for Website Owners

Q: What can I do after receiving a report about vulnerability affecting my website?

Please reach out to the researcher and ask for the vulnerability details so you can patch it. Importantly, make sure that the vulnerability notification was sent from **@openbugbounty.org** email address: all other domains have no affiliation with the Open Bug Bounty project, you can ignore any emails coming from them.

Q: What can I do if I cannot contact a researcher who reported a vulnerability?

All researchers are required to have a twitter account and their email available on their profile. If the after several attempts to contact the researcher, you hear nothing, please contact us and we will try to resolve the situation as soon as possible.

FAQ for Website Owners

Q: Am I required to pay anything to a researcher who reported a vulnerability?

You are not required to pay anything, however, if the researcher helped fixing the vulnerability, you can always write a short recommendation to his or her profile to demonstrate your appreciation of the time and efforts. If the researcher's report and subsequent help were valuable for your organization, you may also consider making a token gift, such as t-shirt, Amazon gift card or a small payment via PayPal.

Q: Can researchers demand a payment in exchange for vulnerability details?

No, researchers must not demand anything in exchange for vulnerability details, this a direct violation of our guidelines on ethics and may lead to permanent suspension of the researcher's account. Please always contact us to report any violations of the guidelines, and we will try to resolve the situation as soon as possible.

FAQ for Bug Bounty Owners

Q: What kind of hosted bug bounty programs do you offer?

We offer managed bug bounty programs for individual website owners, companies and organizations. We also do vulnerability triage for XSS and some other types of vulnerabilities, so you will get only verified and valid findings. For dangerous types of vulnerabilities (e.g. SQL injections or RCEs) you are required to provide your own contact details, so researchers can send you their reports directly. For confidentiality reasons, we do not store or process such reports.

Q: How much does it cost to host a bug bounty program?

The Open Bug Bounty is a non-profit project aimed at making Internet a safer place. Therefore, all bug bounty programs and related triage activities (please see above) are provided at no cost. We never charge any fees.

Q: What are the requirements to setup a bug bounty program?

Please login to the Platform with your email and then create your bug bounty program by carefully filling out all the fields (please see below).

FAQ for Bug Bounty Owners

Q: How can I get more vulnerability reports of better quality?

To motivate skilled security researchers to submit high-quality vulnerabilities that you are interested in, consider adding the following to your bug bounty description:

- As detailed and specific information as possible about the permitted scope of testing and accepted types of vulnerabilities.
- Clear and precise information on the remuneration for all types of findings that you wish to remunerate.
- Reliable contact information so researchers can reach out to you in case of any questions.

Q: What is the suggested remuneration for vulnerabilities?

While some of the hosted bug bounties merely offer small gifts, such as Amazon gift cards, the best way to attract talented researchers to your bug bounty program is to offer monetary payment for valid vulnerabilities. While Google may offer up to $7,500 for an XSS vulnerability, you are certainly not required to pay the same amount. For example, an average payment for a valid XSS may be between $30 and $150. The most important thing to consider is, however, how you treat the researcher: respectful and prompt reply with a modest remuneration is oftentimes preferred to a long and impolite communication followed with a bigger payment.

They Thank Our Researchers

IKEA®

Berkeley
UNIVERSITY OF CALIFORNIA

ebay

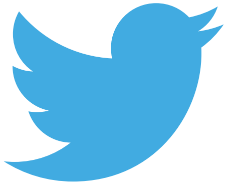
PHILIPS

verizon✓

Virgin

Canon

DELL



YAMAHA

Open Bug Bounty Programs

NASA

BANCO CENTRAL DO BRASIL

WHEELY

GoDaddy™

BRITISH LIBRARY

cc creative commons

GUCCI

WKU®

BRESSER®
GROUP OF COMPANIES

www.openbugbounty.org

openbugbounty