openbugbounty

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

873,874 coordinated disclosures
497,122 fixed vulnerabilities

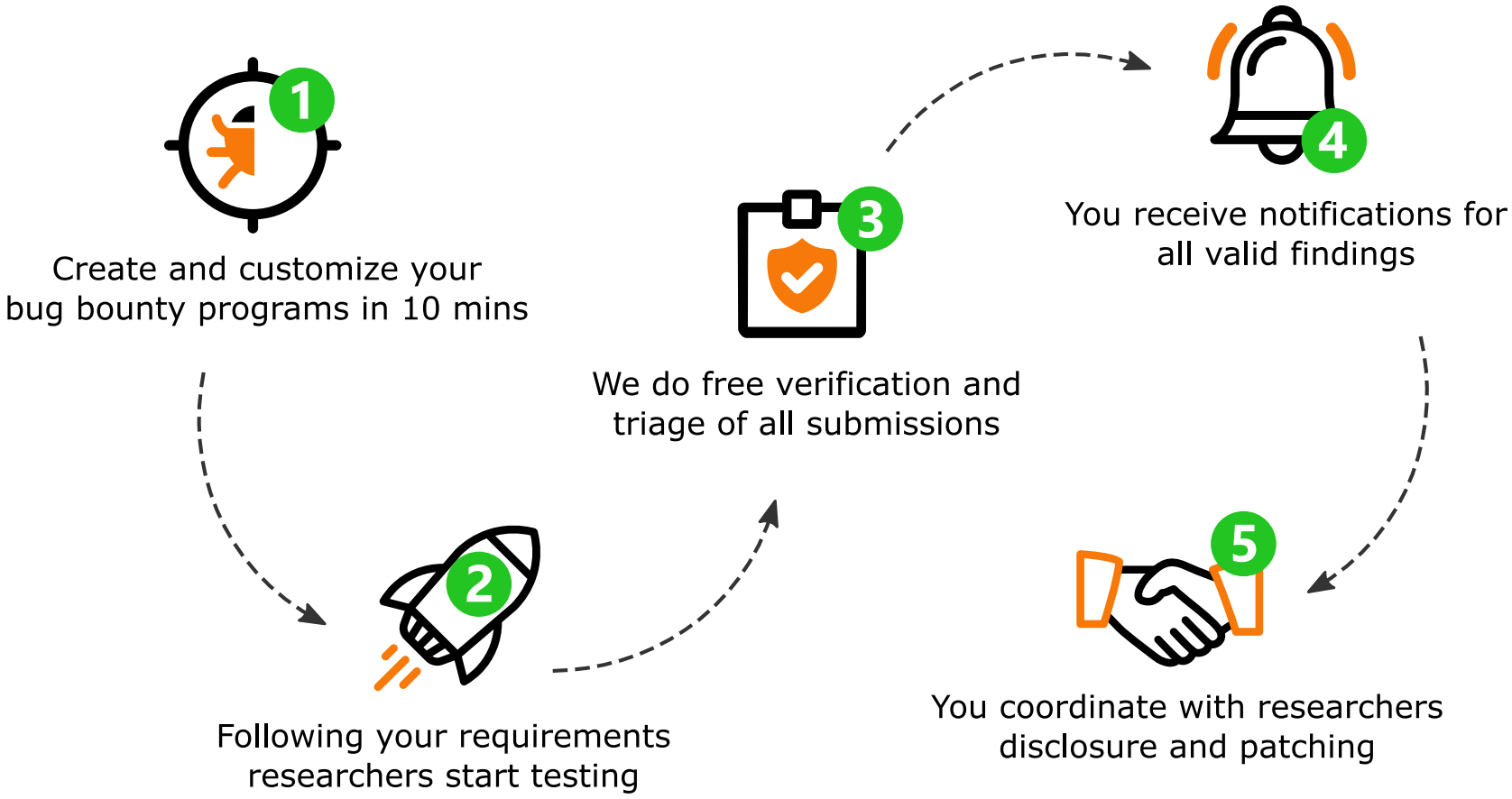
1289 bug bounties with 2,471 websites
21,953 researchers, 1287 honor badges

The Hacker News

Open Bug Bounty selected among the Top 5 Bug Bounty programs to watch in 2021 by The Hacker News

Open Bug Bounty for Security Researchers

Open Bug Bounty for Website Owners



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 in via Twitter, 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:

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.

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).

To avoid storing any user-related data, we use external authentication via Twitter for everyone on the website. 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

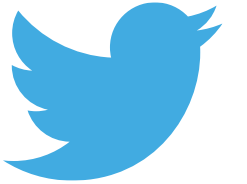
Terms and Conditions

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.

Awards Our Researchers Get



www.openbugbounty.org