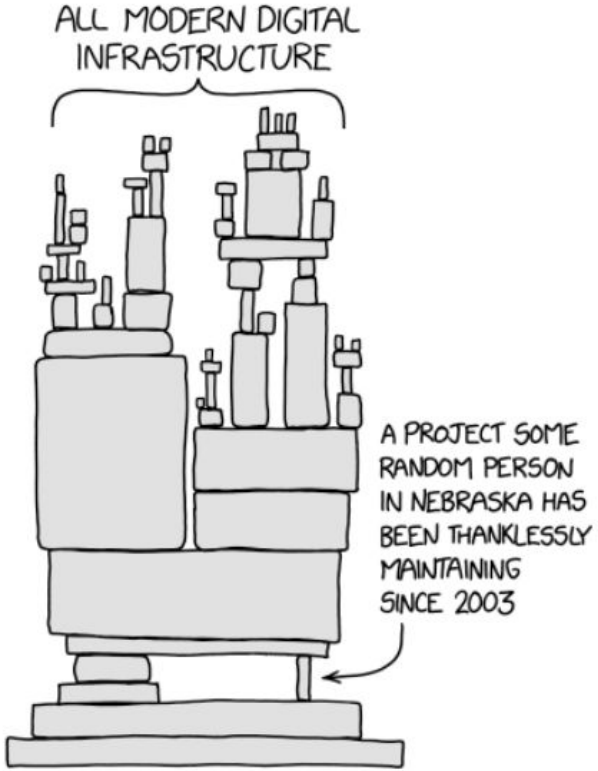
hackerone

Internet Bug Bounty

Pool our resources to strengthen key software dependencies

IBB
INTERNET BUG BOUNTY



Why We Care

All modern digital infrastructure today is powered by a software supply chain consisting largely of Open Source Software (OSS). This isn't just the core elements (programming languages, web servers, databases, operating systems) but hundreds of thousands of products and libraries that are used in mission-critical roles in digital systems.

The best way to defend against the threats facing software is to work together to protect the key dependencies everyone depends upon.

- OSS represents a growing portion of the world's critical attack surface.
- Vulnerability disclosure to OSS maintainers is too often delayed due to lack of clarity on visibility, process, and incentives. Window of vulnerable extends unnecessarily.
- Just as OSS is enhanced through the community, OSS should be secured by the community, and bug bounty programs can help facilitate that joint effort.
- Maintainers of OSS are often woefully underfunded and part-time, yet under pressure to drop all work to fix security bugs.

Internet Bug Bounty

Numerous companies run successful bug bounty programs, paying out millions to improve their security... but who runs and funds bug bounties for open source, community-based software that all of us use? We do!

- The Internet Bug Bounty was launched November 6, 2013, as a joint effort between Facebook, Microsoft, and HackerOne
- The program was initially run by a panel of security professionals from Microsoft, Google, Facebook, iSEC Partners, and Etsy
- IBB was founded to offer rewards for reporting hacks and exploits for a broad range of Internet-related software, such as: Adobe Flash, Python, Ruby, PHP, Django, Ruby on Rails, Perl, OpenSSL, Nginx, Apache HTTP Server, and Phabricator

Successes

$780,000+
in bounties

900+
flaws remediated

230+
unique finders

IBB 2.0

Addressing several areas for improvement in the existing program

Areas for Improvement	IBB 1.0	IBB 2.0
Sustainability	Annual $100k commitments from a small number of supporting organizations is not sustainable or equitable. Program administered by volunteers.	Lightweight scalable funding model that spreads the responsibility among everyone dependent on OSS. Dedicated program director from HackerOne.
Incentives	Perverse incentives continue to exist. Rational finders often delay disclosure as they contact individual companies in an ad hoc manner in order to increase overall bounties received.	Ensures that zero day vulnerabilities are received by the maintainers for remediation without undue delay. Bounty amounts are attractive relative to the total risk such vulnerabilities represent.
Maintainer Support	Maintainers not supported and struggle to keep up with discovered vulnerabilities.	Sustains remediation efforts with a portion of the funding going to the project.

IBB 2.0: Updated Operating Model

Proposed Base Operating Model

1. OSS projects and Partners opt in
2. Partners donate a % of their normal bounty amount per severity toward each eligible vulnerability submitted to the project
3. Sum of all donations for each vuln is awarded
    a. 80% to the finder
    b. 20% to the project
    c. HackerOne deducts from partner's existing bounty budget automatically
4. Monthly report published, including basic details of resolved vulnerabilities and thanking all partners, finders, & projects

Example Funding Structure (per vulnerability)		
	Typical Bounty Table	**10% IBB Contribution (pooled with other partner)**
Critical	$5,000	$500
High	$1,500	$150
Medium	$500	$50
Low	$150	$15

Together We OSS Harder

The power of this scalable model is that it enables collective funding of both finders and projects. Meaningful boost to open source security.

Example Bounties							
Project	**CVE**	**Sev**	**# of Partners**	**Average individual partner cost**	**Amount to Finder**	**Amount to Project**	**Total Bounty**
OpenSSL	2020-0001	Critical	50	$500	$20,000	$5,000	**$25,000**
OpenSSL	2020-0002	Low	50	$15	$600	$150	**$750**
Rails	2020-0003	Critical	10	$500	$4,000	$1,000	**$5,000**
libfoobar	2020-0004	High	5	$150	$600	$150	**$750**

How It Works

Internet Bug Bounty

1

Vulnerability Discovered in Project

2

Disclosed to Maintainer

3

Security Advisory Published by Project CVE-2020-0001

4

Finder submits claim to IBB

5

Finder Rewarded $20k
Project Rewarded $5k

6

Partner bounty pool deducted (50 x $500)

IBB 2.0: Finder Improvements

Helping increase the supply of vulnerability research

Problem	Improvement
Submit to many individual bug bounty programs (BBPs) and hope for a payout. Payout amounts and timing vary.	Submit once; get paid fast, fair, and consistently.
Recon across wide range of BBPs to find vulnerable assets and hope policy allows such third-party submissions.	Submit to one BBP.
Manage conversations with multiple BBPs and contacts, including possibly having to do extra work to prove issue exists in individual program assets.	One report. One point of contact.
Risk that the unique find will be stolen by somebody at an individual BBP and used to gain bounties elsewhere (has happened multiple times).	Submit once. Vulnerability goes to the maintainer and is not exploited by others.

Projects

Phase 1 (Pilot)

What we're looking for...

- **OSS projects that opt in should:**
  - Have a security policy governing receipt of vulnerability reports (e.g., SECURITY.md)
  - Establish a commitment to be responsive to incoming vulnerability reports (e.g., 10 days)
  - Have a process to assign CVEs and/or issue security advisories for valid vulnerabilities reports
  - Have a process to assign severity to vulnerabilities (e.g., CVSS)
  - Provide instructions for donation of 20% bounty split
  - Undergo a good faith 6 month commitment to the pilot

Project FAQ

- **Will we need to adjust our vulnerability submission workflow?**
    - We believe we had designed this model to be compatible with your existing workflows, so nothing should need to change. Please let us know if that is not the case.
- **Can we expect volume to increase?**
    - It is our hope that a successful pilot does result in an increase in the number of remediated vulnerabilities and a more secure project. In our estimations, we would prepare for a 20-50% increase in volume.
- **How will we receive vulnerability reports?**
    - Vulnerabilities will be submitted directly to you by the finder as part of your defined workflow. IBB will not have access to the vulnerability until you have publicly disclosed it as part of a security advisory.
- **What results can we hope to see from the pilot?**
    - We'll provide public monthly reporting of vulnerabilities (including CVEs) and associated payouts, including mentions of all partners.
- **What if our project does not have a way, or does not wish to receive donations?**
    - The funds will be provided to The Open Source Security Foundation in support of their work towards vulnerability disclosures.

Partners

Phase 1 (Pilot)

What we're looking for...

- **10 launch partners (existing HackerOne customers)**
  - Select 25+ OSS projects you want to fund
  - 6 month commitment to the pilot
  - Funds drawn from your existing HackerOne bounty pool
- **Top 10 OSS projects from launch partners will be selected**
  - Projects must meet eligibility criteria
  - Projects must opt-in
- ~~**Commitment that launch partners don't pay bounties for in-scope OSS projects**~~

Pilot Success Criteria

What does success look like to you?

- **In-scope projects become more secure**
- **Increase in vulnerability discovery rates for the in-scope projects**
- **Stable response & remediation times from projects**
- **Positive survey feedback from: partners, projects, and hackers**
- <How would your organization like to quantify success for this pilot?>

Partner FAQ

- **What if I am spending too much?**
  - You may adjust the percentage of your contribution for future bounties.
- **When do I receive security advisories?**
  - You'll notice that as soon as a vulnerability has been accepted and triaged, the bounty will be paid. The full details of the vulnerability will be released according to the upstream project's disclosure policy.
- **Can I sponsor bounties in commercial third-party software? (e.g., SolarWinds)**
  - We believe the model can be applied to commercial software as well, and we plan to pursue this as the top priority for phase 2.
- **What results can we hope to see from the pilot?**
  - We'll provide public monthly reporting of vulnerabilities (including CVEs) and associated payouts, which mention of all the customers who sponsored.
- **How will we react if we find a project has intentionally introduced a vulnerability in order to receive a payment (either as a finder or project)?**
  - We are not aware of any instances occurring across tens of millions of rewards across the industry. If we discover this is happening, the project's sponsorship will be revoked.
- **What if a project does not have a way to receive donations?**
  - The funds will be provided to The Open Source Security Foundation in support of their work towards vulnerability disclosures.

Join us!

Together, we can improve the security of some of the most important open source software that supports the Internet we all depend on, by promoting and rewarding security research.

Interested? Get in touch to get started!

Kayla Underkoffler
kunderkoffler@hackerone.com