Whitepaper

BUG BOUNTY PROGRAM GETTING STARTED CHECKLIST

JUNE, 14TH 2019
INTESAR SHANNAN MOHAMMED
CTO
FX LABS, INC

FX Labs Inc - API Cybersecurity Company
https://fxlabs.io/

Abstract

This whitepaper aims to help organizations understand bug bounty programs and provides an easy checklist to get started.

Audience

CEO, CTO, CISO, Directory of Security, CTO, VP of Engineering, Director of Engineering, etc.

Applicable Assets

Web Applications, APIs, SaaS, IOT, Mobile Apps, etc.

What is covered in this whitepaper?

1. What is a bug bounty program
2. Difference between a private and public program
3. Getting started checklist

What is a Bug Bounty Program

A bug bounty program offers rewards as a financial payout, online credits, recognition, or brand merchandise to individuals or groups who report back security and non-security issues to the organization. These programs allow organizations to identify and resolve problems early on before they become widespread and disruptive.

What is a Private Bug Bounty Program

Some of the large organizations have been offering their own initiatives. These programs make a lot of sense if you are a financial institution, or have compliance to follow or you like real users and customers of your products to report issues directly back to you. Some of the payouts in this category were jaw-dropping and was in the range of $1M - $5M.

Company	Program	Bug Types	Payouts
Google	https://www.google.com/about/appsecurity/reward-program/	Cross-site scripting, Cross-site request forgery, Mixed-content scripts, Authentication or authorization flaws, Server-side code execution bugs.	$3.4M in 2018[1] or $7,500 - $31,000 per bug.
Microsoft	https://www.microsoft.com/en-us/msrc/bounty		$2M in 2018[2] or $15,000 - $100,000 per bug.
Intel	https://www.intel.com/content/www/us/en/security-center/bug-bounty-program.html		$500 - $100,000 per bug.

[1] "7 Huge Bug Bounty Payouts - PCMag India." 15 May. 2019, https://in.pcmag.com/gallery/130389/7-huge-bug-bounty-payouts. Accessed 12 Jun. 2019.
[2] "7 Huge Bug Bounty Payouts - PCMag India." 15 May. 2019, https://in.pcmag.com/gallery/130389/7-huge-bug-bounty-payouts. Accessed 12 Jun. 2019.

Verizon			$5M in 2018[3]

What is a Public or Crowdsourced Bug Bounty Program

Offers an easy way to get started. The recommendation is to offer more than averages in bounty to attract top bounty hunters/researchers.

Name	Positioned	Industries	Avg Payouts
Hackerone[4]	Web, Mobile, API	Technology[5]	$800 / Level-1[6] or $5,000 / Level-5[7]
Bugcrowd[8]	Web, Mobile, API	Technology[9]	N/A
Cobalt[10]	Web Pen Testing	Financial[11]	N/A
Synack[12]	Pen Testing	Government[13]	N/A

[3] "7 Huge Bug Bounty Payouts - PCMag India." 15 May. 2019, https://in.pcmag.com/gallery/130389/7-huge-bug-bounty-payouts. Accessed 12 Jun. 2019.
[4] "HackerOne." Accessed June 12, 2019. https://www.hackerone.com/.
[5] "Bug Bounty Customers - Cyber Attack Case Studies | HackerOne." Accessed June 12, 2019. https://www.hackerone.com/customers.
[6] "Bug Bounty Basics - Essential Guide & Tips | HackerOne." https://www.hackerone.com/resources/bug-bounty-basics. Accessed 16 Jun. 2019.
[7] "Bug Bounty Basics - Essential Guide & Tips | HackerOne." https://www.hackerone.com/resources/bug-bounty-basics. Accessed 16 Jun. 2019.
[8] "Bugcrowd." Accessed June 12, 2019. https://www.bugcrowd.com/.
[9] "Customers | Bugcrowd." Accessed June 12, 2019. https://www.bugcrowd.com/customers/.
[10] "Cobalt.io." Accessed June 12, 2019. https://cobalt.io/.
[11] "Customers and their success stories | Cobalt - Cobalt.io." Accessed June 12, 2019. https://cobalt.io/customers.
[12] "Synack." Accessed June 12, 2019. https://www.synack.com/.
[13] "Crowdsourced Security Trusted by Government Agencies - Synack." Accessed June 12, 2019. https://www.synack.com/government/.

Top Reported Vulnerabilities in a Bug Bounty Program

What can you expect out of these programs? Do these reported issues align with your goals? The following are the most commonly reported issues as per this report[14].

1. **Cross-site Scripting (XSS[15]):**
   Most widely reported vulnerability, over **30%** of reported vulnerabilities are XSS.

2. **Improper Authentication:**
   Missing authentication on a web or API endpoint can lead to direct access of the resource without providing valid credentials or tokens. More than **20%** reported vulnerabilities comes from this category.

3. **Sensitive Information Disclosure:**
   It constitutes **25%** reported vulnerabilities. Personally, identifiable data can reveal as part of the product or service reviews, etc.

4. **Privilege Escalation:**
   It constitutes less than **5%** of the reported vulnerabilities. This issue can happen in two ways. Either because of the missing roles on the endpoints or the user's ability to self escalate privileges.

5. **SQL Injection:**
   It constitutes less than **3%** of the reported vulnerabilities. Can be most disruptive.

6. **Code Injection:**
   It constitutes less than **2%** of the reported vulnerabilities. Possible if you've infrastructure products or dynamic language stack in your backend code.

7. **Insecure Direct Object Reference:**
   It constitutes less than **2%** of the reported vulnerabilities. But represents the Top #1 most exploited (Not reported but actual exploited) vulnerability. Extremely hard to detect and it can easily get sneaked into the code, as new features get added.

8. **Improper Access-Controls:**
   It constitutes less than **2%** of the reported vulnerabilities. Very similar to Insecure Direct Object Reference.

---

[14] "HackerOne Reveals Which Security Bugs Are Making Its ... - Gizmodo." 11 Jun. 2019, https://gizmodo.com/hackerone-reveals-which-security-bugs-are-making-its-ar-1835413571. Accessed 13 Jun. 2019.
[15] "Cross-site Scripting (XSS) - OWASP." Accessed June 12, 2019. https://www.owasp.org/index.php/Cross-site_Scripting_(XSS).

When to choose a Private Program vs a Public Program?

1. If you have typical web applications then crowdsourcing platforms can be a better fit. But if you're a technology company like in networking, infra, storage, etc. then your pro customer base is more qualified to find more critical issues if rewarded properly.
2. SaaS or B2C products are better suited for global bug hunters compare to on-premises or B2B products.

Top challenges with starting a bug bounty programs

1. Cost

You may need at the least $1,000 per bug to start one. A small budget may not attract the right crowd, and most startups can't afford these rates. If your product is not ready then no budget is big enough and you can quickly run out funds for just minor issues.

2. Dedicated Program Manager

A dedicated manager or an engineer is required to create engagement rules, provide sandbox environments, answers questions, monitor, triage, respond, and manage the program. In fact, the medium time to receiving a vulnerability report from on HackerOne is less than 9 hours. This means you can expect to get busy from day-1. Also, the average time to triage, assign priority, criticality and respond to these reports ranges from 1-2 days. If your product is not ready it will simply add large volumes of reports that you need to process in a quick time. Note: this effort may add an additional cost and may tie up one or more of your resources based on your application size and readiness.

3. Engineering Bandwidth:

As vulnerabilities get reported, you can't merely store it into your issue-tracker, you need to fix them as early as possible. This activity requires

- Engineering bandwidth, dedicated and focused team to resolve issues as soon as possible.
- Skills, developers with the right skills to resolve the issues.

4. Release Cycles

You also need to consider your product release cycles. How often do you release patches and newer versions, do you offer on-premises, saas, and managed instances? Fixing issues is not going to be enough if you can't ship it. And if you can't ship fast, these issues will be re-reported by other members and may cost you additionally.

- **SaaS** release cycles are straight forward, and you can release when you're ready
- **Managed Instances**: If you offer this, then you'll have to work with individual customers to find the window to run the updates.
- **On-premises** applying timely patches can be tricky you can't release frequent security updates, your customers won't be able to catch up unless you have the auto updates enabled. And your customers run into the risk of getting breached.

Getting Started Checklist or Prerequisites

#	Item	Comments
1	Manual Testing	Make sure you've done some testing. Otherwise, the reported bugs volume can overwhelm you.
2	Automation Testing	It is critical, so you don't regress and end up paying for the same thing again and again.
3	Vulnerability Scanners	Can easily detect a wide array of issues early on and allow you to fix and release them at your pace.
4	Pen Testing	Can be lengthy and most done just before the release.
5	DevSecOps	Make sure you run automated scans as you build and ship new software.
6	Skills	Train engineering on security best practices and top 10 vulnerabilities best practices. Otherwise, simple fixes can end up taking 10x time.
7	Budget	You need to identify a yearly $100K - $200K budget for this even if you're just getting started.
8	Resource Allocation	Identify engineering resource who can triage, assign, fix, and ship accordingly.

9	Balanced Policy	Don't have a too rigid nor a wide-open policy around what type of issues are acceptable like XSS, SQL, etc. Otherwise, you'll miss out on new threats or your team will be overwhelmed with new problems which they don't know how to fix.

Top Vulnerability Scanners

Name	Asset Class	Continuous Scans	Pricing
Qualys[16]	Web Scanner	Yes	N/A
Tenable[17]	Web Scanner	Yes	N/A
FX Labs[18]	API Scanner	Yes	Fraction

How scanners can be a great pre-requisite to bug bounty programs?

1. **Less expensive:**
   The average cost of a discovered vulnerability can be a fraction. Technically these products will pay for themselves.

2. **Private and less noisy:**
   You'll have enough time to triage, scope, and fix.

3. **Continuous coverage:**
   Provides continuous coverage so you don't regress and enables DevSecOps.

4. **No dedicated resource:**
   No dedicated managers or engineers are required. I.e. perfect for resource crunch startups and SME's.

---

[16] "Web Application Scanning | Qualys, Inc.." Accessed June 12, 2019. https://www.qualys.com/apps/web-app-scanning/.
[17] "Tenable.io Web Application Scanning | Tenable®." Accessed June 12, 2019. https://www.tenable.com/products/tenable-io/web-application-scanning.
[18] "FX Labs." Accessed June 12, 2019. https://fxlabs.io/.

Bug Bounty vs Scanner Coverage

#	Risk	Bug Bounty	Scanners
1	**Cross-site Scripting**	Yes	API & Web
2	**Improper Authentication**	Yes	API & Web
3	**Sensitive Information Disclosure**	Yes	API & Web
4	**Privilege Escalation**	Yes	API
5	**SQL Injection**	Yes	API & Web
6	**Code Injection**	Yes	API & Web
7	**Insecure Direct Object Reference**	Yes	API
8	**Improper Access-Controls**	Yes	API & Web
9	**Advanced DDoS**	N/A	API

ROI:

If your team has done a few prerequisites like scanners, automation, DevSecOps from the checklist, your budget can go a long way. You may not even spend a fraction of your initial budget on your bug bounty programs.

Reviewers:

- Luqman Shareef (FX Labs)
- Abdullah Akbar (FX Labs)
- Riyaz Shaik (FX Labs)
- Amjad Afanah (FX Labs)

References:

https://www.slideshare.net/hacker0x01/5-reasons-not-to-start-a-bug-bounty-program-real-talk-with-hackerone
https://www.vpnmentor.com/blog/the-complete-list-of-bug-bounty-programs/
https://en.wikipedia.org/wiki/Bug_bounty_program