A Bug Bounty Platform you can trust

www.bugrank.io
@bugrank_io

Thanh Nguyen, Founder
Twitter: @redragonvn

Anthony LAI, Co-founder
Twitter: @darkfloyd1014

Nguyen Anh Quynh, Co-founder
Twitter: @capstone_engine
Anthony LAI (aka Darkfloyd)

- VXRL and VXCON Chairperson
- PhD Candidate @HKUST - Vulnerability Research, Malware and ML
- Mentor of Best of Best (BoB), Korea
- D2P Contest Judge @ HITB
- Blackhat Asia and HITB CFP Review Board Member
whoami (2)

NGUYEN Anh Quynh

- Nanyang Technological University, Singapore
- PhD in Computer Science
- Binary analysis, Virtual machine, Operating System, etc
- Blackhat USA/EU/Asia, Defcon, Recon, HackInTheBox, Syscan, etc
- Capstone disassembler: capstone-engine.org
- Unicorn emulator: unicorn-engine.org
- Keystone assembler: keystone-engine.org
- Qiling emulator: qiling.io
Why do we need bug bounty?

1. **More eyes than you could ever pay.** When you open it to the crowd, you get a lot more people looking over your system than you could ever hire. And you only pay the ones who find problems.

2. **Building it right the first time is a myth.** The best developers in the world still leave unexpected vulnerabilities open. You can dream of bulletproof code, or you can be prepared in case your dreams don't come true.

3. **It can save you money.** Breaches are expensive to recover from. Way more expensive than a few thousand dollars for a bounty. Plus some bugs involve eliminating pricing problems or unearned discounts.

4. **It's not a crazy new thing.** Little companies like Google, Facebook, Microsoft, Mozilla and PayPal all have bug bounties, so you won't have to do a ton of explaining to bug hunters. They know the drill.

5. **You don't have to do it all yourself.** Bug bounty platforms services are also available from HackerOne, Bugcrowd.

Ref [https://www.techrepublic.com/article/top-5-reasons-you-need-a-bug-bounty-program/]
There are many bug bounty platforms but ...
BugRank assured that we will have:

- A strong community of well-known white hat hackers.
- End-to-End Encryption Support – The vulnerability report won’t be exposed to anyone else. Not even us can read it.
- Nonprofit & Open Platform – where you don’t need to worry much about fee.
- Skilled and Passionate people behind BugRank to support you to verify the report.
- Rewards will be paid out in USD or Cryptocurrencies.
- Decentralized identity and ranking (to be implemented yet)
BugRank developed & supported by community
Features
BugRank is Open & Non-profit Bug Bounty Platform!

** Many features of BugRank are quite similar to other bug bounty platforms such as Hackerone and Bugcrowd.
Vulnerability finding process

1. Publish vendor program
2. Let the Hackers do their job
3. Validate the submission
4. Reward the hackers
5. Resolve the issue and go on
Hacktivity

- Hacktivity allows users and guests to see the list of bug reports submitted.
- Guests can only check the details of the reports already disclosed.
Program List

• Users and guests can search for Program list and see program details.
• Each program will have specific Policy, Bounty for the Assets.
• BugRank is also a playground for hackers to compete with each other to improve themselves.

• Hall of Fame shows the achievement of both Companies and Hackers.
• Both Company and Hacker have their own dashboard to help them to follow their tasks.

• The Hacker’s Dashboard can choose to show limited info to public
Setup your Program

• To start a Program, you need to set up the Policy and Asset.
• BugRank provides many aspects to help them describe their assets.
End-to-End Encryption

Bugrank supports onsite End-to-End encryption using OpenPGP for bug submissions and comments. Nobody (including Bugrank staff) can read the encrypted bug reports, as well as communication between the hacker and the company.

** Support for End-to-End encryption using blockchain-based public-private keys will be supported in the future version, together with decentralized identity and ranking.
Submit Report

• Hackers are required to input as much detail as possible regarding the vulnerability they found.

• Hackers can choose to Encrypt this report. Only Company and related member can see this report with the Company’s key.
Follow and Resolve the Report

- Company & hacker can see list of open issues that they are working together.
- Work together to resolve the report.
- Company will reward the hacker for their contribution.
Bug Hunter Vs Company - Advantages

Company (offer bug bounty program)
- Get best bug hunter who can hunt high risk and triaged bugs, some can offer high monetary reward.
- Always taking good reports.

Bug Hunter
- Seek companies who offer high reward on bug bounty program
- Hackers with high reputation will have more invitations to join other bounty programs
Bug Hunter Vs Company - Disadvantages

Company (offer bug bounty program)

- Receive false-positive reports and give efforts to verify those bugs.
- Companies can’t afford a lot of resources on bug bounty may be ignored and left behind.

Bug Hunter

- Some try to submit bugs first regardless of fitting scope because of the bounty rewards.
- Novice bug hunter can’t get chance to start without invitation by program owner. Feeling frustrated and quit the program.
To-Do: Recommender System

Objectives

1. Novice bug hunter can get chance to start by taking:
   a. built-in CTF-like assessment game score
   b. trial private program with invitation tokens
2. Recommend intermediate-level bug hunter(s) to program owners.
3. Small companies can be beneficial from bounty program
4. Youngsters and students may participate for fun instead of monetary reward, so we need to grant them opportunities to kick off ("For Community" philosophy).
To-Do: Recommender System

Attributes

• Reputation (Bug Report)
• Bug report view
• Bug bounty follow
• Bug bounty amount or type of prize awarded
• Company with different business nature from which they previously hunt bugs
• Education background
To-Do: Recommender System

Adopt simple algorithms to predict the probability of bug hunters willing to hunt bugs for Company A AND Company A is recommended with suitable bug hunters

For example: Naive Bayes Algorithm
Demo
Welcome to BugRank Community

We are currently reviewing & cleaning-up source code for public release.

https://bugrank.io (beta version)

Contact us at Twitter @bugrank_io, or Email rd@vnsecurity.net & darkfloyd@vxrl.hk