

BUGRANK

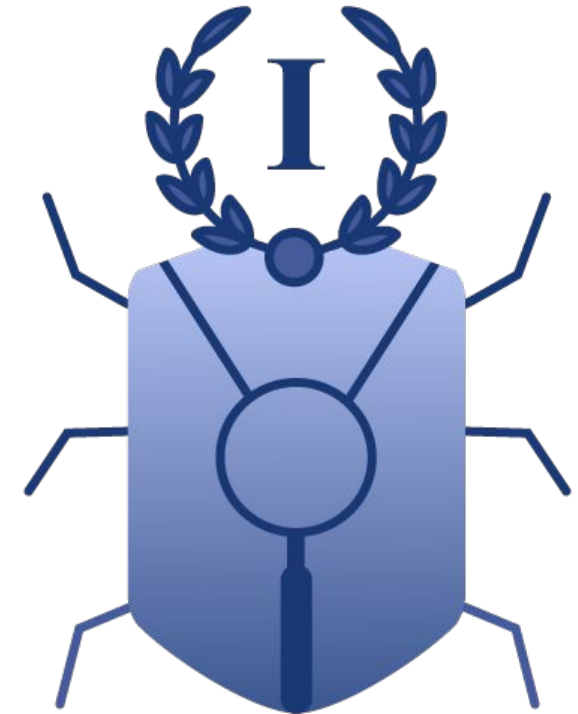
A Bug Bounty Platform you
can trust

www.bugrank.io
[@bugrank_io](https://twitter.com/bugrank_io)

Thanh Nguyen, Founder
Twitter: @redragonvn

Anthony LAI, Co-founder
Twitter: @darkfloyd1014

Nguyen Anh Quynh, Co-founder
Twitter: @capstone_engine



whoami (1)

Anthony LAI (aka Darkfloyd)

- VXRL and VXCON Chairperson
- PhD Candidate @HKUST - Vulnerability Research, Malware and ML
- Bug Report: CVE-2019-8678, CVE-2019-8685, CVE-2019-9886
- 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 ...

The screenshot shows a web browser window with multiple tabs open, including 'Reset passw', '#335330 Sub', 'GCHQ', 'Activate you', 'Video Confe', 'Introduction', 'HKEx Pentes', 'Forgot your', 'BugRank', and 'Sign in'. The address bar shows 'hackerone.com/reports/335330'. The page content includes a navigation bar with 'Hacktivity', 'Directory', 'Inbox', 'Hacker Dashboard', and 'Job Board'. The main content area displays a report for 'Geekboy! (geekboy)' with the following details:

- Reputation: 24436
- Rank: 7th
- Signal: 5.20
- Percentile: 89th
- Impact: 16.89
- Percentile: 86th

The report title is '#335330 Subdomain Takeover to Authentication bypass' with 32 votes. The report details are as follows:

- State: Resolved (Closed)
- Severity: Critical (9.4)
- Disclosed: April 24, 2020 4:50am +0800
- Participants: 2
- Reported To: Roblox
- Visibility: Disclosed (Full)
- Weakness: None
- Bounty: \$2,500

A 'Collapse' button is visible below the report details. The timeline section shows a post from 'geekboy' submitted a report to 'Roblox' on Apr 10th (2 years ago). The vulnerability type is 'Subdomain Takeover'. The description states: 'Due to unclaimed or expired Hubspot instance an attacker is able to claim and serve content from `devre1.roblox.com` and perform different kind of attacks which i shared in impact section.' The affected area is also listed.

The bottom of the browser window shows a taskbar with three PDF files: 'csrsignedinfopack.pdf', 'csrsigned.pdf', and 'agreement-signed.pdf', along with a 'Show all' button.



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.



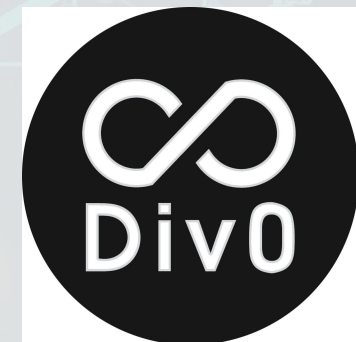
Rewards will be paid out in USD or Cryptocurrencies.

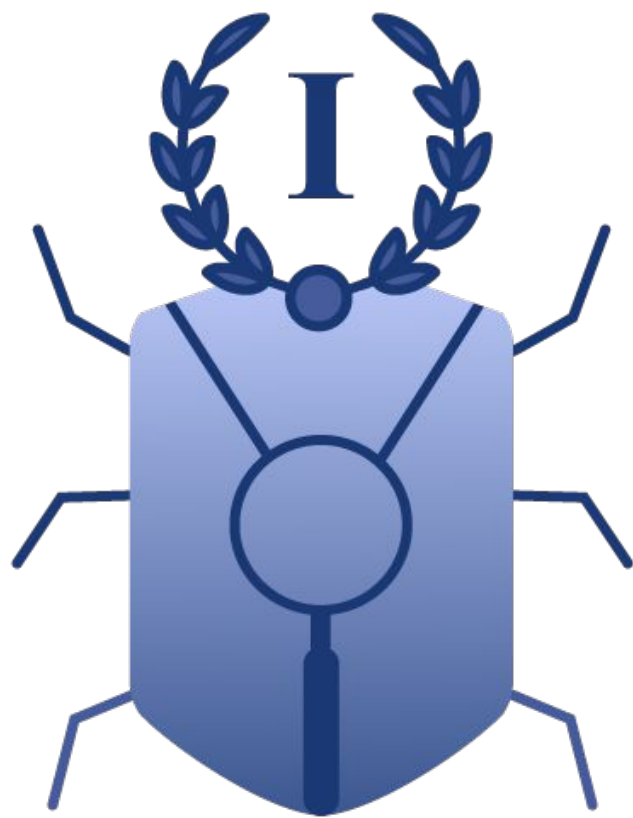


Decentralized identity and ranking (to be implemented yet)



BugRank developed & supported by community





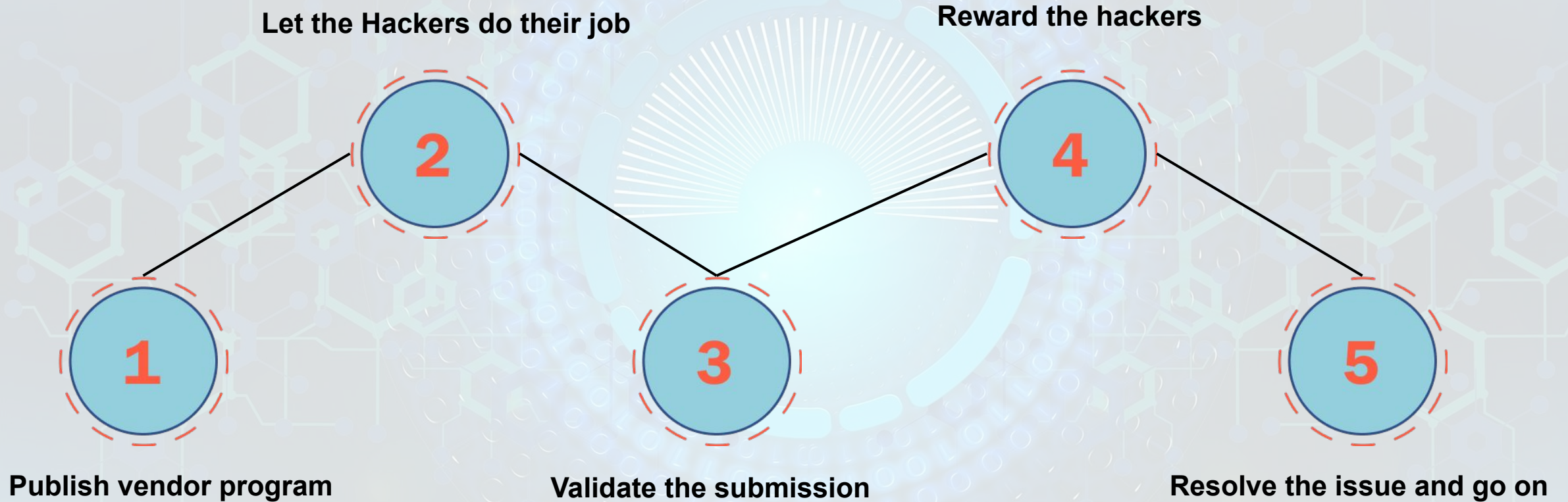
Features

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.*



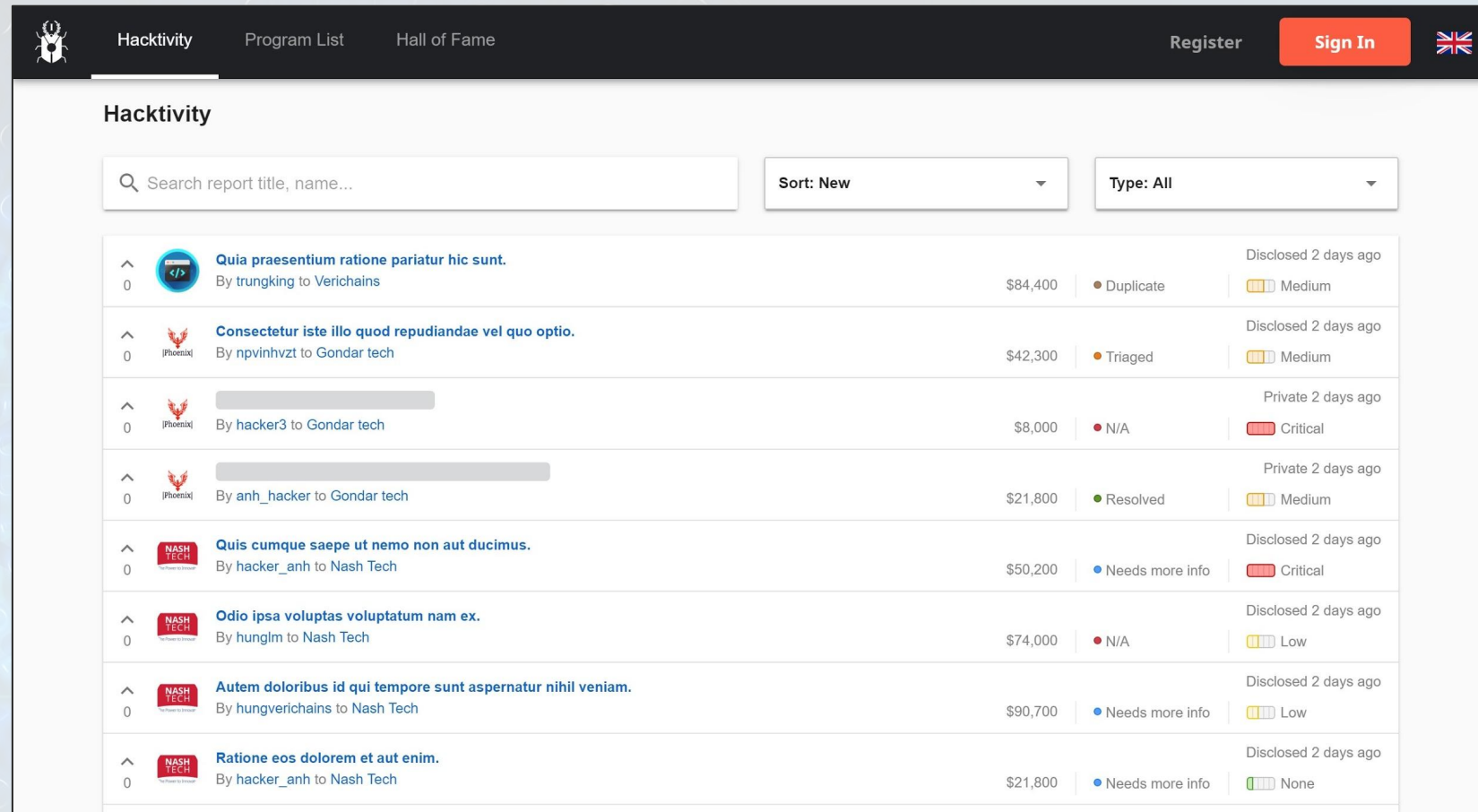
Vulnerability finding process



Hacktivity

- Hacktivity allow users and guest see list of bug reports submitted.

- Guest can only check the detail of the reports already disclosed.

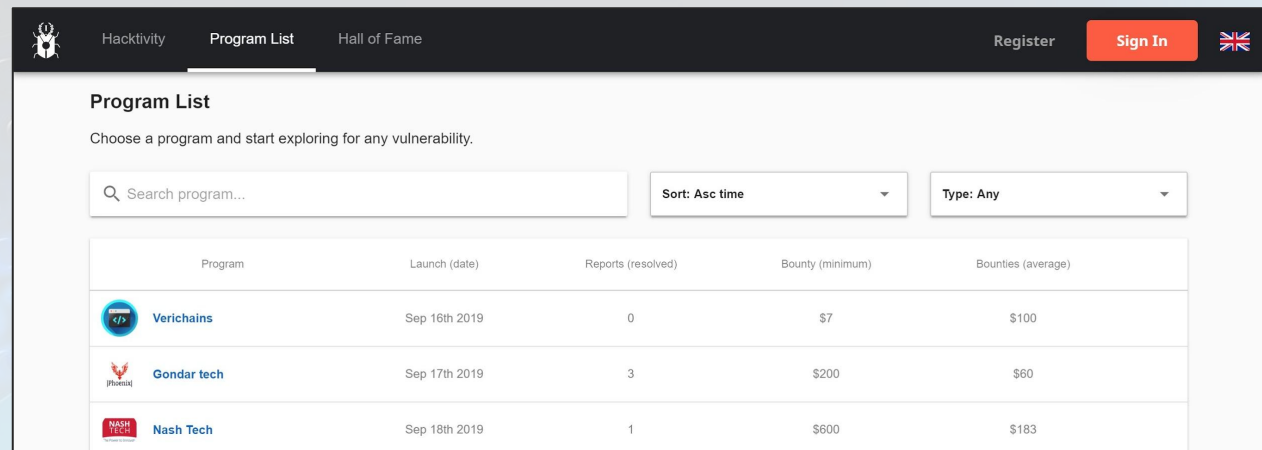





The screenshot displays the Hacktivity website interface. At the top, there is a navigation bar with a bug icon, links for 'Hacktivity', 'Program List', and 'Hall of Fame', and buttons for 'Register' and 'Sign In' (with a UK flag icon). Below the navigation bar, the main content area is titled 'Hacktivity' and features a search bar, a 'Sort: New' dropdown, and a 'Type: All' dropdown. The main content is a list of bug reports, each with a report icon, a title, a description, a bounty amount, a status, and a disclosure date.

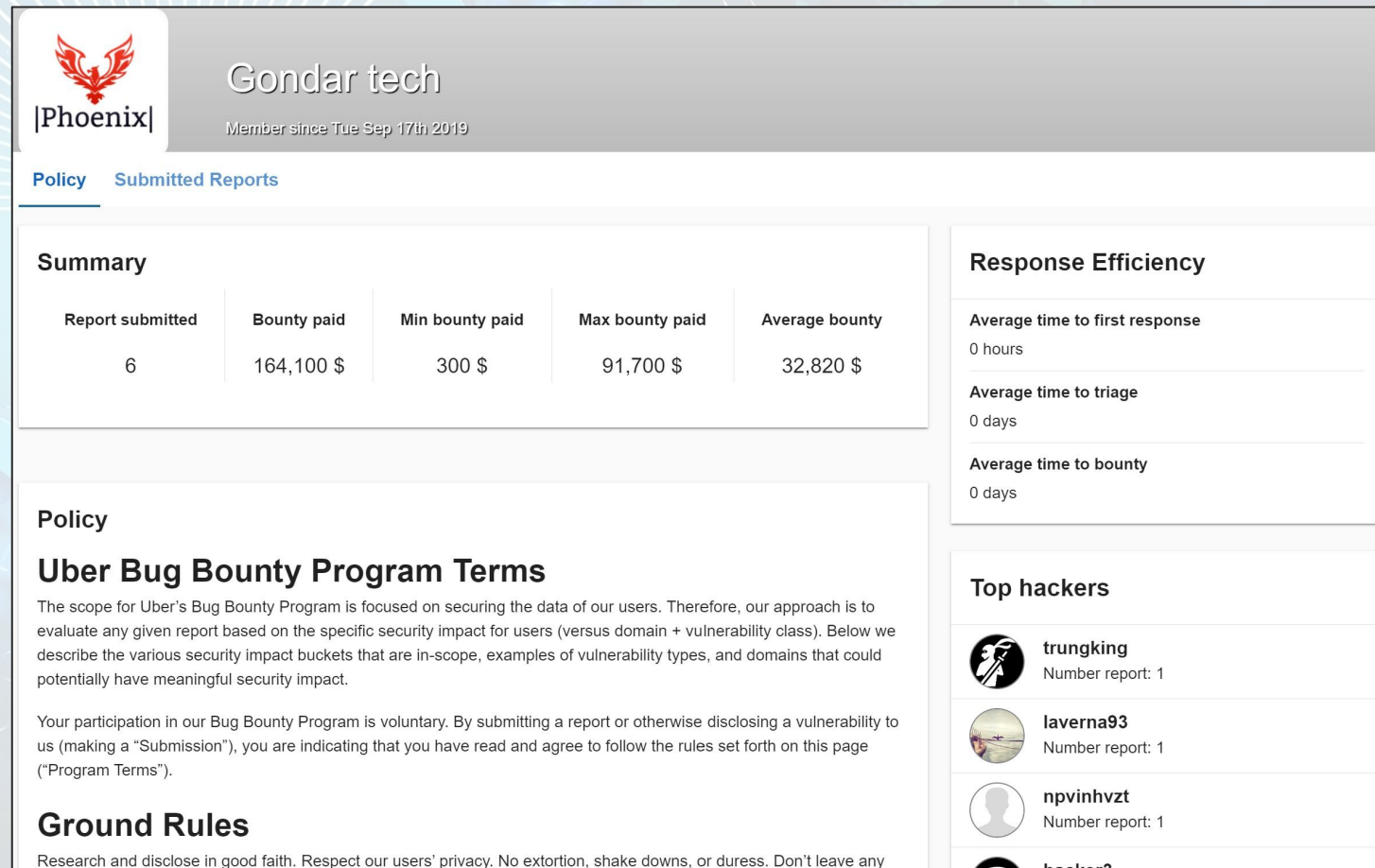
Report Icon	Title	Description	Bounty	Status	Disclosure Date
	Quia praesentium ratione pariatur hic sunt.	By trungking to Verichains	\$84,400	Duplicate	Disclosed 2 days ago
	Consectetur iste illo quod repudiandae vel quo optio.	By npvinhvzt to Gondar tech	\$42,300	Triaged	Disclosed 2 days ago
	[Redacted]	By hacker3 to Gondar tech	\$8,000	N/A	Private 2 days ago
	[Redacted]	By anh_hacker to Gondar tech	\$21,800	Resolved	Private 2 days ago
	Quis cumque saepe ut nemo non aut ducimus.	By hacker_anh to Nash Tech	\$50,200	Needs more info	Disclosed 2 days ago
	Odio ipsa voluptas voluptatum nam ex.	By hunglm to Nash Tech	\$74,000	N/A	Disclosed 2 days ago
	Autem doloribus id qui tempore sunt aspernatur nihil veniam.	By hungverichains to Nash Tech	\$90,700	Needs more info	Disclosed 2 days ago
	Ratione eos dolorem et aut enim.	By hacker_anh to Nash Tech	\$21,800	Needs more info	Disclosed 2 days ago

Program List

- Users and guests can search for Program list and see program details.
- Each program will have specific Policy, Bounty for the Assets.



Program	Launch (date)	Reports (resolved)	Bounty (minimum)	Bounties (average)
 Verichains	Sep 16th 2019	0	\$7	\$100
 Gondar tech	Sep 17th 2019	3	\$200	\$60
 Nash Tech	Sep 18th 2019	1	\$600	\$183



Report submitted	Bounty paid	Min bounty paid	Max bounty paid	Average bounty
6	164,100 \$	300 \$	91,700 \$	32,820 \$

Policy

Uber Bug Bounty Program Terms

The scope for Uber's Bug Bounty Program is focused on securing the data of our users. Therefore, our approach is to evaluate any given report based on the specific security impact for users (versus domain + vulnerability class). Below we describe the various security impact buckets that are in-scope, examples of vulnerability types, and domains that could potentially have meaningful security impact.

Your participation in our Bug Bounty Program is voluntary. By submitting a report or otherwise disclosing a vulnerability to us (making a "Submission"), you are indicating that you have read and agree to follow the rules set forth on this page ("Program Terms").

Ground Rules

Research and disclose in good faith. Respect our users' privacy. No extortion, shake downs, or duress. Don't leave any





Response Efficiency

Average time to first response
0 hours

Average time to triage
0 days

Average time to bounty
0 days



















Top hackers

-  **trungking**
Number report: 1
-  **laverna93**
Number report: 1
-  **npvinhvzt**
Number report: 1
-  **hacker3**

Hall of Fame

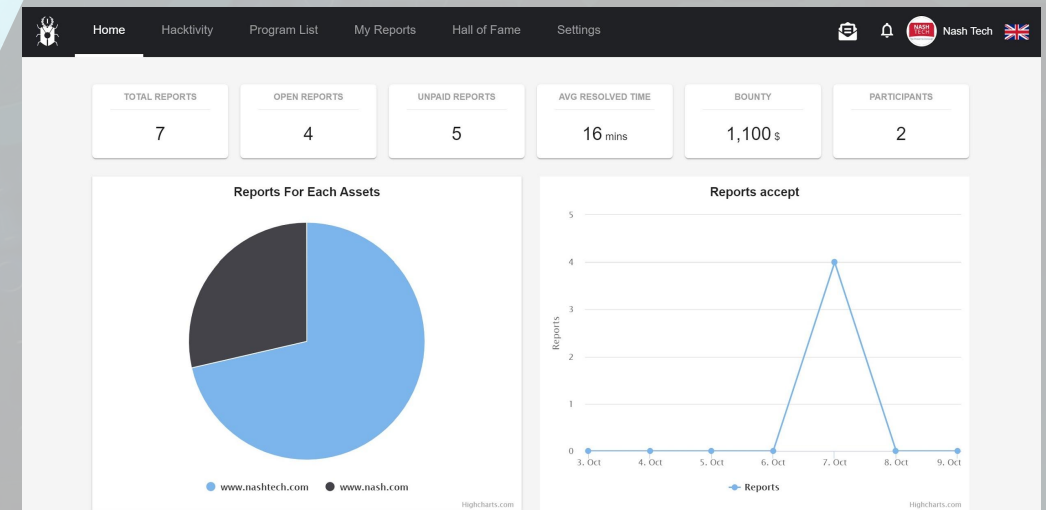
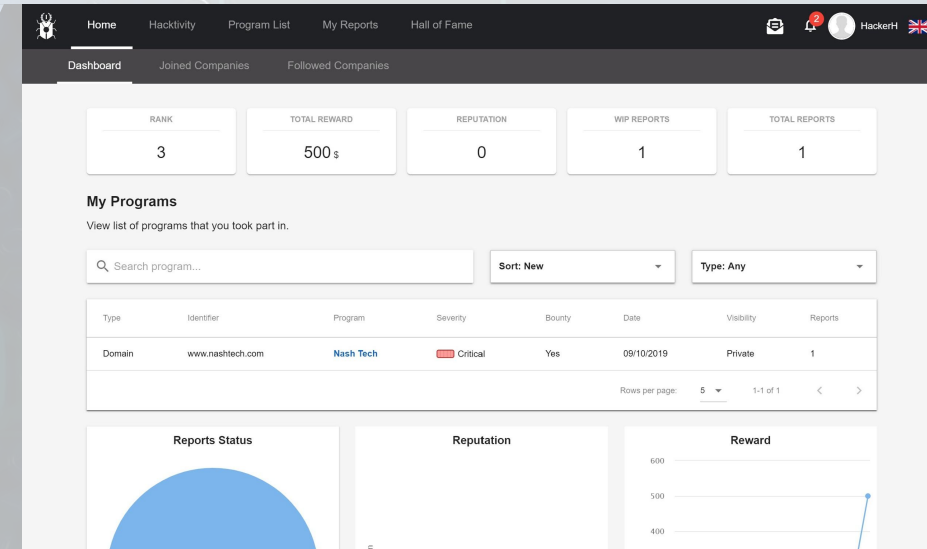
- BugRank is also a playground for hackers to compete with each other to improve themselves.
- Hall of Fame shows the achievement of both Companies and Hackers.

The screenshot displays the 'Hall of Fame' section of the BugRank website. The page is divided into two main columns: 'Top Paid Companies' and 'Top Rewarded Hackers'. Each column features a list of entities with their respective rankings, bounties, and reputations. The 'Top Paid Companies' column lists Gondar tech, Nash Tech, and Verichains. The 'Top Rewarded Hackers' column lists trungking, hacker_anh, and npvinh. Below these columns, there are two rows of smaller entries for both companies and hackers, showing their rankings and bounties.

Top Paid Companies			Top Rewarded Hackers		
  Gondar tech	Ranking: 2nd Bounty: 300.0 \$		  trungking	Ranking: 2nd Bounty: 500.0 \$ Reputation: 3.0	
  Nash Tech	Ranking: 1st Bounty: 1.1 K\$		  hacker_anh	Ranking: 1st Bounty: 1.1 K\$ Reputation: 5.0	
  Verichains	Ranking: 3rd Bounty: 200.0 \$		  npvinh	Ranking: 3rd Bounty: 0.0 \$ Reputation: 0.0	
 vzota	0.0 \$	4th	 hunglm	0.0 \$	0.0 4th
 Gondar	0.0 \$	5th	 thaiht	0.0 \$	0.0 5th
 ACBPRO	0.0 \$	6th	 npvinhvzt	0.0 \$	0.0 6th

User Dashboard

- 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.

The screenshot shows the 'Policy' configuration page. On the left is a navigation menu with categories: General, Your Profile, User Management, Program, Policy (selected), Asset, Security, Encryption, Change Password, Setup guide, and another Setup guide. The main content area is titled 'Policy' and contains a text editor with a 'Write' tab selected. The text in the editor reads: 'In order for Hackers to know how you want to receive vulnerability reports for your assets, please help to publish a vulnerability disclosure policy with detail guidance. You can refer to ISO 29147 or contact us for some advices. No technology is perfect, and pixiv believes that working with skilled security researchers across the globe is crucial in identifying weaknesses in any technology. If you believe you've found a security issue in our product or service, we encourage you to notify us. We welcome working with you to resolve the issue promptly. Disclosure Policy Let us know as soon as possible upon discovery of a potential security issue, and we'll make every effort to quickly resolve the issue. It is not permitted to publicly disclose reports without the express consent of pixiv's security team. Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder. Program Rules While researching, we'd like to ask you to refrain from: Denial of service Spawning'

The screenshot shows the 'Asset' configuration page. On the left is a navigation menu with categories: General, Your Profile, User Management, Program, Policy, Asset (selected), Security, Encryption, Change Password, Setup guide, and another Setup guide. The main content area is titled 'Asset' and contains a table with the heading 'Define all assets here'. There is an 'ADD ASSET' button in the top right corner. The table has columns for Type, Identifier, Maximum severity, Scope, and Bounty. It lists two assets: 'www.nashtech.com' with a 'Critical' severity and 'www.nash.com' with 'No rating'. Each row has icons for adding and editing assets. At the bottom right, there is a pagination control showing 'Rows per page: 20' and '1-2 of 2'.

Type	Identifier	Maximum severity	Scope	Bounty	
Domain	www.nashtech.com	Critical	Yes	Yes	+ -
Domain	www.nash.com	No rating	No	Yes	+ -

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.*

bugrank.io/report/77/new

Privileges: None Low High

User Interaction: None Required

Integrity: None Low High

Availability: None Low High

4 Private Reporter

By choosing this option, your name in this report will be display as Anonymous to the Company and other Hackers.

Hide my identity for this report (this company members cannot see your identity)

Encrypt this report (using your public key and company's public key, you can change it by go

Company public key information:

Key id:	[0x2FC1CD65DF02C3B3]
Algorithm:	rsa_encrypt_sign
User id:	Nash <kusakabe2412+2@gmail.com>
Fingerprint:	636496B949E53484874E52B52FC1CD65DF02C3B3
Created:	Mon Oct 21st 2019

bugrank.io/inbox/bugs:53

Hacktivity Program List My Reports Hall of Fame Settings

Nash My Reports (0) Assigned to me (16)

Asset Type	Domain	Payment Status	None
Vulnerability	Path Traversal Edit	Bounty	\$0
		Is Encrypted	Yes

Participants [Call Staff Review](#)

SUMMARY BY JOHNDUKE

[Encrypted content]

[EDIT SUMMARY](#)

johnduke submitted a report to [Harvey Nash](#)

[Encrypted content]

johnduke posted a comment

[Encrypted content]

Submit Vulnerability Report to Nash Tech

It's great that you discovered a potential vulnerability for Nash Tech's assets. By providing detail information regarding your discovery, you can help Nash Tech quickly identify the issue and resolve it. The more detail you provide, the faster you receive your bounty reward.

1 Asset

Select the asset that contain potential issue.

Search asset

Showing: All Types

www.nashtech.com
Domain.Critical

Currently selected: None

2 Vulnerability

Select the type of the potential issue you have discovered.

If there are more than one Vulnerability Type, please select the best match or submit separate report for each type of Vulnerability.

Showing: Access Control

Search vulnerability

Authentication Bypass Using an Alternate Path or Channel (CWE-288)

Brute Force (CWE-307)

Forced Browsing (CWE-425)

Improper Access Control - Generic (CWE-284)

Currently selected: None

3 Severity

Estimate the severity of this Vulnerability.

CVSS v3.0 Calculator No rating (---)

Attack Vector: Network Adjacent Local Physical

Attack Complexity: Low High

Privileges: None Low High

User Interaction: None Required

Scope: Unchanged Changed

Confidentiality: None Low High

Integrity: None Low High

Availability: None Low High

4 Private Reporter

By choosing this option, your name in this report will be display as Anonymous to the Company and other Hackers.

- Hide my identity for this report (this company members cannot see your identity)
- Encrypt this report (using your public key and company's public key, you can change it by go to Settings > Security > Encryption)

Company public key information:

Key id: [0xAC8B9493B25230D1]
Algorithm: rsa_encrypt_sign
User id: Nash Tech <nash@gmail.com>
Fingerprint: 2DD4A4836106164CA98399BBAC8B9493B25230D1
Created: Wed Oct 9th 2019

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

The screenshot displays a bug bounty platform interface. On the left, a sidebar shows a list of reports with details like report ID, title, reporter, assignee, and time. The main area shows the details for report #3, titled 'Unchecked weapon id in WeaponList message parser on client leads to RCE'. The report status is 'Disclosed (Full) at Wed Sep 18th 2019'. A summary of key metrics is shown in five circles: State (Resolved/Closed), Severity (High, 7-8.9), Bounty (\$1.0 K), Payment Status (Confirmed), and Is Encrypted (Not encrypted). Below this, the asset is listed as 'www.nashtech.com Domain' and the vulnerability as 'Authentication Bypass Using an Alternate Path or Channel'. The participants section shows the reporter and assignee. The summary text describes the issue: 'There are no boundary check, and the range of ild is [-128, 128], so I can modify many things in the data section. In client.dll, there's an object called gEngfuncs, it is a function table that has various functions of the engine. After some calculations on latest CS 1.6 client.dll, I concluded that this function table could be overwritten using the above bug. I have attached a PoC that will pop calc.exe on latest CS 1.6 client when connected to malicious server. The AMXX plugin will catch

- 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.



Advanced Bug Hunter



Advanced Bug Hunter



Preference



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



Advanced
Bug Hunter



Advanced
Bug Hunter



Novice
Bug Hunter

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

A diagram showing the Bayes' theorem formula $P(c | x) = \frac{P(x | c)P(c)}{P(x)}$. Arrows point from labels to parts of the formula: 'Likelihood' points to $P(x | c)$, 'Class Prior Probability' points to $P(c)$, 'Posterior Probability' points to $P(c | x)$, and 'Predictor Prior Probability' points to $P(x)$.

$$P(c | \mathbf{X}) = P(x_1 | c) \times P(x_2 | c) \times \dots \times P(x_n | c) \times P(c)$$

For example: Naive Bayes Algorithm

Demo

The screenshot shows the BugRank dashboard for user Alex Kotovac. The top navigation bar includes Home, Hacktivity, Program List, My Reports, and Hall of Fame. The user's profile shows a notification badge with the number 4 and a UK flag. Below the navigation, there are three tabs: Dashboard (selected), Joined Companies, and Followed Companies. The dashboard features five summary cards: RANK (4), TOTAL REWARD (\$500.0), REPUTATION (5), WIP REPORTS (4), and TOTAL REPORTS (3). The 'My Programs' section includes a search bar, a 'Sort: New' dropdown, and a 'Type: Any' dropdown. A table lists five programs with columns for Type, Identifier, Program, Severity, Bounty, Date, Visibility, and Reports.

Type	Identifier	Program	Severity	Bounty	Date	Visibility	Reports
Domain	*.hkpc.com	World Blockchain	High	Yes	03/04/2020	Private	1
Domain	www.vxrl.hk	World Blockchain	Critical	Yes	30/03/2020	Private	2
Domain	program1.com	company1	Critical	Yes	30/03/2020	Private	1
Executable	Google Chrome	D2P	Critical	Yes	30/03/2020	Private	1



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](https://twitter.com/bugrank_io), or Email rd@vnsecurity.net & darkfloyd@vxrl.hk