1. Introduction

Keeping customer information safe and secure is of utmost priority and a core company value for us at Policybazaar Insurance Brokers Pvt Ltd ("Policybazaar"). Policybazaar welcomes the contribution of external security researchers and looks forward to suitably awarding them for their valuable contribution to the IT security of Policybazaar customers.

2. Eligibility and Responsible Disclosure

To promote the discovery and reporting of vulnerabilities and increase customer safety, any person(s) to Bug Bounty program ("Program") must adhere to the following guidelines:

- "Applicant" is a person ("external security researcher") who applies to Policybazaar for registering under the Program and is provided such authorization, in writing, by Policybazaar. The Applicant shall be required to submit its report to Policybazaar.
- Persons disqualified from the Program – Applicant cannot be

i. an employee of a contractor/vendor of PolicyBazaar or its subsidiaries or affiliates;

ii. a contractor/vendor of PolicyBazaar or its subsidiaries or affiliates;

iii. an immediate family member of a person employed by PolicyBazaar or its subsidiaries or affiliates or group company (defined for these purposes as including spouse, domestic partner, parent, legal guardian, legal ward, child, and sibling, and each of their respective spouses, and individuals living in the same household as such individuals).

- Any person(s) who is NOT an Applicant is NOT eligible to participate in the Program. If such person(s) attempts to interfere, access, modify or control the IT infrastructure including servers, website, applications etc., the same shall be considered as unathorised access and the Company may take appropriate action against such person(s) including Civil and Criminal legal action.
- The Applicant shall not interact with an individual account (which includes modifying or accessing data from the account) without the account owner's explicit consent in writing, which you must produce upon request.
- The Applicant shall not cause privacy violations and disruptions to Policybazaar or its Customers, including and not limited to unauthorized access or destruction of data, downloading sensitive and personal information of customers, and interruption or degradation of Policybazaar services. The Applicant must not violate any applicable laws or regulations, including and not limited to any laws and regulations relating to personal information or sensitive personal information.

- If the Applicant inadvertently accesses any customer's data or any other Policybazaar's data without authorization while investigating an issue, you must promptly cease the activity that might result in further access of the customer data or PolicyBazaar data and immediately notify PolicyBazaar about such information which was accessed (including a full description of the contents of the information). The Applicant shall immediately delete the information/ data from their systems and produce evidence to Policybazaar that such information/ data has been promptly deleted. The Applicant shall in such cases acknowledge the inadvertent access in the Program report which the Applicant shall subsequently submit.
- The Applicant shall not exploit a security issue including any vulnerability, that the Applicant discovers, for any reason other than for testing purpose.
- Upon submission of Program report by the Applicant, Policybazaar shall internally investigate and assess the findings of the report before rewarding the Applicant.
- The Applicant shall sign a non-disclosure agreement with Policybazaar and shall be bound by its provisions thereto. In no case shall the Applicant publish, reproduce or replicate any findings in public domain, without express written consent of Policybazaar.
- The Applicant understands that participation in this Program does not entitle it for any monetary compensation or bug bounty, and the same shall be at the discretion of Policybazaar. The decision of Policybazaar in this context shall be final and binding.

Policybazaar reserves all rights to disqualify individuals from the Program for disrespectful or disruptive behavior or for the violation of any of these guidelines and the Company also reserves the right to initiate appropriate action against such person(s) including Civil and Criminal legal action.

3. Bug Bounty program processes

Policybazaar recognizes and rewards the Applicants who help Policybazaar keep its customers safe by reporting vulnerabilities in our IT infrastructure. Monetary bounties for any Program reports are entirely at Policybazaar' s discretion, based on risk, impact, number of vulnerable users, and other factors. To be considered for a bounty, you must meet the following requirements:

- Adhere to the Eligibility and Responsible Disclosure guideline specified above.
- Report a security bug: identify a vulnerability in our applications which creates a security or privacy risk. Report the vulnerability upon discovery or as soon as is feasible.
- Report a security bug involving one of the products or services that are within the scope of the program. We specifically exclude certain types of potential security issues, listed under "Out of scope"
- Give Policybazaar a reasonable time to respond to the issue
- Before engaging in any action that may be inconsistent with or unaddressed by these guidelines, contact us for clarification by submitting a new query.
- Do not use automated scanners to scan our web applications as this would result in IP blacklisting and disqualification from bug bounty program.

- Comply with all applicable laws.

In turn, we will follow these guidelines when evaluating reports under our bug bounty program:

- We investigate and respond to all valid reports. Due to the volume of reports that we receive, however, we prioritize evaluations based on risk and other factors, and it may take some time before you receive a reply.
- We determine bounty amounts based on a variety of factors, including (but not limited to) impact, ease of exploitation and quality of the report.
- We reserve the right to publish reports (and accompanying updates).
- We verify that all bounty awards are permitted by applicable laws and paid only in compliance with applicable sanction compliance laws.

4. Submitting a security issue / vulnerability

An Applicant, before submitting a Program report on security issue/ vulnerability to Policybazaar, must read these guidelines and send an email to infosec@policybazaar.com, preferably with "Security Issue – External Security Researcher" in the subject line. Once the report has been received, our security team will investigate the issue(s). We will respond to you at the earliest with triage of the issue and/or any additional requests for clarification. Due to the volume of reports that we receive, however, we prioritize evaluations based on risk and other factors, and it may take some time before you receive a reply.

We'll try to keep you informed about our progress throughout the process.

5. In Scope Vulnerabilities

Domain *.policybazaar.com

Android: Play Store Policybazaar owned android applications

iOS: App Store Policybazaar owned iOS applications

- Cross-Site Scripting (XSS) include when an attacker stores malicious script in the data sent from a website's search or contact form.
  - Stored XSS
- No-SQL/SQL Injection allow attackers to inject code into commands for databases that don't use SQL queries, such as MongoDB.
- XML External Entity is a type of custom XML entity whose defined values are loaded from outside of the DTD in which they are declared.
- Insecure JSON Deserialization is passing manipulated serialized objects that can be interpreted by the application leading to its control.

- Remote Code Execution allow an attacker to remotely execute malicious code on a computer.
- Server-Side Request Forgery involves an attacker abusing server functionality to access or modify resources.
- Cross Site Request Forgery allows an attacker to induce users to perform actions that they do not intend to perform.
- Broken Authentication aim to take over one or more accounts giving the attacker the same privileges as the attacked user.
- Privilege Escalation act of exploiting a bug, a design flaw, or a configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
- Business Logical Flaws are flaws in the design and implementation of an application that allow an attacker to elicit unintended behavior.
- Misuse/Unauthorized use of our APIs- refers to the act of wrong-handling of APIs, gaining unsanctioned access, and modifying the key functions
- Leaking customer's sensitive data

6. Out of Scope Vulnerabilities – Web Applications

- Issues related to software/application not under Policybazaar' s control or owned by any third party
- Forms missing CSRF tokens (we require evidence of actual CSRF vulnerability)
- Missing security headers which do not lead directly to a vulnerability
- Clickjacking without an impact
- Text Injection/HTML Injection
- Broken Session Flaws
- Known-vulnerable library (without evidence of exploitability)
- Spam & rate limiting
- SSL/TLS protocol vulnerabilities
- Best practice concerns will be reviewed, but in general, we require evidence of exploitability
- Vulnerabilities only affecting users of outdated or unpatched browsers and platforms
- The brute force which doesn't lead to any bypass/disclosure
- Social engineering attacks
- Username/Mobile Number enumeration
- Any activity that could lead to the disruption of our service (DoS/DDoS)
- Private IP/Non-customer email ID disclosure
- Any other non-exploitable vulnerabilities

7. Out of Scope Vulnerabilities - Android Applications

- Absence of certificate pinning
- Sensitive data stored in app private directory (which cannot be accessed by any other application)
- User data stored unencrypted on external storage
- Lack of binary protection control in android app
- Shared links leaked through the system clipboard
- Any URIs leaked because a malicious app has permission to view URIs opened
- Sensitive data in URLs/request bodies when protected by TLS
- Crashes due to malformed Intents sent to exported Activity/Service/Broadcast Receive (exploiting these for sensitive data leakage is commonly in scope)

8. Out of Scope Vulnerabilities - iOS Applications

- Absence of certificate pinning
- Lack of Exploit mitigations i.e., PIE, ARC, or Stack Canaries
- Path disclosure in the binary
- User data stored unencrypted on the file system
- Lack of binary protection (anti-debugging) controls
- Lack of jailbreak detection

9. Rewards

Rewards Eligibility

The reported vulnerability should showcase business impact and the reporters will be rewarded based on the risk severity classified below and shall be at the discretion of Policybazaar and the decision of Policybazaar in this context shall be final and binding:

- Critical or P0 Severity Issue: $3,000 to $5,000
- High or P1 Severity Issue: $1000 to $3000
- Major Severity Issue: $300 to $1000

Report Vulnerability at infosec@policybazaar.com

10. The Fine Print

Applicants are responsible for paying any statutory taxes associated with rewards. We may modify the terms of this Program or terminate this Program at any time. We will not apply any changes we make to these Program terms retrospectively. Reports from individuals who we are not Applicants or are prohibited by law are ineligible for rewards.

11. Summary

- The Applicant should responsibly disclose through our bug bounty programs. If in doubt, ask us before engaging in any specific action you think might go outside the bounds of our policy.
- Both identifying and non-identifying information can put a Applicant at risk, we limit what we share with third parties. We may provide non-identifying substantive information from your report to an affected third party, but only after notifying you. We will only share identifying information (name, email address, phone number, etc.) with a third party if you give your written permission.
- We may share your report or personally identifiable information without obtaining your prior consent

  (i) only where it is requested or required by law or by any court or governmental agency or authority to disclose, or for the prevention, detection, investigation including cyber incidents, or for prosecution and punishment of offences.

  (ii) With our statutory and other auditors, regulator, vendors engaged by Policybazaar for information technology and cyber security and Policybazaar's group companies, affiliates and subsidiaries.