Gameskraft

Gameskraft Bug Bounty Program (“Program”)

Overview

Gameskraft Technologies Private Limited (“Gameskraft”) is committed to ensuring the security and privacy of its users and products. As one of India's largest online gaming platforms, we highly value contributions from the security research community. Through our Program, we invite ethical hackers to help identify vulnerabilities in our products, services, and platforms, rewarding them for their valuable efforts.

If you believe you have discovered a potential security vulnerability in any of Gameskraft’s products, let us know immediately, and we will make every effort to get the issues addressed as quickly as possible.

Please ensure you understand the Program rules before you report a vulnerability. By participating in this Program and submitting vulnerabilities, you agree to be bound by these rules. Gameskraft provides monetary rewards to vulnerability reporters at its discretion and the reward may vary based upon metrics including (but not limited to) vulnerability severity, impact, and exploitability.

Participation Eligibility

Participation in the Program is open to any individuals except:

- If your age is below 18 years i.e. 18 years and above age is mandatory. However, If a minor is interested in participating, they would need to have a parent or legal guardian represent them in the Program and handle communication and rewards on their behalf, if allowed by platform's rules.
- Your organization does not allow you to participate in these types of programs. You are responsible for adhering to any policies set by your employer that may impact your eligibility to join the Program. If your participation violates your employer's policies, you may be disqualified from taking part or receiving any rewards. All payments will comply with local laws, regulations, and ethical standards. Gameskraft shall not be liable for any disputes between you and your employer related to this issue. Additionally, local laws may impose further restrictions on your participation.

Reward Eligibility

- Vulnerability reports must include clear and complete details, including steps to reproduce, the potential impact and your contact information.
  - Clear textual descriptions of vulnerabilities.
  - Screenshots or video demonstrating the exploit was performed and showing the final impact.
  - Complete steps with the necessary information to reproduce to exploit, including (if necessary) code snippets, payloads, commands, etc
  - Describe the potential impact and risks associated with the vulnerability.
- Only the first reporter of a specific vulnerability will be eligible for a reward. Please check, Tips to Avoid Submitting Duplicate Vulnerability Reports section
- The vulnerability must be within the defined scope of the Program.
- The vulnerability must not be publicly disclosed by the participant to any third party unless prior written approval of Gameskraft is obtained.
- The vulnerability is acknowledged, accepted, resolved by Gameskraft and the participant is the first reporter.
- Participant should have atleast following documents:
  - Valid PAN Copy
  - Valid Aadhar Copy
  - Indian Bank Account Details (with copy of canceled cheque)
- Participants should not be related to Gameskraft as employees or contractors or former employees or in any way related to any Gameskraft employees or Gameskraft contractors or Gameskraft former employees.

- Gameskraft reserves the right to determine reward eligibility based on the severity, uniqueness and impact of the reported vulnerability.

Eligible Products

The following domains and games are within the scope of the Program:

1. **RummyCulture**
    a. Playstore android app: https://play.google.com/store/apps/details?id=com.gameskraft.rummycultureplay
    b. Appstore iOS app: https://apps.apple.com/in/app/rummyculture-play-cash-rummy/id1447534803
    c. APK android app: www.rummyculture.com
2. **RummyPrime**
    a. Playstore android app: https://play.google.com/store/apps/details?id=com.rummy.prime.card.games
    b. APK android app: - www.rummyprime.com

Gameskraft does not claim ownership of your submission. However, by submitting your work to Gameskraft, you grant Gameskraft a non-exclusive, irrevocable, perpetual, royalty-free, worldwide, sub-licensable license to the intellectual property in your submission. This license includes the right to: (i) use, review, evaluate, test, and analyze your submission; (ii) reproduce, modify, distribute, display, publicly perform, commercialize, and create derivative works from your submission, in whole or in part; and (iii) showcase your submission and its content for marketing, sales, or promotion of this Program or other programs (including internal and external sales meetings, conference presentations, tradeshows, and press releases) in all forms of media (existing or future).

You further represent and warrant that your submission is original, that you have not used any material owned by another person or entity, and that you have the legal authority to submit it to Gameskraft.

Qualifying Vulnerability Types

- Remote Code Execution (RCE)
- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Authentication or Authorization flaws
- Privilege escalation
- Sensitive data exposure

- Security misconfigurations
- Cross-Site Request Forgery (CSRF) in sensitive actions
- Insecure direct object references (IDOR)

Non-Qualifying Vulnerabilities

- Low-impact issues such as clickjacking or missing security headers (unless exploitable in a critical manner)
- Issues that require root/jailbreak or physical device access
- Publicly known vulnerabilities that do not specifically affect Gameskraft's applications
- Rate limiting on non-sensitive endpoints
- Weak or outdated content security policies

Out of Scope

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Issues related to outdated browsers or unsupported plugins
- Vulnerabilities related to third-party services or platforms (unless they directly affect Gameskraft's systems)
- Social engineering (e.g., phishing) of Gameskraft employees or users
- Content injection (e.g., harmless HTML/CSS issues)
- Self-XSS or URL redirection (unless a high-risk scenario is proven)
- Issue only reproducible on jailbreak/rooted devices
- Any kind of modification done to APK or IPA files
- All domains or subdomains or apps not listed in the above list of 'Scopes'

Program Rules: Testing Policy and Responsible Disclosure

You will follow the rules specified hereunder, failing which your participation in the Program will be immediately terminated.

- **Do No Harm**: Ensure that your testing does not degrade the experience for other users, impact the stability or performance of our products, or result in downtime. You are prohibited from performing Distributed Denial of Service (DDos) testing or any activities that could potentially lead to service degradation, disruption, or outage. Engaging in such actions constitutes a violation of our Program policy and may result in legal consequences.

- **Legal Compliance**: Testing must adhere to all applicable laws, the terms of this Program.
- **Prohibition on Data Breaches**: No accessing, deleting, or modifying user data during testing.
- **No Public Disclosure:** You will report any security bug discovered by you to Gameskraft and provide Gameskraft with reasonable time to identify and mitigate the issue and shall not disclose the same to any third party unless authorized by Gameskraft.
- **Respect Privacy**: Do not interact with any other user's accounts or private data during testing.
- **Collaborations**: If working in a team, only one reward will be issued, and you must decide how to split it.
- **Only Test Your Account**: Use your own accounts for testing, and do not attempt to exploit vulnerabilities in other users' accounts.
- **Follow-Up**: Researchers are expected to provide additional information if requested and to follow up on any clarification needs from the Gameskraft bug bounty team.
- **No Physical Attacks**: Avoid social engineering, phishing, or physical attacks on Gameskraft staff or infrastructure.

Bug Submission Process

To submit a bug report, please send the following details to **bugbounty@gameskraft.com**

Vulnerability reports must include clear and complete details, including steps to reproduce, the potential impact and your contact information.

1. Clear textual descriptions of vulnerabilities.
2. Screenshots or video demonstrating the exploit was performed and showing the final impact.
3. Complete steps with the necessary information to reproduce to exploit, including (if necessary) code snippets, payloads, commands, etc
4. Describe the potential impact and risks associated with the vulnerability.
5. Provide your name, email address, and any other relevant contact details for follow-up.

Make sure to include all relevant technical details so the bug bounty team can effectively assess and address the report.

Report Review Timeline

- **Initial Acknowledgment**: You will receive an acknowledgment of your submission within **7 business days** of reporting the vulnerability.
- **Assessment**: The Gameskraft bug bounty team will review and assess the reported vulnerability within **30 business days** from the date of receipt of the submission. During this time, the team may reach out to you for further details or clarification.
- **Resolution**: Once the vulnerability is confirmed, Gameskraft will work on remediation. Depending on the complexity, resolution may take up to **60 business days**.
- **Reward Notification**: Once a vulnerability is confirmed and resolved, you will be notified of the reward amount within **60 days** of the vulnerability being fixed. To process rewards, we may require additional documents from you. This could slightly extend the timeline if there are delays in communication.
- **Payment Processing**: Rewards will be processed and paid out within **60 days** after the resolution notification. Payments may be made via direct bank transfer and shall be subject to TDS as per prevailing regulations in this regard. Before processing the payments following self certified documents will be required:
    - Valid PAN Copy
    - Valid Aadhar Copy
    - Indian Bank Account Details (with copy of canceled cheque)
    - GST Registration Certificate, if you are GST registered
    - Claim form (Vulnerability report)
- **Communication**: If there are any delays in processing your reward, the Gameskraft bug bounty team will notify you and provide an updated timeline.

If any delay occurs, the team will inform you about the revised timelines.

Factors Influencing Vulnerability Prioritization

Bounties will be determined & granted only at Gameskraft's discretion.

1. **Business Impact**: Vulnerabilities affecting critical financial systems (e.g., withdrawals, deposits) or user identity verification (e.g., KYC) will be prioritized over others.
2. **User Impact**: Vulnerabilities that could affect a large number of users, such as account takeovers or mass data breaches, will be treated with higher urgency.
3. **Exploitability**: The ease with which the vulnerability can be exploited is a major factor. Simple, easily reproducible issues are more critical than complex or unlikely attack vectors.
4. **Scope**: Vulnerabilities that affect multiple platforms (e.g., RummyCulture, RummyPrime) or across domains are prioritized over those affecting a single platform or service.

5. **Potential for Chain Exploits**: Some vulnerabilities that may seem low-risk on their own could be prioritized higher if they can be chained with other vulnerabilities to escalate the overall impact.

Gameskraft uses this framework to ensure that the most critical and impactful vulnerabilities are addressed as quickly as possible while maintaining the security of its platform.

Reward Structure

The rewards are based on the severity of the vulnerability as determined by Gameskraft's internal risk assessment. Bounties will be determined & granted only at Gameskraft's discretion. Factors such as business impact, exploitability, and ease of remediation will determine the reward.

Vulnerability Severity	**Reward in INR**
Low	Upto Rs. 10,000
Medium	Upto Rs. 20,000
High	Upto Rs. 30,000
Critical	Upto Rs. 50,000

Taxation of Rewards

- **Taxation Compliance**: All rewards issued under the Program are subject to applicable taxes as per applicable India Income Tax Laws and Gameskraft will withhold the applicable percentage of taxes before disbursing the reward. A TDS certificate will be provided at the end of the financial year for your records.

Please consult with a tax professional if you are unsure of your specific tax obligations related to receiving the bounty rewards.

Tips to Avoid Submitting Duplicate Vulnerability Reports

To maximize your chances of success and avoid submitting a duplicate vulnerability report, here are some practical strategies you can follow:

1. Review Public Program Information

- **Check for Known Issues**: Before starting your research, thoroughly review any public information or updates provided by Gameskraft regarding previously reported vulnerabilities or resolved issues. This will give you an idea of which bugs have already been discovered.

2. Follow Up on Public Disclosure Timeline

- **Monitor Disclosure Updates**: Occasionally, after a vulnerability has been patched, some platforms publicly disclose information about the issue. Keeping track of these disclosures can help you avoid redundant testing of already-known vulnerabilities.

3. Focus on Edge Cases and Unique Vectors

- **Be Creative**: Think beyond commonly tested vulnerabilities and target less-explored attack vectors. Many duplicate reports arise from researchers focusing on well-known vulnerabilities like XSS or SQLi in obvious places. Consider:
  - Testing business logic flaws.
  - Combining multiple lower-severity issues to identify a more impactful vulnerability.
  - Focusing on newer or lesser-used features in the games or services.

4. Keep Up with Security News

- **Follow Trends**: Stay updated with the latest security trends and vulnerability types, particularly in gaming platforms. New exploits and techniques are constantly emerging, and being aware of these can help you spot issues that others may not have considered yet.

5. Test Niche Areas

- **Explore Secondary Domains and Features**: Instead of targeting only the main platforms (e.g., the primary login pages or payment gateways), try testing auxiliary features like:
  - KYC and bank verification flows.
  - In-game interactions or game mechanics.

    - Rarely-used API endpoints or edge case functionalities in financial transactions.

6. Use Comprehensive Testing Approaches

- **Go Deep, Not Just Wide**: A surface-level test may reveal common vulnerabilities that have already been reported. Try a more in-depth approach by:
    - Analyzing application logic.
    - Conducting detailed source code analysis if possible.
    - Checking for race conditions, misconfigurations, or multi-step exploit chains.

7. Collaborate and Communicate

- **Ask for Clarifications**: If you're unsure whether a vulnerability has already been reported or is in scope, reach out to the Gameskraft bug bounty team for clarification. This can prevent time spent on testing duplicate issues.

8. Monitor Ongoing Program Updates

- **Stay Informed**: This Program often provides updates about patched vulnerabilities, scope changes, or new features added. Regularly check the Program page for these updates to ensure you're working on fresh opportunities.

9. Submit Reports Early

- **Timeliness Matters**: If you find a vulnerability, submit it as quickly as possible. This Program operates on a first-come, first-serve basis, so submitting early increases your chances of being the first to report the issue.

By following these best practices, you can minimize the likelihood of submitting duplicate reports and increase your chances of submitting unique, valid vulnerabilities that qualify for rewards.

Handling False Positives in the Program

False positives can occur when a reported issue is mistakenly identified as a vulnerability but, after further investigation, is found to not pose any actual security risk. Gameskraft's Program has a structured approach for handling false positives:

1. Evaluation Process

- **Initial Review**: Once a report is submitted, the Gameskraft bug bounty team will conduct a thorough investigation to validate the issue.
- **Technical Validation**: The team will assess whether the reported issue is exploitable or poses a real threat, based on security best practices and internal testing protocols.

2. Communication with Researchers

- If an issue is determined to be a false positive, the researcher will be notified of the findings.
- The team will provide a detailed explanation as to why the issue is classified as a false positive, including any relevant technical details that explain why it does not present a security risk.
- Researchers are encouraged to ask for clarification if needed, and the team will work with them to help understand the determination.

3. No Reward for False Positives

- **Non-Payout**: Reports classified as false positives will not qualify for any reward under the Program.
- Gameskraft encourages quality over quantity, so submitting multiple false positives or non-issues can impact a researcher's future participation in the Program.

4. Constructive Feedback

- **Learning Opportunity**: While false positives won't lead to rewards, they are still valuable for learning. Researchers will be provided feedback to help improve future submissions.
- Researchers can learn from these cases and refine their testing techniques to avoid similar submissions in the future.

5. Re-Validation Requests

- If a researcher disagrees with the false positive classification, they can request a **re-validation**. This will trigger another review of the report by a different security expert to ensure all perspectives are considered.
- Gameskraft is committed to transparency and values collaboration, so the process will remain open and fair.
- Re-validation requests can be raised only once after first review & feedback has been shared.

By fostering a transparent process for handling false positives, Gameskraft ensures the integrity of the Program while encouraging security researchers to provide high-quality, impactful reports.