
WINZO
CHASE
CODE HEALTH AND SECURITY EVALUATION

WinZO CHASE Challenge >>>

About WinZO

WinZO is the largest social gaming and entertainment platform in India. Launched in early 2018, the Company partners with third-party developers to host games on their Android app, where users can enjoy personalized multiplayer gameplay experiences. The platform is available in 12 languages such as English, Hindi, Gujarati, Marathi, with **over 100 million registered users. The WinZO platform facilitates over 4 billion micro-transactions per month across a portfolio of 100+ games** - which can be played against real-time players in micro- transaction-led social formats. The Company envisions a future where the WinZO platform can deliver a culturally relevant and enjoyable experience in the Indian gaming ecosystem, monetized through a unique micro-transaction model. To support this, WinZO has already launched 3 sets of its own Game Developers Fund with a total $26 Million Corpus.

With a vision of becoming a household name for Bharat, catering to their entertainment needs through interactive engagements, Paavan Nanda (co-Founder, WinZO, Zostel & ZO Rooms) and Saumya Singh Rathore (co-Founder, WinZO, Ex-Chief of Staff & Growth- ZO Rooms, Zostel, Ex-Times Group), are aggressively building the platform to not just capture market opportunities but also explore and maximize potential of social interactions as consumption drivers.

About Contest

CHASE challenge is an initiative by WinZO to drive young engineering minds towards ethical hacking and contribute to the robustness of the security processes at WinZO. We're committed to the safety and security of our services and to the integrity of its data. We look forward to working with the security community to find vulnerabilities in order to keep our businesses and customers safe.

Security at WinZO

Security is a crucial element at WinZO, and we're committed to protecting our users from all kinds of malicious activities and ensuring a secured playing experience. We take the security of our users very seriously and strive to investigate and resolve all reported vulnerabilities and exploits.

Challenge Details >>>

Eligibility

All students who are currently enrolled at an academic program in the following institutes are eligible to participate in the contest :-

1. IIIT Delhi
2. NSIT
3. IIT Delhi
4. Delhi Technological University

(All the participants would be required to register using their official college e-mail IDs for verification).

Timelines

Registration Starts	-	12:00 PM, 7th April, 2023
Event Launch Webinar	-	7:00 PM, 12th April, 2023
Challenge Submission Starts	-	12th April, 2023
Challenge Submission Ends	-	11:59 PM, 23rd April, 2023
Rewards Announcement	-	To be decided by the team.

Click here to Register

Program Rules

Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be eligible for a reward.

- Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
- When duplicates occur, we only award the first valid report that was received (provided that it can be fully reproduced).
- Multiple vulnerabilities caused by one underlying issue will be awarded one bounty.
- Social engineering (e.g. phishing, vishing, smishing) is prohibited.
- 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 the accounts provided by the organization.
- Security issues already known to WinZO will not be awarded in this program
- Security issues having a measurable business impact will only be considered for the rewards
- All the rewards, PPIs & Internship offer related decisions will be at the sole discretion of WinZO
- The bugs reported will be analyzed by the WinZO team and if they qualify under the conditions of the program, their severity will be identified through internal measures.

In-Scope Assets

WinZO Android App-Download URL
WinZO iOS App - Download URL

Report Submission

For all the identified vulnerabilities, below form shall be used to submit the report.
Link to the form - https://forms.gle/Wp8QSmzTmEpMMqhD7

Out-of-Scope Vulnerabilities

The following issues are considered out of scope:

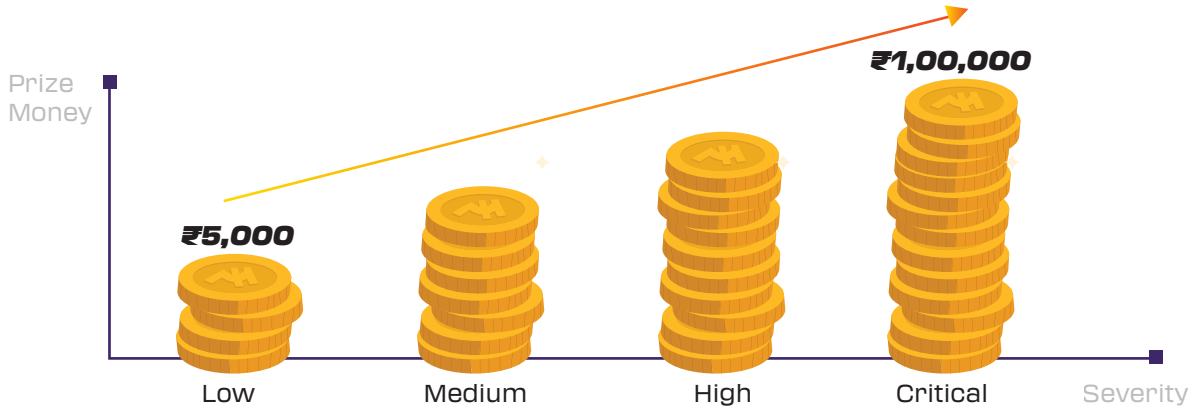
- Physical or social engineering attempts
- Mail configuration issues including SPF, DKIM, DMARC settings
- Best practice concerns like cookie is not marked secure and http only, missing HSTS, SSL/TLS configuration, missing security headers, etc.
- Reports that state that software is out of date/vulnerable without a proof-of-concept
- Highly speculative reports about theoretical damage
- Vulnerabilities as reported by automated tools without additional analysis as to how they're an issue
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- Subdomain takeovers - please demonstrate that you are able to take over the page by leaving a non-offensive message, such as your username
- CSV injection
- Rate limiting/Brute Force Attacks
- Content injection issues
- Clickjacking on pages with no sensitive actions
- Missing cookie flags on non-authentication cookies
- Issues that require physical access to a victim's computer/device
- Stack traces, Path disclosure or Directory listings
- Denial of Service(DoS) and Distributed Denial of Service(DDoS) attacks

Out-of-Scope Vulnerabilities for Android/iOS Application

- Exploits using runtime changes
- Snapshot/Pasteboard/Clipboard data leakage
- Android backup vulnerability
- Irrelevant activities/intents exported
- Android Application Permissions
- Local Data Storage Issues unless it is exploitable
- Application crashes

Rewards

Prize Money- The prizes can go from ₹5,000 to ₹1,00,000 for a bug reported depending on the severity of the bug as per CVSS framework along with the business impact associated with the bug.



Certificates and Goodies- All the winners will be awarded with exciting goodies, WinZO merchandise & certificates of excellence. All the participants will also receive certificates for their submissions

Internships & PPIs

Best performers are also eligible for Internships & Pre-placement Interview offers at WinZO.

Disclosure Policy

This is a private “Find a Bug” challenge, please do not discuss this program or any vulnerabilities (even resolved ones) outside of the program without express consent from the organization.

Our team is committed to addressing all security issues in a responsible and timely manner, and so we expect you to strictly adhere to the following guidelines -

- 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.
- Please submit a detailed description of the issue to us, along with the steps to reproduce it. We trust the security community to make every effort to protect our users’ data and privacy.
- 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 the explicit permission of the account holder.

T&Cs

- You must comply with all the laws of the platform as well as local laws of the country or region you reside in.
- Any conduct of the security researcher that at any time appears to be unlawful, violates the rules applicable may lead to disqualification of the submission and/or any possible reward earned.
- By submitting your report to WinZO, you’re agreeing to its use in checking for vulnerabilities exposed and subsequent security measures, as well as; any further external publishing and/or internal use of the same by WinZO.
- By participating in the program, you’re acknowledging the fact that WinZO won’t have any responsibility of any kind towards any damage caused by virtue of participating in this program directly or indirectly.

Contact us

For any queries regarding the challenge, kindly contact us at the below email address
security.team@winzogames.com