

FinSec Hackathon 2026 is the first edition of the inaugural national-level cybersecurity hackathon in India, organized at Westin, Powai, Mumbai, on 28 May 2026. The much-awaited cyber event in India is organized by DSCI. FinSec Hackathon 2026 pits teams of frontline defenders against each other in a series of challenges to explore and hunt threats from the Blue Team's perspective in a regulated and competitive environment, testing your knowledge, quick thinking, and expertise in cybersecurity. Teams will gain points by submitting tokens/flags to the scoring system.

Team Structure

1. **Operations Team:** Composed of individuals from the competition organizing staff. Any requests for assistance or complaints should be addressed to this team. SPOCs will be notified on the day of the event.
2. **Competition Team:** Refers to the duo participating in the contest.
3. **Team Captain:** A participant from the Competition Team designated as the Point of Contact (PoC). The Operations Team will engage with the Team Captain for all communication pertaining to the competition.

Competition Team Composition

1. On the day of the competition, the organizers will facilitate the Competition Teams with a physical workspace, internet access, electricity, and meals.
2. It is the responsibility of the Competition Teams to arrange and cover the costs of their own travel and accommodation for the event venue; the organizers will not reimburse any expenses incurred by the Competition Teams for their participation in the FinSec Hackathon.
3. Each Competition Team is allowed a maximum of two (2) members. The primary participant, or Team Captain, is required to submit the details of the second participant.
4. Competition Teams must submit all required participant information via the provided registration link before the registration deadline.
5. Any Competition Team that provides false information or an incomplete form will be disqualified. Teams must consist of members with Indian nationality and must submit government-issued photo identification and address proof.
6. All members of the Competition Team must fulfil the specified eligibility criteria.
7. All members of the Competition Team must be at least 18 years of age.
8. Throughout the competition, the Competition Team will designate a Team Captain to serve as the point of contact with the Operations Team, both prior to and during the event.
9. Members of the Competition Team are expected to conduct themselves in a professional and ethical manner at all times during the competition.

Game Conduct

1. All members of the Competition Team must adhere to the host site's policies and rules, which are in effect alongside the published game rules throughout the competition.
2. The Operations Team may classify any violations of the rules or unethical behaviour as unprofessional conduct if deemed intentional or malicious.
3. Teams are strictly forbidden from disclosing challenges, solutions, or sharing screenshots on social media or any public platforms. Non-compliance will lead to immediate disqualification and may result in legal proceedings, as necessary.
4. Teams must work on their own; collaboration with other teams or sharing answers to secure multiple rankings is considered unprofessional conduct.
5. All network activity is under surveillance. Any attempts to compromise the CTF infrastructure will be seen as a breach of the game rules, resulting in the offending teams being disqualified or banned from the event.
6. Competition Teams are prohibited from executing DDoS/DoS attacks against the challenges or the CTF infrastructure.
7. Rules made by the Operations Team are conclusive and must be followed.
8. There will be no extensions for work lost or flags not submitted due to hardware malfunctions.
9. Competitors will not receive extra time for breaks, including those for meals or restroom use. Access to the challenges will be terminated following the end of the competition.
10. Each challenge will explicitly mention whether the use of automated tools is permitted. For challenges where automated tools are not allowed, any use of such tools, including scripts, scanners, or automated frameworks, may lead to disqualification.
11. For challenges where automated tools are allowed, only one request per user is allowed for web challenges. For fuzzing activities, a maximum of two (2) threads is allowed.
12. The intent of the competition is to evaluate participants' technical skill, analytical thinking, and original problem-solving capability. The use of AI platforms or generative tools (e.g., ChatGPT, Claude, Gemini, GitHub Copilot, etc.) is prohibited. Any use of such tools will lead to disqualification.
13. The Competition Team is responsible for arranging their own setup and any tools they require, as the organizers will not supply any tools.
14. Credentials for the CTF platform will be issued to the Competition Teams before the event. Teams are expected to change the default login password on the CTF platform.

Scoring System and Winner Announcements

1. Scores will be determined according to the game descriptions outlined in the materials provided to the Competition Teams.

2. The Operations Team will be responsible for keeping track of scores, which will be displayed for public viewing during the competition. The display of scores will cease after the competition has ended.
3. The Operations Team reserves the right to demand supporting evidence or a detailed explanation for any completed challenge.
4. The organizers will evaluate and rank each team based on a set of predetermined criteria, and the final scores will be compiled to identify the winners according to the standards set by the organizers.
5. The Operations Team has the authority to modify or enhance the rules as necessary to ensure the smooth running of FinSec Hackathon 2026.
6. Rulings made by the Operations Team are conclusive and will stand as the final judgment.