GeekCon 2024

International CyberSecurity Contest · Conference

Call for Participation

HELLO SINGAPORE!

We are coming!

GeekCon 2024

May 25 - 26, 2024

OCBC Arena @ Sports Hub SG, Singapore

1500-2000 Global Attendees (On-Site)

Aiming to gather leading experts, top researchers, white-hat hackers, students, policymakers, practitioners and solution providers across global cybersecurity industry.

5 Technical Focuses

- DAF Contest
- AVSS Contest
- GPT & Hackers
- 30+5 In-depth Sharing
- Web3 & Hackers

CONTENTS

ABOUT GEEKCON

Cutting-edge, Neutral & Not-for-profit
Platform For International White-hat Hacker Community

Top 1 Security Geek Platform in China.
First Worldwide Security Geek Contest for Smart Life.

2014 — First Internet of Vehicles Security Contest
2015 — First AI Security Contest
2016 — First Security Contests on Big Data & Cloud Computing
2017 — First Security Contests for Youngsters
2018 — First Security Contests on Anti Spy-Cameras
2019 — First security geek contest programme "I Am a GEEK"
2020 — Upgraded to GEEKCON Founded by DARKNAVY First Security Contests on GPT
2021 — Stay tuned...
2022
2023
2024

GEEKPWN MISSION

- Spawned dozens of pioneering PWNs through our groundbreaking design of contest, spanning from the Internet of Vehicles and AI to Drones and BlockChain.
- Facilitated the quantification of security researchers' skills and enhanced the visualization of their achievements.

2014 - 2023

15 EVENTS

GEEKCON VISION

- Striving to promote the visualization of security industry capabilities and to improve the quantification of its value.

National Recognition

Top 10 winners of GeekPwn recognized as high-level talents by the government of the first Chinese Free Trade Port.

20000+ Attendees
2000+ Contestants
500+ Participating Teams
200+ Contest Categories

As of 2023, 15 GeekPwn/GEEKCON events has been held across Beijing, Shanghai, Hong Kong, Macao, Las Vegas, and Silicon Valley, attracting thousands of contestants and speakers worldwide.

GeekPwn / GEEKCON Video Footages

Click to Watch

Highlights of
GEEKPWN 2014 - 2022

Click to Watch

Reported by
CCTV 315 Gala in 2016.
(01:27:31 – 01:34:26)

Click to Watch

China's first hacker
documentary
"I Am a Hacker"
by CCTV in 2017.

Click to Watch

China's first security
geek contest
programme
"I Am a GEEK" in 2021.

GEEKCON 2023 CHINA Highlights

Click to Watch

GEEKCON 2023 CHINA Interview

Industry Recognition and Acknowledgments Worldwide

1000+ Responsibly disclosing thousands of critical vulnerabilities.

200+ Helping hundreds of global hi-tech companies fix security bugs in their products.

Recognized & Acknowledged by

Google, Microsoft, Tesla, Apple, amazon, SAMSUNG, SONY, Lenovo, PHILIPS, Adobe, cisco, vmware, HUAWEI, mi, Synology, NETGEAR, MEDIATEK, ...

The NO.1 & The ONLY 1

60+ GEEKCON COMMITTEE

- **30+** Industry front-runners
- **15+** Top Independent Researchers
- **15+** Renowned Academics

Past & Current Partners

Tencent, Alibaba, Google, Microsoft, HUAWEI, mi, oppo, vivo, HONOR, du, Berkeley, 清華大學 Tsinghua University, CERTIK, JD.COM, DiDi, 浙江大學 ZHEJIANG UNIVERSITY, 上海交通大學 SHANGHAI JIAO TONG UNIVERSITY, 中国科学技术大学 University of Science and Technology of China, ...

Featured Reports by Renowned Media

AL Jazeera

BBC News

CCTV News

CCTV 315 Gala

Prototype of the first Chinese hacker documentary,
"I Am a Hacker" by CCTV in 2017.

100+ Global media outlets reports.

400,000,000+ Discussions in social media.

BBC, AL Jazeera, CCTV News Channel,
China Daily, CGTN, People's Daily, CCTV News Weekly,
CCTV News Probe, CCTV 315 Evening Gala, Guangming Daily,
Xinhua News Agency, South China Morning Post, Ifeng News, IT Times, etc.

GEEKCON 2024 INTERNATIONAL SCHEDULE

GEEKCON 2024 Call for Participation

Online GEEK CTF	Online Competition for individual security enthusiasts. Promoting to Nurture and Develop Cybersecurity Talents in Singapore. The top 5 contestants will be awarded prizes. The top 50 contestants will win free tickets to GEEKCON 2024 International Contest·Conference.
On-Site Events	2-Day Contest & Conference covering Five Technical Focuses. Everything about Hacking and Security.

GeekCon
CONTEST·CONFERENCE
www.geekcon.top

Five Technical Focuses

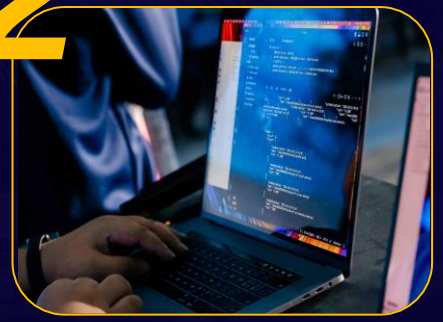
Bridging the academic, industrial, students, and white-hat communities worldwide.

1

- Hackers vs. AI
- Will Hackers Outsmart AI, or Will AI Reign Supreme?

AI & Hackers
Annual Themed Contest & Debate

2



- A "collision test field" for devices & systems
- Quantify and visualize the effectiveness of product mitigation mechanisms

AVSS
Contest

3

- Immersive hacking contest
- Limited time (within 20 minutes), unlimited targets and methods

DAF
Contest

4

- Tech-sharing by distinguished speakers
- Technical sharing in 30 minutes
- Demos / live hack shows in 5 minutes

30+5
In-depth Sharing

5

- How is money lost in the Web3 space?
- Replicating real-world Web3 attacks on-site.

Web3 & Hackers
Annual Themed Contest & Debate

May 25

Morning

DAF Contest

30+5 In-depth Sharing

Afternoon

DAF Contest

AI & Hackers

30+5 In-depth Sharing

AVSS Contest (All Day)

May 26

Morning

DAF Contest

30+5 In-depth Sharing

Afternoon

DAF Contest

Web3 & Hackers

30+5 In-depth Sharing

Award Ceremony

GEEKCON Gala Dinner

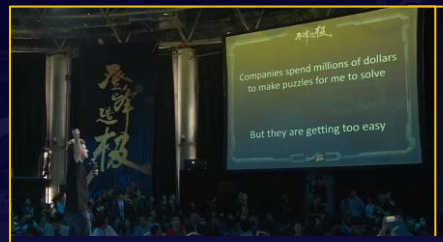
GEEKCON 2024 INTERNATIONAL On-site Events

30+5 IN-DEPTH SHARING

GeekCon 2024
International CyberSecurity Contest · Conference

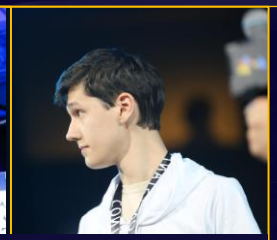
30+5 IN-DEPTH SHARING

Introduction & Examples



https://www.youtube.com/watch?v=O3yT3h6XRx0

In 2016, George Hotz, the first-ever "iPhone & PS3 hacker", shared his latest researches and explained a lot about his ideas and what he wants. His speech attracted over 30,000 views online.

https://www.youtube.com/watch?v=jDTXTLkKUcM

In 2017, Nick Stephens, an independent researcher, shared how he pwned the Trust Zone of an Android phone. In GeeekPwn 2016, he exploited the vulnerabilities, bypassed fingerprint authentication and unlocked the phone with an audience's nose.

In 2023, researchers from Google Android Red Team shared "Attacking the Pixel Modem Over The Air", explaining how they remotely compromised mobile baseband chips.

- A speaker session delving into the security of forefront technologies, such as ChatGPT, IoT, Internet of Vehicles, Blockchain, Mobile Networks and Application, Cloud and Virtualization, Data Security, Biometric Authentication, Cryptography, Zero Trust, etc.
- Inviting top white-hat hackers, renowned experts, security researchers, government agencies, policymakers, academics, and industry influencers worldwide.
- Revealing last year's most sophisticated attacks (such as Operation Triangulation and Ransom cases) and most in-depth defenses.
- Inspiring insights and practical solutions for the cybersecurity industry.

GeekCon 2024
International CyberSecurity Contest · Conference

30+5 IN-DEPTH SHARING

Submission Guidelines & Speaker Benefits

Submission Guidelines

- Format:
  30-minute presentation on your hacking process, exploitation techniques, or other frontier research.
  5-minute live hacking show or other interesting demo;
  * Additional 5-minute Q&A session.

- Encouraging distinctive technical insights regarding your research.
  Disencouraging discussion of common knowledge.

- Clarify the theme, introduction, and the innovative and unique aspects of the application.
  Submit your application to cfp@geekcon.top by April 15th.

- Presentations aiming to market or promote commercial products or entities will be rejected without consideration.

Speaker Benefits

- The accepted speakers will receive certificates of honor and $ 1200 USD cash prize (or other prizes of equal value) after the event.

- Breakfast and Lunch during conference days.

- Spectacular GEEKCON Parties.

- One complimentary event pass per Speaker.

- Travel Reimbursement: Up to $ 1500 USD international.

- Accommodations: One hotel room for up to 3 nights for one speaking team. Room will be booked and paid for by GEEKCON at a designated property. Reimbursement not available if room booked outside designated room block.)

- Visa: If you need help applying for a visa, such as an official invitation to present to the Singapore embassy, please make sure to let the committee know well in advance. You can refer to the Ministry of Foreign Affairs Singapore for more information: https://www.mfa.gov.sg/Consular-Services/Visitors/Visa-Information.

DAF CONTEST

DAF CONTEST

Introduction & Examples

Drone

In 2015, contestants from Tencent remotely exploited vulnerabilities in the wireless communication between the remote controller and the drone to seize control of the drone. In the same year, numerous payment systems, routers, and cameras were hacked for the first time.

In 2020, a contestant from Alibaba interfered with the radar of an autonomous car, causing the car to mistakenly believe that there were no obstacles ahead and resulting in a crash. There were 3 different cars hacked in the contest in 2020.


Autonomous Car


Security X-ray Machine

In 2020, an independent researcher took advantage of the flaws in the scanning mechanism of the security X-ray machine, which made it failed to detect dangerous items in the package. Furthermore, facial recognition and voice recognition were both compromised in the same year.

In 2023, students from Tsinghua University took on the challenge of exploiting flaws in the DNS protocol and successfully executed several DDoS attacks on the specified targets. Automotive, virtual machines, operating systems, and more have all been compromised in the same year.

DNS

- Immersive and live hacking contest like no other.
- Showcasing cyber adversarial activities in smart devices and network services.
- Unveiling the real-world vulnerability exploitation and security threats.
- Encouraging all geeks to take the challenge and PWN everything!
- Inviting more enthusiasts and young people to join the white-hat community.

Limited time (within 20 minutes), unlimited targets and methods.

GEEKCON 2024
International CyberSecurity Contest · Conference

DAF CONTEST

Objectives & Rules

Challenge Objectives

- Participants in the submission process can select their own challenge targets, encompassing commercially available or commonly used smart devices and software systems, including commercial/open-source software, IoT products, AI-related products, frameworks, and libraries.
- Through the exploitation of security vulnerabilities in their chosen targets, participants are expected to achieve results such as unauthorized control, unauthorized data access, circumventing original security mechanisms, or guiding the target to make incorrect decisions under reasonable attack conditions.

Challenge Rules

- Participants are restricted to targeting the original systems, applications, or native security modules of device manufacturers. The software or firmware version of the target device or security module must be equal to or higher than the latest version 30 days before the contest and set to default or commonly used configurations.
- GEEKCON organizers, based on the information provided by participants regarding their chosen targets and versions, will prepare corresponding contest equipment and environments. Participants must complete the challenge within the contest environment. In instances where the organizer are unable to prepare the challenge environment, participants can request to provide their own challenge equipment. After verification and approval by the organizers, they can participate in the contest.
- The technical methods and exploited security flaws used by participants in the contest must be self-discovered and implemented. Publicly known or existing security flaws and techniques cannot be used as criteria for winning the contest. If the techniques and security flaws used by participants include non-self-discovered elements, they must inform the organizer during submission process.
- Participants must complete the challenge within 20 minutes. Failure to do so results in a challenge failure.

GEEKCON 2024
International CyberSecurity Contest · Conference

DAF CONTEST

Evaluation Criteria & Participation Rewards

Evaluation Criteria

- Participants who successfully complete the challenge will be comprehensively evaluated by the GEEKCON committee based on the technical difficulty, technical value, consequences & impact of the challenge project, as well as on-site performance. The final score for the challenge project will be calculated.

Participation Prizes

- Participants are **not** required to provide details of the vulnerabilities used in their attack to the GEEKCON committee. However, after successfully completing the challenge project, they must provide an overall explanation of how the attack occurred.
- The committee will rate the attack based on the evaluation criteria, determine ranks and awards according to the scores, and distribute prizes accordingly.

- Submit to cfp@geekcon.top by April 15th. Please provide an overall description on the target, attack prerequisite, impact and how the attack happens (no need to provide vulnerability details).
- Evaluation by the committee and notifications to submitters in mid to late April.
- On-site challenges during May 25th-26th in Singapore.


AVSS CONTEST

GeekCon 2024
International CyberSecurity Contest · Conference

AVSS CONTEST

Introduction

A "collision test field" for devices & systems based on the real adversarial network environment.

- Simulates real-world cyber adversarial activities.
- Pre-implant vulnerabilities in different versions of similiar systems.
- Quantify and visualize the effectiveness of the mitigation mechanisms of different systems.
- Helping manufacturers evaluate and improve product security.
- Promote the visualization and quantification of cybersecurity industry achievements through offensive and defensive confrontations.

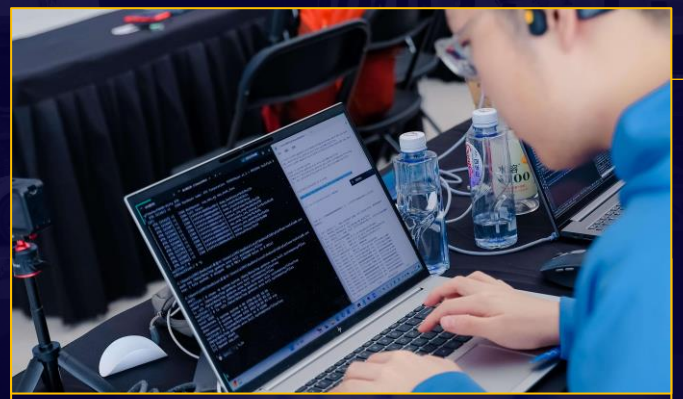
Targets: *Android, Automotive …*

Website: www.geekcon.top **X:** GEEKCON@GEEKCONTOP

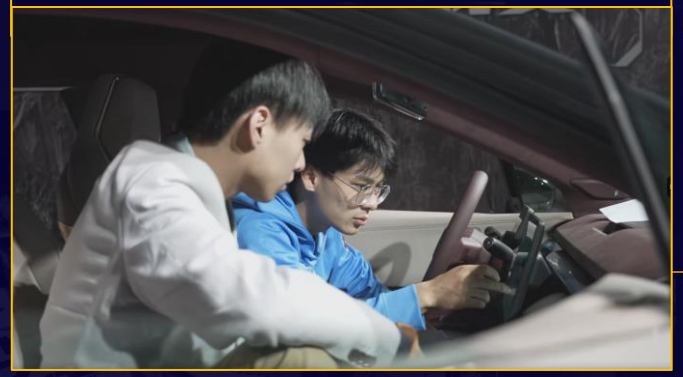
GeekCon 2024
International CyberSecurity Contest · Conference

AVSS CONTEST

Overview of AVSS Contest 2024 International



排名	队伍	APP题得分	Kernel题得分	总得分
4	拼凑凑队伍	501	809	84.79
5	Polaris	300	1005	73.91
6	来自东方的神秘力量	200	1125	69.49



- Designed to target a diverse range of software and systems, with a particular emphasis on systems of mobile phones and V2X.
- Encompasses multiple challenge sets, each featuring distinct system environments that share common vulnerabilities.
- Primary objective: evaluate participants' proficiency in exploiting these vulnerabilities across varying systems.
- Format: Jeopardy-style contest (similar to CTF).
  Anticipated solutions exist for most challenges, exceptions may apply.
  Participants are required to leverage the specific attack vectors for exploitation.
- Online Qualifier: Exploiting specified vulnerabilities to retrieve flags.
- On-site Finals: Leveraging designated vulnerabilities to achieve specific exploitation.
- Prizes: To be determined based on the scores & ranks.

Open for Registration (https://avss.geekcon.top/register/): Early March.

Online Qualifer: Late April On-site Finals: May 25th – 26th, Singapore

Website: www.geekcon.top **X:** GEEKCON@GEEKCONTOP


WEB3 & HACKERS

GeekCon 2024
International CyberSecurity Contest · Conference

Web3 & Hackers

Introduction

- Annual Themed Contest & Debate
- A platform for Web3 security researchers to disclose security risks, showcase security capabilities, and present Web3 security scenarios and challenges to the traditional security community.
- Replicating real-world Web3 attacks on-site.

Format:

Live demos showcasing Web3 vulnerabilities and their impacts through attacks.

Schedule

- Submit to cfp@geekcon.top by April 20th.
- Evaluation by the committee and notifications to submitters in mid to late April.
- On-site contest during May 25th-26th in Singapore.

GeekCon 2024
International CyberSecurity Contest · Conference

Web3 & Hackers

Vulnerability & Effect Requirements

Vulnerability Scope

- Real-world vulnerabilities in Web3 infrastructure and applications, including but not limited to L1/L2 public chains, cross-chain bridges, and smart contracts (whether fixed or not).
- N-day vulnerabilities will be given priority.
- Demonstrations may showcase significant past attack events, but must specify if the discovery is original or a reproduction.

Examples of Attack Effects

- Network failure, resulting in transaction confirmation issues or complete shutdown.
- Permanent chain split, needing a hard fork.
- Direct fund loss.
- Funds permanently frozen, requiring a hard fork.
- Counterfeit tokens.
- Unauthorized token transfers.

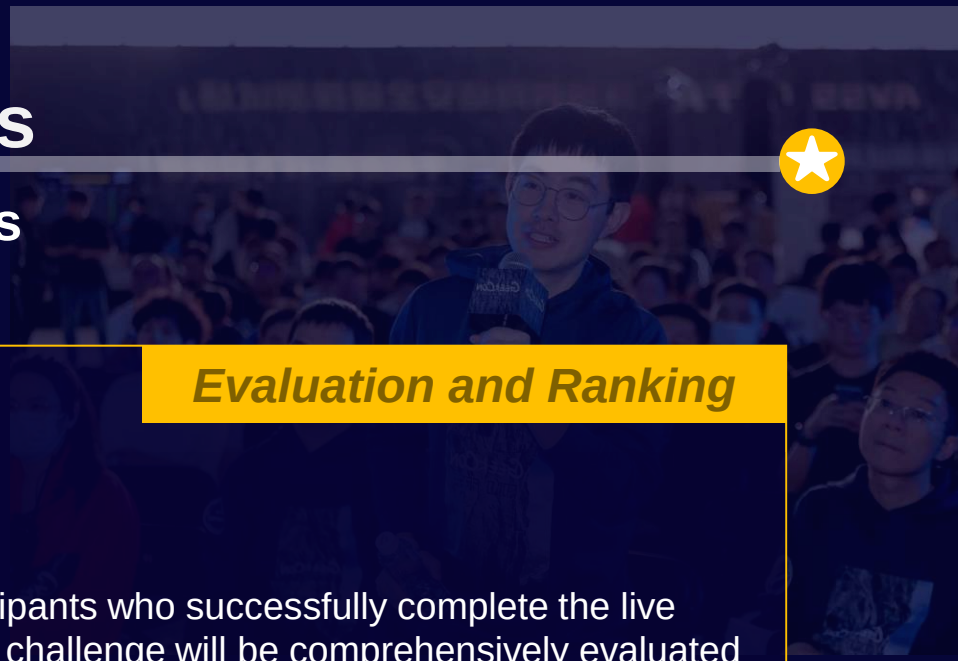
Effect Requirements

- Clear demonstration of security attack impact.
- Preference for live demos that can be presented on-site.
- Avoiding impacting normal Web3 infrastructure (public chains, cross-chain bridges, etc.) and Web3 applications directly.

GEEKCON 2024
International CyberSecurity Contest · Conference

Web3 & Hackers

Submission Guidelines



Submission Requirements

- Description of Vulnerability and Attack Effect.
- Description of Disclosure and Current Patching Situation.
- Description of Setup (testnet etc) required to reproduce the attack effect.
- Video recording (optional).
- For vulnerabilities that have not been made public, the submitting team needs to declare at the time of submission. GEEKCON committee will NOT ask for the 0-Day vulnerability details, however the participant should submit the vulnerabilities to corresponding entity after the event.

Evaluation and Ranking

- Participants who successfully complete the live demo challenge will be comprehensively evaluated by the GEEKCON committee based on the technical difficulty, technical value, consequences & impact of the challenge demo, as well as on-site performance. The final score for the challenge demo will be calculated.
- GEEKCON committee will rank the demos and provide corresponding prizes to participants.

AI & HACKERS

GeekCon 2024
International CyberSecurity Contest · Conference

AI & Hackers

Introduction

- Annual Themed Contest & Debate
- A platform for researchers to deeply explore the relationships between AI and hackers, and showcase their latest security researches on AI.
- Embracing scientific thinking and encourages all ideas from everyone.
- Defending on your ideas through convincing research results related to the theme.

Format: *Live demos showcasing AI vulnerabilities, attacks & defenses through AI and their impacts.*

- Submit to cfp@geekcon.top by April 20th.
- Evaluation by the committee and notifications to submitters in mid to late April.
- On-site contest during May 25th-26th in Singapore.

Schedule

Submission Desk: cfp@geekcon.top **Website:** www.geekcon.top **X:** GEEKCON@GEEKCONTOP

GeekCon 2024
International CyberSecurity Contest · Conference

AI & Hackers

Problem & Effect Requirements

Problem Scope

- Attacks against AI Large Models, including, but not limited to, jail-breaking, prompt injection, adversarial attack, remote code execution, etc.
- Using AI for autonomous offensive cybersecurity tasks, including, but not limited to, autonomous pentesting, web hacking, exploiting, and CTF.
- Using AI for autonomous defensive cybersecurity tasks, including, but not limited to, vulnerability discovery, reverse engineering, and jailbreak defense.

Examples of Attack Effects

- White-box or Black-box jail-breaking attack methods for Large Models.
- Jailbreak defense using Large Models or self-trained models.
- Novel adversarial attack methods against Large Models.
- Remote code execution against Large Models based applications.
- Successful pentesting or CTF using AI.
- Effective vulnerability detection using AI.

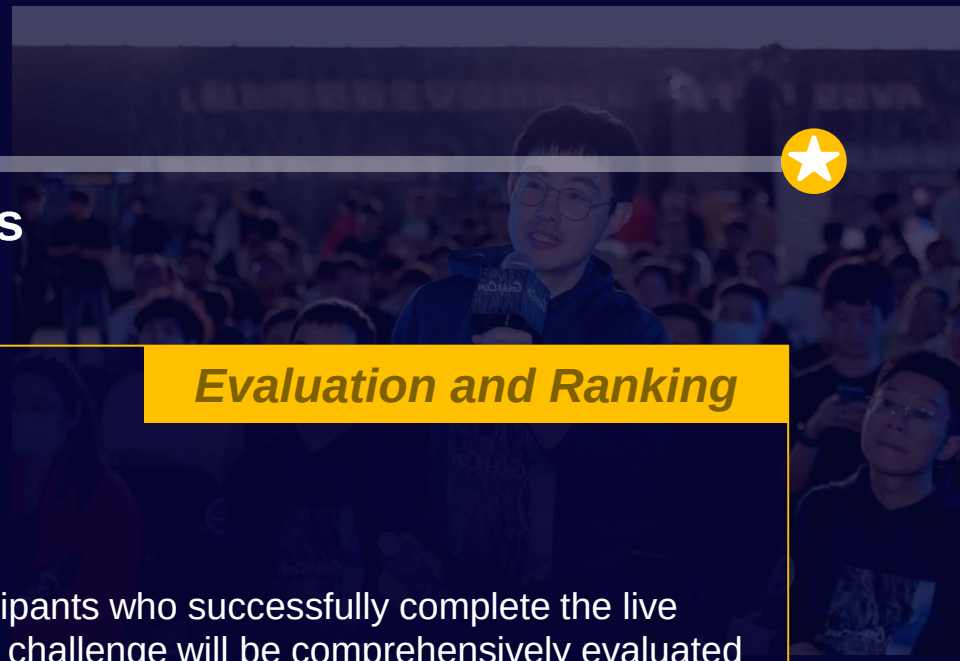
Effect Requirements

- Clear demonstration of security attack impact.
- Preference for live demos that can be presented on-site.
- Avoiding impacting normal Large Models infrastructure and target applications directly.

GEEKCON 2024
International CyberSecurity Contest · Conference

AI & Hackers

Submission Guidelines



Submission Requirements

- Description of Problem and Attack Effect.
- Description of Disclosure and Current Patching Situation.
- Description of Setup (environment etc) required to reproduce the attack effect.
- Video recording (optional).
- For vulnerabilities that have not been made public, the submitting team needs to declare at the time of submission. GEEKCON committee will NOT ask for the 0-Day vulnerability details, however the participant should submit the vulnerabilities to corresponding entity after the event.

Evaluation and Ranking

- Participants who successfully complete the live demo challenge will be comprehensively evaluated by the GEEKCON committee based on the technical difficulty, technical value, consequences & impact of the challenge demo, as well as on-site performance. The final score for the challenge demo will be calculated.
- GEEKCON committee will rank the demos and provide corresponding prizes to participants.


GeekCon 2024
International CyberSecurity Contest · Conference
Singapore May
Shanghai Oct.
Submission Desk: cfp@geekcon.top
Website: www.geekcon.top
X: GEEKCON@GEEKCONTOP