



MWC3 Cybersecurity Capture-the-Flag (CTF)

Sponsored by:



WESTERN MICHIGAN UNIVERSITY
Cybersecurity

Competition Rules & Guidelines

Competition Overview

The MWC3 Cybersecurity Capture-the-Flag (CTF) is a technical cybersecurity competition in which participants solve challenges to locate hidden “flags.” Challenges may include topics such as cryptography, reverse engineering, web exploitation, digital forensics, and general security concepts.

Participants earn points by successfully submitting flags discovered through analysis, exploitation, or investigation.

The objective is to apply technical cybersecurity knowledge in a controlled environment and demonstrate practical problem-solving skills.

Eligibility

Participants must be registered attendees of the MWC3 conference.

Teams may consist of:

- 1–2 competitors per team (unless otherwise specified by the competition organizers).
- Participants must compete under their registered name and institution.

Competition Format

The competition will follow a Jeopardy-style CTF format, where:

- Challenges are organized into categories.
- Each challenge is assigned a point value.
- Teams attempt to solve as many challenges as possible during the allotted competition time.
- Points accumulate based on successful flag submissions.
- Flags will typically follow a format such as:
 - `mwc3{example_flag}`

Allowed Resources

Participants may use:

- Personal laptops
- Local tools and scripts
- Standard cybersecurity tools (e.g. but not limited to, Wireshark, Burp Suite, Ghidra)
- Programming languages
- Public documentation and manuals
- General internet research
- Competitors are expected to rely primarily on their own technical knowledge and skills.

Prohibited Resources

The following are strictly prohibited during the competition:

Generative AI Tools

Use of any generative AI system is forbidden.

This includes but is not limited to:

- ChatGPT
- Gemini

- Copilot
- Claude
- Bard
- DeepMind tools
- Any AI-assisted coding or analysis tools
- Participants must also disable AI features embedded in software or IDEs.

Violation of this rule will result in immediate disqualification.

5.2 Collaboration Outside Your Team

Participants may not:

- Receive help from individuals outside their registered team
- Communicate with external experts for solutions
- Share flags or solutions with other teams

5.3 Attacking the Infrastructure

Participants may not:

- Attack the CTF platform itself
- Perform denial-of-service attacks
- Exploit infrastructure outside of intended challenge environments
- Interfere with other teams' machines

Only the systems explicitly provided as challenges may be targeted.

Flag Submission Rules

Flags must be submitted through the official scoring platform.

Submission rules:

- Flags must be exact
- Flags are case sensitive
- Each challenge flag may only be scored once per team
- Multiple submissions are allowed until the correct flag is found
- The latest valid submission before the deadline will count toward scoring.

Scoring

Points are awarded based on challenge difficulty.

The final leaderboard ranking is determined by:

- Total points
- Earliest submission time (in the case of ties)

Competition Duration

The competition will run during the scheduled MWC3 competition period.

Once the time expires:

- Flag submissions will close
- No additional scoring will occur

Teams are encouraged to submit flags before the deadline.

Integrity & Fair Play

Participants are expected to uphold professional and academic integrity.

Any of the following may result in disqualification:

- Cheating
- Use of prohibited tools
- Sharing solutions with other teams
- Interfering with competition infrastructure

Organizers reserve the right to review network traffic and system activity if suspicious behavior is detected.

Organizer Authority

Competition administrators and judges have final authority on:

- Rule interpretation
- Challenge scoring
- Disqualification decisions

Their rulings are final.

Final Notes

This competition is designed to challenge and develop cybersecurity skills through hands-on problem solving.

Participants are encouraged to:

- Think creatively
- Apply real-world security techniques
- Work collaboratively within their team

Good luck, and happy hacking.



Presented by WRAVEN – the Western Research Advisory for
Vulnerabilities, Exploits & Networks

Sponsored by the Western Michigan University Cybersecurity
Studies Center