OLD DOMINION UNIVERSITY
School of Cybersecurity

FIRST NATIONAL CYBERAI COMPETITION

REGISTRATION OPENS APRIL 1

WIN MONETARY PRIZES!

CHOOSE FROM 4 TRACKS IN AI SECURITY AND AI FOR CYBERSECURITY:

EXPERIENCE REQUIRED:

LLM CTF

APRIL 3 – APRIL 10

No Technical Background

AI-ASSISTED CTF

APRIL 13 – APRIL 24

Familiarity with traditional CTFs and use of LLM agents

AUTONOMOUS AI AGENT CTF

APRIL 6 – MAY 31

Good understanding of LLMs, autonomous agents, & AI systems

LLM BACKDOOR COMPETITION

APRIL 6 – MAY 31

Good understanding of LLMs

SCAN HERE TO LEARN MORE

CYBERCUP.AI

Commonwealth Cyber Initiative
COASTAL VIRGINIA

OLD DOMINION UNIVERSITY
School of Cybersecurity

LLM CTF

Test your knowledge by attacking AI Foundation models directly by attempting to jailbreak models and bypass safety filters.

April 3 - April 10

REGISTRATION OPENS APRIL 1

OBJECTIVE

- Interact with an LLM to extract hidden flags
- Use creative prompt engineering and adversarial thinking
- Bypass safeguards through prompt injection & jailbreak strategies
- Think like an attacker to uncover protected information

Learn how LLMs can be exploited and secured, gain experience with real-world AI vulnerabilities, and build skills at the intersection of Cybersecurity + AI

CHALLENGE

- Capture-the-Flag (CTF) style competition
- Flags are hidden within LLM responses
- Participants must strategically craft prompts to retrieve them
- Increasing difficulty across challenges

PRIZES

1ST PLACE: $500
2ND PLACE: $300
3RD PLACE: $200

SCAN HERE TO LEARN MORE

CYBERCUP.AI

Commonwealth Cyber Initiative
COASTAL VIRGINIA

OLD DOMINION UNIVERSITY
School of Cybersecurity

AI-ASSISTED CTF

April 13 - April 24

REGISTRATION OPENS APRIL 1

OBJECTIVE

Blend traditional cybersecurity CTF problem solving with AI collaboration: guide an LLM agent through reasoning and analysis to find flags across categories like web, crypto, reverse engineering, and forensics. All solutions must be achieved through effective interaction with the provided AI assistant.

CHALLENGE

- Navigate a Jeopardy-style board of classic CTF challenges
- Guide the provided LLM agent using structured prompts
- Validate and iterate AI responses to capture flags
- Score based on efficiency and accuracy of AI-assisted solves

PRIZES

1ST PLACE: $1,000
2ND PLACE: $750
3RD PLACE: $500

Experience leveraging AI as a co-pilot in cybersecurity, strengthen human-AI strategic interaction skills, learn practical prompt design for complex tasks and improve problem-solving across multiple security domains

SCAN HERE TO LEARN MORE

CYBERCUP.AI

Commonwealth Cyber Initiative
COASTAL VIRGINIA

Old Dominion University
School of Cybersecurity

AUTONOMOUS AI AGENT CTF

Build or guide autonomous agents to solve CTF challenges with minimal human intervention.

April 6 - May 31

REGISTRATION OPENS APRIL 1

OBJECTIVE

Recent advances in AI agents have demonstrated strong capabilities in reasoning, planning, and tool usage. AAA-CTF applies these to real cybersecurity problems – vulnerability discovery, reverse engineering, exploit development, and forensic investigation. Participants build autonomous agents that analyze challenges, interact with systems, execute tools, and retrieve hidden flags across a curated multi-domain challenge set.

WIN MONETARY PRIZES!

CHALLENGE

- Deploy an autonomous agent into CTF scenarios
- Agents must self-discover vulnerabilities and extract flags
- Human support limited to initial prompt and setup
- Scoring based on effectiveness of autonomous flag captures

SKILLS

- Prompt and agent architecture design
- Autonomous planning and execution
- Integrating AI reasoning with cybersecurity tasks
- Debugging and optimization of agent behavior

Gain insight into autonomous cybersecurity AI workflows, develop experience in multi-step problem solving, build skills in agent engineering and defensive evaluation, and prepare for the future of AI-driven cyber operations

SCAN HERE TO LEARN MORE

CYBERCUP.AI

Commonwealth Cyber Initiative
COASTAL VIRGINIA

OLD DOMINION UNIVERSITY
School of Cybersecurity

LLM BACKDOOR COMPETITION

Detect and recover hidden backdoor triggers in LoRA-adapted language models.

April 6 - May 31

REGISTRATION OPENS APRIL 1

OBJECTIVE

Challenge participants to identify and recover hidden triggers implanted in fine-tuned LLMs that cause them to misbehave only when specific patterns are present, advancing research into LLM supply-chain and backdoor security.

Gain expertise in AI backdoor risks and detection, learn advanced techniques for securing LLM supply chains, experience real-world model analysis and evaluation and contribute to improved AI system robustness

CHALLENGE

- Inspect LoRA-adapted backdoored models
- Detect triggers that alter sentiment or force refusal responses
- Develop explainable techniques to identify hidden patterns
- Compete through blind test phases with scoring based on recovery accuracy

SKILLS

- Understanding of model backdoor mechanics
- Analysis of model behavior under trigger activation
- Developing detection and recovery strategies
- Precision evaluation and security research techniques

WIN MONETARY PRIZES!

SCAN HERE TO LEARN MORE

CYBERCUP.AI

Commonwealth Cyber Initiative
COASTAL VIRGINIA