

# STALA 2027

## Workshop on Security Testing and Assurance for LLMs and Agents

Systematic Testing → Security Evidence → Quantitative Assurance



Co-located with

**NDSS 2027**

Seoul, Republic of Korea

Workshop: 22 March 2027



# CALL FOR PAPERS

Paper submission deadline:

**11 December 2026, 23:59 AoE**

### Topics include:

- LLM and agent security testing
- Fuzzing and automated red teaming
- Jailbreak and prompt-injection testing
- Agent hijacking and tool security
- RAG, memory and context poisoning
- Privacy leakage and backdoors
- Defense and guardrail evaluation
- Sandboxing and access-control testing
- Long-horizon and multi-agent testing
- Coverage and test adequacy
- Residual-risk and assurance methods
- And more... (check our website!)

### Submission formats:

- **Full papers:** up to 8 pages, excluding references
- **Short, position & experience papers:** up to 4 pages, excluding references

Negative results, benchmark/dataset contributions, early methods and experience reports are welcome!

Papers will be submitted via HotCRP, with accepted papers published in the proceedings by the Internet Society!



Workshop website:

<https://stala-workshop.github.io>



Scan for STALA website

### Organising Committee

Lichao Wu

Wenkai Xu

Stjepan  
Picek

Alexandra  
Dmitrienko

Nan Lu

University of Bristol

University of  
Warwick

University of Zagreb &  
Radboud University

University of  
Duisburg-Essen

University of Bristol