

Willkommen!



Agenda

IRIS-Side Event 07.06.2024, Sem. A.1.10			
Special Topic: Security Gamefication & AI			
Start	Ende	Themen	Vortragende
13:00	13:10	Welcome	Stefan Eder
13:10	14:00	OWASP Top 10 for Large Language Model Applications and other resources	Peter Kieseberg
14:00	14:30	Cyber Exercises auf Europäischem Level	Timea Pahi
14:30	15:00	Pause	
15:00	15:30	Tabletop Exercises für Jurist*innen	Peter Kieseberg
15:30	16:00	Addressing the challenges of Insider Threat with AI	Gregor Langner
16:00	16:30	PenQuest & Reinforcement Learning	Sebastian Eresheim
16:30		After Work	

OWASP Top 10 for Large Language Model Applications



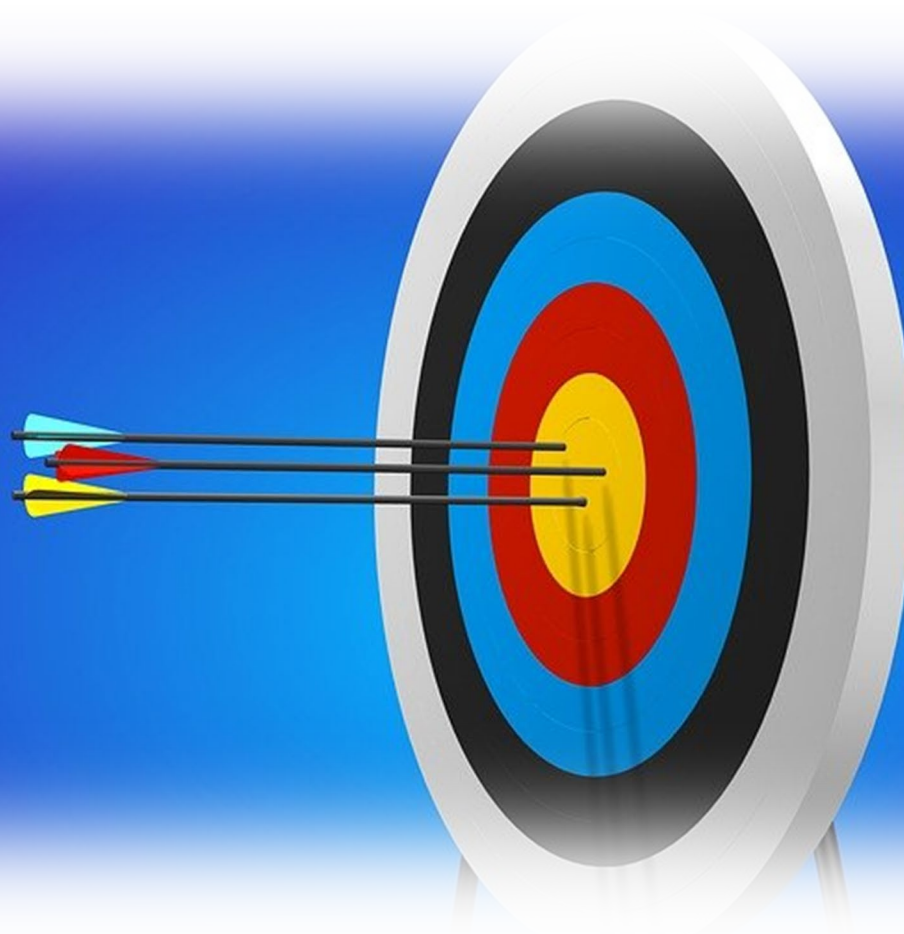
Important technology



Legal aspects



Targeting AI – AI as Attack Vector



What to look for now?





OWASP Top 10 for LLM Applications

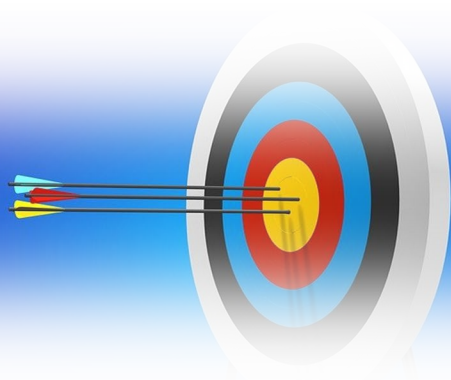
Structure

- Description
- Common Examples of Vulnerability
- Prevention and Mitigation Strategies
- Example Attack Scenarios
- Reference Links



10, 9 ...

- LLM01: Prompt Injection
- LLM02: Insecure Output Handling
- LLM03: Training Data Poisoning
- LLM04: Model Denial of Service
- LLM05: Supply Chain Vulnerabilities
- LLM06: Sensitive Information Disclosure
- LLM07: Insecure Plugin Design
- LLM08: Excessive Agency
- LLM09: Overreliance
- LLM10: Model Theft



OECD AI Incidents Monitor (AIM)



 Enter a concept or a keyword and press enter. Use advanced options to further narrow the search.

Reset

ADVANCED SEARCH OPTIONS ^

Date range:

Last week



Country

Austria

Industry

Select industry

AI principle

Select AI principle

Severity

Select severity

Harm type

Select harm type

Affected stakeholders

Select affected stakeholders

Type of search

Any of the concepts/keywords (OR)



☐ Future threats only

The Future



Conclusions



Contact: Peter Kieseberg

Institute of IT Security Research

St. Pölten University of Applied Sciences

Campusplatz 1, 3100 St. Pölten

peter.kieseberg@fhstp.ac.at

