



Sandy Dunn
Quark IQ LLC
sandy@quarkiq.com

HACKFORT 2024

Great AIML Resources

OWASP Resources

[OWASP Top 10 for Large Language Model Applications](#)

[OWASP Top 10 for LLM Website](#)

[OWASP LLM AI Cybersecurity & Governance Checklist](#)

[OWASP LLM Verification Standard](#)

Research Papers

[Ignore This Title and HackAPrompt: Exposing Systemic Vulnerabilities of LLMs through a Global Scale Prompt Hacking Competition](#)

[FakeWatch \faEye: A Framework for Detecting Fake News to Ensure Credible Elections](#)

[Beyond Memorization: Violating Privacy Via Inference with Large Language Models](#)

Great Presentation on AI & Security

[Lakera AI : Lessons Learned from Crowdsourced LLM Threat Intelligence](#)

Learn Prompting

[Learnprompting.org](#)


Deep Fakes

[FBI-NSA-CISA Contextualizing Deepfake Threats to Organizations](#)

Chatbots & Models

Perplexity	Perplexity AI is a chatbot-style search engine that uses natural language processing (NLP) and machine learning to provide answers to user queries.
ChatGPT	Still the one
Grog	Exists to show speed but it is very fast!
HuggingFace	The Hugging Face Hub is a platform that allows users to host, share, and collaborate on machine learning models, datasets, and applications. It acts as a hub for the AI community.
Gemini (Google)	Good at vision (understanding images)
Claude	Considered leading with safety
POE	Access to multiple models

AIML & Prompting Classes

Coursea Generative AI with Large Language Models	Excellent Course
Microsoft AI for Beginners	
Prompt Engineering for ChatGPT	
Ronnie Shear 	Taken quite a few - favorite LinkedIn Instructor

Google AI Courses	
AWS Foundations of Prompt Engineering	
Data Camp	Taken several and paid for annual - good
Kaggle	Buzzed through a few

AIML Podcasts	
The AI Breakdown	Newsletter Podcast
This Day in AI	Podcast
Machine Learning Street Talk	Podcast
The AI Breakdown	Newsletter Podcast
MLSecOps	Podcast

Good AI Books		
The New Fire: War Peace and Democracy in the Age of AI	Ben Buchanan	The politics in AI
The Myth of Artificial Intelligence	Erik J. Larson	
Not with a Bug, but with a Sticker	Ram Shankar Siva Kumar (Author), Hyrum Anderson (Author),	AI Security Challenges
AI Super Powers	Kai-Fu Lee	
The Alignment Problem	Brian Christian	

