Mindluster Platform

About the course Hacking generative Ai

Course Presenter : IBM Technology

Hacking generative Ai, in this course we will learn about the techniques and strategies used to analyze, test, and potentially exploit generative AI systems like ChatGPT, DALLÂ·E, and other large language models. You'll explore real-world methods such as prompt injection, jailbreak attacks, and adversarial prompting, as well as how these methods can bypass ethical filters and safety restrictions. The course also covers data leakage risks, reverse engineering model behavior, and simulating AI red teaming scenarios. Throughout, weâ€™ll emphasize ethical considerations and defensive countermeasures to build more secure AI systems. By the end of the course, you'll understand how generative models can be vulnerableâ€”and how developers and security experts can protect them. Prepare to dive deep into the inner workings of generative AI and its security landscape. IBM Technology

Computer Science Category's Courses

Course Lesson(16)

Lesson 1 : **AI Realism with NE YO and Ed Ulbrich How AI affects artists from IP to CGI**

Lesson 2 : **Gen AI for Good with James Hodson Using AI to create a better tomorrow today**

Lesson 3 : **Change Agents with Ethan Mollick How AI agents will reinvent productivity**

Lesson 4 : **Hacking generative AI Limiting security risk in the age of AI**

Lesson 5 : **AI Pilots to Progress The lowdown on what makes AI projects successful**

Lesson 6 : **Leaders v learners It all comes down to AI accessibility with Reshma Saujani**

Lesson 7 : **Can you afford gen AI**

Lesson 8 : **Not just a chatbot Build virtual agents that are actually helpful with gen AI**

Lesson 9 : **Rewriting the future how devs are driving gen AI**

Lesson 10 : **How AI helps you win Fantasy Football with ESPN s Greeny**

Lesson 11 : **Modernizing code with AI Code Assistants**

Lesson 12 : **Use generative AI to help save people from screaming â€œrepresentativeâ€**

Lesson 13 : **The human side of HR â€” Fostering genuine connections with AI**

Lesson 14 : **Scale your tech with a dynamic duo â€” AI and hybrid cloud**

Lesson 15 : **The art of delegating to AI Using AI agents and chatbots to do the boring work**

Lesson 16 : **AI in Action Podcast Trailer**

Related courses

Linear Algebra for Computer Scientists

Insertion Sort

Bubble Sort

GCSE Computer Science

Random Access Memory

Binary Trees

for Business Contact
business@mindluster.com