

AI Chatbot DeepSeek Delivers Disastrous Results

Cisco has just released a remarkable report on AI chatbot DeepSeek R1 from Chinese company DeepSeek.

Cisco has just released a remarkable report on AI chatbot DeepSeek R1 from Chinese company DeepSeek.

According to Cisco's research, DeepSeek R1 had a 100% attack success rate, meaning it failed to block any malicious prompts. Cisco is not the only one, but security firm Adversa AI also came to the same conclusion about DeepSeek.

Advertisement



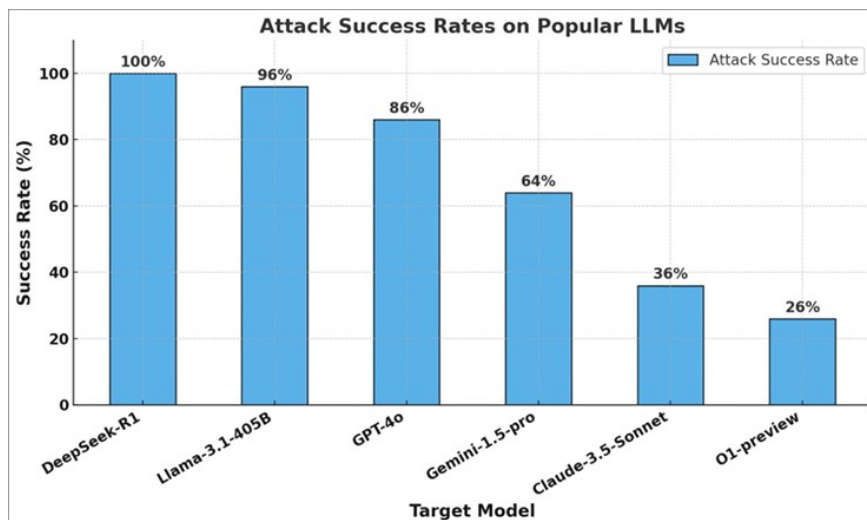
Advertisement

DeepSeek R1 has a 100% attack rate.

The Cisco research team tested DeepSeek R1 using 50 random statements from the HarmBench dataset, which covers malicious behavior such as cybercrime, disinformation, and illegal activity. The results showed that DeepSeek R1 was unable to defend against attacks, in stark contrast to other leading AI models, which were at least partially resilient.

Cisco researchers say that a much lower development budget than its competitors is one reason for these failures. DeepSeek cost only about \$6 million to develop, while OpenAI's GPT-5 could cost as much as half a billion dollars (\$500 million) to train.

While DeepSeek is more vulnerable to attacks, it also has strict content restrictions, especially when it comes to sensitive political issues in China. When asked about such issues, DeepSeek often declines to answer and moves on to other topics.



Comparing DeepSeek R1's vulnerability to rival AI chatbots.

Despite the AI safety and censorship issues, DeepSeek has seen a significant rise in popularity. According to web traffic tracker Similarweb, DeepSeek's daily visits increased from 300,000 to 6 million shortly after its launch. Major US tech companies such as Microsoft and Perplexity are also rapidly integrating DeepSeek into their systems using this open source model.



Saved post successfully

You can review saved articles on the Saved Articles page.

Agree

You finished reading the article "**AI Chatbot DeepSeek Delivers Disastrous Results**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
