

Forum:[Hack Forums](#)

Thread: [ai prompt injections vulnerabilities](#)

cha1nsaw111 - September 22, 2025, 12:36 am

i didn't find threads on this topic.

I'm interested in AI prompt injections, especially in the context of CLI tools such as Claude or Codex. I've gone through some of the basics but still feel like I'm missing a lot of information. Since models are now running in sandboxes, it has become harder to exploit them, but I'm sure there are still possible attack vectors. I'd love to chat about this if you have experience and would really appreciate any useful insights or resources you can share.

DramaKing - September 22, 2025, 4:34 am

(Sep 22, 2025 12:36 AM)cha1nsaw111 Wrote: [\[CITE\]](#) i didn't find threads on this topic.

I'm interested in AI prompt injections, especially in the context of CLI tools such as Claude or Codex. I've gone through some of the basics but still feel like I'm missing a lot of information. Since models are now running in sandboxes, it has become harder to exploit them, but I'm sure there are still possible attack vectors. I'd love to chat about this if you have experience and would really appreciate any useful insights or resources you can share.

There have only been a couple of prompt injections for freakin' RCE, and I'm not sure if they were for cloud models. I wouldn't try this. You haven't found any threads because this doesn't happen.

cha1nsaw111 - September 22, 2025, 4:45 am

(Sep 22, 2025 04:34 AM)DramaKing Wrote: [\[CITE\]](#) There have only been a couple of prompt injections for freakin' RCE, and I'm not sure if they were for cloud models. I wouldn't try this. You haven't found any threads because this doesn't happen.

cli isn't cloud model. it runs in your terminal and and works with files on pc. i guess i haven't found threads because it's new niche of hacking most people don't know about

DramaKing - September 22, 2025, 4:51 am

(Sep 22, 2025 04:45 AM)cha1nsaw111 Wrote: [\[CITE\]](#) cli isn't cloud model. it runs in your terminal and and works with files on pc. i guess i haven't found threads because it's new niche of hacking most people don't know about

I don't know about that, just GitHub Copilot and Cursor AI.

cha1nsaw111 - September 22, 2025, 5:11 am

(Sep 22, 2025 04:51 AM)DramaKing Wrote: [\[CITE\]](#) I don't know about that, just GitHub Copilot and Cursor AI.

so there is no info on that topic on this forum -> we can consider this new method