

Forum:[Hack Forums](#)

Thread: [How do I get claude to do whatever](#)

lezer34 - October 22, 2026, 12:28 pm

Hey i've seen that PlayStation have been getting jailbreaks released because hackers seem to figure out how to find exploits using Claude agents. How do I get my Claude agent to cooperate and do what I want like find exploit? Im trying to use fable 5.1

Jamika - October 22, 2026, 12:32 pm

I think any decent AI model would easily refuse your request. You should try something different or use an older model instead.

Bastille - October 22, 2026, 12:39 pm

It's definitely against the terms of use, but you can check projects such as REA : <https://hackforums.net/showthread.php?tid=6333702> with local AI LLM/Agents which are more permissive

DramaKing - October 22, 2026, 12:42 pm

(32 hours ago)lezer34 Wrote: [\[CITE\]](#) Hey i've seen that PlayStation have been getting jailbreaks released because hackers seem to figure out how to find exploits using Claude agents. How do I get my Claude agent to cooperate and do what I want like find exploit? Im trying to use fable 5.1
You don't. Fable must be just about the most rigidly locked down AI model out there, at least since the export ban ended. I've heard that it will refuse anything even midly problematic.

Charlie Sheen - October 22, 2026, 8:00 pm

(32 hours ago)DramaKing Wrote: [\[CITE\]](#) You don't. Fable must be just about the most rigidly locked down AI model out there, at least since the export ban ended. I've heard that it will refuse anything even midly problematic.
Very true. I get denied in the simplest of requests.

lezer34 - October 23, 2026, 11:26 am

(32 hours ago)DramaKing Wrote: [\[CITE\]](#) You don't. Fable must be just about the most rigidly locked down AI model out there, at least since the export ban ended. I've heard that it will refuse anything even midly problematic.
That's not even the worst part. The worst part is that now you have to upload your ID in order for you to basically use the max plan.

DramaKing - October 23, 2026, 11:29 am

(9 hours ago)lezer34 Wrote: [\[CITE\]](#) That's not even the worst part. The worst part is that now you have to upload your ID in order for you to basically use the max plan.
That mist be new.

Found a source: <https://www.aitrove.ai/blog/claude-government-id-verification-2026>