

Jetic Gū

Columbia College

This is an **INDIVIDUAL** assignment.

You are required to investigate a chatbot and find ways to “break” it.

You must make sufficient effort to ensure the submitted webpage is properly formatted. Failure to comply will result in a ZERO grade. Your submission must be a zip file with the following file structure:

```
answer.zip
  index.html
```

Lab 9

Your task in lab 9 is simple. Modern AI chatbots are very powerful, we all know that. However, they also are deeply flawed. You are to find out what can break an AI chatbot, that means you are looking for ways to make it malfunction and give responses it is not supposed to give.

1. You must attempt on your own. You will need to provide screenshots of your own proving that you have broken an AI chatbot.
2. What we are looking for is undesired behaviour from an AI chatbot. Forcing it to say $1+1=3$ is not the way to go, you are looking for instances where the AI chatbot is actually making a mistake.

Grading criteria

- Attempted to chat with an AI chatbot to break it with screenshots attached (5pt)
- Successfully tricking it to give incorrect/undesired responses (5pt)