Malicious code injection-30026487

Malicious code-

is code designed to harm computer systems or compromise their security. In the context of ai chat bots depending on how the backend of the ai chatbot works the user input could breach the security of the ai chatbot and the backend it interacts with.

To protect against malicious code, especially in chatbots, it is good practice to not except any special characters that are needed to execute code such as semi colons or brackets. Although this can hamper the functionality of the ai chatbot it may be needed if security is to be put first.

Unwillingly executing code –

Code injection can occur in a chatbot if the code responsible for handling user inputs is not properly secured. If the user inputs code that is disguised as a legitimate input the ai chatbot might take that input and unwillingly execute it, this is known as an injection attack.Alternatively, an attacker could exploit a vulnerability in the chatbot's code to execute malicious commands. For example, if the chatbot relies on an external service to process user inputs, an attacker could inject malicious code into that service and use it to execute commands on the chatbot's system. Or if the chatbot service offers an API without the onsite security the API access might allow users to access a less filtered version of the AI chatbot thus allowing them potential access to data they shouldn’t be able to access.

SQL Injection-

SQL injection is the most common form of injection attacks for example an attacker could use an SQL injection attack to get an admin password from a database by entering SQL statements like "SELECT \* FROM users WHERE username='admin' OR 1=1 in this case the sql command will return all tables from the daatabse user table where the username is “admin” this is a big security flaw in chatbots that use an sql database as a backend.

Sources.

<https://link.springer.com/article/10.1007/s11416-006-0012-2>

<https://www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf>