Khoi Duong

Prof. Chang

CS589

2/29/2024

WEEK 6 HW1

01 ==> Agent: Search Wikipedia

GitHub source code: https://github.com/MynameisKoi/CS589/blob/main/Agents

Before we start, *python3 -m venv venv* and *source ./venv/bin/activate* to go to the virtual environment.

Next, install the requirements with *pip install -r requirements.txt*

Then, we apply the code from Agents to paste into our app.py

Run our code and we have a problem:

```
(venv) koiisme@DESKTOP-LVBMC2V:~/CS589/Agents$ python3 app.py
Traceback (most recent call last):
   File "/home/koiisme/CS589/Agents/app.py", line 46, in <module>
     from langchain.agents.agent toolkits import create python agent
   File "<frozen importlib. bootstrap>", line 1075, in handle fromlist
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
/agents/agent_toolkits/__init__.py", line 50, in __getattr__
relative_path = as_import_path(Path(__file__).parent, suffix=name)
File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
_core/_api/path.py", line 30, in as_import_path

path = get_relative_path(file, relative_to=relative_to)
   File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
_core/_api/path.py", line 18, in get_relative_path
     return str(file.relative to(relative to))
  File "/usr/lib/python3.10/pathlib.py", line 818, in relative_to
raise ValueError("{!r} is not in the subpath of {!r}"
ValueError: '/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/lang chain/agents/agent_toolkits' is not in the subpath of '/home/koiisme/CS589/Age
nts/venv/lib/python3.10/site-packages/langchain core' OR one path is relative
and the other is absolute.
(venv) koiisme@DESKTOP-LVBMC2V:~/CS589/Agents$
```

It turns out that additional code to langchain_experimental to resolve the security problem of LangChain (Stack Overflow Q&A & Arbitrary Code Execution in langchain | CVE-2023-39659 | Snyk)

Here is the solution from Stack Overflow:

It seems in October 2023, some logic related with agents was moved to a module called "experimental".

You first need to install this new library:

```
pip install langchain_experimental
```

and then shift the module from where you import certain classes. *PythonREPLTool* and *create_python_agent* needs to be imported from the new langchain_experimental module while other classes remain still.

Classes that need to be imported from the new module:

```
from langchain_experimental.agents.agent_toolkits import create_python_agent
from langchain_experimental.tools.python.tool import PythonREPLTool
```

Classes that still use the old notation:

```
from langchain.python import PythonREPL
from langchain.agents import load_tools, initialize_agent
from langchain.agents import AgentType
```

For more information you can read this thread: https://github.com/langchain-ai/langchain/discussions/11680

Update the requirements.txt and install langchain experimental

Change line 46 in app.py into:

```
from langchain_experimental.agents.agent_toolkits import create_python_agent Also line 49:
```

```
from langchain experimental.tools.python.tool import PythonREPLTool
```

Run again and we see that:

```
(venv) koiisme@DESKTOP-LVBMC2V:~/CS589/Agents$ python3 app.py
/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain/chat mo
dels/ init .py:31: LangChainDeprecationWarning: Importing chat models from l
angchain is deprecated. Importing from langchain will no longer be supported a
s of langchain==0.2.0. Please import from langchain-community instead:
`from langchain community.chat models import ChatOpenAI`.
To install langchain-community run `pip install -U langchain-community`.
  warnings.warn(
/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain core/ a
pi/deprecation.py:117: LangChainDeprecationWarning: The class `langchain commu
nity.chat_models.openai.ChatOpenAI` was deprecated in langchain-community 0.0.
10 and will be removed in 0.2.0. An updated version of the class exists in the
langchain-openai package and should be used instead. To use it run `pip insta
11 -U langchain-openai and import as from langchain_openai import ChatOpenAI
  warn deprecated(
Traceback (most recent call last):
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
/chains/llm_math/base.py", line 50, in raise_deprecation
    import numexpr # noqa: F401
ModuleNotFoundError: No module named 'numexpr'
```

The terminal guides us to change line 51 in the code into:

```
from langchain_openai import ChatOpenAI
```

Run again and we see:

```
Traceback (most recent call last):
  File "/home/koiisme/CS589/Agents/app.py", line 63, in <module>
    tools = load_tools(["llm-math", "wikipedia"], llm=llm)
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
/agents/load_tools.py", line 596, in load_tools
    tool = LLM TOOLS[name](llm)
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
/agents/load_tools.py", line 152, in _get_llm_math
    func=LLMMathChain.from llm(llm=llm).run,
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
/chains/llm_math/base.py", line 186, in from_llm
    return cls(llm chain=llm chain, **kwargs)
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
core/load/serializable.py", line 120, in init
    super(). init (**kwargs)
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/pydantic/
v1/main.py", line 339, in init
   values, fields set, validation error = validate model( pydantic self .
class , data)
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/pydantic/
v1/main.py", line 1048, in validate model
    input data = validator(cls , input data)
  File "/home/koiisme/CS589/Agents/venv/lib/python3.10/site-packages/langchain
/chains/llm math/base.py", line 52, in raise deprecation
    raise ImportError(
ImportError: LLMMathChain requires the numexpr package. Please install it with
 pip install numexpr`.
(venv) koiisme@DESKTOP-LVBMC2V:~/CS589/Agents$ pip install numexpr
Collecting numexpr
  Downloading numexpr-2.9.0-cp310-cp310-manylinux 2 17 x86 64.manylinux2014 x8
6 64.whl (375 kB)
                                      --- 375.2/375.2 KB 4.3 MB/s eta 0:00:00
Requirement already satisfied: numpy>=1.13.3 in ./venv/lib/python3.10/site-pac
kages (from numexpr) (1.26.4)
Installing collected packages: numexpr
```

The solution is to install numexpr with *pip install numexpr*

All updates on what to install are updated in requirements.txt

Run again and we have the result:

```
> Entering new AgentExecutor chain...
Thought: I need to use a calculator to find the answer to this math problem.
Action:
  "action": "Calculator",
  "action_input": "300*0.25"
Observation: Answer: 75.0
Thought: Could not parse LLM output: I have successfully calculated the answer to the math problem.
Observation: Invalid or incomplete response
Thought: I need to use a calculator to find the answer to this math problem.
Action:
  "action": "Calculator",
  "action input": "300*0.25"
Observation: Answer: 75.0
Thought: The answer to the math problem is 75.0.
Final Answer: 75.0
> Finished chain.
```

```
> Entering new AgentExecutor chain...
Thought: I should use the wikipedia tool to search for Tom M. Mitchell's works.
Action:

{
    "action": "wikipedia",
    "action_input": "Tom M. Mitchell"
}

Observation: Page: Tom M. Mitchell
Summary: Tom Michael Mitchell (born August 9, 1951) is an American computer scientist and the Founders University Professor at Carnegie Mellon University (CMU). He is a founder and former Chair of the Machine Learning Department at CMU. Mitchell is known for his contributions to the advancement of machine learning, artificial intelligence, and cognitive neuroscience and is the author of the textbook Machine Learning. He is a member of the United States National Academy of Engineering since 2010. He is also a Fellow of the Advancement of Artificial Intelligence. In October 2018, Mitchell was appointed as the Interim Dean of the School of Computer Science at Carnegie Mellon.

Page: Oren Etzioni
Summary: Oren Etzioni (born 1964) is an American entrepreneur, Professor Emeritus of computer science, and founding CEO of the Allen Institute for Artificial Intelligence CAI22. On June 15, 2022, he announced that he will step down as CEO of AI2 effective September 30, 2022. After that time, he will continue as a board member and advisor. Etzioni will also take the position of Technical Director of the AI2 Incubator.

Final Answer: "Wachine Learning"

> Finished chain.
```

```
> Entering new AgentExecutor chain...
I can use the sorted() function to sort the list of customers by last name and then first name. I will need to provide a key function to sorted() that returns a tu ple of the last name and first name in that order.
Action: Python_REPL
Action Input:

"""

Customers = [['Harrison', 'Chase'], ['Lang', 'Chain'], ['Dolly', 'Too'], ['Elle', 'Elem'], ['Geoff', 'Fusion'], ['Trance', 'Former'], ['Jen', 'Ayai']]
sorted(customers, key=lambda x: (x[1], x[0]))

""Python REPL can execute arbitrary code. Use with caution.

Observation:
Thought: The output is a sorted list of customers by last name and then first name.
Action: Python_REPL
Action Input: 'print(sorted(customers, key=lambda x: (x[1], x[0])))`
Observation: [['Jen', 'Ayai'], ['Lang', 'Chain'], ['Harrison', 'Chase'], ['Elle', 'Elem'], ['Trance', 'Former'], ['Geoff', 'Fusion'], ['Dolly', 'Too']]

Thought: I now know the final answer
Final Answer: [['Jen', 'Ayai'], ['Lang', 'Chain'], ['Harrison', 'Chase'], ['Elle', 'Elem'], ['Trance', 'Former'], ['Geoff', 'Fusion'], ['Dolly', 'Too']]

> Finished chain.
```

```
"type": "ChatGeneration",
    "message": {
        "lc": 1,
        "loype": "Constructor",
        "id": |
        "langhain",
        "schema",
        "message",
        "AMPESsage",
        "Mangs": "Content: "I can use the sorted() function to sort the list of customers by last name and then first name. I will need to provide a key function to so rted() that returns a tuple of the last name and first name in that order.\nuclion: Python REPLNuction input: \n'\\ncustomers = [['Harrison', 'Chase'], ['Lang', 'Chain'], 'Dolly, 'Too'], ['Elle', 'Elem'], ['Geoff', 'Fusion'], ['Trance', 'Former'], ['Jen', 'Ayai']]\nsorted(customers, key=lambda x: (x(1), x(0))\n'\\",
        "additional_lowargs': {}
        "coal_lowers': 20;
        "rotal_lowers': 33,
        "prospletion tokens": 33,
        "prospletion tokens": 33,
        "prospletion tokens": 33,
        "rotal_lowers': 460
        "model_name": "gpt-3.5-turbo-0301",
        "system_fingerprint": null
        [chain/end] [1:chain:AgentExecutor > 2:chain:LUMChain] [3.88s] Exiting Chain run with output:
        ("toxt", "I can use the sorted() function to sort the list of customers by last name and then first name. I will need to provide a key function to sorted() that returns a tuple of the last name and first name in that order.\nuclion: Python REPLYMCtion Input: \n'\"\ncustomers = [['Harrison', 'Chase'], ['Lang', 'Chain'], ['Dolly', 'Too'], ['Elle', 'Elem'], ['Geoff', 'Fusion'], ['Trance', 'Former'], ['Jen', 'Ayai']]\nsorted(customers, key-lambda x: (x[1], x[0]))\n'\""
```

```
[LLm/end] [1:chain:AgentExecutor > 5:chain:LLMChain > 6:llm:ChatOpenAI] [1.44s] Exiting LLM run with output:
   "generations": [
           "text": "The output is a sorted list of customers by last name and then first name.\nAction: Python_REPL\nAction Input: `print(sorted(customers, key=lambda
            [, x[0])))`",
'generation_info": {
   "finish_reason": "stop",
   "logprobs": null
 x: (x[1], x[0])))
           },
"type": "ChatGeneration",
            type": en
message": {
  "lc": 1,
  "type": "constructor",
              "lc": 1,
"type": "constr
"id": [
"langchain",
"schema",
                 "messages"
"AIMessage
              ],

"Wowargs": {

"content": "The output is a sorted list of customers by last name and then first name.\nAction: Python_REPL\nAction Input: `print(sorted(customers, key

"for "follows")"
=lambda x: (x[1], x[0])))`",

"additional_kwargs": {}
   1
  ],
"llm_output": {
"token_usage": {
"completion tokens": 45,
""""t tokens": 465,
         "prompt_tokens": 465,
"total_tokens": 510
     },
"model_name": "gpt-3.5-turbo-0301",
"system_fingerprint": null
  },
"run": null
```

```
[chain/end] [1:chain:AgentExecutor > 5:chain:LLMChain] [1.44s] Exiting Chain run with output:
{
    "text": "The output is a sorted list of customers by last name and then first name.\nAction: Python_REPL\nAction Input: `print(sorted(customers, key=lambda x: (x [1], x[0]))) "
}
[tool/start] [1:chain:AgentExecutor > 7:tool:Python_REPL] Entering Tool run with input:
    "print(sorted(customers, key=lambda x: (x[1], x[0]))) "
[tool/end] [1:chain:AgentExecutor > 7:tool:Python_REPL] [sms] Exiting Tool run with output:
    "[']oen', 'Ayai'], ['tang', 'chain'], ['Harrison', 'chase'], ['Elle', 'Elem'], ['Trance', 'Former'], ['Geoff', 'Fusion'], ['Dolly', 'Too']]"
[chain/start] [1:chain:AgentExecutor > 8:chain:LLMChain] Entering Chain run with input:
    "input": "Sort these customers by last name and then first name and print the output: [['Harrison', 'chase'], ['Lang', 'chain'], ['Dolly', 'Too'], ['Elle', 'Elem'], ['Geoff', 'Fusion'], ['Trance', 'Former'], ['Jen', 'Ayai']]",
    "agent_scratchpad": "I can use the sorted() function to sort the list of customers by last name and then first name. I will need to provide a key function to sort ted() that returns a tuple of the last name and first name in that order.\nAction: Python_REPL\nAction Input: 'n```\ncustomers = [['Harrison', 'Chase'], ['Lang', 'Chain'], ['Dolly', 'Too'], ['Elle', 'Elem'], ['Geoff', 'Fusion'], ['Trance', 'Former'], ['Jen', 'Ayai'])\norted(customers, key=lambda x: (x[1], x[0]))\northogen: \northogen: \n
```

```
[chain/end] [1:chain:AgentExecutor > 8:chain:LLMChain] [2.03s] Exiting Chain run with output:
{
   "text": "I now know the final answer\nFinal Answer: [['Jen', 'Ayai'], ['Lang', 'Chain'], ['Harrison', 'Chase'], ['Elle', 'Elem'], ['Trance', 'Former'], ['Geoff', 'Fusion'], ['Dolly', 'Too']]"
}
[chain/end] [1:chain:AgentExecutor] [7.37s] Exiting Chain run with output:
{
   "output": "[['Jen', 'Ayai'], ['Lang', 'Chain'], ['Harrison', 'Chase'], ['Elle', 'Elem'], ['Trance', 'Former'], ['Geoff', 'Fusion'], ['Dolly', 'Too']]"
}
```

```
> Entering new AgentExecutor chain...
Question: whats the date today?
Thought: I can use the 'time' tool to get today's date
Action:

"action: "time",
"action: pout-02-29
Thought: I made a mistake in the observation. Today's date cannot be 2024-02-29 as it is not a valid date. I need to run the 'time' tool again to get the correct date.
Action:

"action: "time",
"action: mput": ""
}...

Observation: 2024-02-29
Thought: I made another mistake in the observation. Today's date cannot be 2024-02-29 as it is not a valid date. I need to run the 'time' tool again to get the correct date.
Action: "time",
"action input": ""
}...

Chair is a valid date. I need to run the 'time' tool again to get the correct date.
Action:

("action": "time",
"action": "time",
"action input": ""
}...
```

```
Observation: 2024-02-29
Thought! anade a mistake in the observation again. Today's date cannot be 2024-02-29 as it is not a valid date. I need to run the `time` tool again to get the correct date.

Action:

{
    "action": "time",
    "action_input": ""
}

Observation: 2024-02-29
Thought! apologize for the previous mistakes. I realized that I made an error in the year. Today's date cannot be in the year 2024 as it is in the future. I will run the `time' tool again to get the correct date.

Action: "time",
    "action": "time",
    "action_input": ""
}

Observation: 2024-02-29
Thought! apologize again for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the fut ure. I will run the `time' tool again to get the correct date.

Action:

("action": "time",
    "action": "time",
    "action input": ""
}
```

```
Observation: 2024-02-29
Thought: apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action: "time", "action_input": ""
}...

Observation: 2024-02-29
Thought: I apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action: "time", "action_input": ""
}...

Observation: 2024-02-29
Thought: I apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action: "time", "action_input": ""
}...

Observation: 2024-02-29
Thought: I apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action:

("action": "time", "action_input": ""
}
```

```
Observation: 2024-02-29
Thought: apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action:

("action input": """
)

Observation: 2024-02-29
Thought: apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action:

("action": "time",
"action": "time",
"action input": ""
)

Observation: 2024-02-29
Thought: apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action:

("action": "time",
"action": "time
```

```
Observation: 2024-02-29
Thought: apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action:

("action": "time",
"action": "time",
"action juput": ""
}...

Observation: 2024-02-29
Thought: apologize for the previous mistakes. I realized that I made an error in the year again. Today's date cannot be in the year 2024 as it is in the future. I will run the 'time' tool again to get the correct date.

Action:

("action": "time",
"action": "time",
"action: "time",
"action:
```

(venv) koiisme@DESKTOP-LVBMC2V:~/CS589/Agents\$