API roulette - Name the issues

The script
What you need to know
Assignment

The script

Create a new file and fill it with the following script:

```
import flask
from flask import request, jsonify

app = flask.Flask(__name__)
app.config["DEBUG"] = True

# Create some test data for our catalog in the form of a list of dictionaries.
cheeseType = [
    {'id': 0,
     'title': 'Gouda',
     'author': 'The XSS Rat',
     'description': 'Dutch: Goudse kaas, "cheese from Gouda") is a sweet, creamy, yellow cows milk cheese originating from the Netherlands. ...',
     'year': '1992'},
{'id': 1,
     'title': 'Casu marzu',
     'author': 'The XSS Rat',
     'description': 'Casu martzu[1] (Sardinian pronunciation; literally rotten/putrid cheese)is a traditional Sardinian sheep milk cheese that contains live insect'
     'year': '2020'},
{'id': 2,
     'title': 'Roquefort',
     'author': 'The XSS Rat',
     'description': 'Roquefort is a popular French cheese, reported to be a favourite of Emperor Charlemagne. In France, it is called the cheese of kings and popes'
     'year': '2020'}
]

users = [
        {'id':0,
        'username':'test',
        'pass':'test'
        }
]
# A route to return all of the available entries in our catalog.
@app.route('/api/v2/resources/cheese/all', methods=['GET'])
def api_all():
    return jsonify(cheeseType)

@app.route('/api/v1/admin', methods=['GET'])
def ret_users():
    return jsonify(users)

app.run(host="0.0.0.0",port=5001)
```

A couple of adjustments here that will count for several issues, can you find them?

What you need to know

This starts on port 5001 so make sure you connect on that port via your browser.

Assume you are logged in as a low priviledge user with no access to admin functionality.

The developers do not know about the old admin interface.

Assignment

This script when launched is vulnerable to serveral issue types from the API top 10, can you name them?

‼ Solution