Om Khadka, U51801771
Sources: N/A
Collabs: N/A

Challenge 2

The concept of this attack is a brute-force attack of all possible permutations of a password format that we know to be used by the admin (name-d-m-y).

A script is used for this attack, which does the following:

1. Define 4 arrays
    a. **days**, contains all possible days of the month
    b. **months**, contains all possible months of the year
    c. **years**, contains all possible birth years (since admins are millennials, I put in a range from 1980 to 2000)
    d. **names**, all possible admin names
2. Then we go through each possible name-d-m-y combination, doing the following
    a. Make a form of
        username : admin
        name : om khadka
        password : the current name-day-month-year combination
    b. Send a POST request to **http://localhost:8080/login** with that form.
        i. If the output is successful, print the HTML body & end
        ii. Otherwise, continue with the next password combination

A successful attack should look like this:

```
omimahomie@LAPTOP-CEUFRM7P:~/cs357/loginLab$ python3 ch2.py
Total possible combinations: 31248

Starting brute force attack...

SUCCESS! Password found: bob-08-06-1991

Body:
<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Success - Challenge 2</title>
    <link rel="stylesheet" href="style.css">
   </head>
<body class="green">
  <div class="wrapper">
    <h2>ACCESS GRANTED</h2>
    <h2>c6d3371904d7587d38b3ba0d7bb59cc2e5597ac60da647ccc60cadd714a744a6</h2>
  </div>

</body>
</html>

Total iterations: 9692
```

Note that it may take up to 5 minutes for this attack to finish.

Hash: c6d3371904d7587d38b3ba0d7bb59cc2e5597ac60da647ccc60cadd714a744a6