

Om Khadka, U51801771

**Sources:** N/A

**Collabs:** N/A

# Challenge 1

The concept of this attack is a brute-force attack to try out various popular passwords.

A script was used to crack this website. The logic of the script goes as follows:

Given a password list...

1. Filter that list to a proper array of each potential password (**passwords**)
2. For each password in **passwords**, make a form variable that contains the following:
  - username : "admin"
  - name : "om khadka" ← You can change this if u want
  - password : current **passwords**
3. Send a POST req. to <http://localhost:8080/login> with that login data.
4. Once a successful password was found, print the data.

A successful attack should output smth like this:

```
omimahomie@LAPTOP-CEUFRM7P:~/cs357/loginLab$ python3 ch1.py
SUCCESS! Password found: maggie
=====
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 1</title>
  <link rel="stylesheet" href="style.css">
</head>
<body class="green">
  <div class="wrapper">
    <h2>ACCESS GRANTED</h2>
    <h2>e55dd338693da6e0d5338fb9986fa78699769b3e82b340c4ebcf3adf206a0085</h2>
  </div>
</body>
</html>
=====
END
```

**Hash:** 00174a1e889a7effbef7fbc7f86dae33606fe5a305a3e2312ec1f9995fb112c