

SVKM'S NMIMS (Deemed-to-be University)  
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT AND ENGINEERING  
MUMBAI CAMPUS  
**LAB Manual**  
**PART A**  
(PART A: TO BE REFERRED BY STUDENTS)

## Experiment No. 2

### A.1 Aim:

To implement a password strength checker

### A.2 Prerequisite:

Understanding of Authentication methods

### A.3 Outcome:

**After successful completion of this experiment students will be able to**

1. Appreciate the importance of proactive password checking.
2. Can able to comprehend how vulnerable the system could be if password selection is done incorrectly.

### A.4 Theory:

Authentication is the process of binding of identity to a subject. This process validates the user's credentials and determines whether the user is allowed to access a system or a resource or not. The authentication information comes from one or more of the following

- What entity knows (*e.g.*, password)
- What entity has (*e.g.*, badge, smart card)
- What entity is (*e.g.*, fingerprints, retinal characteristics)
- Where entity is (*e.g.*, In front of a particular terminal)

An authentication process consists of obtaining authentication information, analyzing the data and determining if it is associated with that entity.

Passwords are the most common mechanism used for authentication mainly for two reasons: ease of use and simple. However it suffers from many problems such as the user may forget the password; an attacker may know the password and replay the password.

The authentication system using passwords should have mechanism that enforces the user to select strong or good passwords. The aim of the system should be that the attacker should take lot of time to crack the password.

A strong password must have the following components:

At least one uppercase letter

At least one lowercase letter

At least one numeric digit

At least one special character

String length should be of at least 8 characters

## PART B

(PART B: TO BE COMPLETED BY STUDENTS)

*(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)*

Roll. No. A022	Name: Kartik Padave
Class: B. Tech 3 <sup>rd</sup> Year	Batch: 1
Date of Experiment: 24/12/2021	Date of Submission: 24/12/2021
Grade:	

### B.1 Software Code written by student:

*(Paste your Java code completed during the 2 hours of practical in the lab here)*

```
import time, os

class passwordchecker:
    def __init__(self):
        self.password = input("Enter your password: ")

        self.authentication = {
            'uppercase': 0,
            'lowercase': 0,
            'number': 0,
            'special character': 0,
            'length': 0
        }

    def check_length(self):
        if len(self.password) < 8:
            self.authentication['length'] = -1
        else:
            self.authentication['length'] = 1

    def check_strength(self):
        for i in self.password:
            if i.islower():
                self.authentication['lowercase'] = 1
            elif i.isupper():
```

```
self.authentication['uppercase'] = 1
elif i.isdigit():
    self.authentication['number'] = 1
else:
    self.authentication['special character'] = 1

def print_strength(self):
    if self.authentication['lowercase'] > 0 and self.authentication['uppercase'] > 0 and
self.authentication['number'] > 0 and self.authentication['special character'] > 0 and
self.authentication['length'] > 0:
        print("Secure password")
    else:
        print("Insecure password")

print("Program to see if password is strong or not")
time.sleep(3)
_ = os.system('cls')

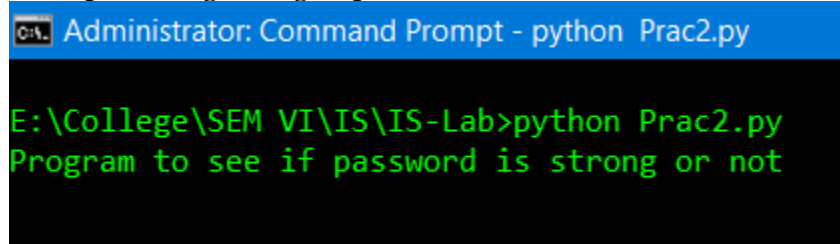
password = passwordchecker()
password.check_length()
password.check_strength()
password.print_strength()
```

## B.2 Input and Output:

*(Paste your program input and output in following format, if there is error then paste the specific error in the output part. In case of error with due permission of the faculty extension can be given to submit the error free code with output in due course of time. Students will be graded accordingly.)*

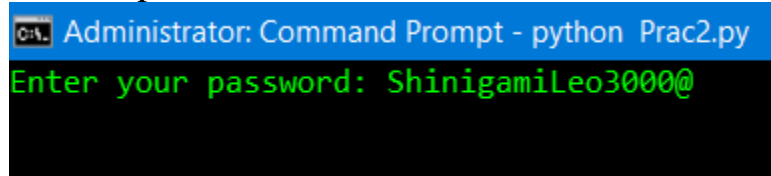
### Input:

1. Input string acting as password



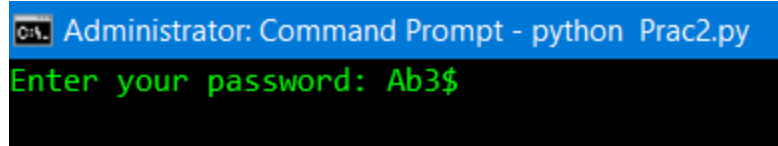
```
Administrator: Command Prompt - python Prac2.py
E:\College\SEM VI\IS\IS-Lab>python Prac2.py
Program to see if password is strong or not
```

### Case 1 Input:



```
Administrator: Command Prompt - python Prac2.py
Enter your password: ShinigamiLeo3000@
```

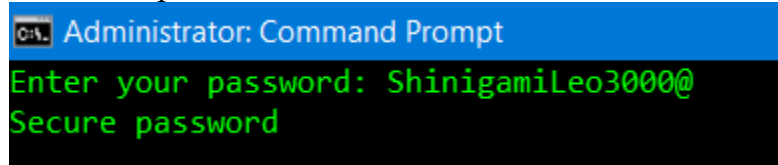
### Case 2 Input:



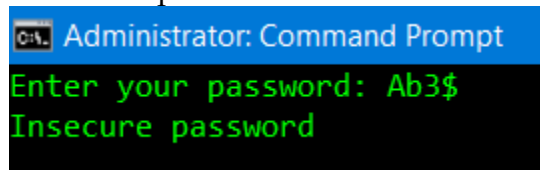
### Output:

Output screenshots with different cases

Case 1 Output:



Case 2 Output:



## B.3 Observations and learning:

*(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)*

### For case 1:

All the requirements for a secure password are fulfilled. It has at least 1 uppercase, at least 1 lowercase, at least 1 number, at least 1 special character and length of password is longer than 8 characters. Hence, the output is given as Secure password.

### For case 2:

Length of password is less than 8 characters which makes it very insecure password and hence the output is given as insecure password.

## B.4 Conclusion:

*(Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)*

### After successful completion of this experiment:

1. We know the importance of proactive password checking.
2. Helps us to comprehend how vulnerable the system could be if password selection is done incorrectly.

## B.5 Questions of Curiosity

*(To be answered by student based on the practical performed and learning/observations)*

Q1: Discuss the various attacks on passwords

There are 5 common types of attacks on passwords:

a. Phishing

Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily. Sometimes they lead you to fake "reset your password" screens; other times, the links install malicious code on your device.

b. Man-in-the-Middle attack

Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords.

c. Brute Force Attack

If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.

d. Dictionary Attack

A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.

e. Credential Attack

If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website. Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in. Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them.

Q.2 Explain some other authentication methods in brief.

**1. Multi-Factor Authentication**

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security.

**2. Certificate Authentication**

Certificate-based authentication technologies identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver's license or a passport. The certificate contains the digital identity of a user including a public key, and the digital signature of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.

**3. Biometric Authentication**

Biometrics authentication is a security process that relies on the unique biological characteristics of an individual. Biometric authentication technologies are used by consumers, governments and private corporations including airports, military bases, and national borders. The technology is increasingly adopted due to the ability to achieve a high level of security without creating friction for the user.

**4. Token Authentication**

Token-based authentication technologies enable users to enter their credentials once and receive a unique encrypted string of random characters in exchange. You can then use the token to access protected systems instead of entering your credentials all over again. The digital token proves that you already have access permission.