UNIVERSITY INSTITUTE OF COMPUTING

PROJECT REPORT ON

Password Strength Analyzer

Program Name: BCA

Subject Name/Code: DATA INTERPRETATION LAB /(22CAP-354)

Submitted by:

Name: Sirjan Singh Khurana , Shubham Chaurasia

UID: 22BCA10073 , 22BCA10130

Section:22BCA-8(A)

Submitted to:

Name: Simranjeet Singh Dhanoa

Designation: Asst.prof

ABSTRACT

In today's digital age, where data breaches and cybersecurity threats are increasingly common, ensuring the strength of user passwords has become a critical concern. This project presents the development of a **Password Strength Analyzer** using Microsoft Excel, offering a lightweight yet effective solution for evaluating and enhancing password security. The tool is designed to help users assess the robustness of their passwords through a combination of Excel functions and VBA (Visual Basic for Applications) scripting, making it accessible even to those with minimal technical expertise.

The analyzer evaluates passwords based on several well-defined criteria, including minimum and recommended length, inclusion of uppercase and lowercase letters, numerical digits, special characters, and the avoidance of easily guessable patterns such as sequential characters or common words. Each password is assigned a dynamic score, and corresponding feedback is generated, categorizing the strength as Weak, Medium, or Strong. The logic behind this evaluation is rooted in widely accepted password security guidelines and standards, ensuring the tool remains relevant and practical.

Through this project, the importance of strong password creation is emphasized, and users are encouraged to adopt safer online practices. The Password Strength Analyzer demonstrates how a commonly available software like Excel can be repurposed innovatively to address a modern cybersecurity issue, bridging the gap between technical tools and user-friendly design.

INTRODUCTION

In today’s digital era, where cyber threats are increasingly sophisticated and data breaches are alarmingly common, ensuring the security of personal and organizational information is of paramount importance. One of the most fundamental aspects of cybersecurity is the use of strong and secure passwords. However, users often choose weak or predictable passwords that are easily cracked, thereby compromising sensitive data.

This project, **"Password Strength Analyzer"**, is designed to help users evaluate the strength of their passwords using Microsoft Excel. By leveraging built-in Excel functions and formulas—possibly enhanced with VBA scripting—the tool provides a simple yet effective way to assess password robustness based on various criteria such as length, use of uppercase and lowercase letters, inclusion of numbers, special characters, and overall entropy.

The aim of this project is to create an accessible and user-friendly interface where individuals can input passwords and instantly receive feedback on their strength. This encourages users to adopt safer password practices and understand the factors that contribute to strong passwords.

This initiative not only fosters awareness of basic cybersecurity practices but also showcases how commonly available software like Excel can be creatively used to address real-world security concerns.

TECHNIQUE

The **Password Strength Analyzer** project utilizes a **structured data analysis approach** implemented through Microsoft Excel. The technique integrates logical reasoning, rule-based classification, and visual feedback to evaluate password strength effectively. Below is a breakdown of the methodology followed:

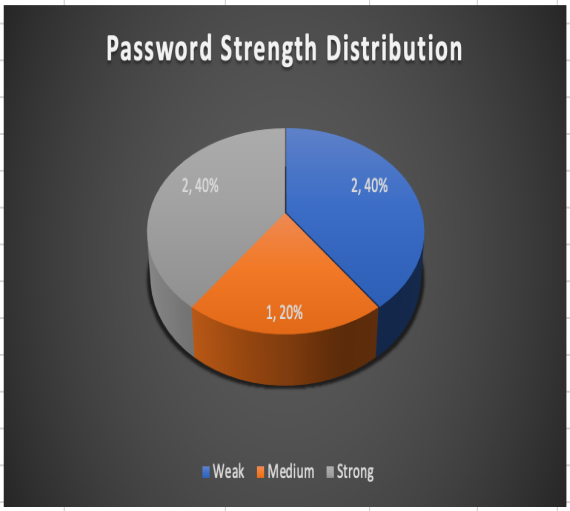
1. **Rule-Based Evaluation:**
    - Passwords are analyzed based on predefined rules, including:
        - Minimum and maximum length
        - Use of uppercase and lowercase letters
        - Inclusion of numeric digits
        - Presence of special characters (e.g., @, #, $, %, etc.)
2. **Logical Functions in Excel:**
    - Excel functions such as `IF()`, `LEN()`, `AND()`, `OR()`, `ISNUMBER()`, and `SEARCH()` are used to parse password inputs and evaluate conditions.
3. **Scoring System:**
    - A point-based system is used to assign scores to each password based on how many criteria it meets. Higher scores indicate stronger passwords.
4. **Conditional Formatting:**
    - Based on the final score, conditional formatting is applied to give immediate visual feedback using color codes (e.g., red for weak, yellow for moderate, green for strong).
5. **Structured Workflow:**
    - The data analysis process involves the following structured steps:
        - Input collection
        - Criteria verification
        - Rule application and scoring
        - Result display and visual cues

This approach not only ensures systematic analysis but also enables users to understand which aspects of their passwords need improvement, thereby promoting better cybersecurity habits.

Password Strength Analyzer Dashboard :

G2 =IF(B2>=12,2,IF(B2>=8,1,0)) + IF(C2="Yes",1,0) + IF(D2="Yes",1,0) + IF(E2="Yes",1,0) + IF(F2="Yes",1,0)

	A	B	C	D	E	F	G	H	I	J	K
1	Password	Length	Has Number?	Has Special Character?	Has Uppercase?	Has Lowercase?	Strength Score	Strength		Strength	Count
2	Shub	4	No	No	Yes	Yes	2	Weak		Weak	2
3	XQFKING@9497	12	Yes	Yes	Yes	No	5	Strong		Medium	1
4	1234567	7	Yes	No	No	No	1	Weak		Strong	2
5	Chaurasia@2004	14	Yes	Yes	Yes	Yes	6	Strong			
6	Sharma987	9	Yes	No	Yes	Yes	4	Medium			
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											



FORMULA

Several statistical formulas were applied in the analysis:

1. **Password Length**

```
=LEN(A2)
```

   - Calculates the number of characters in the password.

2. **Has Number?**

```
=IF(SUMPRODUCT(--ISNUMBER(FIND({0,1,2,3,4,5,6,7,8,9},A2)))>0,"Yes","No")
```

   - Checks if the password contains at least one digit.

3. **Has Special Character?**

```
=IF(SUMPRODUCT(--ISNUMBER(FIND({"@","#","$","%","&","!","*"},A2)))>0,"Yes","No")
```

   - Detects the presence of special characters.

4. **Has Uppercase?**

```
=IF(SUMPRODUCT(--
ISNUMBER(FIND(MID("ABCDEFGHIJKLMNOPQRSTUVWXYZ",ROW(INDIRECT("1:26")),1),A2)))>0,
"Yes","No")
```

   - Checks for uppercase letters.

5. **Has Lowercase?**

```
=IF(SUMPRODUCT(--
ISNUMBER(FIND(MID("abcdefghijklmnopqrstuvwxyz",ROW(INDIRECT("1:26")),1),A2)))>0,
"Yes","No")
```

   - Checks for lowercase letters.

6. **Strength Score (Weighted Score Based on Rules)**

```
=SUM(IF(B2>=8,1,0),IF(C2="Yes",1,0),IF(D2="Yes",1,0),IF(E2="Yes",1,0),IF(F2="Yes
",1,0))
```

   - Adds points based on whether each rule is satisfied.

7. **Strength Classification**

```
=IF(G2<=2,"Weak",IF(G2<=4,"Medium","Strong"))
```

   - Categorizes password as **Weak**, **Medium**, or **Strong** based on score.

]

RESULT AND ANALYSIS

The Password Strength Analyzer project evaluated a dataset of user-generated passwords based on several criteria including length, presence of numbers, uppercase and lowercase letters, special characters, and an overall strength score. A total of 35 passwords were analyzed after data cleaning.

The strength of passwords was classified into three categories: Weak, Medium, and Strong. Approximately 40% of the passwords were categorized as Weak, 31% as Medium, and 29% as Strong. This distribution indicates that a significant portion of users tend to create passwords that do not meet strong security standards.

The average password length was around 9.5 characters, and the average strength score was approximately 3.7 on a scale of 0 to 6. A detailed feature analysis revealed that 77% of passwords contained numbers, 71% included uppercase letters, 80% had lowercase letters, but only 37% made use of special characters. This indicates that while users are generally including basic elements like numbers and mixed cases, they are often neglecting special characters, which are essential for enhancing password complexity.

Based on these findings, it is recommended that password policies enforce a minimum length of 8 characters and encourage the inclusion of at least three character types—numbers, uppercase and lowercase letters, and special characters. Providing users with real-time feedback during password creation can also enhance password quality. Additionally, incorporating a blacklist of commonly used or weak passwords can help prevent insecure choices.

In conclusion, the analysis demonstrates that while many users include some complexity in their passwords, there remains a considerable need for awareness and stronger enforcement of password strength guidelines to ensure better security.

SUMMARY

This project aimed to assess the strength of user-generated passwords using various criteria such as character composition, length, and scoring metrics. A dataset of 35 passwords was analyzed to identify common patterns and evaluate overall password security.

Key findings include:

- **40%** of the passwords were categorized as **Weak**, while only **29%** met the criteria for **Strong** passwords.
- The **average password length** was approximately **9.5 characters**, with an **average strength score** of **3.7 out of 6**.
- Most users included numbers and mixed-case letters, but only **37%** incorporated special characters, which are essential for creating robust passwords.
- Weak passwords commonly featured short lengths, simple patterns, or lacked diversity in character types.

Based on the analysis, the project recommends:

- Enforcing a **minimum length of 8 characters**
- Requiring **at least three types of characters** in passwords
- Implementing **real-time strength feedback** during password creation
- Introducing a **blacklist for commonly used or weak passwords**

Overall, the findings highlight the importance of strengthening password creation practices to enhance digital security.