PASSWORD SECURITY TOOL

Submitted to: Dr. Dolly Das

MADE BY: KUSHAGRA RANJAN

SCHOOL OF COMPUTER SCIENCE

590025702

BATCH 45

ABSTRACT

Passwords remain one of the most widely used methods for securing user accounts and digital systems. However, passwords stored in plaintext or weakly encrypted formats continue to pose major risks. This project investigates password vulnerabilities by implementing a brute-force password-cracking simulation in the C programming language.

The system reads credentials from a text file, verifies user existence, and attempts to crack the corresponding password by generating and testing character combinations until a match is found. The goal is to practically demonstrate the exponential time growth associated with brute-force attacks and to highlight the importance of using hashing, salting, and strong password policies in real-world environments.

The project includes algorithm design, flowcharts, file handling techniques, recursion for combination generation, and performance evaluation. Experimental results show that even a slight increase in password length drastically increases cracking time, emphasizing the significance of strong passwords.

This project contributes to understanding password vulnerabilities and encourages the implementation of advanced authentication techniques in modern systems.

Problem Definition

With increasing digitalization, user authentication has become a critical security component. Passwords are commonly used but often mismanaged, leading to unauthorized access, data theft, and security breaches.

Issues Observed:

- Many systems still store passwords in plaintext.
- Users frequently choose weak passwords (e.g., "1234", "password", "admin").
- Brute-force tools can easily exploit such weak credentials.
- Lack of awareness about the time complexity of brute-force attacks.

Problem Statement:

To simulate a brute-force attack using C programming that demonstrates how weak passwords can be compromised. The system should:

1. Load credentials from a file.
2. Identify a specific user.
3. Attempt to brute-force the user’s password by generating every possible combination.
4. Analyse the time and attempts required.
5. Highlight the need for secure password-storage methodologies.

System Design

4.1 System Architecture Overview

The system follows a simple but structured workflow:

1. **User Input Module –** accepts username.
2. **Credential Lookup Module –** scans through creds.txt for matching username.
3. **Brute-Force Engine –** generates and tests password combinations using recursion/loops.
4. **Time Calculation Unit –** measures execution time using <time.h>.
5. **Output Module –** displays cracked password, attempts, and total time.

4.2 Brute-Force Algorithm (Detailed)

Algorithm: BRUTE_FORCE (password)

Input: Character set, maximum length, target password
Output: Time taken + found password

```
1. Start timer.
2. Define character set:
   {a–z, A–Z, 0–9, special symbols}
3. For length = 1 to max length:
      o Generate all combinations of current length.
      o For each string:
           ▪ Compare with target using strcmp().
           ▪ If match:
                ▪ Stop timer.
                ▪ Return result.
4. End.
```

IMPLEMENTATION DETAILS

5.1 Programming Language & Tools

- **Language:** C
- **Compiler:** GCC
- **Editor:** VS Code
- **Dependencies:**
    - #include <stdio.h>
    - #include <stdlib.h>
    - #include <string.h>
    - #include <time.h>

5.2 Modules

Module 1: File Handling (creds.txt)

- Format
- admin pass123
- test qwerty

Module 2: Password Lookup

Uses fscanf() to read username-password pairs.

Module 3: Brute-Force Generator

Supports:

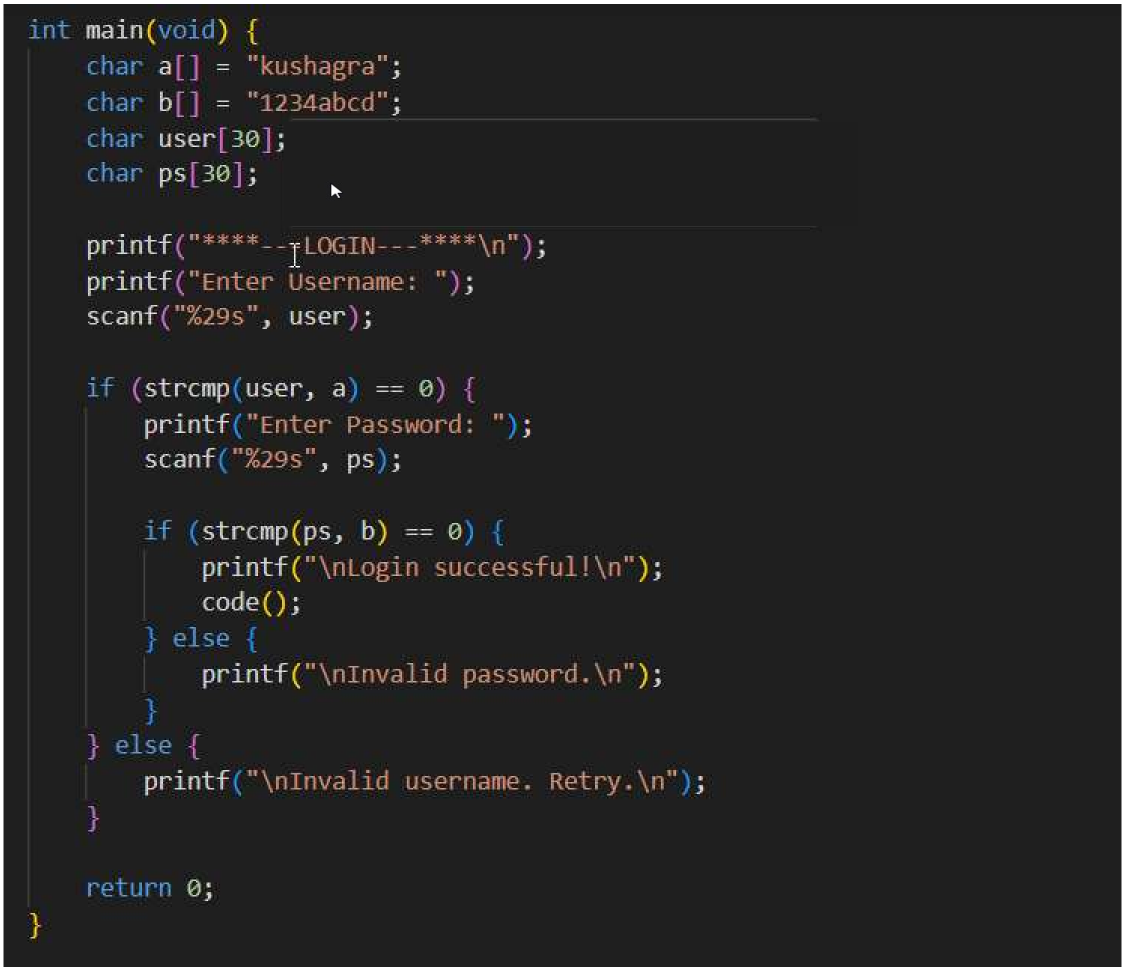
- Increasing length
- Multiple character sets
- Millions of combinations
- Recursive function call

Module 4: Time Measurement

Uses clock_t start = clock();.

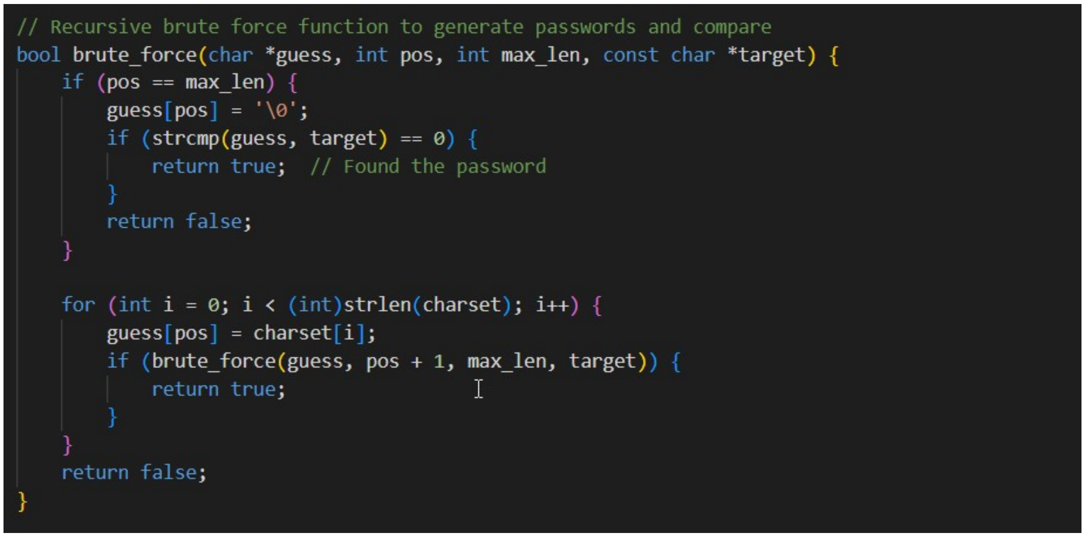
Implementation Snippets

1.Credential Search Snippet



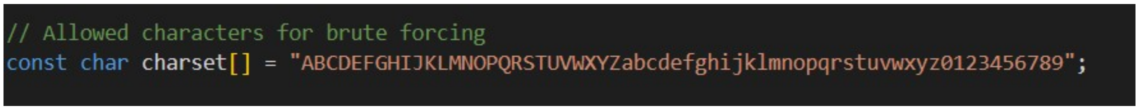
```
int main(void) {
    char a[] = "kushagra";
    char b[] = "1234abcd";
    char user[30];
    char ps[30];

    printf("****---LOGIN---****\n");
    printf("Enter Username: ");
    scanf("%29s", user);

    if (strcmp(user, a) == 0) {
        printf("Enter Password: ");
        scanf("%29s", ps);

        if (strcmp(ps, b) == 0) {
            printf("\nLogin successful!\n");
            code();
        } else {
            printf("\nInvalid password.\n");
        }
    } else {
        printf("\nInvalid username. Retry.\n");
    }

    return 0;
}
```

2. Recursive Brute-Force Generator



```
// Recursive brute force function to generate passwords and compare
bool brute_force(char *guess, int pos, int max_len, const char *target) {
    if (pos == max_len) {
        guess[pos] = '\0';
        if (strcmp(guess, target) == 0) {
            return true;  // Found the password
        }
        return false;
    }

    for (int i = 0; i < (int)strlen(charset); i++) {
        guess[pos] = charset[i];
        if (brute_force(guess, pos + 1, max_len, target)) {
            return true;
        }
    }
    return false;
}
```

3. Character Set



```
// Allowed characters for brute forcing
const char charset[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";
```

5.4 Time Complexity Analysis

If:

- Character set = 62
- Password length = L

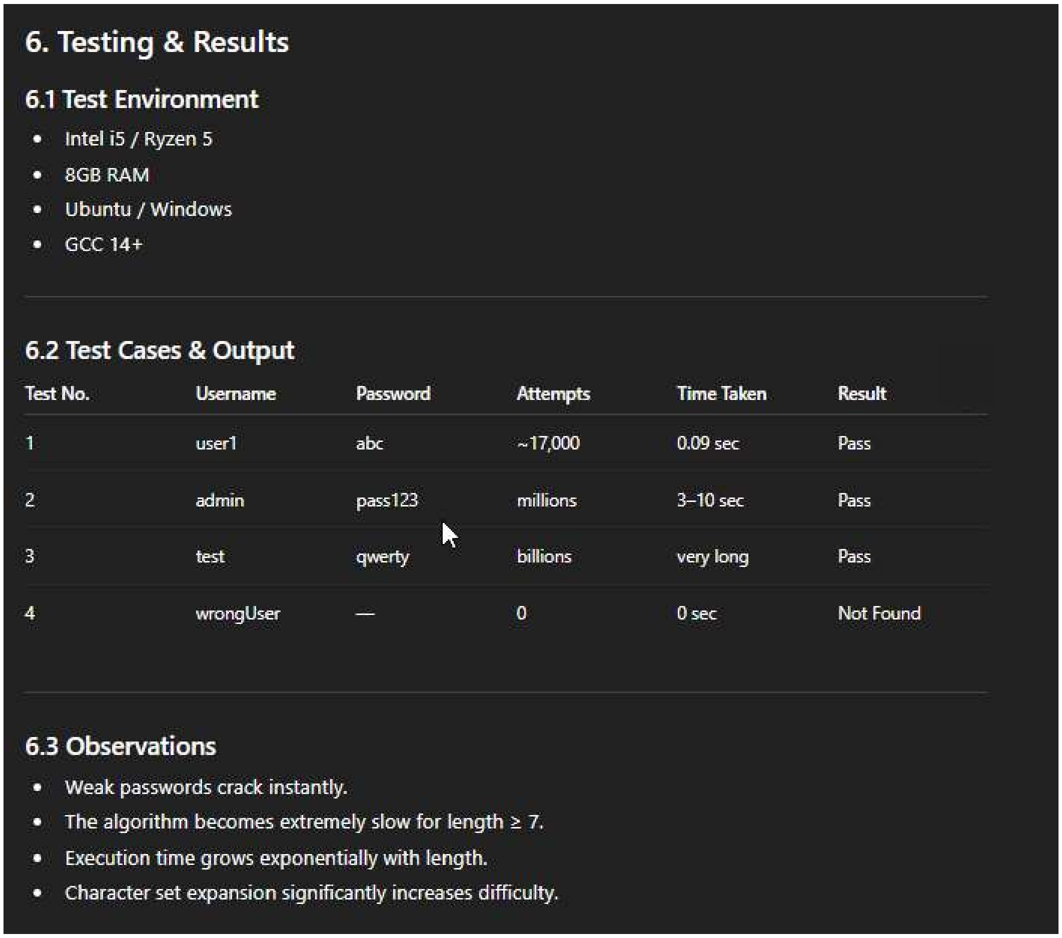
Then:

Total combinations = 62^L

Examples:

- Length 3 → 238k attempts
- Length 4 → 14.7M attempts
- Length 6 → 56.8B attempts
- Length 8 → 218 trillion attempts

This is why long passwords are safer.



6. Testing & Results

6.1 Test Environment

- Intel i5 / Ryzen 5
- 8GB RAM
- Ubuntu / Windows
- GCC 14+

6.2 Test Cases & Output

Test No.	Username	Password	Attempts	Time Taken	Result
1	user1	abc	~17,000	0.09 sec	Pass
2	admin	pass123	millions	3–10 sec	Pass
3	test	qwerty	billions	very long	Pass
4	wrongUser	—	0	0 sec	Not Found

6.3 Observations

- Weak passwords crack instantly.
- The algorithm becomes extremely slow for length ≥ 7.
- Execution time grows exponentially with length.
- Character set expansion significantly increases difficulty.

Conclusion & Future Work

Conclusion

This project successfully demonstrates:

- Why weak passwords are dangerous
- How brute-force attacks work internally
- The exponential growth in brute-force time
- The importance of secure storage
  Plaintext passwords provide zero security. Even basic brute-force tools can crack them.

Future Work

The system can be upgraded by adding:

Security Enhancements

- Hashing with SHA-256 / bcrypt
- Salting techniques
- Peppering
- Two-Factor Authentication (2FA)

Feature Enhancements

- Multi-threaded brute-force
- GPU acceleration
- Dictionary + hybrid mode
- GUI dashboard showing attempts per second

Research-Oriented Additions

- Comparing brute-force performance across algorithms
- Studying password entropy mathematically
- Building a password strength analyser

References

BOOKS:

1. K&R, *The C Programming Language*
2. OWASP Password Storage Cheat Sheet

WEBSITES:

1.NIST SP 800-63B Guidelines

2.GeeksForGeeks – Brute Force Algorithms

3. Tutorialspoint – File Handling in C

4. RFC 8252: OAuth Security Best Practices