Lab7

IT-314

Jish Chanchapra

202201501

1. Errors Identified in the Program:

-Data Reference Errors (Category A):

1. Uninitialized variables (e.g., MABUF)
2. Array boundary issues (e.g., TOKS[MAXWORDS][IDSZX])
3. Pointer memory management (e.g., invalid qq in hexdmp())
4. Uninitialized variables (e.g., DBDIN, RECUNI)
5. Array boundary issues (e.g., TADIN[], RECUNI[] without bounds checking)
6. Invalid file handle in HDLUopen() if open() fails
7. Pointer dereferencing issues (e.g., p in existfile())
8. Uninitialized variables (e.g., TADIN[tt].SEQ, RECUNI[tt].crc)
9. Array boundary issues (e.g., buf[nw] in setCRC() and evalCRC())
10. Pointer memory management issues (e.g., p in setRECdflt() and printREC())
11. Pointer dereferencing issues with pf in sortfcmp2
12. No array boundary checks for IXDB and IXDIN
13. Potential buffer overflow in printix with IXDB[ii].RBA
14. Pointer dereferencing issues in tabfullscan with memmove and array KPAGE.R[].
15. Lack of bounds checks for arrays VGRP[] and KPAGE.R[], leading to potential undefined behavior.
16. Missing null pointer checks for structures like UOW, which could cause segmentation faults.

-Data-Declaration Errors (Category B):

1. Missing explicit declarations (e.g., I32)
2. Shadowing issues (e.g., variable buf in todayMABUF())
3. Implicit size assumptions in structures (e.g., TYPTADIN)
4. Undeclared or missing types (e.g., I8, I32)
5. Undefined types (e.g., I16, I32, U16)
6. Inconsistent declaration (e.g., buf in newpage() function)
7. Implicit type conversions leading to incorrect results in sortfcmp2
8. Undefined variables like UOW in indexfull()
9. Implicit type conversion issues between long (e.g., posl) and int (e.g., tt), which could lead to bugs.
10. Incorrect initialization checks for variables like qrows, nrmcnt, and delcnt in tabfullscan() across various command cases.

-Computation Errors (Category C):

1. Mixed-mode arithmetic
2. Division by zero checks not present
3. Mixed-mode arithmetic in functions (e.g., dbstate(), tell())

4. Potential division by zero in computations (e.g., openTAB())
5. Mixed-mode arithmetic issues in setCRC() and evalCRC()
6. No division by zero check for computations based on file lengths
7. Sorting logic issues in sortIXDB, especially with mixed data types
8. Lack of division by zero checks, particularly in modulus calculations
9. Integer overflow risks in the loop for(int i=0; i LT rio; i++) without proper bounds checks.
10. Division by zero potential in the operation stio%LRECU without ensuring LRECU is non-zero.

-Control Flow Errors (Category E):

1. Possible infinite loop in exitenable()
2. Infinite loop potential in hdlcheck()
3. Incorrect return value handling in dbstate()
4. Possible infinite loops in matchSYSDIN()
5. Unchecked return values in readREC()
6. Possible infinite loops in findkey
7. Missing default case in switch(cmd) in indexfull()
8. Missing default case in the switch(cmd) block, relying on an assert statement for unexpected values.
9. Loop termination issues with while(NOT stopscan), which could lead to infinite loops or performance problems.

2.Effective Category of Program Inspection:

- Data Reference Errors (Category A)

3. Errors Not Easily Identified via Program Inspection:

- Concurrency Issues: Race conditions in multi-threaded environments.
- Memory Leaks: Difficult to identify without runtime analysis.
- Performance Degradation: Impact on large datasets not visible without profiling.

4. Applicability of Program Inspection Techniques:

- Yes it is Valuable for Memory Safety,Array Bounds Checking,Control Flow Validation. And also Complement with Dynamic testing.