UE19CS257C - Secure Programming wih C

Grocery Shop Management

Vihar Devalla, Aasim Mohammed, Ashwin Srinvasa Ramanujan

Synopsis

Creating a Grocery Shop Management program which allows the user to login in as User or Admin. The User can buy and pay for his groceries using his account. The account contains his details and money balance. The User details are stored in an external file. The Admin has privileges to change the prices of groceries and execute system commands to read the User details.

Static Analysis Tool : splint

Possible Vulnerabilities

PrivEsc using Buffer Overflow

The inputs given for the user to login could have no stack protection and hence allow the user to move to a function of his own choice. The exploit could allow a User member to get Admin access and manage prices himself.

Sol: Implement Stack Protection

Integer Overflow

The money balance could cause a negative integer overflow and wraparound to get the max amount (2^32 -1).

Sol: use unsigned int

Privilege Escalation and System Command Execution

The given system call for reading the files could be exploited to execute any arbitrary command and a possible privilege escalation if an SUID is set.

Sol: prevent system calls and/or avoid inputs for system calls from any user.