FIT3173 Software Security

Week 6 Tutorial: Code Review with a Tool

This tutorial will give you some experience in using static code analysis tools as part of a code security review.

1. Download and install one or more free code security review tools. For example, the following are available for download in a ZIP archive (with installation instructions) from Moodle in the 'Week 6 Tutorial' area:
    a. RATS (for C or C++ code)
    b. FlawFinder (for C or C++ code)

In this task, you are required to use **FlawFinder** to analyze some of the small vulnerable programs used for illustrations in the lectures. If you have time, try RATS.

To install **FlawFinder:**

1. Unzip flawfinder-1.27.tar.gz;
2. Go to the unzipped folder and type the install command:

```
sudo make install
```

Analyze the following programs via the following command:

```
./flawfinder program.c
```

1. `auth_overflow.c` (or its variants `auth_overflow2.c` and `auth_overflow3.c`): programs with buffer overflow vulnerabilities (available for download on Moodle from Week 4 Lecture Materials and Week 5 Tutorial Materials).
2. `fmt_vuln.c`: program with format string vulnerability from Lecture 4 (available from Week 6 tute Moodle).
3. `code_inj.c`: program with a command injection vulnerability from Lecture 4 (available from Week 6 tute Moodle)
4. `int_overflow_vuln.c` and `int_overflow_safe.c`: programs with an integer overflow vulnerability (`int_overflow_vuln.c`) and a program with the vulnerability eliminated (`int_overflow_safe.c`), from Lecture 5. (available from Week 6 tute Moodle)
5. `int_sign_vuln.c`: program with an integer sign vulnerability

Discussion: for which of the above, note which of the known vulnerabilities were found by the tools? Were there any others found? Are they valid vulnerabilities or "false positives"? Were there any known vulnerabilities that were not found? If so, were they one of the vulnerabilities

that the tool is designed to find but did not (“false negatives”), or is the tool not designed to find them?

To install **RATS**:

1. Install **Expat** lib: extract Expat-2.1.0, go to the unzipped folder and type the install command:

   ```
   ./configure

   sudo make install
   ```

2. Insall **RATS**: Expat-2.3, go to the unzipped folder and type the install command:

   ```
   ./configure

   sudo make

   sudo make install
   ```

Analyze the programs via the following command:

```
./rats program.c
```