Code Review with a Tool

This lab will give you some experience in using static code analysis tools as part of a code security review. Please follow the below instructions to install *FlawFinder and RATs*, which are both free code security review tools, to analyze some of the small vulnerable programs used for illustrations in the lectures. You can download these vulnerable programs from Moodle.

To install **FlawFinder:**

1. Download source of flawfinder

   ```
   wget https://dwheeler.com/flawfinder/flawfinder-2.0.11.tar.gz
   ```

2. Uncompress the file and become root to install

   ```
   tar xvzf flawfinder-*.tar.gz
   ```

3. Go to the unzipped folder and type the install command:

   ```
   cd flawfinder-*
   sudo make prefix=/usr install
   ```

Analyze the following programs via the following command:

```
flawfinder program_name.c
```

1. `auth_overflow.c` (or its variants `auth_overflow2.c` and `auth_overflow3.c`): programs with buffer overflow vulnerabilities.
2. `fmt_vuln.c`: program with format string vulnerability.
3. `code_inj.c`: program with a command injection vulnerability.
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`).
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. Download the source of **Expat**

```
wget https://src.fedoraproject.org/repo/pkgs/expat/expat-2.1.0.tar.gz/dd7dab7a5fea97d2a6a43f511449b7cd/expat-2.1.0.tar.gz
```

2. Install **Expat** lib:

```
tar xvzf expat-2.1.0.tar.gz && cd expat-2.1.0
./configure
sudo make
sudo make install
```

3. Download the source of **RATS**:

```
wget https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/rough-auditing-tool-for-security/rats-2.3.tar.gz
```

4. Install RATS

```
tar xvzf rats-2.3.tar.gz && cd rats-2.3
./configure
sudo make
sudo make install
```

Analyze the programs via the following command:

```
rats program_name.c
```