Homework 1: Practice of CI (Continuous Integration) and Static Analysis

1. CI with static analysis

   (1) Create **Jenkins** and **SonarQube** docker container and run them.
   (2) The source files are located at https://github.com/wangch64/sechw1.git
   (3) Please create a Jenkins project with **CI pipeline** that can do the following jobs **in different stages** (e.g., Pull, Security Check, Build and Run):
      (a) Pull the source files from Github.
      (b) Perform security check by flawfinder for C codes and SonaQube Scanner for the PHP and Python codes.
      (c) Build the C codes.
      (d) Run some executable files (C and Python: pickletest.py).
   (4) Check the Console Output and Stage View in Jenkins.
   (5) Check the Static Analysis results in SonarQube Server.
   (6) See some **hints** in Appendix.

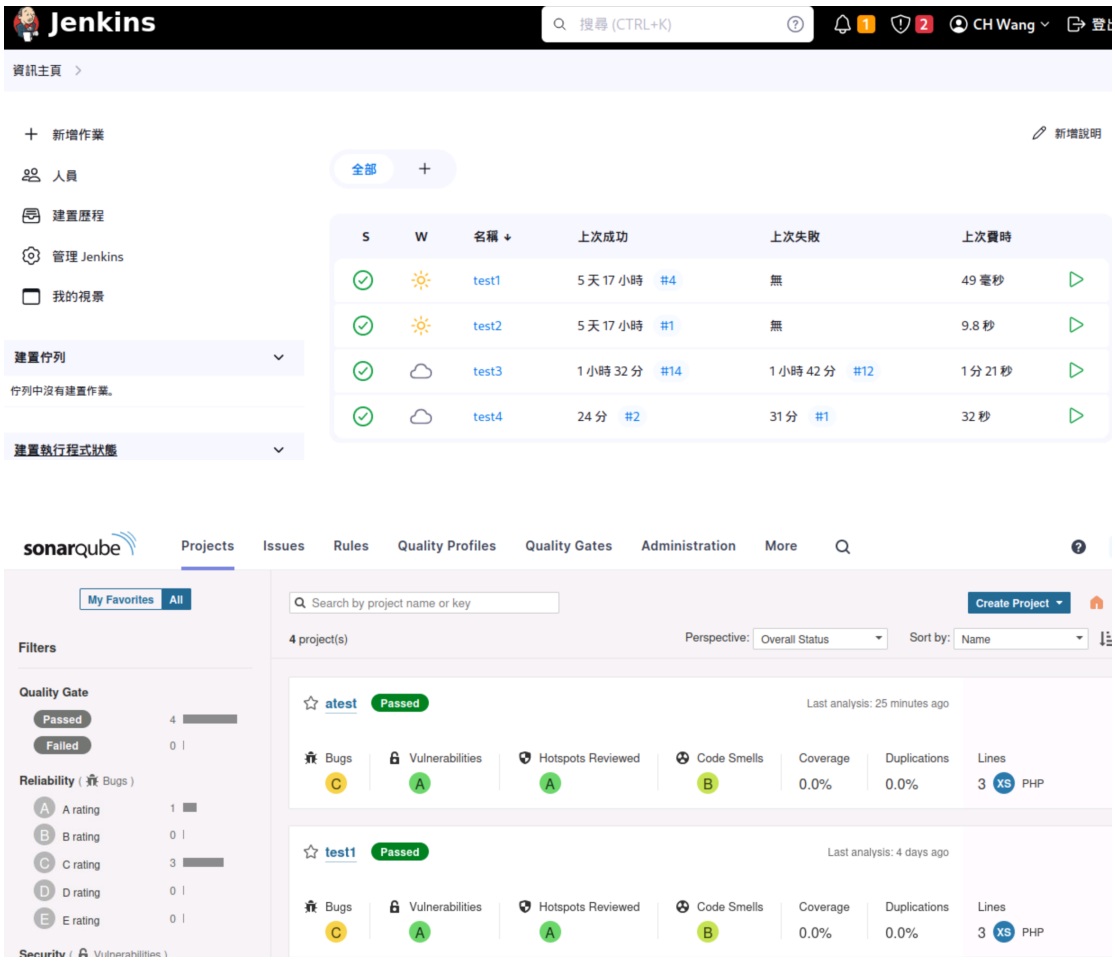

Fig. 1 Jenkins and SonarQube

2. Understand buffer overflow attack (Try large buffers)

(1) Explain the possible vulnerabilities for the C program shown in Fig. 2.
(2) Exploit it (**with stack smashing**) by using some debug tools, e.g., GDB.
(3) Try to fix the problems and explain your solution.

```
#include <stdio.h>
#include <string.h>
#include <stdbool.h>
int PrivateGame(void);
bool ValidorNot(void);

int PrivateGame(void)
{
        system("/usr/bin/xeyes");
        return 0;
}
int main(void) {
        bool PWverify;
        puts("Welcome to Ones University!");
        puts("Enter your password:");
        PWverify = ValidorNot();
        if (!PWverify) {
                puts("Password Error!! Please try again.");
                return -1;
        }
        else puts("Welcome. Your password is correct.");
        return 0;
}
bool ValidorNot(void) {
        char Password[324];
        gets(Password);
        if (!strcmp(Password, "DevSecOps"))
                return(true);
        else return(false);
}
```

Fig. 2 Vulnerable C program

Appendix:

Some Hints:

1. In pipeline, if you want to clone a git to a non-empty folder, you should first delete that folder!

   sh 'if [-d "sechw1"]; then rm -R sechw1-pre; fi'

2. In pipeline, if you want to change the folder, you can use the following code example:

```
dir("sechw1-pre") {
        sh 'pwd'
        sh 'xxxx xxxx xxxx'
}
```

3. If you want to run python program, you can use the commands:

   sh 'python3 xxx.py'

4. If you want to create a big binary file, you can use the following code example in shell:

   echo `perl -e 'print "1"x20 . "\xc0\x51\x55\x55\x55\x55"'`> a1

   ** **Note that** you can try **320 – 340 bytes** for input test.

5. Some useful commands in GDB

   disass main
   disass PrivateGame

   b *main+xx

   x/100gx $rsp-384