Sistemas de Software Seguros
Segurança de Software
2024/2025
Class Project: Experiments with Static Analysis

1. Objective

This class project aims to experiment with the Flawfinder and WAP static analysis tools to search for vulnerabilities.

2. Flawfinder

Flawfinder is a simple static analysis tool that can be used to check programs written in C and C++. The tool is in the `apps/flawfinder/` directory.

Use Flawfinder to analyze the C file of `qwik-smtpd.c`. The file is available at `/home/ss/apps/vulnApp`.

Determine if the warnings corresponding to the following lines correspond or not to actual vulnerabilities. In other words, are they false positives or not? Lines: 152; 211; 422.

The man page of Flawfinder can be obtained at:

https://dwheeler.com/flawfinder/flawfinder.pdf

3. WAP

WAP is a static analysis tool that can be used to discover vulnerabilities and remove them in web applications written in PHP. The tool is in the in the `apps/WAP/` directory.

a) Checking that the vulnerability exists

Use WAP to analyze `Zipec` (Zenoss iPhone Event Console), a web application allowing Zenoss users to view currently active events/alarms for their infrastructure, from an iPhone.

The application is located at `/home/ss/apps/vulnApp`. You should run the following steps to run WAP over `Zipec`, to attempt to discover various classes of vulnerabilities but without correcting the code, i.e., without removing the vulnerabilities found:

```
cd ~/apps/WAP/wap-2.1
./wap -a -all -p /home/ss/apps/vulnApp/zipec-0.32
```

The command needs to be executed from: `/home/ss/apps/WAP/wap-2.1/`

NOTE: one **always needs to use the full path** and NOT the relative path to indicate the file to be analyzed!!!!
Check which classes of vulnerabilities the tool discovered and check if the vulnerabilities it outputted correspond or not to actual vulnerabilities.

b) Checking that the correction is correct

Despite we run WAP without performing the correction of the code, the tool indicates how the code could be corrected. Check out if the proposed correction is valid and enough to avoid the exploitation of the indicated vulnerabilities.

Delivery of the Report

The output of the class project is a report answering all the questions and including the justifications for the responses. Each group should deliver the report either by submitting it in the course Moodle page or, if there is some difficulty with this method, by emailing it to TP class professors. The file type should be a pdf.

Deadline: 2 December 2024 (there will be no extensions)