INF226 Obligatory assignment

Hvar Eggereide and Syver Storm-Furru

2016-10-02

Contents

1 Introduction **2**

2 Software **3**
2.1 OpenMRS 3
2.2 HPE Fortify 4
2.2.1 Audit Workbench 4
2.3 OWASP ZAP 4
2.4 FindBugs 4

1 Introduction

For our obligatory assignment we were tasked with analyzing OpenMRS, a medical patient journal system. The analysis is performed both using static and dynamic code analysis tools (HPE Fortify and FindBugs for static analysis and OWASP ZAP for dynamic), as well as a thorough run-through of the installation process and software usage.

2 Software

2.1 OpenMRS

OpenMRS is, according to the website, the "world's leading open source enterprice electronic medical record system platform".[1] It is used in hospitals all over the world, for example in Nigeria, South Africa, India and the United States, and is supported by many different governments, NGOs, and both for- and non-profit organizations. The software has a stated goal of being uasble with no programmming knowledge, and to be a common platform for which medical informatics efforts in developing can be built.

Title Technical Specifications

OpenMRS is a client-server platform, with a web frontend. It is programmed in Java 7, using Tomcat 6 or 7 as the server framework, and MySQL 5.6 as the database backend. It also exposes a programming API to users, and is modular and extendable.

Setup The setup process of OpenMRS is quite involved and time consuming when attempting to do so on a personal computer, requiring both Tomcat, Java and MySQL to be setup. The official documentation is useful, but different parts of it uses different versions of e.g. Tomcat, so it can be confusing. It also provides install instructions for Windows and Linux distributions with Aptitude, but not for OSX or other Linux distributions.

As mentioned, OpenMRS doesn't run on the newest version of MySQL (at the time of writing MySQL 5.7), and the install instructions do not mention this. The process of figuring this out, and of removing and reinstalling a previous version of MySQL, proved to be a lengthy detour on an already long road. The instructions are also not very specific when noting which files you need to run OpenMRS in Tomcat, whether it is the source code, which was difficult to build and only return a test suite on a normal compile, a readily packaged complete install (which did not work properly), or a .war file that should be uploaded to the Tomcat server.

We first attempted setting up OpenMRS on OSX 10.11, but ran into problems when trying to install the correct version of MySQL, and therefore retried in an empty virtual machine running Linux (tested with both Lubuntu and Kali Linux). Following the install instructions were a lot easier when running Debian based distributions containing Aptitude, but we still had to find and install a previous version of MySQL.

Once everything was installed OpenMRS had some extra setup that was required, done through a web interface. This was mostly easy once the correct version of MySQL was in place. You were also given a first username and password that was, respectively, 'admin' and 'Admin123'.

[1] OpenMRS. *About OpenMRS*. `http://openmrs.org/about`. 2016.

Usage

2.2 HPE Fortify

Fortify is a static code analysis tool suite, developed by Hewlett-Packard Enterprise. It aims to "make application security a natural part of the new SDLC, enabling time to market by building security in".[2]

Fortify is a propietary solution, but is available with an academic license for free.

2.2.1 Audit Workbench

Audit Workbench is the static code analysis software contained in the Fortify package. It is an IDE built on top of Eclipse, specially designed for static analysis.

2.3 OWASP ZAP

ZAP is a dynamic analysis tool developed by OWASP, the Open Web Security Project. The software acts as a proxy between the host computer and a web application, performing different types of automatic scans, as well as having tools for manual searches for security vulnerabilities.[3]

2.4 FindBugs

[2]HPE. *Application Security.* `http://www8.hp.com/lamerica_nsc_carib/en/software-solutions/application-security`. 2016.

[3]OWASP. *OWASP ZAP 2.4 Getting Started Guide.* 2016.