CS3205 Information Security Capstone Project

Semester 1 2017/2018

Tool Assessment Report

Team 1	Name	Student #
Member #1	Ang Kiang Siang	A0125528E
Member #2	Cao Wei	A0144422R
Member #3	Chai Wai Aik Zander	A0076510M
Member #4	Choo Rui Bin	A0124636H
Member #5	Chua Li Qun Shawn	A0129612J

1 Tools/Software Utilised

The following sub-sections lists the tools and software that we will utilise for the various components of this project.

1.1 Web server

We will be using Apache HTTP Server to host our web server (Version: 2.4.27). To ensure that the web traffic is communicated via HTTPS, an SSL certificate issued by a trusted publisher will be used (see Authentication).

1.2 Authentication

To authenticate the users, JSON Web Token (JWT) can be employed to transmit information securely between parties. It can be signed with a secret (HMAC) or a public / private key pair (RSA). JWT will be useful in maintaining authentication on our web system, authenticating the user with the token to access other services available. On top of that, we can implement HTTPS to ensure a secured channel for user authentication - we will be using the *.comp.nus.edu.sg RSA certificate for this.

1.3 Database management

MySQL, an open-sourced database management system, will be used to maintain the database for our web project. MySQL provides a scalable and user-friendly database, allowing us to cater to the efficient storage of the fast expanding medical records that our system will be handling. In addition, MySQL also offers features such as stored procedures and triggers to enable us to perform an extended validation and control on the data.

The latest stable version as of this report writing is 5.7.19.

1.4 Languages

We will be utilising the following programming languages for the project.

Server-side: PHP (Latest Stable Version: 7.1.8)
Client-side: HTML/5, CSS, JavaScript

1.5 Testing framework

We will utilise PHPUnit as our unit testing framework for the server-side PHP. It is the standard for PHP testing and is based on the xUnit architecture, which is similar to that of JUnit, something that we are familiar with.

In addition, we can also use HttpUnit **(**https://github.com/StackExchange/httpunit) for testing compliance of web and net servers with desired output.

1.6 Sanitization

We can use HtmlPurifier, a PHP standards-compliant HTML filter library to remove malicious contents from the user inputs such as XSS with an specially audited whitelist.

1.7 Pentesting

Kali Linux (by Offensive Security) is an option available to us. It consists many useful tools for our pentesting needs.

The tools listed here are non-exhaustive: Metasploit Framework (Exploitation), sqlmap (SQL Injection), Nikto (Web Server Scanner), Dirbuster (Web Directory Traversal), Nessus and OpenVAS (Vulnerability Scanners), nmap (Port and Service Scanner).

1.8 Communication

Telegram will be used as our main communication medium. Its cloud-based concept allows for seamless access from multiple devices, making it easy for us to communicate from either our phones or PCs.

1.9 Source code control/Issue management

GitHub will be used for source code control. We chose GitHub because it is a reliable system used by many developers in the industry. It also allows to keep track of the different changes made, and who made them, saving us the trouble of keeping track ourselves. In addition, since this is a private repository, other teams will not be able to view our source code until we are permitted to release them.

We will also be using GitHub's issue tracker for issue/bug management. GitHub's issue focuses on collaboration and reference. It will be easier for the developers to keep track of the undergoing feature adding and bug fixing.

A link to our project repository can be found here: https://github.com/zandercx/cs3205_t1.

1.10 Documentation

Google Docs will be used for collaboration and editing of the documentation relating to the project. As all of us have Google Accounts and are familiar with Google Docs, this serves as the best choice.