

**BIT304 FINAL YEAR PROJECT I**

**LITERATURE REVIEW**

**MANTRA: Automated Penetration Testing for Web Application Using Flask Python Web Framework**

Ida Bagus Budanthara (E1500366)

Submitted to the

FACULTY OF COMPUTING AND DIGITAL TECHNOLOGY

(SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY)

In partial fulfilment of the requirements

for the degree of

Bachelor of Information Technology (HONS)

HELP UNIVERSITY

SEPTEMBER - DECEMBER 2018

1. **Introduction**

Penetration testing is a method that used to evaluate the security of a system or computer network by performing attack simulation. Penetration testing itself can be performed to uncover the weaknesses of a system especially its security and determine the ways in which the system can be compromised by a potential attacker (Fried, 2000). According to OWASP Web Application Security Testing Methodology that is focused on web application security, the process involves active analysis of web application to find technical issues and vulnerabilities of website application. The security issues that have been discovered will be given to the system owner included with report that contains information about estimated impact as well as the technical solutions of those problems (OWASP Foundation, 2008).

Penetration testing has proven effective in helping analyse security issues on the system. Penetration testing technique cannot only be applied to application system, but can also be applied to computer network and operating system. It has a main purpose to find and then try to exploit the vulnerabilities that have been known or been detected on the tested system.

Analyzed from the existing web penetration testing, its utilities is almost similar as another penetration test application and it is an open source application. The difference are on the programming language and framework used. Based on what we have discussed, we create an automated penetration testing for web applications using the Flask website framework for Python programming language called MANTRA which has advantages in the installation process, a simpler display that aims to make web developers and penetration testers easy to use this web application.

1. **Benefit and Challenges of Penetration Testing**
2. **Benefits of Penetration Testing**

Penetration testing is a very important part of evaluating and repairing the security of an organization or system. One of purpose of penetration testing is to improve the security of a system or network simulated using technique used by an attacker. Penetration testing can also help an organization quantify the impacts and likelihood of the vulnerabilities. This will allow the organization to prioritize and implement corrective measures for reported known vulnerabilities (Bacudio, Yuan, Chu, & Jones, 2011).

There is a difference between vulnerability scanning and penetration testing. The vulnerability scanning determines the flaws or problems that already exist, while penetration testing evaluates the system against real attacks. Penetration testing is able to attack the system and evaluate the readiness of the system. In addition, vulnerability scanning is not identifying the significance of an intrusion, but only lists the possible potential vulnerabilities. The penetration testing is an authorized way to break the architecture of the system using attacker‘s technique (Tewai & Misra, 2015).

1. **Challenges of Penetration Testing**

There are many challenges that can provide good opportunity to find out better solution to disable and achieve better quality. Major challenges of penetration testing, such as (Tewai & Misra, 2015):

* Lack of time, because doing penetration testing would take time to find out vulnerabilities in the system.
* Security issues that could be another challenge for penetration testing that is not provide a full evidence either from hacker or network flaws but can only mitigate them.
* Automation testing that performed by using some tools that can reduce test execution time and perform regression testing after some modification or enhancements. Penetration testing is a reliable way to solve security problems of the tested system. If performed normally and consistently as a part of security policy then organization overall security definitely improves.

1. **Proposed System**

With the development of information technology in the world nowadays, the most common problem in website development is security issues in development process. There are still many website application developers who pay little attention to information security from website applications that are being developed. There are many possible data leakage if it considers that the application system security is not important. The worst possibility may be occurred when unauthorized people can take over access control in the website application system by exploiting vulnerabilities from the website application. To prevent those adverse activities, an action needed to identify security issues in applications, especially websites called penetration testing.

The main purpose of this application is to facilitate the penetration tester to conduct a security audit process to website application system that is that can run automatically and efficiently. This application helps website developers in providing information on security vulnerabilities contained in a website application. This application has the function of automatically scanning and exploiting the tested website application, then will produce report that contains detailed information about the vulnerabilities that have been discovered and been exploited by the system.

1. **Methodology and technique**

**Methodology**

Agile is a methodology that will we use in this project. We choose this methodology because this methodology is suitable for developing information systems that have changing business requirements. This methodology also called Scrum because it has one of the most popular nimble software development frameworks. The goal of Scrum is to provide software that serves to demonstrate more frequently and quickly during a software development project.

The main benefit of the Scrum framework is repetitive development and the opportunity to automate penetration tests. Therefore, security vulnerabilities can be found and be resolved more frequently, positively contributing to the protection of the overall information system (Tomanek & Klima, 2015).

Therefore, we choose agile methodology because it is suitable for developing website application systems and can easily handle the cycle of continuous improvement. This methodology also focused on teamwork, so that it allows us all as developers to communicate with each other to develop the expected website applications.

**Technique**

For our project, we would use white box testing. White box testing also called as structural testing, structural testing technique that designs test cases based on the information derived from source code. The white box tester, which in the case are our team, as the developers of the website application know what the code looks like and writes test cases by executing methods with certain parameters. White box testing is concern with the internal mechanism of a systems, it mainly focus on control flow or data flow of a programs (Nidhra & Dondeti, 2012).

With white box testing, the pen tester performs the attack with full knowledge of the infrastructure, defence mechanisms and communication channels of the target organization (Farkhod Alisherov A. & Y., 2009). We can design test cases that test the internal functioning of the website application from the developer’s perspective. White box testing mainly focus on internal logic and structure of the code. White-box conducted because we full knowledge on the program structure. With this technique, it is possible to test every branch and decision in the website application. When the internal structure is known, it will be able to look at different coverage criteria. One of the crucial is decision coverage. The test is precise only if we recognize what the application is supposed to do. We would be able to see if the program separates from its intended goal by using white box testing.

1. **Platform Used**

**Operating System**

1. **Ubuntu 16.04 LTS**

Ubuntu is a Linux-Based operating system that developed by the community that is perfect for personal computer and servers. It contains all the applications need to develop our website application because easy to use and many tools are compatible with Ubuntu Linux operating system (Allen & Owens, 2010).

**Application Building**

1. **Python**

Python is an OOP (Object Oriented Programming) language, and we have in fact been using many object-oriented concepts already. We chose Python as it easy to use, has supported for many libraries and it does not need to be compiled such as Java for our back-end in the website application (Heinold, 2012).

1. **Flask**

Flask is a python web framework that takes advantage of the work already done by Werkzeug to properly interface WSGI (Web Server Gateway Interface). Flask is a one of development in Python libraries that used for website development and it is support for many packages with various dependencies (Flask, 2017).

1. **SQLite**

SQLite is an open source, embedded relational database. We use SQLite to provide a convenient way for our website applications to manage data without the overhead that often comes with dedicated relational database management systems. SQLite has a well-deserved reputation for being highly portable, easy to use, compatible, efficient, and reliable (Allen & Owens, 2010).

1. **HTML & CSS**

Hypertext Mark-up Language (HTML) is a standardized tagging text for website application development. HTML has usability for tagging text files to achieve any element on website page such as graphic, colour, font and hyperlink. HTML contains a set of code that can help our team to develop the interface of our webpage system. HTML combined with Cascading Style Sheets (CSS) that will be able to help our team to manage the tag and style of the developed website application.

1. **Sublime Text 3**

Sublime Text 3 is a text editor for proprietary cross-platform. It is user friendly and support many mark-up and programming languages. We can be able to add a function that needed with plugins.

1. **Browser**

Browser needed to develop our website application system. We will test our website in browser. We use several browsers to test our system, such as Google Chrome and Mozilla Firefox.

1. **Git**

Git is a postmodern version control system that offers the familiar capabilities of CVS or Subversion. Git stretches the very notion of version control systems (VCS) by its ability to offer almost all of its features for use offline and without a central server (Mccullough, 2018).

1. **UML**

UML refers to a graphical language for specifying, visualizing, constructing, and documenting the artefacts of a software-intensive system. UML offers a standard way to write a system’s blueprint, including conceptual components such as actors, business process, system’s components and activities.

1. **Adobe Photoshop CS6**

Adobe Photoshop is a raster graphics editing that developed by Adobe System. We use Photoshop to make the prototype of our website application. We use this application for prototyping interface design of our website.

**Creating Project Document**

1. **Microsoft Words**

Microsoft Words is a popular graphical word processing application that developed by Microsoft. This application is easy to use, Microsoft Words have a feature that help our team to manage the document easily and can process the image in the word document. We use Microsoft Words 2016 for creating our final project documents.

1. **Microsoft Power Point**

Microsoft Power Point is used to presenting our project. This application is easy to use. This application will help our team to make the presentation be attractive. We use for this application is Microsoft Power Point 2016.

1. **Microsoft Visio**

Microsoft Visio is an application to make diagram and vector graphic that developed by Microsoft. We use this application to make class diagram and use case diagram. For developing this project, we use Microsoft Visio 2016.

1. **Gantt Project**

Gantt Project is an open source tool for project scheduling and management. This application helps our team to create tasks and milestones, organize tasks in a work breakdown structure, draw dependency constraints and create baselines. However, every task duration should be input as days and cannot be set as hours. It might also be confusing for beginners who just started using Gantt Project.

1. **Conclusion**

The web application technology has been developing very fast with the development of programming technologies nowadays. It will be hard to do a testing especially a security test if a system has been using the new technology. The alternative way to overcome security issues from website application is to use an automated application in testing. It can be concluded that penetration testing is required to find the flaws or vulnerabilities of the tested website application.

For a detailed web application test, it is necessary to use all the tools available, such as detecting XSS (Cross Site Scripting), SQL Injection, LFI (Local File Inclusion), RCE (Remote Command Execution) and other vulnerabilities. That is a laborious and time-consuming job if done manually, even the web developer understands how to build the system but they might be not understand how to secure it as well. Therefore, the automatic security testing such as MANTRA as an automated penetration testing that will conduct an analysis and exploitation to the website application and provide report of testing process to the web developer or the penetration tester everything processed and generated automatically. Discovered vulnerabilities information from this tools will be better to be manually checked for the verification purposes. The automated penetration test applications have a deficiency since they are not be able to independently decide on the appropriate action to be taken on the basis of the semantics of the content viewed and analysed. The experience and knowledge of the tester who conducts penetration testing is a crucial factor for quality and a complete analysis of web applications. But the existence of automated penetration test application is still necessary due to help the work of penetration tester and the website developer to develop and secure the website application from potential threats.

1. **References**

Allen, G., & Owens, M. (2010). *The Definitive Guide to SQLite*.

Bacudio, A. G., Yuan, X., Chu, B.-T. B., & Jones, M. (2011). AN OVERVIEW OF PENETRATION TESTING. *International Journal of Network Security & Its Applications (IJNSA)*, *3*(6), 19–38.

Farkhod Alisherov A., & Y., F. S. (2009). Methodology for Penetration Testing. *International Journal of of Grid and Distributed Computing*, *2*(2), 43–50.

Flask. (2017). *Flask Documentation*.

Fried, S. (2000). Introduction to Penetration Testing. *Data Security Management*, 9.

Heinold, B. (2012). *A Practical Introduction to Python Programming*.

Mccullough, M. (2018). *Getting Started With Git*.

Nidhra, S., & Dondeti, J. (2012). Back Box and White Box Testing Techniques – A Literature Review. *International Journal of Embedded Systems and Applications (IJESA)*, *2*, 29–50.

OWASP Foundation. (2008). *OWASP Testing Guide*.

Tewai, A., & Misra, A. K. (2015). Evaluation and Taxonomy of Penetration Testing. *International Journal on Recent and Innovation Trends in Computing and Communication*, *3*(8), 5297–5302.

Tomanek, M., & Klima, T. (2015). Penetration Testing in Agile Software Development Projects. *International Journal on Cryptography and Information Security (IJCIS)*, *5*, 1–7.