

Title	A tool that use several scripts to detect cross-site scripting vulnerabilities
Student name:	Yang Ding
Supervisor name:	Nawfal Fadhel

Aims/research question and Objectives

The main project aim is to develop a penetration testing tool on cross-site scripting (XSS) vulnerability based on several open source penetration testing tools. The new software will use different script from open source software and perform the testing using those scripts. The testing result will combine results from all the scripts and give an overall list of XSS vulnerability of the target.

The main objectives of the project are listed below:

- 1. Determine the tools/script that been used to build the software.**
There are many scripts can be used to detect XSS vulnerability, but they are using different programming language and some of them contain different functions that are not related to XSS vulnerability, the first objective is to walkthrough the code of them and pick some of the tools that can be integrate together.
- 2. Develop a tool running on Linux that can detect XSS vulnerability using several scripts.**
Once the scripts been used are decided, the next objective is to build up the code that can make them work as one whole program. The program should have several basic requirements, for example the program should work on Linux and use command line to run. The software should provide an easy to use command line interface for user to give some basic information about the target website and the testing, then perform the testing automatically. After the test it should be able to give a list of vulnerabilities been found and specified where the vulnerability exist.
- 3. Deploy a target virtual machine that running several vulnerable applications.**
Having the tools that can perform penetration testing, what is need next is the target machine for the test. Usually the XSS attack towards normal website is going to be illegal, but there are open source project that can provide a virtual machine or web application to be used for training purpose, those are going to be what been used in this project. Those virtual machines/applications will be deployed on a target computer and only can be accessed in the same intranet.
- 4. Perform the penetration testing towards virtual machine using the tool been developed and the scripts independently, gathering the result from all scripts.**
Having a target that can be used in the test, the objective next is to run some test using the tool been developed. All the result of the testing will focus on the number of vulnerabilities found and the times it takes to finish the testing. This will give a brief overview on if the tool works as expected and if it does, how well it performed.

Summary of proposed research and analysis methodology

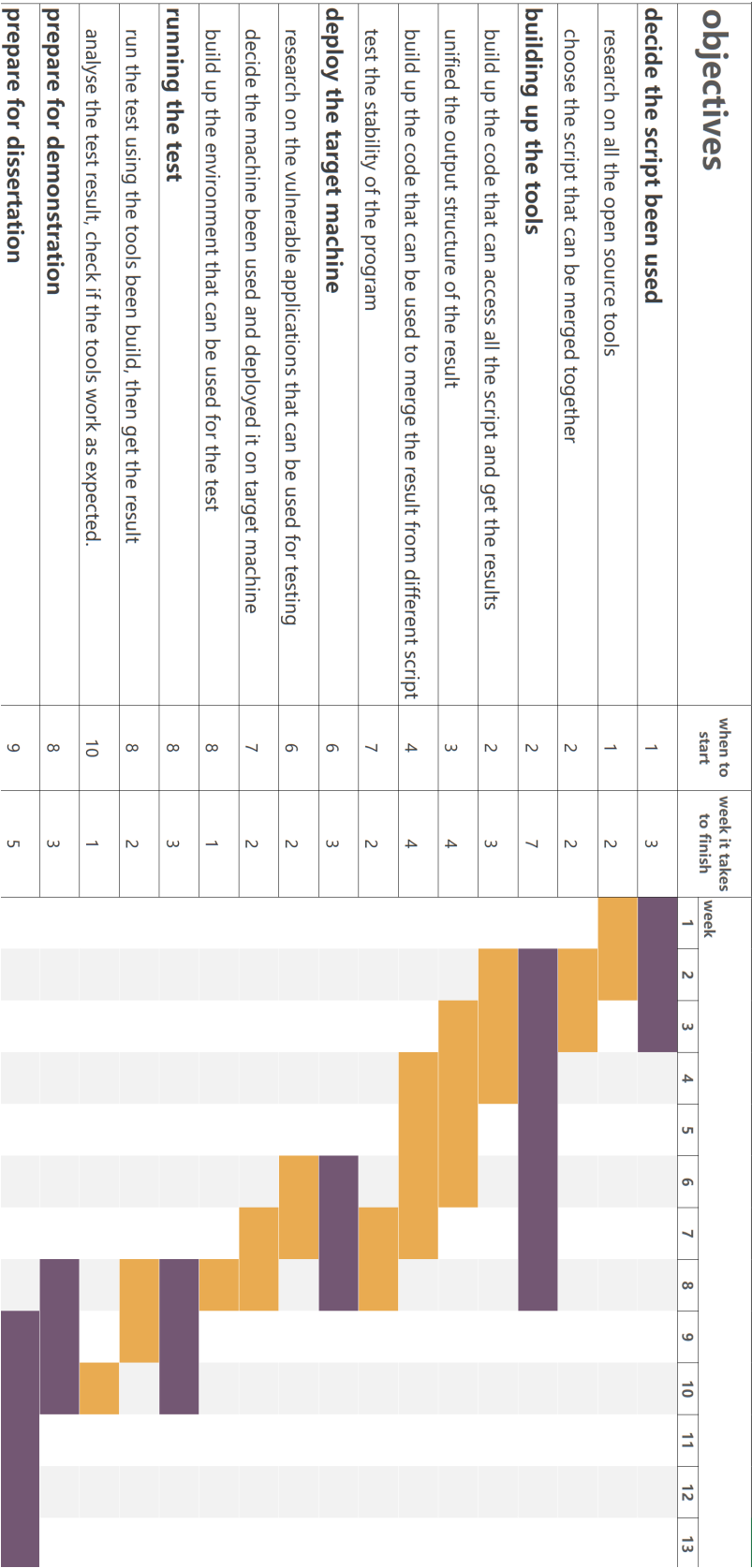
The project is to build a software, so the main part of the project is all about coding. For coding part, there will be no research and analysis included, the only analysis needed is to make sure that the tool meets the original needs after the coding. For the final product, several requirements are needed, listed as follow:

1. The tools should use C/Java/python as programming language, the actual language been used is not decided yet, it will be decided based on the scripts been choose, as the software should be able to communicate with the scripts. The limitation of only the scripts with same language can be able to build into one program will also influence the decision of what scripts to choose.
2. The program should let user be able to change the scripts using in the program, which means user should be able to modify the scripts for program.
3. As most of the scripts work best on Linux system, the tools been build should also work on Linux systems, it should be able to interact with the user though command line, and using it to gain basic information that are needed for the test (URL/IP of the target, scripts to use, file to store the vulnerabilities list, etc.) .
4. After getting the information that is needed for the test, the program should run the test automatically.
5. The program output should store in a .txt files and that output should be able to merge the result from all scripts chosen by user. This also means the same vulnerabilities been found using different script should be merge into one on the list.

Research plan – Gantt chart or Pert chart

The research plan is shown as below using Gantt chart:

Main objective is shown in purple bar, sub-task is shown in yellow bar.



Ethical statement

The goal of the project is to build a tool that can find a list of XSS vulnerabilities of a target system, the tools will only be able to find those vulnerabilities and have no functions to break into the system using this tool. This tool only provides a way to detect the vulnerabilities of the system, it will be useful for protecting the system rather than attack and break into it. Considering the focus of this tool is only detect the vulnerability in order to improve the security of the system, no illegal or unethical problem exists in the project.

Legal and commercial aspects

For legal aspects, as the tool this project is building is used to detect the XSS vulnerability in a system, and XSS attack is one of the most used attack method in cyber-attacks, this software can work as a support tool to find out what vulnerabilities the target been attacked has during a criminal investigation. The testing result from the tool can be an evidence of the vulnerabilities a system has and that could help investigation in understand the attack method of the hacker.

Commercially, the tool can be used in penetration testing to a server of a company, so it can help the company knowing the weak point of their system then be able to fix it. As the tool is mainly a combination of already existing penetration testing tools, it is easy for company to change the component in it then modified the tool to run specified penetration testing scripts they want, which can help simplified the workload of the testing process.