

A tool that uses several scripts to detect cross-site scripting vulnerabilities

Problem

Cross-site scripting (XSS) attack is one of the most common used method to attack a digital system. According to Open Web Application Security Project (OWASP), XSS attack is at the seven place of OWASP top 10 web application security risk in 2017 [1]. In order to deal with this problem, many developer have figure out different way to protect a system from XSS attack. The project aims 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.

Background

According to the data from CVE security vulnerability database [2], from 1999 to 2019, 12.5% of the recorded vulnerabilities are XSS attacks. In 2019, 1593 vulnerabilities are based on XSS (only considering the vulnerabilities that have been identified), make it the second common vulnerabilities of the year, detailed data shown in the figure 1 below.

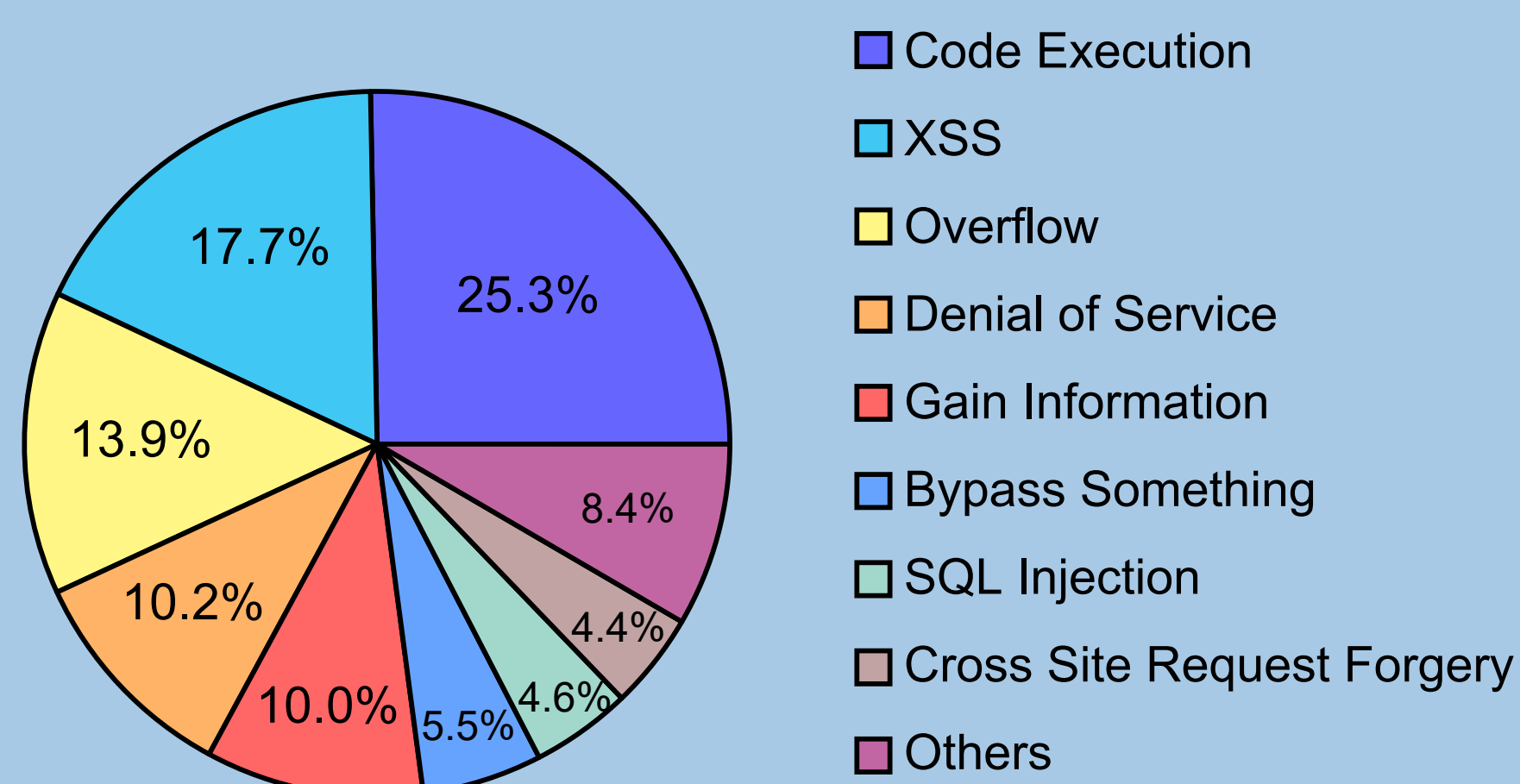


figure 1: percentage of different vulnerabilities been found in 2019

Figure 2 show the number of 8 common vulnerabilities during 2010-2019 (data gained from CVE security database [2]). The data shows that XSS is one of the most common vulnerabilities been used in cyber attack, and in recent year, there are more and more XSS vulnerabilities been found.

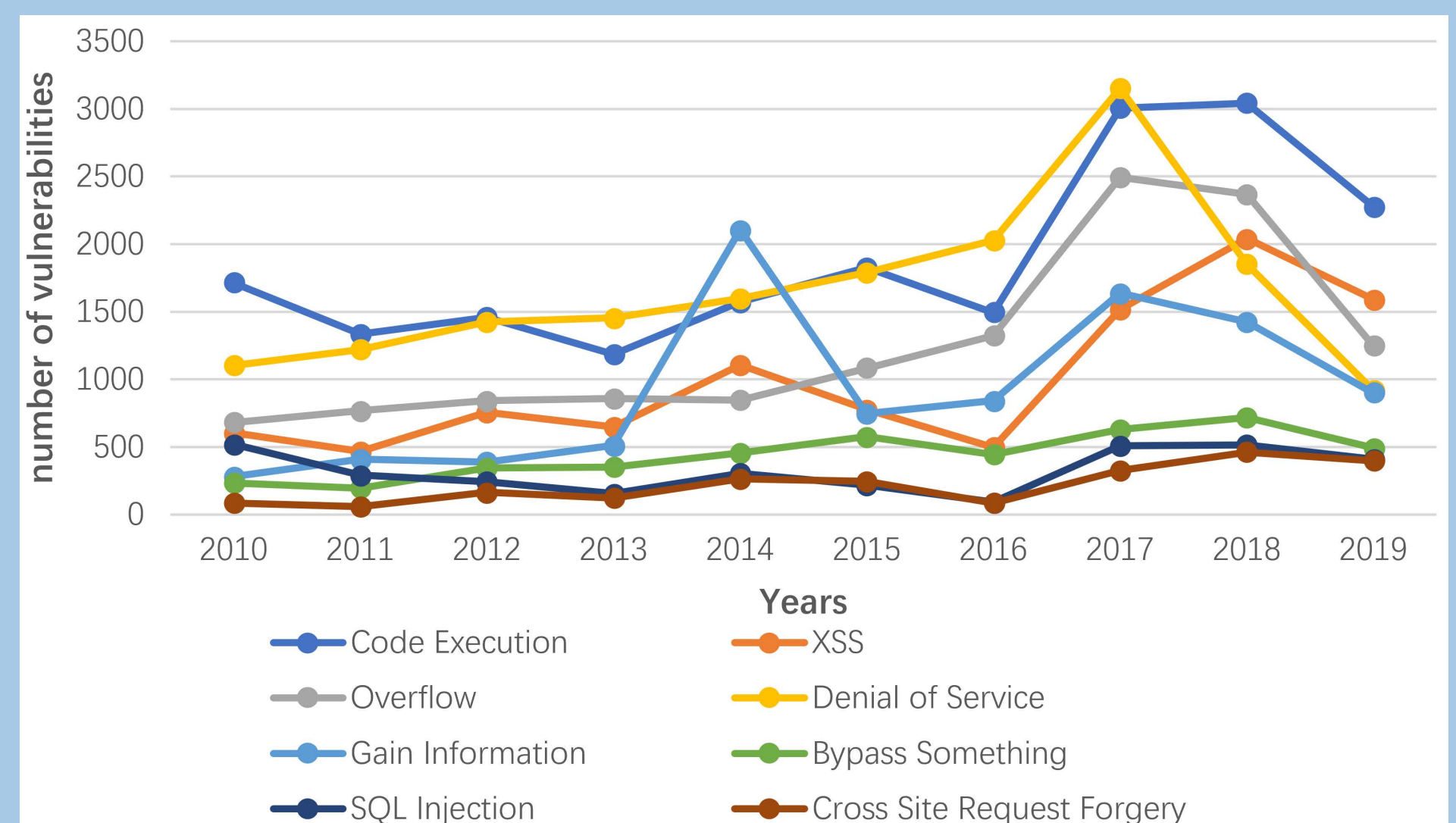
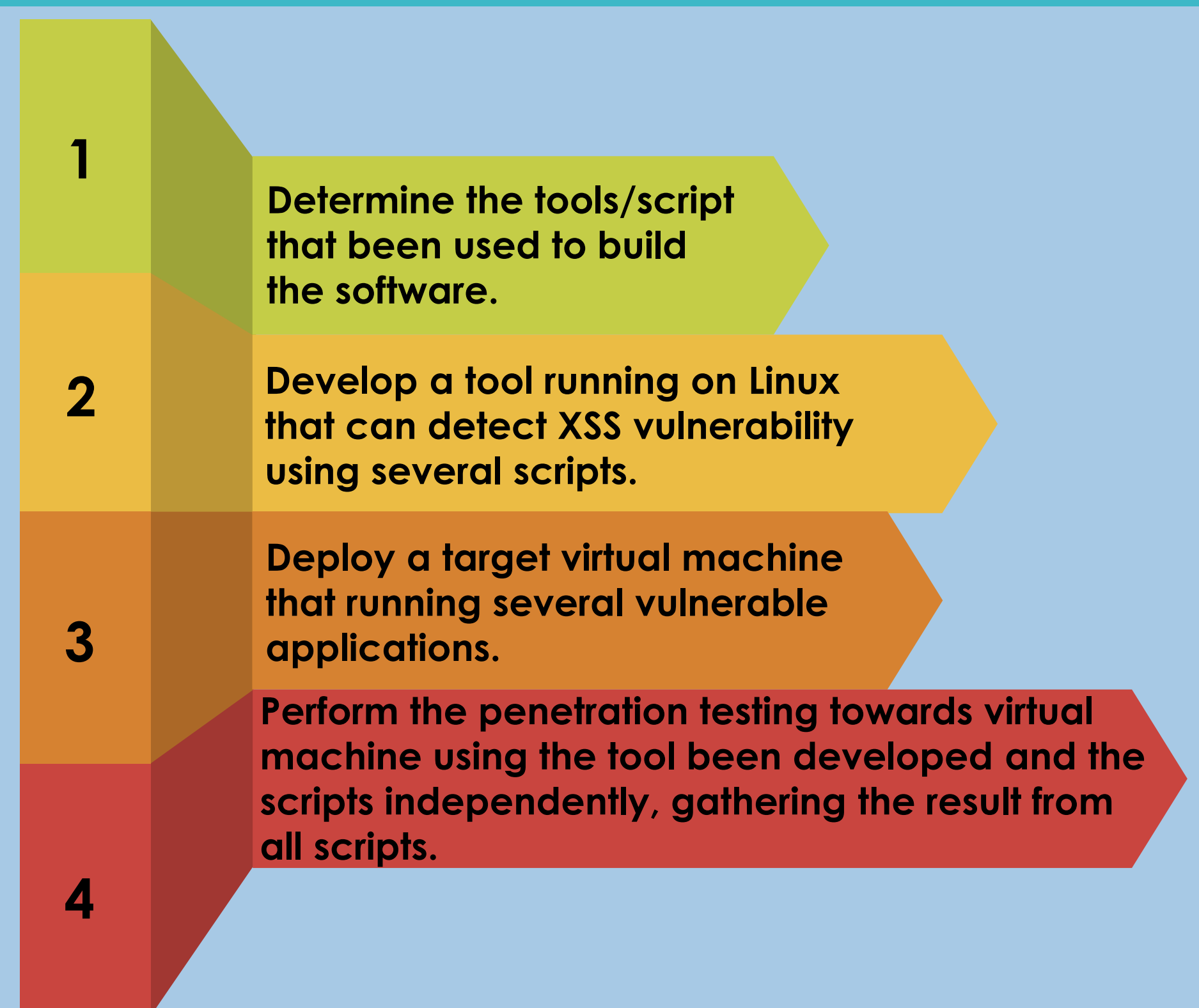


figure 2: number of 8 common vulnerabilities from 2010 to 2019

Objectives



Outcome

The final outcome of this project will provide a software that can be used to detect XSS vulnerabilities using different script given by the program user. this will help detecting the vulnerabilities of the system and help programmer to better protect it. It is also going to be easy for user to change the script been used , of even modified the program to detect other kinds of cyber security vulnerabilities, which will provide huge convenience to user when doing penetration testing.

Reference:

- [1] "QWASP Top Ten" [Online]. Available: <https://owasp.org/www-project-top-ten/>
- [2] "Vulnerability distribution of CVE vulnerability by types" [Online]. Available: <https://www.cvedetails.com/vulnerabilities-by-types.php>