Peer review of Group 6 : "Understanding Exploited Vulnerabilities"
Economics of Cyber Security - Assignment block 2
28/09/2015

Summary

In this report, the main idea is to try to make a link between vulnerabilities that are already known and the ones, among the known vulnerabilities, that are exploited. A lot of data is available online and way of sorting it must be done. In a second part, students have tried to make a correlation between the number of vulnerabilities in a system and the level of security, and between the popularity of systems like WordPress or Joomla!, and the number of reported vulnerabilities.

The students, in this report, have decided to deal with Cross-Site Scripting (called XSS) and SQL injections vulnerabilities. To try to measure the level of risk, some metrics are put in place in organizations. They are most of the time sorted by categories (management, operational or technical metrics).

In practice, we can find different standard offering a method or a range of metrics, like CVSS or the « Microsoft Exploitability Index » for example, to estimate the level of risk. The conclusion of the group towards this is that there is a gap between existing metrics and what is desirable in term of risk measurement.

To answer the question try to get more information about whether a system is secured or not, students have set up four metrics.

The first one deals with the percentage of SQL-injection and XSS vulnerabilities that are actually exploited by attackers and is based on the database coming from cvedetails.com

The second one is about reported exploits, both XSS and SQL injections, in Security Focus.

Metric number 3 was put in place to analyse whether there is a correlation between the exploitation of a vulnerability and the CVSS score of the vulnerability.

Finally, metric number 4 is focused on the CMS vulnerabilities, and especially the link between market share (and, popularity of software as well) and reported vulnerabilities.

After studying the data, student shave been able to show that a very few percentage of vulnerabilities is actually exploited, that there's a relevant correlation between market share and number of reported vulnerability for both WordPress and Joomla! softwares, and that we can put some limitations in the data and evaluation scores that can be found on the internet.

Strengths

This whole report is clear and understandable, due to the fact that some points are well introduced.

Metrics are simple, and thus easy to understand and to measure.

The conclusion of part 6.3 (Metric 2 : Reported Exploits) is interesting and relevant in the way that you explain your results and take your distances with the data and you do not make a general conclusion regarding what to measured.

Concerning the global metrics, the explanations of metrics chosen are good and well structured. Your charts are, most of the time, easy to read and clear.

Major Issues

Concerning the first metric, the method isn't clearly explained and thus we don't really know how sure are the figures mentioned. A little bit more explanation may be given to help us understanding this, and make us being more convinced about the figures. Furthermore a conclusion could have been sketched regarding the small amount of vulnerabilities effectively exploited.

Concerning metric n.4, we can discuss the viability of the model, and the results shown, because here we can see a significant correlation between the number of reported vulnerabilities and the market share of the two products listed, but we can wonder whether it would be the same conclusion for other products.

Minor Issues

One suggested thing would be to introduce a little bit more the two kinds of vulnerabilities (XSS and SQL injections), by explaining in what consist these types of attacks.

All R codes are provided in appendix, which is very good, but no mention of the way you dealt with or succeeded into processing the data is mentioned in the report, whereas it must have been an important part of the time spent on this assignment.