World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:05, 2017

Benchmarking of Pentesting Tools

Authors : Esteban Alejandro Armas Vega, Ana Lucila Sandoval Orozco, Luis Javier García Villalba

Abstract : The benchmarking of tools for dynamic analysis of vulnerabilities in web applications is something that is done periodically, because these tools from time to time update their knowledge base and search algorithms, in order to improve their accuracy. Unfortunately, the vast majority of these evaluations are made by software enthusiasts who publish their results on blogs or on non-academic websites and always with the same evaluation methodology. Similarly, academics who have carried out this type of analysis from a scientific approach, the majority, make their analysis within the same methodology as well the empirical authors. This paper is based on the interest of finding answers to questions that many users of this type of tools have been asking over the years, such as, to know if the tool truly test and evaluate every vulnerability that it ensures do, or if the tool, really, deliver a real report of all the vulnerabilities tested and exploited. This kind of questions have also motivated previous work but without real answers. The aim of this paper is to show results that truly answer, at least on the tested tools, all those unanswered questions. All the results have been obtained by changing the common model of benchmarking used for all those previous works.

Keywords : cybersecurity, IDS, security, web scanners, web vulnerabilities
Conference Title : ICIT 2017 : International Conference on Information Technology
Conference Location : Paris, France
Conference Dates : May 18-19, 2017

Open Science Index, Computer and Information Engineering Vol:11, No:05, 2017 publications.waset.org/abstracts/70338.pdf