OWASP Top 10 (2017) as an armor against Cyber-crime

Konstantinos Giovas, George Iakovakis

giovas@aueb.gr, giakovakis@aueb.gr

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory

Dept. of Informatics, Athens University of Economics & Business (AUEB), Greece

Introduction

The Open Web Application Security Project (OWASP) is a security report that outlines the top ten most harmful vulnerabilities. In this report, our main goal is to make a deep analysis in the OWASP Top 10 project [9] pointing out why each vulnerability happens, the impact that may cause to the organization, the types of attacks that may occur and the prevention/detection techniques that have to be adopted in order to achieve sufficient security. In order to do this, we need automated tools that are necessary to reach our goal. In this research, we are going to present a list of automated tools such as vulnerability scanners, monitor and logging tools and antivirus software. There will be a brief outline for every tool and tables that will provide useful information about every tool like its strong and weak points, the price of the tool, the scalability and others.

Definitions

In order to comprehend the main section of our results it is vital to explain the next definitions:

- **Vulnerability Scanner**: A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. The modern vulnerability scanner often has the ability to customize vulnerability reports as well as the installed software, open ports, certificates and other host information that can be queried as part of its workflow.

- **Monitor and Logging tool**: Monitor and Logging tools are types of software that monitor log files. Servers, application, network and security devices generate log files. Errors, problems, and more information are constantly logged and saved for analysis.

- **Antivirus Software**: Antivirus software, or anti-virus software (abbreviated to AV software), also known as anti-malware, is a computer program used to prevent, detect, and remove malware.

Classification Tables of Mitigation Tools

Our results are mainly presented on three tables. ***Table 1*** shows an example of Vulnerability Scanners presentation. The tools are classified according to the following criteria: (i) Strengths, (ii) Weaknesses, (iii) Free trial, (iv) Cost/Price, (v) Scalability, (vi) Technical Support, (vii) Vulnerability assessment, (viii) Reports and Analytics, (ix) Ease of use - GUI offered, (x) Compatibility.

Table 2 shows an example of Monitoring and Logging Tools presentation. The examined tools have been classified based on the following parameters: (i) Strengths, (ii) Weaknesses, (iii) Free trial available, (iv) Cost/Price, (v) Scalability, (vi) Technical Support, (vii) Reports and Analytics, and (viii) Ease of use - GUI offered.

Subsequently, ***Table 3*** shows a presentation example of antivirus software. Antivirus software, which are classified using the following nine criteria (i) Strengths, (ii) Weaknesses, (iii) Price, (iv) On-Demand Malware Scan, (v) On-Access Malware Scan, (vi) Website Rating, (vii) Malicious URL Blocking, (viii) Phishing Protection, (ix) Behavior Based Detection and results are listed in ***Table 3***.

Tool name	Strengths	Weaknesses	Free trial	Cost/Price	Scalability	Technical Support	Vulnerability assessment	Reports & Analytics	Ease of use, GUI offered	Compatibility
Acunetix[1]	- Ease of use features and functionalities - Quick setup with a wide range of test - Network & web vulnerability scan	- Lack of AD support and static review process - Does not allow webservers audit - Scan may be slow when run over the Internet	Yes	From 3.685€	Yes	Yes	Yes	Yes	Yes	Windows

***Table 1**: Example of Vulnerability scanners presentation*

Tool name	Strengths	Weaknesses	Free trial available	Cost/Price	Scalability	Technical Support	Reports and Analytics	Ease of use, GUI offered
Solarwinds Network Performance Monitor (NPM) [2]	- Easy to implement and customize - Free fully functional demo - Ease of scalability	- Expensive - There are some user interface issues	Yes	From 2440€	Yes	Yes	Yes	Yes

***Table 2:** Example of Monitor and Logging tools presentation*

Tool Name	Strengths	Weaknesses	Price	On-Demand Malware Scan	On-Access Malware Scan	Website Rating	Malicious URL Blocking	Phishing Protection	Behavior Based Detection
McAfee AntiVirus Plus [3]	- Strong protection - Good scores in hands-on tests - Perfect score in anti-phishing tests	- Fewer features in iOS - PC Boost web Speedup works only in Chrome	From 19.99$/device(year)	Yes	Yes	Yes	Yes	Yes	Yes

***Table 3:** Example of Antivirus Software presentation*

Conclusions and Results

The purpose of this survey was to categorize security tools which deal with threats and vulnerabilities that arise in this new era. The rationale for implementing our research was to identify the most effective tools and present them based on specific criteria so that any interested parties can benefit. Our scope is not to suggest a specific tool, but through its analysis and presentation with the use of appropriate criteria, to help stakeholders choose the right one, i.e., the one that suits better to their own information systems. Results showed that most vulnerability scanners that we examined meet most criteria and the decision regarding which to use is ultimately, based on strengths, weaknesses, cost and compatibility with multiple platforms. A closer look at their shortcomings can help one avoid attacks on an information system. A combination of the tools can also provide better protection. With regards to the monitoring and logging tools, interested parties can select from a wide range of solutions. The analysis we made helps them decide which one suits better to their systems. Weighing the pros and cons and in conjunction with cost, scalability, technical support and reports, our research can act as a guideline for reaching a decision.

References

1. Acunetix.com. 2021. Acunetix. [Online]. Available from: https://www.acunetix.com/
2. Solarwinds.com. 2021. Solarwinds.com. [Online]. Available from: https://www.solarwinds.com/network-performance-monitor
3. Mcafee.com. 2021. Mcafee.com. [Online]. Available from: https://www.mcafee.com/consumer/en-us/store/m0/index.html
4. Clarke J. (2009). *SQL injection attacks and defense*. Burlington, MA: Syngress Pub.
5. Lawal M.A, Sultan A.B., Shakiru A., 2016. Systematic Literature Review On SQL Injection Attack. International Journal Of Soft Computing. 1(11), pp. 26-35.
6. Thome et al. 2017. Security Slicing for Auditing Common Injection Vulnerabilities. Journal Of Systems and Software. 137(1)
7. Alwan Z., Younis M., 2017. Detection and Prevention of SQL Injection Attack: A Survey. International Journal of Computer Science and Mobile Computing. 6(8), pp. 5-17.
8. Rajasekar N., Imafidon C., 2011. Exploitation Vulnerabilities in Cloud-Storage. GSTF International Journal on Computing. 1(2).
9. Owasp.org. 2019. Owasp.org. [Online]. [20 July 2019]. Available from: https://www.owasp.org/index.php/
10. Rapid7.com. 2019. Rapid7. [Online]. [22 July 2019]. Available from: https://www.rapid7.com/products/appspider/
11. Indusface.com. 2019. AppTrana. [Online]. [22 July 2019]. Available from: https://apptrana.indusface.com/
12. Theoharidou M., Tsalis N., Gritzalis D., "In Cloud we trust: Risk-assessment-as-a-service", in Proc. of the 7th IFIP International Conference on Trust Management, pp. 100-110, Springer (AICT 401), Spain, 2013.
13. Tsalis N., Mylonas A., Gritzalis D., "An intensive analysis of the availability of security and privacy browser add-ons", in Proc. of the 10th International Conference on Risks and Security of Internet and Systems, Springer (LNCS), Greece, 2015.
14. Tsalis N., Virvilis N., Mylonas A., Apostolopoulos A., Gritzalis D., "Browser blacklists: A utopia of phishing protection", in Security and Cryptography, Springer (CCIS), 2015.
15. Tsalis N., Theoharidou M., Gritzalis D., "Return on security investment for Cloud platforms", in Proc. of the Economics of Security in the Cloud Workshop, pp. 132-137, IEEE Press, UK, 2013.
16. Gritzalis D., Iseppi G., Mylonas A., Stavrou V., "Exiting the risk assessment maze: A meta-survey", ACM Computing Surveys, Vol. 51, No. 1, pp. 11.1-11.30, January 2018.
17. Gritzalis D., Tsoumas V., "An assurance-by-ontology paradigm proposal: Elements of security knowledge management", in: Information Assurance and Computer Security, Vol. 6, pp. 15-30, Johnson T. (Ed.), IOS Press, The Netherlands, 2006.
18. Stergiopoulos G., Valvis E., Anagnou-Misyris F., Bozovic N., Gritzalis D., "Interdependency analysis of junctions for congestion mitigation in Transportation Infrastructures", ACM SIGMETRICS PER Review, Vol. 45, No. 2, pp. 119-124, 2017.