needs same attack dataset to evaluate. In dynamic analysis, providing this type dataset is very difficult. So, accuracy comparison is neglected. The proposed mechanism has simple and effective architecture and implementation which is hybrid analysis based, and very low algorithm overhead. It is cost effective and fastest method in compared. The proposed mechanism attempts to prevent four most common risk types "Injection", "Insecure Direct Object References", "Invalidated Redirects" and "Forwards and Missing Function Level Access Control" which involve parameter tampering (Menemencioğlu & Orak, 2017).

In this research, the accumulated data is examined in detail from geographical point of view.

Implementation web application is in Turkey. Except from Turkey, the most vulnerability attacks are from USA and Russia, Ukraine and China. This can be involved economic and technological development level except Ukraine. In other words, the attackers are mostly located in most developed countries.

Ukraine can be assessed as a splash of the Russian effect when the political impression is considered. Total Europe vulnerability value is about 7 percent.

The distribution of IP series and the rate of A class IP distribution imply the existence of vulnerability detection mechanisms or attack mechanisms like a crawler. Future work will give some thought to these mechanisms.

These appreciations lead the IP based or location based restriction in web based applications, firewall software and hardware products. Future works can focus on IP matching algorithms in the light of the retrieved information in this research.

REFERENCES

Boyle, B. A., & Alwitt, L. F. (1999). Internet Use within the U.S. Plastics Industry. *Industrial Marketing Management*, *28*(4), 327–341. http://doi.org/10.1016/S0019-8501(98)00012-1

Lee, I., Jeong, S., Yeo, S., & Moon, J. (2012). A novel method for SQL injection attack detection based on removing SQL query attribute values. *Mathematical and Computer Modelling*, *55*(1–2), 58–68. http://doi.org/10.1016/j.mcm.2011.01.050

Menemencioğlu, O., & Orak, İ. M. (2017). A Simple Solution to Prevent Parameter Tampering in Web Applications. In *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities* (pp. 1–20). IGI Global. http://doi.org/10.4018/978-1-5225-1938-6.ch001

Menemencioğlu, O., Sonuç, E., Karaş, İ. R., & Orak, İ. M. (2013). Academic Curriculum Vitae based Faculty Information System. In *XV. Akademik Bilişim Conference Proceedings* (pp. 1123–1127). Antalya, Turkey. Retrieved from http://ab.org.tr/ab13/kitap/menemencioglu_sonuc_AB13.pdf

Natarajan, K., & Subramani, S. (2012). Generation of Sql-injection Free Secure Algorithm to Detect and Prevent Sql-Injection Attacks. *Procedia Technology*, *4*, 790–796. http://doi.org/10.1016/j.protcy.2012.05.129

Schwartz, E. J., Avgerinos, T., & Brumley, D. (2010). All You Ever Wanted to Know About Dynamic Taint Analysis Forward Symbolic Execution (but might have been afraid to ask) A Few Things You Need to Know About Dynamic Taint Analysis Forward Symbolic Execution (but might have been afraid to ask) The Root. *Policy*, 1–5.

Zhang, H., Kuan Tan, H. B., Zhang, L., Lin, X., Wang, X., Zhang, C., & Mei, H. (2011). Checking enforcement of integrity constraints in database applications based on code patterns. *Journal of Systems and Software*, *84*(12), 2253–2264. http://doi.org/10.1016/j.jss.2011.06.044