The Combination of OWASP Top 10 and GDPR regulation as a Restraining Tool Against Cyber-crime

Panagiotis Vagenas, George Iakovakis

pan.vagenas@gmail.com, giakovakis@aueb.gr

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory

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

Introduction

In this research, we examine the possibility OWASP Top 10 and GDPR to be used as tools in fighting cyber-crime. We perform a detailed analysis of each flaw included in OWASP Top 10 (2017). In the analysis of those flaws, we include both the technical and the administrative issues that could lead to an incident, and we examine the potential impact from those risks with an emphasis in data leakage, and we propose technical and administrative measures that mitigate the risk. We also perform a high-level overview of the GDPR, with an emphasis on those requirements that can be used as a guide to enforce measures and policies that help in preventing data breaches. We then examine data-breach statistics from widely accepted reports, to conclude whether OWASP Top 10 and GDPR can be used as tools that could prevent those breaches.

OWASP Top Ten Analysis

The OWASP Top 10 document [1] in its latest version (released in 2017), includes ten flaws and risks and give a high-level description of each one of them. The specific risks and flaws to be included in this document are chosen based on exploitability, detectability, and impact of these flaws. The evaluation of each flaw is done by the project's members, which include a variety of security experts from around the world who have shared their expertise to produce the final Top 10. ***Table 1*** shows OWASP Top 10 overview.

#	Vulnerability	Exploitability	Prevalence	Detectability	Impact
A1	**Injection**	Easy	Common	Easy	Severe
A2	**Broken Authentication**	Easy	Common	Average	Severe
A3	**Sensitive Data Exposure**	Average	Widespread	Average	Severe
A4	**XML External Entities**	Average	Common	Easy	Severe
A5	**Broken Access Control**	Average	Common	Average	Severe
A6	**Security Misconfiguration**	Easy	Widespread	Easy	Moderate
A7	**Cross-Site Scripting**	Easy	Widespread	Easy	Moderate
A8	**Insecure Deserialization**	Difficult	Common	Average	Severe
A9	**Using Components with Known Vulnerabilities**	Average	Widespread	Average	Moderate
A10	**Insufficient Logging & Monitoring**	Average	Widespread	Difficult	Moderate

Table 1: *OWASP Top 10 overview [1]*

General Data Protection Regulation (GDPR)

The 2016/679 General Data Protection Regulation (GDPR) is a European Union's data protection and privacy regulation [2]. The EU Parliament approved GDPR on 14 April of 2016, and it was enforced on 25 May 2018. GDPR replaces the Data Protection Directive 95/46/EC and is designed to regulate the processing by an individual, a company, or an organization of personal data relating to individuals in the EU. GDPR defines a minimum data protection framework, leaving the details to be defined by the individual member states. GDPR forces organizations to take all the required measures to protect individuals by defining a set of rights that every EU citizen can exercise.

Tools in Fighting Cyber-Crime

In the fight against cyber-crime, many tools can help to mitigate the risks from issues described in the OWASP Top 10. An organization should be able to identify its assets need protecting and utilize the appropriate tools for this purpose. In this research, we discuss the available solutions and briefly present some tools that are widely used.

- IDS/IPS: Intrusion Detection System (IDS) is an application that monitors a resource for malicious activity or policy violations. An Intrusion Prevention System (IPS) is an IDS with response capabilities, it can also take specific actions depending on the detected activity or violation.
- Web Application Firewalls [3]: a security policy enforcement point positioned between a web application and the client endpoint. It may be a stand-alone device or integrated into other network components.
- Penetration Testing Tools [4]: Penetration Testing is a process that simulates a cyber-attack in a computer system to evaluate its security

Results Performance

A web application is increasingly a standard attack vector. From all data breaches, about 29% in 2017, 18% in 2018, and 25% in 2019 were leveraging web applications' flaws as their attack vector. For specific industries, web applications are becoming the favorite attack vector for adversaries. For example, payment data breaches in which web applications servers are the main attack vector, are constantly gaining popularity year over year [5].

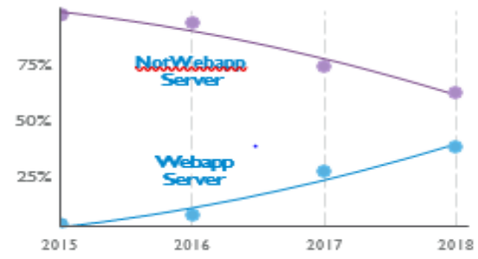

Figure 1: *Web application server vs not web application server assets in payment data breaches over time [5]*

In those incidents that a web application is the attack vector, it usually includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms [5]. Regarding the exploits of code-level vulnerabilities, according to data provided by Defiant [6] the most popular vulnerabilities adversaries are trying to exploit fall all under the flaws described in OWASP Top 10 2017. This data concerns a single month (May of 2019), but it is worth noticing that XSS was the most popular attack with more than 235 million hits recorded (out of about 3.611 billion attacks), while SQLi comes second with more than 103 million attacks.

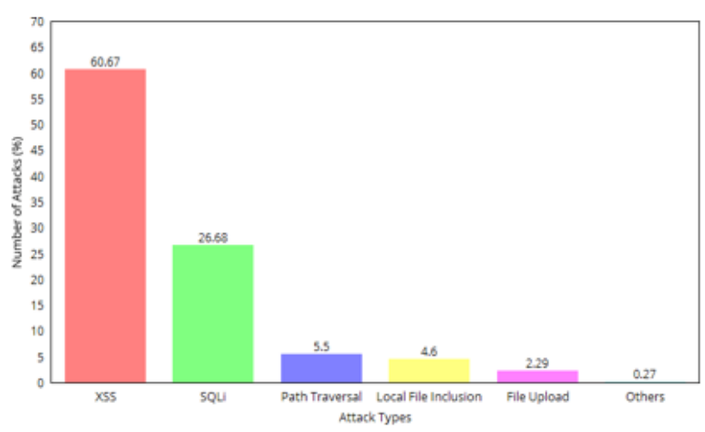

Figure 2: *Attack flaws malicious actors were trying to exploit in May 2019 [6]*

Conclusions

OWASP Top 10 2017 version includes ten flaws related to web applications. These flaws are ordered in the Top 10 based on exploitability, detectability, and impact of each flaw. All these flaws can seriously undermine the confidentiality, integrity, or the availability of web applications. It must be clear at this point, that all but the last web applications security flaws described in OWASP Top 10 can lead to the compromise of data. As these flaws concern web applications, it is worth noticing what are the attack vectors in data breaches and how often web applications are used as an initial foothold in those breaches. Seeing this the other way round, GDPR forces organizations to apply required measures and policies to avoid data breaches. In case a web application is included in the organization's assets, those measures should include at least protection from flaws included in OWASP's Top 10 as most of them can lead to a data breach. Applying those measures can potentially protect an organization from the most prevalent attacks targeting web applications. Which means, using the GDPR as the force and OWASP Top 10 as the tool, organizations can significantly improve their security against cyber-crime.

References

1. OWASP Top 10 - 2017, The Ten Most Critical Web Application Security Risks. English. OWASP, 2017. URL: https:// www. owasp. org/ index. php/ Category: OWASP Top Ten Project
2. General Data Protection Regulation (GDPR) Overview | IT Governance UK. URL: https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation
3. Pubal J. "Web Application Firewalls". SANS Institute, Mar. 13, 2015. URL: https://www. sans.org/reading-room/whitepapers/application/web-application-firewalls-35817
4. Bishop M. "About penetration testing". In: *IEEE Security & Privacy* 5.6 (2007), pp. 84–87.
5. Verizon. *Data Breach Investigations Report (DBIR) 2019*. Verizon, 2019. URL: https://www. verizonenterprise.com/verizon-insights-lab/dbir/ (visited on 05/28/2018).
6. Defiant. 2019. *Home - Defiant*. [online] Available at: <https://www.defiant.com/>
7. Mylonas A., Tsalis N., Gritzalis D., "Hide and seek: On the disparity of browser security settings" (poster), 9th Symposium on Usable Privacy and Security (SOUPS-2013), United Kingdom, July 2013.
8. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures", International Journal of Critical Infrastructure Protection Vol. 12, pp. 46-60, 2016.
9. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in Proc. of the 8th International Conference on Availability, Reliability & Security, pp. 248-254, IEEE Press, Germany, 2013.
10. 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.
11. 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.
12. Tsalis N., Stergiopoulos G., Bitsikas E., Gritzalis D., Apostolopoulos T., "Side channel attacks over encrypted TCP/IP Modbus reveal functionality leaks", in Proc. of the 15th International Conference on Security and Cryptography (SECRYPT-2018), pp. 53-63, Portugal, July 2018.