ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (7-8), Month: October - December 2020, Available at: www.researchpublish.com

How to Prioritize Remediation of Cybersecurity Weaknesses in Web Applications

Wael M. Alagi, Sultan AlSharif

Saudi Aramco, Dharan, Saudi Arabia

***Abstract*: In large organizations with a vast number of in-house developed web applications, identifying security weaknesses (vulnerabilities) is not a major challenge; because automated tools utilizing various techniques, such as Taint Analysis and Data Flow Analysis, are capable of identifying millions of vulnerabilities in application's source-code based on OWASP Top 10 classification. One of the main issues challenging security analysts is the prioritization and classification of vulnerabilities. While the assessment tools will provide "lists of vulnerabilities classified by the OWASP Top 10 or some other compliance-oriented scheme" (Laura Bell, 2017), it is still not practical to timely-address risk mitigation of web applications. Most security teams would prefer to first address remediations based on the business-critical applications that manage confidential data. An example could be a B2B website that handles financial transactions. But adopting this approach will render other more popular websites, handling less sensitive information, at the bottom of the remediation list.**

***Keywords*: In-house developed applications, business-critical applications, web-page utilization, reprioritize remediation.**

1. INTRODUCTION

Organizations can incorporate web-page utilization (or web-page popularity) as another source of information to reclassify and prioritize vulnerabilities. The technique is to plan remediation by incorporating the information obtained from sources, such as web application server logs, to determine the popularity of web pages; and determine which ones are most visited by the end users. This information is then combined with the existing classification schemes to formulate a prioritized remediation plan.

Because most visited webpages with identified security weaknesses will have higher risk of exploitations in comparison to low-utilized web pages; and by combining the utilization data with existing classification schemes, security analysts will be equipped with a more practical approach to contextually prioritize remediation activities, based on usage statistics, in addition to the existing classifications provided by OWASP Top 10.

2. TECHNIQUE IMPLEMENTATION

Every web application consists of a collection of web pages and associated files including source-code files, which are checked for vulnerabilities using Static Application Security Testing (SAST). The result of scanning the source code files using automated tools will generate a significant number of findings with enough details to explain the criticality, location, and type of findings, plus many other details in a consolidated report.

Most scanning reports summarize the findings in a tabular format called heat map (Table 1: Sample Security Vulnerability Matrix). The below sample heat map demonstrates the total number of findings, where the need — for a more refined approach using a systematic scheme to reclassify and reprioritize remediation efforts — is needed when dealing with hundreds of web applications.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (7-8), Month: October - December 2020, Available at: www.researchpublish.com

Table 1: Sample Security Vulnerability Matrix

	Security Findings		
	Definitive	Suspect	Information
High	3,435	1,209	2,000
Medium	50,408	34,309	4,400
Low	3,009	43,454	14,220

The computing environment, hosting any web application, logs the user engagement for each web page; and accordingly, various information about the popularity, number of visits, and time spent on each web page can be obtained to support this technique.

By combining the security findings classifications generated by the security scanning tools and the web hosting environments logs details, we can reprioritize and reclassify the findings and update their criticality based on the newly obtained details.

This can be achieved by dividing the utilization data into percentile groups and combine it with the vulnerability heat map to develop a new matrix. The following table is an example of a reclassification matrix:

Table 2: Reclassification Matrix

	Web-page utilization percentile		
	80-100%	60-80%	0-60%
High	▬	▬	▬
Medium	↑	↑	▬
Low	↑	↑	↑

3. CAN MACHINE LEARNING (ML) ALGORITHMS HELP IN THIS SCENARIO?

By combining the web page utilization data with existing classification schemes, security analysts will be equipped with a more practical approach to contextually prioritize remediation activities. This approach will also improve timely remediation and limited resource utilization to address security weaknesses.

By utilizing ML models to combine both sources of information (scanning reports and web application logs), this technique can be further improved to automate the process and yield more accurate results. But this is also dependent on the size of data to be processed, and the number of web applications to be assessed.

REFERENCE

[1] Laura Bell, M. B.-S. (2017). Agile Application Security: Enabling Security in a Continuous Delivery Pipeline. O'Reilly Media, Inc. OWASP. (2018, June 3). OWASP Top Ten Project. Retrieved from OWASP: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project