International Journal of Engineering & Technology, 8 (1.9) (2019) 87-91

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Risk Analysis of Information System in Academic Institution based on Business Perspective: A Case Study

Prajna Deshanta Ibnugraha[1,2*], Lukito Edi Nugroho[1] ,Paulus Insap Santosa[2]

1Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Yogyakarta, Indonesia
2School of Applied Science, Telkom University, Bandung, Indonesia
**Corresponding author E-mail: prajna.deshanta.i@mail.ugm.ac.id*

Abstract

Information system of academic institution is used to manage data from students, staffs and lecturers that consists a lot of critical information like student grades, accounts and other private information. However, some of information system have SQL injection vulnerability which occurs data security breach. It has possibility to make reputation damage and other business impact in academic institution. Therefore, objective of this study is to analyze risk based on business perspective as basic process to select suitable mitigation. OWASP is exisiting method that considered as proper method for risk analysis in this study because it has explicit metrics related business approach. Based on experiment result, business impact of vulnerability can be measured. However, some metrics still need to be developed to get more precision result that describe real impact for business of institution.

Keywords: *Risk analysis, OWASP, information system, SQL injection.*

1. Introduction

Information system is built to support business of academic institution. It involves a lot of information. Therefore, IT security is needed to be implemented in information system to protect critical information. IT security incidents in information system cause serious problem for institution. Data security breach is incident that often occured in information system of academic institution. It causes negative sentiment that impacts to reputation and financial of institution (Sinanaj, Muntermann, & Cziesla, 2015). The caused of data security breach mostly is SQL injection (OWASP, 2013)(Huang, Liu, Fang, & Zuo, 2016). Therefore, security assessment and risk analysis related with SQL injection are important process to know about security level of information system in academic institution.

Risk analysis is process to assess impact of vulnerability to organization. Risk rating is important part of risk analysis to give level status of vulnerability like high, medium or low. Output of risk analysis is useful for institution as basic information to make mitigation priority. DREAD, OWASP and CVSS are methods that often used to rate risk of vulnerability.

This study has objective to analyze risk of SQL injection vulnerability in case study with business approach. The anaysis result will be evaluated to get precision information about business impact. OWASP risk rating is selected to this study because it has explicit metrics related business approach.

2. Related Works

Some previous studies have discussed about risk analysis. Cifuentes et al. analyzed security vulnerability of mHealth application. mHealth is application that has functions for medical information, education and awareness, remote monitoring, diagnostic support, treatment support, communication and training for healthcare workers. The most vulnerabilities were found in remote monitoring with 31% high risk, 16% medium risk and 53% low risk (Cifuentes, Beltrán, & Ramírez, 2015). OWASP approach was used to determine level of risk.

Williams assessed security risk of Raspberry Pi. NIST guidelines was used to determine security category like management security control, operational security control and technical security control (Williams, 2015). OWASP Top10 was also used as guideline of security testing. Result of assessment was rated by OWASP ranking.

Bale et al. analyzed security vulnerabilities and risk of academic information system. Facilitated Risk Analysis Process (FRAP) is method that used to identify and measure security risk (Petrus, Bale, & Sediyono, 2014). Bale et al. audited the procedure of academic information system and try to find possibility of vulnerability. Mitigation plan was constructed after risk analysis was made.

Copyright © 2019 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

3. Method

This study involves risk rating methods as part of risk analysis. The Open Web Application Security Project (OWASP) is research community that results application and guidelines in IT security. The one of OWASP product is OWASP risk rating method (OWASP, 2015). It is used to rate security vulnerability and the equation of OWASP risk rating can be shown below (Joh & Malaiya, 2011) (equation 1)

$$\text{Risk level} = \sum_i L_i \times I_i \quad (1)$$

Likelihood (Li) is often defined as probability of security attack event that adverse organization (Nyre & Jaatun, 2013). In OWASP, likelihood consists of threat agent factors and vulnerability factors (table 1).

Table 1: Likelihood factors of OWASP risk rating

Factors	Metrics
Threat Agent	Skill Level (SL)
	Motive (M)
	Opportunity (O)
	Size (S)
Vulnerability	Easy of discovery (ED)
	Easy of exploit (EE)
	Awareness (A)
	Intrusion detection (ID)

Calculation of likelihood can be shown in equation 2 :

$$Likelihood = \frac{SL + M + O + S + ED + EE + A + ID}{8} \quad (2)$$

Impact (Ii) is often defined as negative effect from security incident to organization. Impact factors consist of technical and business (table 2).

Table 2: Impact factors of OWASP risk rating

Type of Impact	Metrics
Technical	Loss of Confidentiality (Lc)
	Loss of Integrity (Li)
	Loss of Availability (Lav)
	Loss of Accountability (Lac)
Business	Finacial Damage (FD)
	Reputation Damage (RD)
	Non-compliance (NC)
	Privacy Violation (PV)

Calculation of technical and business impact can be shown in equation 3 and equation 4.

$$Technical\ Impact = \frac{Lc+Li+Lav+Lac}{4} \quad (3)$$

$$Business\ Impact = \frac{FD+RD+NC+PV}{4} \quad (4)$$

Final score of risk can be mapped as level by OWASP factors mapping table (table 3).

Table 3: OWASP factors mapping

IMPACT	HIGH	MEDIUM	HIGH	CRITICAL
	MEDIUM	LOW	MEDIUM	HIGH
	LOW	NOTE	LOW	MEDIUM
		LOW	MEDIUM	HIGH
		LIKELIHOOD		

4. Experiment Details

Experiment is done to running system of information system in academic institution. Steps of experiment can be shown below (Ibnugraha, Nugroho, Widyawan, & Santosa, 2016) :

1) Identify SQL injection vulnerability

Adding single quotation mark (‘) in the end of URL is done to identify SQL injection vulnerability (Makino & Klyuev, 2015). Application will display error message related with database if application has SQL injection vulnerability. Manual testing is done as first step in vulnerability identifying where the tester does not need automatic tool to find vulnerability. The tester only uses knowledge and experience to find SQL vulnerability in information system of academic institution. However, automated testing is also used to verify vulnerability (Goel & Mehtre, 2015).

2) Attack Vulnerability

Attack process is done to get details of explored information.

3) Analyze security risk

Risk analysis is done by using OWASP risk rating.

Experiment uses blackbox method from external testing. It means that researcher does not have knowledge about information system and experiment is done from outside institution (Bacudio, Yuan, Bill Chu, & Jones, 2011)(Shah & Mehtre, 2015). The scenario of experiment can be shown in fig. 1.

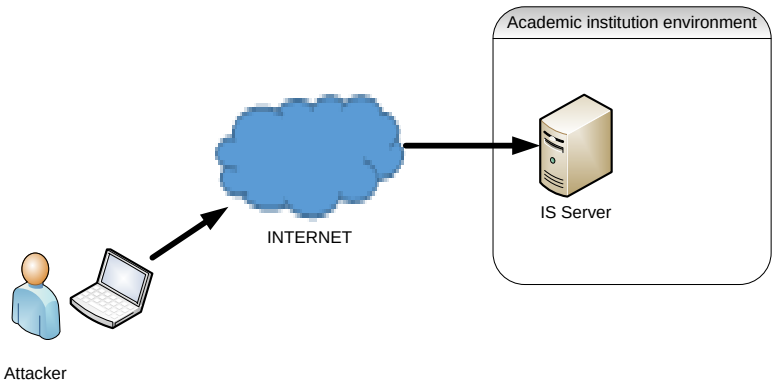


Fig. 1: Experiment scenario

5. Result and Discussion

Information can be explored using experiment steps above. Most of information is in important category like username, password, email address, home address, bank account, student grades, telephone number, date of birth and place of birth (McCallister, Grance, & Kent, 2010). The information was found in 30 tables from 24 databases. Score of metric refers to OWASP provisions to assess condition of experiment (OWASP, 2015). Mapping process of experiment conditions to OWASP score can be shown in diagram below (fig. 2) :

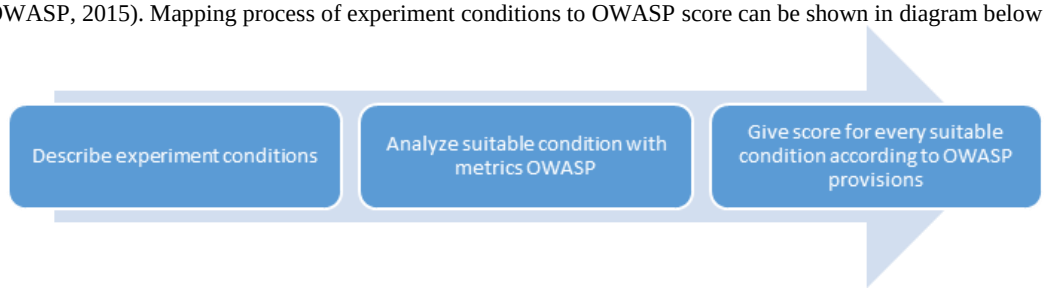


Fig. 2: Mapping diagram from experiment conditions to OWASP score

The condition resulted by experiment and score mapping, can be explained below :

1) In exploring information, attacker must have skill about penetration testing. In experiment details, attacker does not need special access. Public network can be used to attack target. Grade of students can be changed by attacker so it has possibility to get reward for attacker. Based on condition 1, score of threat agent factors can be represented in fig. 3

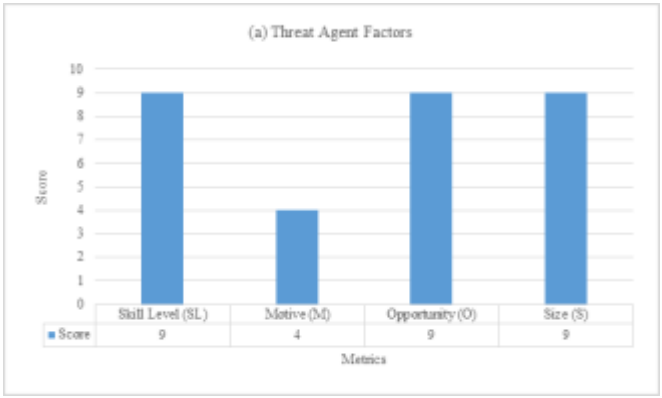


Fig. 3: Score of threat agent factors

2) SQL injection vulnerability has been released by OWASP Top10. The vulnerability can be found by tools like acunetix. Attacker can explore information in information system by tools like Havij. Information system also does not have log that record user activity in application. Based on condition 2, score of threat agent factors can be represented in fig. 4



Fig. 4: Score of vulnerability factors

3) A lot of critical information can be explored and it has possibility to interrupt service of information system. However, wrong information can be found by administrator of information system. Based on condition 3, score of threat agent factors can be represented in fig. 5

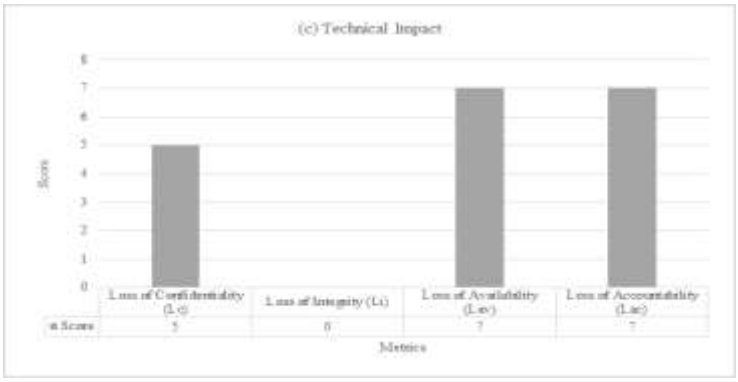


Fig. 5: Score of technical impact

4) Critical information in information system is derived from lecturers, staff and students. It can be account information, students grade and other private information. If attacker publish critical information, reputation of academic institution will be affected. However, financial loss will not occur directly. Based on condition 4, score of threat agent factors can be represented in fig. 6

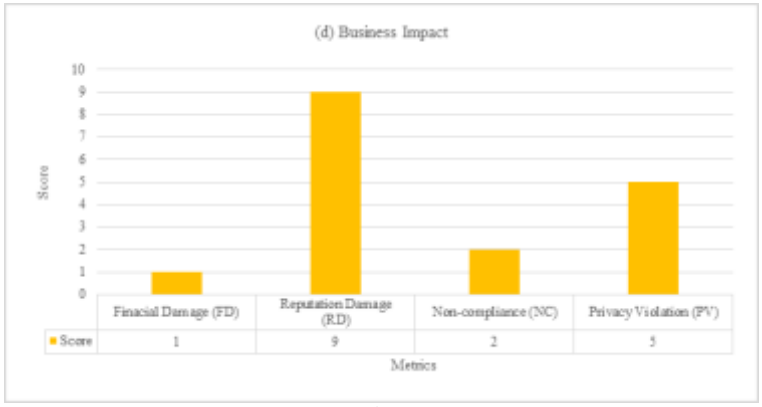


Fig. 6: Score of business impact

Based on experiment result, score and level for OWASP component can be shown in table 4.

Table 4: Score of OWASP component

Component	Condition	Formula	Score	Level
Likelihood	1,2	Equation 2	8.25	High
Technical Impact	3	Equation 3	4.75	Medium
Business Impact	4	Equation 4	4.25	Medium

The final level can be measured using equation 1 and the result can be mapped with table 3 above. In final calculation, technical impact has high level. Similar result also occurs in business impact that it has high level.

In this study, risk analysis has been successfully measured. However, OWASP risk rating uses equal weighting for every factor so it needs customization to result specific and precision business analysis (OWASP, 2015). In different environment of organization, business impact factors should have different analysis and result. Adaptive weighting is needed to complete risk analysis based on business approach. Therefore, identification of specific factors related business perspective needs to be done in future work to result more precision analysis. Weighting factors also needs to be considered by involving multiple criteria condition.

6. Conclusion

IT security incidents impact to business aspect of academic institution. Data security breach often occurs in academic institution environment and it is often caused by SQL injection attack. Therefore, risk analysis based on business aspect is needed by academic institution to measure level of vulnerability. OWASP is risk rating method that selected in this study because it has explicit metric related business perspective. In case study, reputation damage is the most influential metric than other metrics like privacy violation, non-compliance and financial damage. In experiment result, level of SQL injection vulnerability can be measured by OWASP score and it has high business impact for academic institution. However, the method still has no relation with environment metric like type of institution and type of asset. Therefore, it still needs aspect development to result precision level related business impact.

References

[1] Bacudio, A. G., Yuan, X., Bill Chu, B. T., & Jones, M. (2011). An Overview of Penetration Testing. International Journal of Network Security & Its Applications, 3(6), 19–38. https://doi.org/10.5121/ijnsa.2011.3602

[2] Cifuentes, Y., Beltrán, L., & Ramírez, L. (2015). Analysis of Security Vulnerabilities for Mobile Health Applications. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 9(9), 999–1004.

[3] Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Procedia Computer Science, 57, 710–715. https://doi.org/10.1016/j.procs.2015.07.458

[4] Huang, C., Liu, J., Fang, Y., & Zuo, Z. (2016). A study on Web security incidents in China by analyzing vulnerability disclosure platforms. Computers and Security, 58, 47–62. https://doi.org/10.1016/j.cose.2015.11.006

[5] Ibnugraha, P. D., Nugroho, L. E., Widyawan, & Santosa, P. I. (2016). Risk Analysis of Database Privilege Implementation in SQL Injection Case. Jurnal Teknologi, 78: 5-7, 113–116.

[6] Joh, H., & Malaiya, Y. K. (2011). Defining and assessing quantitative security risk measures using vulnerability lifecycle and cvss metrics. In international conference on security and management (SAM) (pp. 10–16). Retrieved from http://www.cs.colostate.edu/~malaiya/p/johrisk11.pdf

[7] Makino, Y., & Klyuev, V. (2015). Evaluation of web vulnerability scanners. In Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2015 (Vol. 1, pp. 399–402). https://doi.org/10.1109/IDAACS.2015.7340766

[8] McCallister, E., Grance, T., & Kent, K. (2010). Guide to protecting the confidentiality of personally identifiable information (PII). Recommendations of the National Institute of Standards and Technology (Vol. 800–122). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-122

[9] Nyre, Å. A., & Jaatun, M. G. (2013). Seeking Risks: Towards a Quantitative Risk Perception Measure. In Availability, Reliability, and Security in Information Systems and HCI (Vol. 8127, pp. 256–271). Springer Berlin Heidelberg.

[10] OWASP. (2013). Top 10 2013 – Top 10. Retrieved June 26, 2016, from https://www.owasp.org/index.php/Top_10_2013-Top_10

[11] OWASP. (2015). OWASP Risk Rating Methodology. Retrieved from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[12] Petrus, J., Bale, M., & Sediyono, E. K. O. (2014). Risk Management in Information Technology Using Facilitated Risk Analysis Process (FRAP) (Case Study: Acedemic Information System of Satya Wacana Christian University). Journal of Theoretical and Applied Information Technology, 68(2), 339–351.

[13] Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques, 11(1), 27–49. https://doi.org/10.1007/s11416-014-0231-x

[14] Sinanaj, G., Muntermann, J., & Cziesla, T. (2015). How Data Breaches Ruin Firm Reputation on Social Media ! – Insights from a Sentiment-based Event Study. In 12th International Conference on Wirtschaftsinformatik (pp. 902–916).

[15] Williams, M. G. (2015). A Risk Assessment on Raspberry PI using NIST Standards. International Journal of Computer Science and Network Security, 15(6), 22–30.