International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Analysis of Penetration Testing Knowledge Web Application Base FAQ XYZ Company Using the Open Web Application Security Project (OWASP)

Muchridho[1], Hustinawaty[2]
[1]Business Information System, Gunadarma University, Depok, West Java, Indonesia-16424
[2]Business Information System, Gunadarma University, Depok, West Java, Indonesia-16424

***Abstract*— *This research was conducted to determine weaknesses in the XYZ Company FAQ web knowledge base application by applying penetration testing. Research is done by gathering information about web applications, analyzing security holes in web applications and conducting tests based on security holes that have a moderate level of risk (intermediate) and based on one of the most common protections included in OWASP Top 10 Security Risks.*

***Keywords*— *Web Application, OWASP Top 10 Security Risks, Penetration Testing, Vulnerability, Knowledge Base Web Application FAQ.*

I. INTRODUCTION

Following Law No. 24 of 2011 concerning the Social Security Organizing Agency, XYZ Company is designated as the Social Security Organizing Agency (XYZ Company). The XYZ Company law requires companies to register workers as XYZ Company participants. Social Security Organizers are expected to keep abreast of global technological developments by providing online information services. Realizing the magnitude of the responsibility to provide benefits to the workforce and the company, XYZ Company develops applications that provide information related to XYZ Company through web-based knowledge-based FAQ web applications. With the availability of a knowledge base web application FAQ, participants can get information such as general explanation about social security, participation related to XYZ Company (Construction Services, Non-Wage Recipients, Wage Recipients, Membership), service information, contact center information, and electronic channel applications that are owned XYZ Company.

Behind the convenience of participants in accessing information system services in the form of a website owned by XYZ Company, there are also several security issues that trigger an attack by parties who are not responsible for data theft that can lead to fraud either for workers, companies or for XYZ Company. So that it takes operational security standards for checking applications that will be launched by XYZ Company. Penetration testing is one of the operational standards that must be carried out before the application of FAQ information is launched which is useful to ensure the security of IT service applications and fix bugs that exist in the application so that the implementation will not find security gaps that can be detrimental to workers, companies and XYZ Company.

Penetration Testing is an activity where someone tries to simulate an attack that can be done against a particular organization/company network to find weaknesses that exist in that system/network [1]. In conducting this Penetration Testing using the Blackbox Testing method which refers to the OWASP Web Application Penetration Testing. The Penetration Test target is the Knowledge Base FAQ Web Application owned by XYZ Company.

Before conducting scientific writing testing using OWASP, the writer looks for references related to web application-based security system testing methodologies. Fernando in his research proposed an Open Source Security Testing Methodology Manual (OSSTMM) method for conducting security testing on the XYZ University admission system [1]. Ashraf in his research introduced about giving an overview of the security risks of web-based applications with Model View Controller (MVC), using ASP.Net or PHP [2]. Nugroho in his research presented to determine the Impact of Security Risks Based on the OWASP Approach in three domains that proved the existence of SQL Injection and XSS vulnerability [3]. In this research, to detect security holes based on web applications can be done using several methods such as OWASP, ISSAF, OSSTMM and NIST [4]. But among the four methods, the appropriate and efficient method of penetration testing in web application-based security holes is OWASP. Besides, OWASP is also a charitable non-profit organization that is equipped with a standard guide to facilitate the tester to do penetration testing.

OWASP has ensured that all information and learning materials can be accessed easily and for free so that everyone can improve the security of their website. The material they offer in the form of documentation, tools, videos, and forums. In OWASP Top 10 Security Risks, there are 10 risks which, according to OWASP, are the most common in web applications, namely: Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, and Insufficient Logging & Monitoring.

Based on the foregoing, the author takes the title "Analysis of Penetration Testing Web Application Knowledge Base FAQ XYZ Company Using the Open Web Application Security Project (OWASP)". It is expected that with the results of this analysis, the author can provide detailed information regarding security gaps found in the BP Knowledge Knowledge Center's web Knowledge Base FAQ application and provide recommendations for improvement to the XYZ Company.

II. Research Method

According to G. J. Simons, information security is a way we can prevent fighting (cheating) or, at the very least, protection of differences in information-based systems, while the information itself has no physical meaning.

A. *Penetration Testing*

Penetration Testing (Pentest) is a method for evaluating the security of a computer system and network. Evaluation is done by doing an attack simulation. The results of this pentest are very important as feedback for the system manager to improve the security level of his computer system. Pentest report will provide input on the condition of system vulnerability making it easier to evaluate the current computer security system [6].

Penetration Testing has a standard (PTES) that is used as a reference in its implementation which is divided into several stages [7]:

1. Pre-engagement Interactions are the stages where a pentester explains the pentest activities that will be carried out to the client (company). Here a pentester must be able to explain the activities to be carried out and the final objectives to be achieved.
2. Intelligence Gathering is the stage where a pentester tries to gather as much information about the target company that can be obtained by various methods and various media. Things that need to be used as a basis for gathering information are the characteristics of network systems, the workings of network systems, and the methods of attack that can be used.
3. Threat Modeling is the stage where a pentester looks for vulnerabilities based on information that was collected in the previous stage. At this stage, a pentester not only seeks security holes but also determines the most effective loopholes to use.
4. Vulnerability Analysis is the stage where a pentester combines information about an existing security hole with an attack method that can be done to carry out the most effective attack.
5. Exploitation is the stage where a pentester attacks the target. However, this stage is mostly done by brute force method without having the element of precision. A professional pentester will only exploit when he already knows for certain whether the attacks carried out will succeed or not. But of course, there are unexpected possibilities in the target security system. However, before carrying out an attack, the pentester must know that the target has a security hole that can be used. Carrying out attacks blindly and hoping for success is not a productive method. A professional pentester always perfects his analysis first before carrying out an effective attack.
6. Post Exploitation is the stage where a pentester manages to enter the target network system and then analyzes the existing infrastructure. At this stage, a pentester studies the parts in the system and determines the most critical part for the target (company). Here a pentester must be able to connect all parts of the existing system to explain the impact of the greatest attack/loss that can occur on the target (company).
7. Reporting is the most important part of pentest activities. A pentester uses a report (report) to explain to the company about penetration testing done such as: what is done, how to do it, the risks that can occur and most importantly is a way to improve the system.

B. *Open Web Application Security Project (OWASP)*

OWASP is a non-profit organization that focuses on web app security. OWASP provides many resources for learning more about web app security. As one of its principles, OWASP ensures that all information and learning materials can be accessed easily and for free so that everyone can improve the security of their website. The material they provide in the form of documentation, tools, videos, and forums [8].

As proof of their commitment, OWASP provides several documents to help developers create secure websites and applications. The following are 5 documents that are often cited as important guidelines for developers [8].

1. OWASP Developer Guide
2. OWASP Application Security Verification Standard (ASVS)
3. Security Knowledge Framework
4. Developer Cheat Sheet Series
5. OWASP Top 10 : Checklist Standard Security Website

C. *OWASP Testing Guide v4 Checklist*

By using the OWASP method, the penetration tester has provided a series of steps for testing security gaps in web-based applications. At the same stage, the description and tools that are explained can be used to test security holes in web applications. With this being a distinct advantage for the OWASP method as one of the basic reference methodologies for penetration testing for web applications that exist in the XYZ Company [9].

There are 10 stages of the OWASP Testing Guide v4 Checklist [9]:

1. Information Gathering
2. Configuration and Deploy Management Testing
3. Identity Management Testing
4. Authentication Testing
5. Authorization Testing
6. Session Management Testing
7. Data Validation Testing
8. Error Handling
9. Cryptography
10. Business Logic Testing
11. Client Side Testing

III. Research Methods

In principle, this case study is to evaluate the security risk of the Knowledge Base FAQ Web Application using OWASP Top 10 Security Risks, which is expected from the results of penetration testing can be the basis for improvement and evaluation before the application is released into the production environment. The impact of existing security holes if there is no penetration testing process is the vulnerability of data theft, session logins, and company reputation. The following steps are taken in the Penetration Testing process as illustrated in figure 1 [10]:

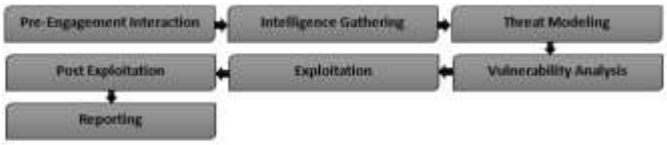

Fig. 1. Stages of Penetration Testing

In conducting this Penetration Testing using the Blackbox Testing method which refers to the OWASP Web Application Penetration Testing v4. The following is a checklist that needs to be done during Penetration Testing based on OWASP Web Application Penetration Testing v4 as illustrated in figure 2 [11] :

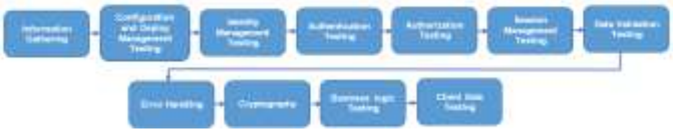

Fig. 2. Checklist OWASP Web Application Penetration Testing

IV. IMPLEMENTATION

Referring to OWASP Web Application Penetration Testing v4, the security holes obtained are categorized based on the likelihood and impact of all risks as in table number 1 [9]:

Table 1. OWASP identification results of the analysis

Stages	Description	Tools	Result
Information Gathering - Identify application entry points (OTG-INFO-006)	Identify from hidden fields, parameters, methods HTTP header analysis	Burp proxy, OWASP ZAP Proxy	Issue Low - HTML Headers
Information Gathering - Fingerprint Web Application (OTG-INFO-009)	Identify the web application and version to determine known vulnerabilities and the appropriate exploits.	Whatweb, Wappalyzer	Issue High - Insecure Component - PHP 5.5.9
Configuration and Deploy Management Testing - Test Network/Infrastructure Configuration (OTG-CONFIG-001)	Understand the infrastructure elements interactions, config management for software, backend DB server, WebDAV, FTP in order to identify known vulnerabilities.	Nessus	Issue High - Network/Infrastructure Configuration
Session Management Testing - Testing for Cross Site Request Forgery (OTG-SESS-005)	URL analysis, Direct access to functions without any token.	Burp Proxy (csrf_token_detect), burpy, ZAP	Issue Medium - Anti CSRF Tokens Scanner
Data Validation Testing - Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)	Check for input validation, Replace the vector used to identify XSS, XSS with HTTP Parameter Pollution.	Burp Proxy, ZAP, Xenotix XSS	Issue Medium - Reflected XSS (Cross-Site Scripting)

Of all the results of testing using the list of methods of OWASP Web Application Penetration Testing v4, a summary of testing is generated according to the following categories as in table number 2:

Table 2. OWASP Summary Category

No	Category	Pass	Issues	N/A	Not Started
1	Information Gathering	8	2	0	0
2	Configuration and Deploy Management Testing	7	1	0	0
3	Identity Management Testing	4	0	3	0
4	Authentication Testing	7	0	3	0
5	Authorization Testing	4	0	0	0
6	Session Management Testing	7	1	0	0
7	Data Validation Testing	26	1	0	0
8	Error Handling	2	0	0	0
9	Cryptography	2	0	1	0
10	Business logic Testing	9	0	0	0
11	Client Side Testing	12	0	0	0
Jumlah		**88**	**5**	**7**	0

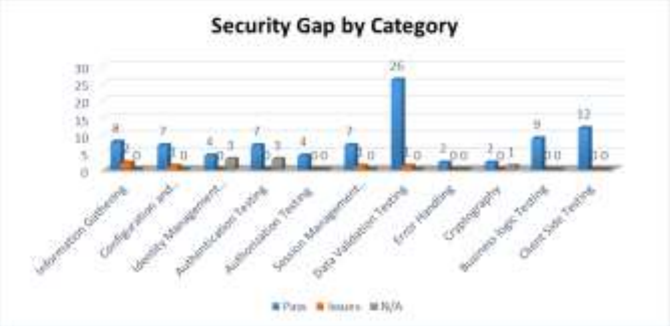

Fig. 3. Chart Security Gap Identification Results by Category

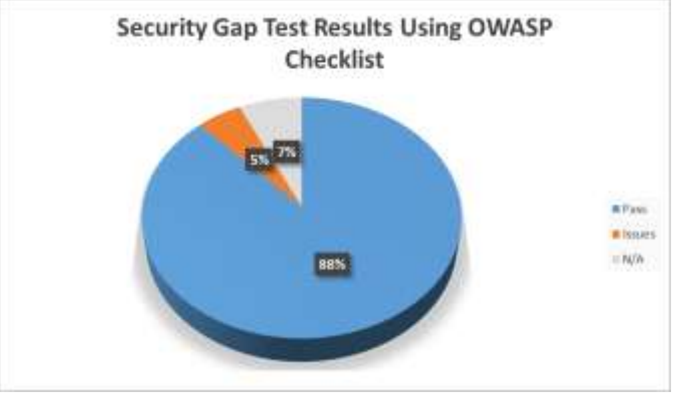

Fig. 4. Chart Test Results Based on OWASP

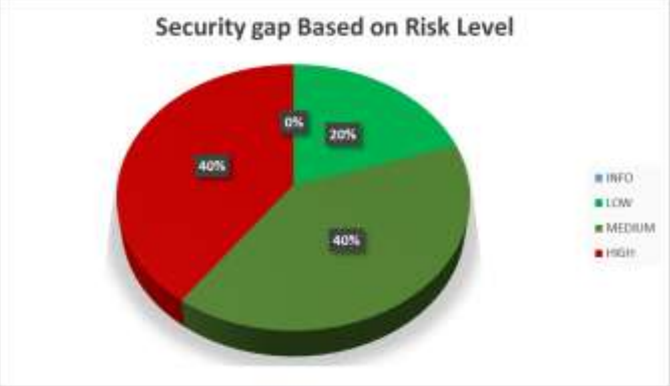

Fig. 4. Chart Test Results Based on Risk Level

Out of 100 test scenarios, 88 tests passed the identification of security holes, 5 found security issue issues, and 7 were not tested. From 5 issues found 1 finding was low impact, 2 findings were a medium impact, and 2 findings included high impact.

V. Conclusions and Recommendations

The purpose of the Penetration Testing activity has been fulfilled. The exploitation of the XYZ Company Knowledge Base Web Application FAQ results in security gaps found in the Medium category. This attack can still be developed again because it can be an Attack-vector for other attacks. Because this activity was not carried out destructively, this finding became the main objective of this Penetration Testing activity.

From the findings of this security, hole will be informed to developers to make improvements to the application security holes. This stage will be the standard procedure for the release of web-based applications on the Labor XYZ Company. This is as an IT application security control to avoid fraud related to information leakage, application bugs, and data integrity.

From the results of Penetration Testing activities that have been carried out on the XYZ Company Web Application, it is necessary to have mitigation measures to prevent the security gap from being used by irresponsible parties. The following are the recommendations for mitigation for the most significant findings outline:

1. The application still has high and medium security holes, so it needs to be improved on these security holes.
2. Give the evaluation results and recommendations on the findings of the security gap.
3. Penetration testing is the standard method for checking web application security holes.

References

[1] ITG.ID (2019). Penetration Testing Menyempurnakan Program Keamanan Informasi. [Online]. Available At : https://itgid.org/pengertian-penetration-testing/ . [Accessed 27 July 2019]

[2] Fernando, Y. I., Abdillah, R., 2016, Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM), Jurnal CoreIT, Vol. 2, No.1, Hal 33 – 40.

[3] Rafiq, A., Touseef, P., Ashraf, M. A., Analysis of Risks against Web Applications in MVC. NFC IEFR Journal of Engineering and Scientific Research, Vol. 5, No. 1, hal. 1-6.

[4] Hutagalung, R. H., Nugroho, L. E., Hidayat, R., 2017, Menentukan Dampak Resiko Keamanan Berbasis Pendekatan Owasp, Prosiding SNATI F Ke-4 Tahun 2017, Kudus, Indonesia.

[5] Juliharta, I. G. P. K., 2012, Business Impact Analysis Sistem dan Jaringan Komputer Menggunakan Metode Network Security Assessment, EKSPLORA INFORMATIKA, Vol. 2, No. 1, Hal 89 – 100.

[6] CatatanForensikDigital (2013). Penetration Test (PenTest). [Online] Available at : https://catatanforensikadigital.wordpress.com/2013/11/14/penetration-test-pentest-2/. [Accessed 27 July 2019].

[7] OWASP.ORG (2019). Penetration testing methodologies. [Online]. Available : https://www.owasp.org/index.php/Penetration_testing_methodologies. [Accessed 27 July 2019].

[8] OWASP.ORG (2017). OWASP Top 10 - 2017. [Online]. Available at : https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. [Accessed 27 July 2019].

[9] OWASP.ORG (2017). OWASP Testing Guide v4 Table of Contents. [Online]. Available at : https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents. [Accessed 27 July 2019].

[10] COOLNETKID (2014). Apa itu Penetration Testing ?. [Online]. Available at : https://coolnetkid.wordpress.com/2014/05/24/penetration-testing/. [Accessed 27 July 2019].

[11] OWASP.ORG (2014). Web Application Penetration Testing. [Online]. Available at : https://www.owasp.org/index.php/Web_Application_Penetration_Testing. [Accessed 27 July 2019].