ISSN: 2581-1274

Analysis of Web Server Security Against Structure Query Language Injection Attacks in ASEAN Senior High Schools

Murniati [a,1], Rizal Munadi [b,2,*], Teuku Yuliar Arif [b,3]

[a] *Electrical Engineering Graduate Program, Electrical, and Computer Engineering Department, Engineering Faculty, Syiah Kuala University*
[b] *Electrical, and Computer Engineering Department, Engineering Faculty, Syiah Kuala University*
Jalan Tgk. Syech Abdurrauf No. 7, Darussalam, Banda Aceh, Indonesia
[1] *murtijnd@gmail.com;* [2] *rizal.munadi@unsyiah.ac.id*;* [3] *yuliar@unsyiah..ac.id*

ARTICLE INFO

Article history:
Accepted

Keywords:
SQLI
Web server
Security holes
Intruder
School

ABSTRACT

Cyber crime continues every day that is always trying to exploit security holes that can be infiltrated. The techniques used vary greatly and the intended target can befall anyone, whether government institutions, private institutions, organizations and even educational institutions. One of the techniques used by intruders is the SQLI attack on the web server. This disorder can cause the information presented to be unavailable normally. once control of the database successfully taken over by the attacker, the data will be easily controlled and other attacks can be done against the client. In this study, an assessment of SQLI attacks on senior high schools in some ASEAN countries was conducted. The analysis was performed on the web server of senior high school in seven ASEAN countries. In this article, methods the forensic used to analyze web servers against attacks SQLI. There is still a lot of web server that vulnerable to SQLI. From the analysis obtained on average 20.86% for the type of SQLI in each country. Of the 70 samples of the website showed a study of web server with techniques SQLI is the highest risk level of 27% in Web Server Singapore and lowest risk level of 7% on a Web Server the Philippines.

I. Introduction

Today, the development of information technology continues to experience tremendous trends and offer convenience for the society in finding information provided on the website. The accessibility of information through website is strongly supported by the availability of an adequate and fast internet network as well as the public's literacy on information. Website as information window is designed with the aim to facilitate access for stakeholders with updated information. To that end, the website is built firmly and managed by the information section so that information can be guaranteed its availability.

On the other hand, every day, cyberspace criminals perform various ways of infiltration and action to find loopholes against thousands of websites. If an intruder successfully attacks a site, unnoticed by the system administrator, then the site becomes vulnerable to various acts of misuse of access and can lead to various crimes. By using certain techniques, the hacker may have infected their site with malicious code. Unwittingly by site owners, for example, hackers can record keystrokes, steal login credentials for online financial transactions. In Symantec's Internet Security Threat Report explained that some financial Trojans began stealing not just online banking credentials but cryptocurrency wallet logins and any other account details that may help maximize profits [1]. The accumulation of trojan attacks continues to occur annually and the top ten ranking

statistics of trojans by 2017 are illustrated in Fig. 1. Based on those possibilities, the security of a website becomes necessary to be improved so that abuse can be minimized.

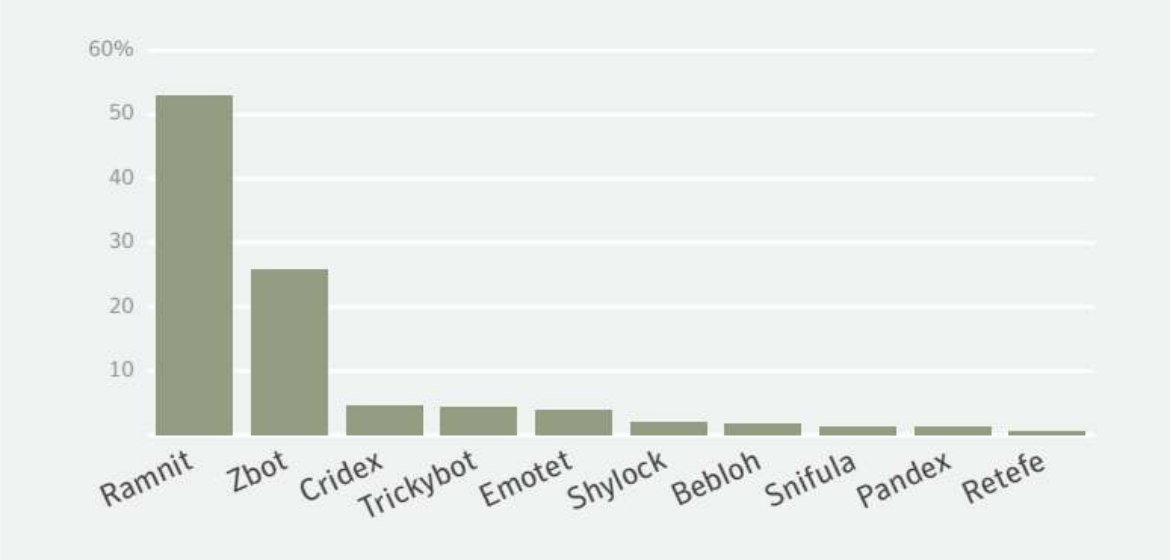

Fig. 1. Top 10 financial Trojans 2017 [1]

Crime in the field of information technology continues to emerge and is difficult to avoid. Many people have reported infiltrations on schools, governments, organizations and companies websites that can damage and destroy important assets of companies and such in the digital form. In order to avoid the disruption of information systems that have been built, it is necessary system maintenance periodically. In recent years, the safety factor of website becomes the main subject of concern.

Therefore, websites that have security holes can serve as the entrance by hackers to penetrate web servers. The damage caused by this illegal act is very dynamic and depends on the extent of the damage. This is due to the highly variable behavior of attackers, from being just for fun to deliberately attacking websites. This is what makes the web server a target of various types of attacks, both minor and major so it can be fatal for information systems that have been built.

One form of crime on the internet is disrupting network systems and databases. To carry out the action, many ways can be done by attackers. For example by using Structure Query Language Injection (SQLI). This technique most widely used to destroy and easily damage the network database system. SQLI works by manipulating commands to enter codes in order to attack the database so that it can easily be used to acquire information and change existing databases [2].

In the previous research, the technique of striking the security attacks of the SQLI has been applied to the local web server and also in Bangladesh on a number of education websites [2]. In line with previous research, surveys and testing were conducted with a focus on the website of senior high school in the ASEAN region. The assumption is hypothetical in this study that there is a defect on the website that has been built and has the potential to be infiltrated by the attacker. Therefore, the aspect of security breaches on senior high school websites in ASEAN countries is of interest to be elaborated further in this study.

II. Literature Review

A. Web Server

Web server is a software installed in the computer server that serves to receive a request for a web page through HTTP or HTTPS from the user or client and then send it back in the form of a web page of an HTML document. The server responds to the multiple clients by sending web pages such as HTML documents and linked objects. The client and web server transaction process occur based on the client request to the required information through the DNS server. Based on the request, the web server responds and sends the requested documents or information. This process is

shown in Fig. 2. The frequent interactions based on information requests make the web server one of the attackers' targets. Therefore it is necessary to build a security against the attack on the web server and its infrastructure that support it [3].

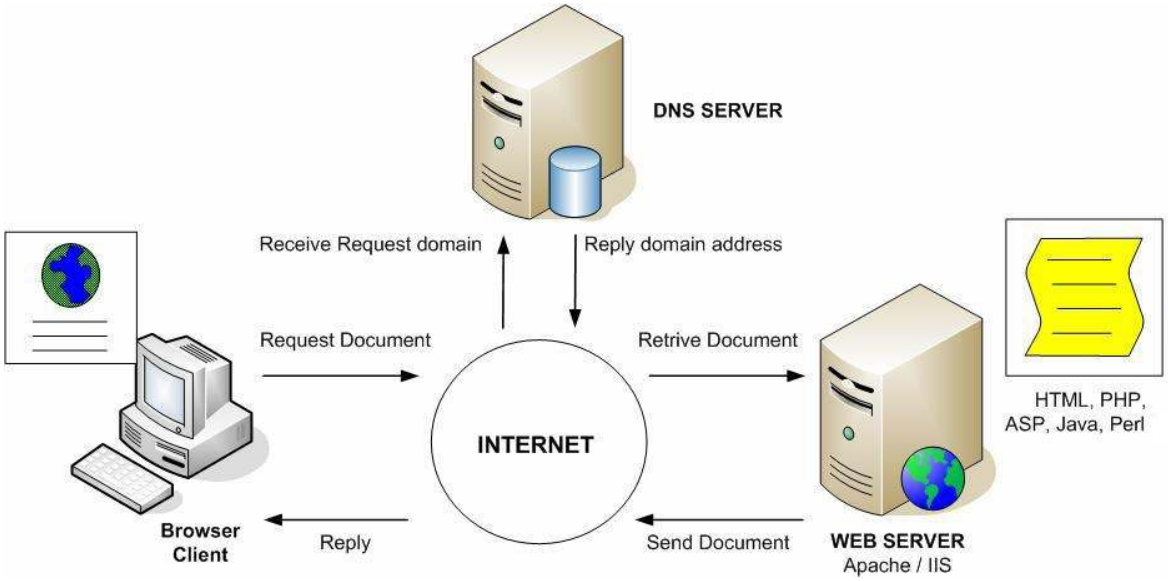

Fig. 2. Web Server Application [4]

B. Security gaps

A security gap is a weakness that threatens the value of integrity, confidentiality, and availability of an asset. The security gaps are not just in the form of software bugs or network security weaknesses. This incident can also be caused by weaknesses by poorly trained personnel, missing parts of the document, or from procedures that cannot be executed appropriately. Security gaps can be categorized into three parts, which are, the weaknesses in the system itself, the access point to the weakness of the system, and the ability of a hacker to attack. The analyzing process required a way to identify the attack quickly and a complement to the security system that can monitor, capture and store digital evidence so how, why and when the attack occurred will be known. Therefore a forensic mechanism is required on the network, so the evidence required for further analysis is not lost or changed [5].

This vulnerability assessment activity is highly recommended to be done on a regular basis. It can be done per week or per month. This is due to the trend of malicious attacks that continue to grow. Start as early as possible by doing small things that can maintain the security of information systems, because there is nothing safe in the virtual world [6].

C. Structure Query Language Injection

Structure Query Languange Injection is an attack that takes advantage of the omission of a site that allows a user to input certain data without filtering the malicious character. The input can be entered into the search box or in certain parts of a site. The command put by the attacker is usually a data containing a certain link that can lead the victims to a special web that is used by the attacker to take the victims' personal data. SQL injection is a series of SQL statements which are given as input to the application and along with the 'query' in the application the SQL statements behave differently which may have hazardous results[7].

In SQL syntax, single quotes (') mean the initial and final restrictions of a string value. When single quotes (') are injected into applications that have weaknesses for SQL commands, they can disrupt string constraints and cause application errors, thus indicating potential SQLI vulnerabilities. For example the use of single quotes (') that can cause an error in an application [8]. Basically, there are 3 types of SQLI that are often found [8]:

1) *Error Based SQL Injection*
   Error based SQLI is an error message that appears and indicates a vulnerability on the website. Error based technique consists in forcing the database to perform some operation in which the result will be an error. This error message indicates a weakness of the application being used and error information can be misused by the attacker. For example, a command of SQL query: `SELECT * FROM products WHERE id_product=$id_product` then this query structure is reformulated and typed to be executed in the URL from browser as `http://www.example.com/product.php?id=10.`

2) *Blind SQL Injection*
   Blind SQLI does not display error messages and does not display existing data or information, sometimes it is also difficult to exploit the Blind SQLI type because in the process it gives true or false questions. For example, a command of Blind SQLI:
   `http://www.smaduajkt.sch.id/show/php?id=1+and+1=1--` (true)
   `http://www.smanduajkt.sch.id/show.php?id=1+and+1=0--` (false)

3) *Double SQL Injection*
   Double Blind SQL Injection attacks use a time delay when processing SQLI queries. If the web has a gap, it will execute the request according to the URL's manipulation done by the attacker. If the query is correct, it will be executed in a few seconds, but if the query is executed immediately, then the request given by the attacker is false. Double Blind SQLI technique is a blend between blind SQLI/classical SQLI with time delay. If the URL is coupled with time delay will generate the command in accordance with the requested request, the web application can be injected using SQLI attacks.

D. SQLI Process

In the SQLI attack process, attackers take advantage of login system or search page. SQLI is often happens because developers do not make sure that the input values received from web forms, cookies, and input parameters have already been validated before SQL query commands are executed by the database server. This action is done to know whether it is vulnerable to SQLI attacks or not, and to test the presence or absence of SQLI error when given the URL of a web that has been manipulated [9].

III. Method

The first step in this study was to survey some senior high schools object in seven ASEAN capitals countries: Indonesia, Malaysia, Philippines, Brunei Darussalam, Vietnam, Singapore, and Thailand. Each country is limited to only ten senior high schools being evaluated. Then, several senior high school websites were scanned to test the hypothesis whether they were vulnerable to SQLI attack. The test was conducted in Banda Aceh for 2 months using OWASPZAP 2.5.0 tools. On average, the testing process carried out 2 sample websites every day with normal internet access conditions and will spend 7-8 hours. If the network condition is not good, the process can run up to 12 hours or should be repeated again because no results obtained. The same process was carried out for all senior high schools that were targeted in this study.

In the SQLI attack process, attackers take advantage of login system or search page. SQLI often happens because developers do not make sure that the input values received from web forms, cookies, and input parameters have already been validated before SQL query commands are executed by the database server to know whether it is vulnerable to SQLI attacks or not. On a Web Server, the vulnerability levels of SQLI attacks can be detected by scanning a website by using a tool or software that can detect the presence of vulnerabilities in the web server that contains bugs. The form of parameters that become high benchmarks of the low security of a web server is by being able to insert the codes like:

1) *Single quotation marks (')*
2) *Single or double minus sign (-), (--)*
3) *Add show.php?id=1' behind the URL*
4) *Add show.php?id=1+and+1=1 behind the URL (true condition)*
5) *Add show.php?id=1+and+1=2 behind the URL (false condition)*

OWASP ZAP Tool is used to scan websites to know the vulnerability to SQLI attacks. The process by using the tool can be seen in Fig. 3.

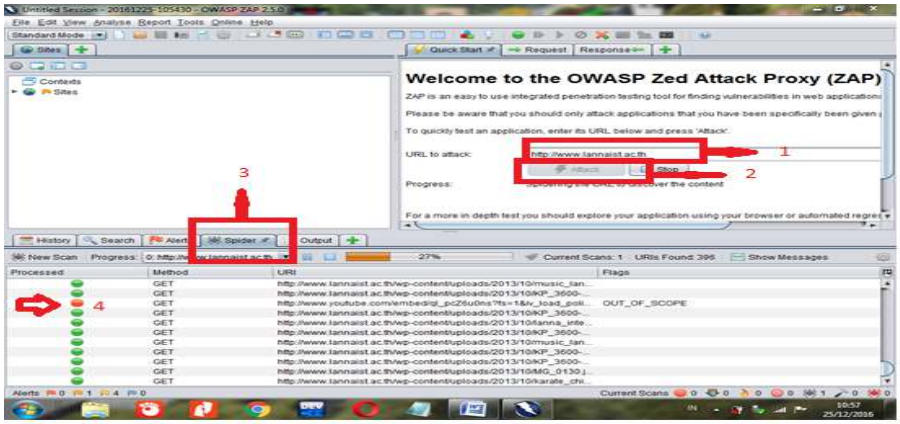

Fig. 3. Scanning information process

In Fig. 3., some indicators are marked. There are four stages and marks as a pointer. This figure can be described as follow. Point 1 is the place of writing the URL of the attack, after entering the URL, select Attack at point 2, then point 3 is a Spider tab to read the entire contents of the URL and the red dots can be seen at point 4 which informs that server log has sensitive information that can be misused by irresponsible attackers. Spider tab results are read up to 100% complete, then proceed to the scanning process. Because the scanning process is done in more detail, this is what this makes the scanning process time consuming and long. Then to make it easier to map vulnerabilities and later analysis process, vulnerability is divided into three categories, low, medium and high.

IV. Results And Discussion

A. Results and Discussion

In this section, the results of the analysis that have been done based on the research methods presented in the previous chapter will be described. The discussion is directed to problems with web server security with SQLI attack technique in seven ASEAN countries. The website data were obtained from seven ASEAN countries, then in this study based on the test scenario conducted, 70 website samples will be analyzed. Based on the collected data, 149 high-risk URL data were successfully obtained. This shows that the monitoring from the administrator is necessary and should be done periodically. Therefore, the administrator is expected to always control it every time, and to avoid unexpected things created by the irresponsible people (the hacker).

In this process, blind SQLI works based on true or false statements, If a request is executed and generates true value, the web will return a certain content but if the execution returns a false value, it will return to another content. After finished scanning 70 samples of each country, there are 10 Sample to be tested with SQLI techniques. The data can be calculated as shown in Table 1

Table 1. The calculation of the High Risk in each Country

No	Country	SQL Injection
		High
1	Indonesia	12
2	Malaysia	19
3	Singapore	40
4	Vietnam	16
5	Philippines	11
6	Brunei Darussalam	36
7	Thailand	15
	Total	149

The Table 1 describes the number of high risk or problematic URLs on each website of the senior high schools in ASEAN countries, where the number enables the criminals to commit crimes in the form of damaging database server and the appearance of the website. The above data then is made in percentage, so it can be known how safe the web servers are in each ASEAN countries

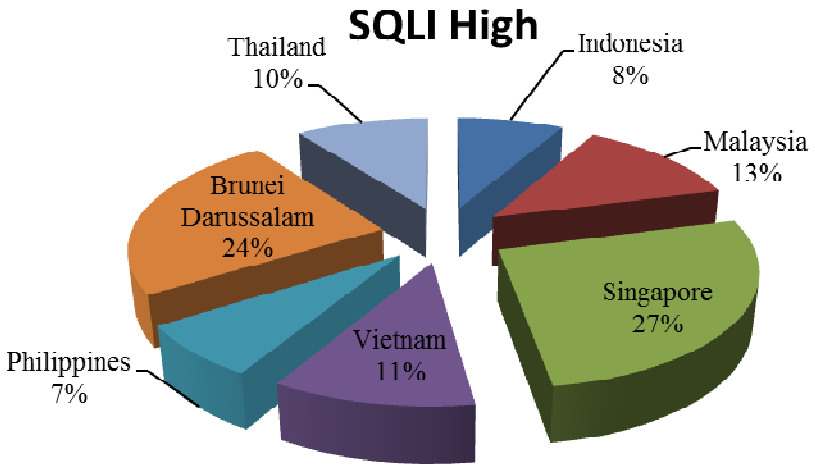

Fig. 4. The distribution of security gaps with SQLI techniques in ASEAN senior high school

In Fig. 4., it highlights the percentage of the high-risk level in each country, Philippines 7%, Indonesia 8%, Thailand 10%, Vietnam 11%, Malaysia 13%, Brunei Darussalam 24% and the last is Singapore with 27%. In this case the most risky country is Singapore due to a number of the Websites which still use low version of web server, and the CMS is also low version, such as the Apache 2.2.31 and the old version CM, WordPress 4.8.3, where the high-end web server already has security improvements, and it is also possible that the administrators do not update much, so it gets the biggest gap from the scanning results by using OWASP ZAP.

V. Conclusion

From the scanning results, it can be concluded that SQLI technique attack the websites and it was found a number of vulnerabilities in senior high school web servers in ASEAN, with Philippines 7%, Indonesia 8%, Thailand 10%, Vietnam 11%, Malaysia 13%, Brunei Darussalam 24 % and the last is Singapore with 27%. The number is certainly not too large but indicates that there are still many web servers in ASEAN countries that are not managed properly, therefore it can be easy for the hackers to enter and breach the server. From the analysis of web server security that exists in 7 ASEAN Countries, 149 URLs are vulnerable to SQLI attacks at high levels. In the future it is hoped that there will be a continuation of this research using more than one technique and more than 70 sample data, so it can be known early on whether a web server is safe or not, so it can be handled directly by the user's administrators.

References

[1] Symantec, "ISTR Internet Security Threat Report," *Internet Secur. Threat Rep.*, vol. 23, 2018.

[2] Yao-Wen Huang, Chung-Hung Tsai, D. T. Lee, and Sy-Yen Kuo, "Non-Detrimental Web Application Security Scanning," in *15th International Symposium on Software Reliability Engineering*, pp. 219–230.

[3] T. Winograd, M. Tracy, and W. Jansen, "Guidelines on Securing Public Web Servers Recommendations of the National Institute of Standards and Technology," *NIST Spec. Publ. 800-44*, no. 800–44 Version 2, 2007.

[4] Susanto, Four Ways on How Web Server Works Briefly With its Image in a Network, June 16th 2016(https://jogjahostingterbaik.com), accessed on 21st May 2018

[5] A. Pomeroy and Q. Tan, "Effective SQL Injection Attack Reconstruction Using Network Recording," in *2011 IEEE 11th International Conference on Computer and Information Technology*, 2011, pp. 552–556.

[6] Y.Tiwari and M.Tiwari. Article: A Study of SQL of Injections Techniques and their Prevention Methods. *International Journal of Computer Applications* 114(17): 31-33, March 2015.

[7] N. Venkataramanan, "Proposing a Framework for Digital Network Forensic Evidence Accumulation in Cloud Environment," vol. 10, no. 10, pp. 2963–2972, 2017.

[8] S. Agrawal and U. Singh, "Prevention of SQL Injection Attack in Web Application With Host Language," pp. 1468–1470, 2017.

[9] Z. S. Alwan and M. F. Younis, "Detection and Prevention of SQL Injection Attack : A Survey," vol. 6, no. 8, pp. 5–17, 2017.