JOIN (Jurnal Online Informatika)
Volume 4 No. 2 | December 2019: 63-68
DOI: 10.15575/join. v4i2.394

Security Scanner for Web Applications Case Study: Learning Management System

Rian Andrian[1], Ahmad Fauzi[2]
[1,2]Universitas Pendidikan Indonesia, Purwakarta, Indonesia
[1]riandrian@upi.edu, [2]ahmad.fauzi@upi.edu

Abstract- In software engineering, web applications are software that are accessed using a web browser through a network such as the Internet or intranet. Web applications are applications that can be relied on by users to do many useful activities. Despite the awareness of web application developers about safe programming practices, there are still many aspect in web applications that can be exploited by attacker. The development of web applications and the Internet causes the movement of information systems to use them as a basis. Security is needed to protect the contents of web applications that are sensitive and provide a safe process of sending data, therefore application security must be applied to all infrastructure that supports web applications, including the web application itself. Most organizations today have some kind of web application security program or try to build/ improve. But most of these programs do not get the results expected for the organization, are not durable or are not able to provide value continuously and efficiently and also cannot improve the mindset of developers to build/ design secure web applications. This research aims to develop a web application security scanner that can help overcome security problems in web applications.

***Keywords*- Security, Web Application, Security Scanner, Learning Management System**

I. INTRODUCTION

In software engineering, a web application is an application that is accessed using a web browser over a network such as the Internet or intranet. Web application is also a computer software application that is developed in a programing language that is supported by web browsers (such as ASP, Perl, Java, Java Script, PHP, Python, Ruby, etc.) and relies on the browser to display the application.

Web applications are applications that can be relied upon by users to carry out many beneficial activities. Apart from the awareness of web application developers about safe programming practices, there are still many gaps in web applications that can be exploited by irresponsible parties [1]. Talking about problems related to security in the digital age can not be separated from the 3 main principles, namely: Confidentiality, Integrity, and Availability or better known as the CIA.

The development of web applications and the Internet has caused the movement of information systems to use them as a base. Many systems are not connected to the Internet but still use a web application base as the basis for the information system installed on the Intranet network. For this reason, information system security based on web applications and Internet technology depends on the security of the web application system. Security is needed to protect the contents of sensitive web applications and provide a secure data delivery process, therefore application security must be applied to all infrastructure that supports web applications, including the web application itself.

Most organizations today trying to build / improve web application security. However, most of these programs do not get the expected results for the organization, do not last long or are unable to provide value in a sustainable and efficient manner and also cannot improve the mindset of developers to build / design secure web applications [2].

This research will develop a web application security scanner that can help solve security problems in web applications. In its implementation, this web application security scanner besides checking security on a website, can also provide feedback on how to resolve security problems found. This research will use a learning management system that has been developed in previous research by the research team as a case study.[3]

II. METHOD

The CIA Principals should be used as guidelines that must be understood and implemented to maintain the security level of the web applications that we build.

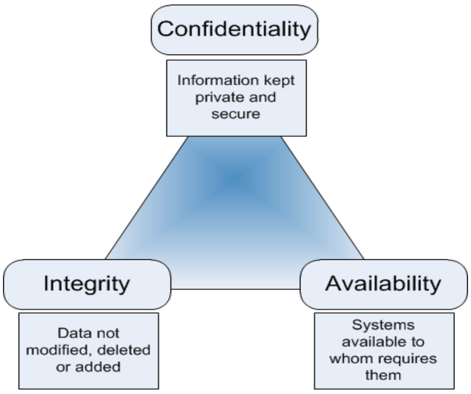
Confidentiality
Information kept private and secure
Integrity
Data not modified, deleted or added
Availability
Systems available to whom requires them

Figure 1. CIA Priciple

Received: October 29, 2019; Revised: December 14, 2019; Received: January 11, 2020; Published: February 14, 2020

A. Confidentiality

Confidentiality means that the data or information on a website can only be read or accessed by people who do have the authority to access it. To anticipate the ignorant hands of strangers, developers can anticipate this by creating roles from every user they have. For example, Role other than the administrator cannot change the website theme and / or plugin. So it is not possible to change the theme by a user other than the administrator. By sharing Role like this data or information such as user list will only be seen by the administrator while the user profile can be accessed by each user. Thus the level of security can be said to be increasingly high.[4]

B. Integrity

Integrity has the understanding that data inside a server or website can only be changed or deleted by someone who has the authority to do so. For example the process of transfer from server to client or vice versa (can be upload or download), it turns out to change the file being transferred, this indicates that a website application that is being used is insecure. Similarly, if there is a virus attack that can change a file, whether it changes the name or contents. Sometimes a user with a Role lower than the administrator can (in certain ways, including by accident) do this even if he cannot access the data that is being changed or destroyed. This action is sometimes an action that is not intentionally by the user, but still occurs due to an error in the web application being used.

To make a website more secure, this of course must be avoided. One way is to apply one of the processes that must be present in a software engineering process, namely the testing process. The testing process is divided into two namely: - Black box testing - White box testing Simply put, black box testing is testing applications intended for users who are actually accessing the website (act like end user - act as a user / user). As for white-box testing, it specializes in testing functions that have been written in certain programming languages (PHP, Perl, ASP, Javascript, etc.). These tests are divided into three tests based on application input or function, i.e. tests using input values: What is desired bordered Beyond the limits when indeed detected errors from this testing should be corrected immediately before this error is found by hackers who then use it to exploit our website.[5]

C. Availability

Availability means that the website must be accessible if the user wants to use it. If a website can be accessed without errors, it means that the website has fulfilled this availability principle. This means that a website must be accessible if it is needed, the website must be available 24 hours 7 weeks (24/7).[6]

If confidentiality means that only authorized users can view certain data stored on a server or website, availability means that the website must be accessible if the user wants to use it. It may seem confusing and not different from the first principle, but these two principles are very much different because it is seen from two different perspectives. Availability only emphasizes the accessibility of a website.

D. Real Time Feedback Concept

A Real time system is a system whose truth is logically based on the truth of the results of the system output and the timeliness of the results issued. The application of using a system like this is to monitor and control equipment such as motors, assembly lines, telescopes, or other instruments. Telecommunications equipment and computer networks usually also require real-time control [7]. The concept of real time feedback will be applied in the development of a Web Security Analyzer system where the system will scan the website and provide results (security holes) along with solutions / references on how to fix the vulnerability.[8]

E. Scanning Algorithm Source code

Scanning is a process for periodic checking of a system. The scanning process that occurs on e-learning websites is mostly done manually without being done regularly (Scheduling). Therefore this study proposes a system that can perform an automatic scanning process where the system gets a data from several resource sharing to do the matching process of security holes in a website by using the concept of template matching that is applied using the Microservice Architecture. The concept of this website scanning process is by matching requests and responses received from the payload sent to the web server. The following formula is the security gap scanning scheme in a website [9][10].

The following is a flowchart of the template matching algorithm contained in Figure 2.

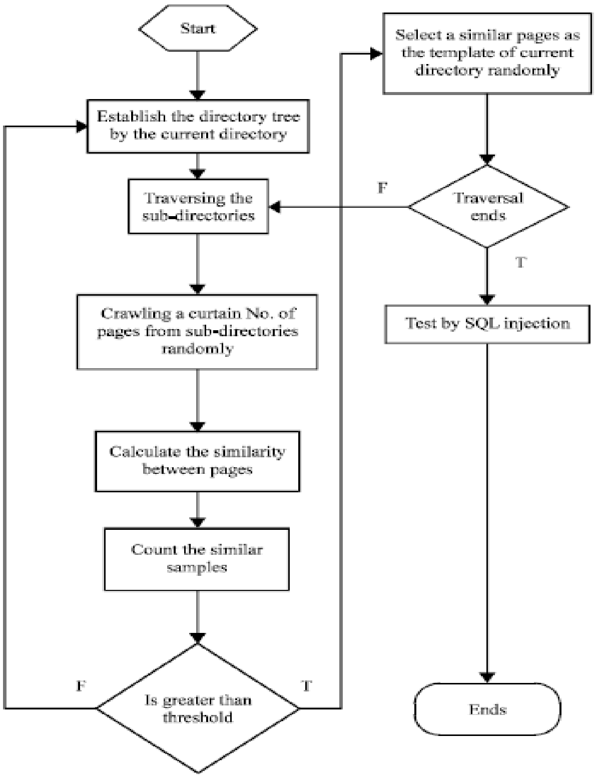
Start
Establish the directory tree by the current directory
Traversing the sub-directories
Crawling a curtain No. of pages from sub-directories randomly
Calculate the similarity between pages
Count the similar samples
Is greater than threshold
F
T
Select a similar pages as the template of current directory randomly
Traversal ends
F
T
Test by SQL injection
Ends

Figure 2. flowchart of the template matching algorithm

F. Moodle

Moodle (Modular Object-Oriented Dynamic Learning Environment) is an open source learning management system. Moodle can be downloaded for free, used, modified by anyone with a GNU (General Public License) license. Users can download Moodle at the address: http://www.moodle.org.[11]

Moodle supports student-centered learning (student center learning) and distance learning (distance learning). Through this learning concept, students can easily access material and participate in learning anywhere without the limitations of distance and time. In addition, teachers can provide material not limited by distance, space and time. The teacher can upload material in the form of words, presentations, audio, videos, links from other websites, etc.[12]

In this study, in its development using a software development approach Life Cycle (SDLC). SDLC is a workflow used in the design, development and system testing process so as to produce a quality product (Dwivedi 2016). The SDLC model used is the throwaway prototyping model. The process of building a system using a throwaway prototyping model consists of planning, analysis (design, implementation), design and implementation.

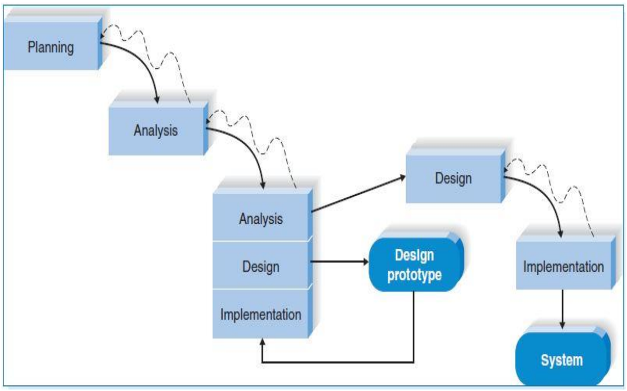

Figure 3. Throwaway prototyping model

III. RESULT AND DISCUSSION

Requirement analysis is carried out in the development of the system starting from the operating environment, functional requirements and non-functional requirements.

A. Operating Environment Requirements

The following is an overview of the needs of the operating environment from developing a developed system:

Table 1. Operating Environment Requirements

No	System	Requirements
1	Server Side	Operating System: Linux DBMS : MySQL Web Server : Apache
2	Client Side	Operating System: Windows/ Linux Browser : Firefox, Internet Explorer, Chrome

B. Functional Requirement

Functional requirements in developing a system are system functionalities that must be met on a developed system, the following is a list of functional requirements in developing a security scanner for web applications developed in this study:

Table 2. Functional Requirements

ID	Requirements
FR01	The system facilitates the Admin to add Users to the system.
FR02	The system facilitates the Admin to configure the system.
FR03	The system facilitates the User to input a Website URL to check its security level.
FR04	The system can scan the level of system security.
FR05	The system can help users to provide information gaps contained in a system.
FR06	The system can provide corrections to errors whether they are logic or non-logic errors.
FR07	The system can provide solutions to gaps that can be in accordance with existing standards
FR08	The system facilitates the user to see a list of applications that have been scanned.

C. Non-Functional Requirement

Non-functional requirements are requirement that must be considered because it is a benchmark of the quality of a system. The following is an explanation of the non-functional requirements of the system developed:

Table 3. Non-Functional Requirements

ID	Parameter	Requirements
NFR01	Availability	The system must be available when it will be used in the scanning process.
NFR02	Reliability	The system can be relied upon to provide information on gaps contained in a system and provide recommendations for improvement
	Ergonomy	N/A
NFR03	Portability	The system can be accessed properly through desktop and mobile browsers
	Memory	N/A
	Response time	N/A
	Safety	N/A
NFR04	Security	Data security must be maintained properly

The system design is created based on the results of the requirement analysis, then the system design stage is carried out. In this phase the system design will be made using a use case diagram complete with the scenario. We can see how the functional system works to meet the needs of users by the use case diagram.[13]

D. Use Case Diagram

Below is the system design carried out in the development of a security scanner for web applications with a learning management system case study.

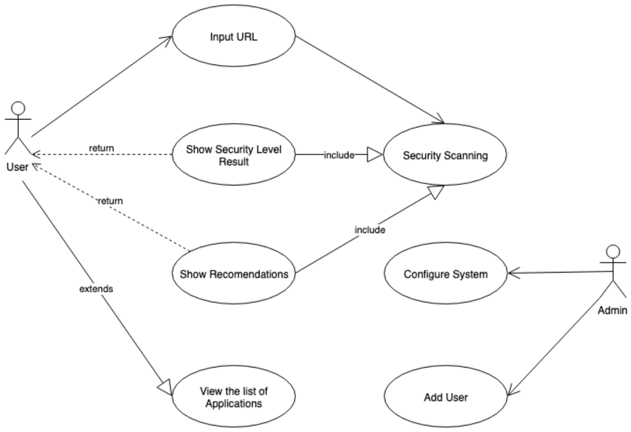

Figure 4. Use case diagram security scanner for web applications

Following are the actors involved in the use case diagram above along with a brief description of each actor:

Table 4. Actors

No	Actor	Descriptions
1	Admin	Actors with this role have the authority to manage the system in general and ensure all the needs of other actors associated with this system can be met.
2	User	Actors with this role are the main users who will benefit from the security scanner system.

The following is a list of use cases along with a brief description of each use case in the diagram above:

Table 5. Use Cases

No	Use Case	Descriptions
1	Configure System	The security scanner system provides facilities to configure the system in order to provide ease of management of the system carried out by the admin.
2	Add User	The system provides a user addition form.
3	Input URL	The system provides input URL from the web application to be checked for security level.
4	Security Scanning	The system checks the web application that has been inputted by the User's URL.
5	Show Security Level Result	The system provides corrections to errors whether they are logic or non logic errors.
6	Show Recommendations	The system provides recommendations for solutions to gaps that can be in accordance with existing standards (OWASP, Acunetix etc.)
7	View the list of Applications	The system provides features that can display a list of applications that have been scanned by the user.

E. System Architecture

The following is an overview of the security scanner architecture for web applications with a learning management system case study developed in this study:

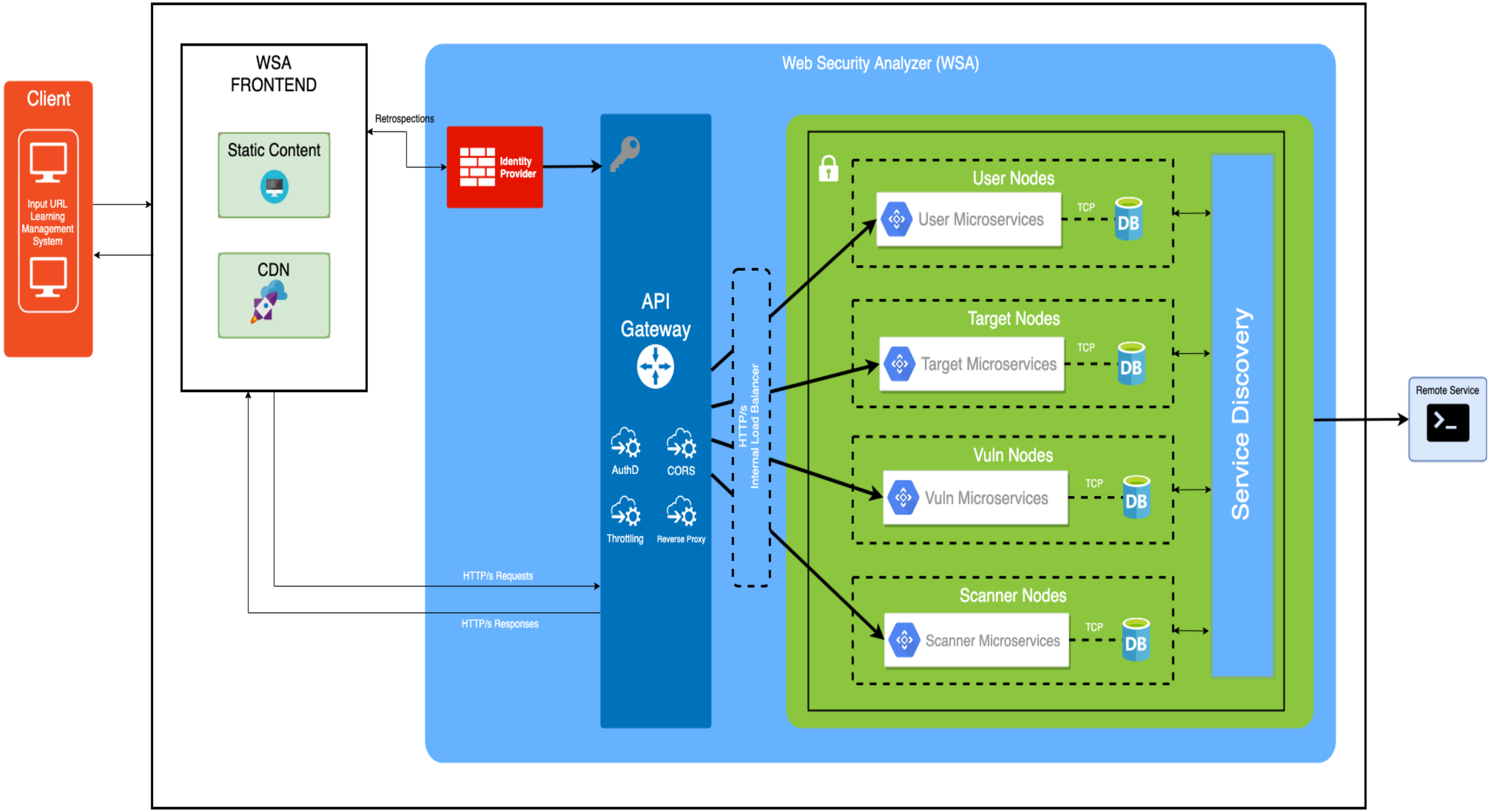

Figure 5. System Architecture

The following is an explanation of each component in the security scanner architecture for web applications with a case study learning management system developed:

1. Client: The user of the system who can perform various actions through the User Interface and will receive the output displayed by the system.
2. WSA Frontend (UI): Functioning as a User Interface Page that display all system requirements.
3. Identity Provider (IDP): Is a platform that accommodates all needs, both authentication and authorization. Identity Provider is used to limit access to all services needed in accordance with the role of each user, then forwarded to all services needed through the Gateway API. Restrictions on access rights at the Identity Provider are often referred to as Role Base Access Control (RBAC).
4. API Gateway: Platform that used to manage all Application Programming Interface (API). All API are stored in the API gateway. API gateway functions as a front-run access to connect public access into a cluster of certain services. Therefore the API gateway is widely used as a solution for managing service needs to be published, especially the needs of Microservice Architectures.
5. User Node / User Microservices: Functioning as a special service to store and manage all needs related to entity users. User Microservice as the main gateway that is connected to a Identity Provider (IDP) as one of the attributes to authenticate.
6. Target Nodes / Target Microservices: Functioning as a service that accommodates all sites to be scanned, all sites are stored in a storage at the Target Microservice at the same time managed, classified and analyzed according to the IP Address that is found automatically.
7. Scanner Nodes / Scanner Microservices: This component is the main service for scanning the specified website on the target microservice. All sites will be scanned for vulnerabilities, then Scanner Microservice will provide scanning results obtained automatically and then will be stored for reporting purposes.
8. Vuln Nodes / Microservices: Components that have a service function that manages all data sent from the scanning process at Scanner Microservices. All of these results are managed in accordance with reporting needs that are generated automatically by this component.

V. CONCLUSION

Application security must be applied to all infrastructure that supports web applications, including the web application itself. This research develops a web application security scanner that can help solve security problems in web applications.

IV. REFERENCES

[1] H. Shahriar, “Web Security Vulnerabilities: Challenges and Solutions A Tutorial Proposal for ACM SAC 2018,” pp. 1–5, 2018.

[2] H. Bang, M., & Saraswat, “Building an effective and efficient continuous web application security program.,” *nternational Conf. Cyber Situational Awareness, Data Anal. Assess. (CyberSA).*, 2016.

[3] P. Singh, K. Thevar, P. Shetty, and B. Shaikh, “Detection of SQL Injection and XSS Vulnerability in Web Application,” no. 3, pp. 16–21, 2015.

[4] M. (2006). R. P. L. B. B. I. Salahudin, *Rekayasa Perangkat Lunak.* Bandung, 2006.

[5] Roland Petrasch, “Scalable Autograder and LMS Model-based Engineering for Microservice Architectures using Enterprise Integration Patterns for inter-service Communication.,” 2017.

[6] A. Masood and J. Java, “Static analysis for web service security - Tools & techniques for a secure development life cycle,” in *2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015*, 2015.

[7] I. Dwi, “Real Time System,” 2017.

[8] X. Liu, Q. Chen, L. Li, and S. Chi, “An efficient web vulnerability scanning method based on template matching,” *Inf. Technol. J.*, vol. 13, no. 5, pp. 934–940, 2014.

[9] P. Mazlami, G., Cito, J., & Leitner, “Extraction of Microservices from Monolithic Software Architectures.,” 2017.

[10] S. Li, “Understanding quality attributes in microservice architecture,” in *Proceedings - 2017 24th Asia-Pacific Software Engineering Conference Workshops, APSECW 2017*, 2018, vol. 2018-January, pp. 9–10.

[11] A. Alzahrani, A. Alqazzaz, N. Almashfi, H. Fu, and Y. Zhu, “Web Application Security Tools Analysis,” *Stud. Media Commun.*, vol. 5, no. 2, p. 118, 2017.

[12] P. R. L., P. R. L., L. C. S., D. Jagli, and A. Joy, “Rational Unified Treatment for Web application Vulnerability Assessment,” *2014 Int. Conf. Circuits, Syst. Commun. Inf. Technol. Appl.*

[13] M. J. Kargar and A. Hanifizade, “Automation of regression test in microservice architecture,” in *2018 4th International Conference on Web Research, ICWR 2018*, 2018, pp. 133–137.