Analysis of Cross Site Request Forgery (CSRF) Attacks on West Lampung Regency Websites Using OWASP ZAP Tools

Ilham Firman Ashari[1]*, Vina Oktariana[2], Ringgo Galih Sadewo[3], Salman Damanhuri[4]
Institut Teknologi Sumatera[1], [2], [3], [4]
Prodi Teknik Informatika[1], [2], [3], [4]
Indonesia
firman.ashari@if.itera.ac.id[1], vina.118140062@student.itera.ac.id[2], ringgo.118140076@student.itera.ac.id[3], salman.118140110@student.itera.ac.id[4]

Abstract*— Technological developments in the field of increasingly advanced computers and networks have caused many organizations to use web applications to provide business services. With the increasing popularity of the internet, the number of cyber-attacks has also increased. To overcome these negative impacts, the role of network security is very necessary. The Cross Site Request Forgery (CSRF) method is a penetration technique aimed at exploiting website security vulnerabilities and there is one tool commonly used to find security vulnerabilities on websites, namely OWASP ZAP. The research has succeeded in proving security vulnerabilities on the website of the West Lampung district by conducting attack simulations. From the results of the experiment, it was found that there were 12 alerts with low risk on the website of West Lampung Regency. In 12 alerts there are 53 URL pages that are vulnerable to attack.

***Keywords*— CSRF, OWASP, Vulnerabilities, Penetration, Website**

***Abstrak*— Perkembangan teknologi pada bidang computer dan jaringan yang semakin maju menyebabkan banyak organisasi menggunakan aplikasi web untuk menyediakan layanan bisnis. Dengan meningkatnya popularitas internet, jumlah serangan dunia maya juga semakin meningkat. Untuk mengatasi dampak negatif tersebut, peran keamanan jaringan sangat diperlukan. Metode *Cross Site Request Forgery* (CSRF) merupakan teknik penetrasi yang ditujukan untuk mengeksploitasi kerentanan keamanan situs web dan terdapat salah satu tools yang biasa digunakan untuk menemukan kerentanan keamanan di situs web yaitu OWASP ZAP. Pada penelitian telah berhasil membuktikan kerentanan keamanan pada website kabupaten lampung barat dengan melakukan simulasi serangan. Dari hasil percobaan didapatkan ada 12 *alert* dengan risiko *low* pada *website* Kabupaten lampung barat. Pada 12 *alert* terdapat 53 *URL pages* yang rentan dilakukan serangan.**

***Kata Kunci*—CSRF, OWASP, Celah Keamanan, Penetrasi, Website**

I. INTRODUCTION

The rapid growth in the development of computer network technology and the internet has caused many organizations to use web applications to provide business services [1]. The web can provide access to information from anywhere and at any time [2]. With the increasing popularity of the internet [3][4], the number of cyber-attacks has also increased. Hackers, in addition to hacker behaviour, the negative impact of the threat of connecting computer networks to the internet include viruses, trojan horses, and so on. To overcome these negative impacts, the role of network security is very necessary. Network security will provide services and protection for computer networks connected to the internet, so that they can operate normally and exchange data safely and reliably [5]. CSRF is different from various other attacks which mostly use up the existing resources on the system, CSRF attacks are carried out to exercise direct control over the databases on the system [6].

The Cross Site Request Forgery (CSRF) method is a penetration technique aimed at exploiting website security vulnerabilities. CSRF is a technology to fake the identity of site users [7]. An example of the result of this CSRF technique is the ability to change the account parameters of the victim such as name, age, address, and password [8].

One of the tools commonly used to find security vulnerabilities on websites is OWASP ZAP. Where on the tool there is a "warning" in the tool that indicates a security vulnerability on the target website. There are 3 indicators of security vulnerability in the OWASP ZAP tool, namely, the red colour represents the 'high' security vulnerability indicator, orange represents the 'medium' security vulnerability indicator, and blue represents the 'low' security vulnerability indicator [9].

Research conducted by [10] To determine the level of risk in the main commodity price information system using the Open Web Application Security Project (OWASP) Risk

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1393, Copyright ©2022
Submitted : April 23, 2022; Revised : July 27, 2022; Accepted : August 30, 2022; Published : August 31, 2022

Rating method to detect security vulnerabilities in website-based applications. This study produces 2 factors to estimate Likelihood and Impact, from each factor there are 3 risks found, namely risk severity High, risk severity Medium and risk severity Low. The results of this risk assessment can help system managers and developers to be aware of the risks that may occur so that they can take action to prevent and overcome these risks.

Another research conducted by [11], Based on the analysis that has been done, the SMP Negeri 3 Semarapura School Website has not implemented Rate limiting in the Login and Search sections of the Library feature. Without this limitation function, simulation of entering as many usernames and passwords as possible can be done until it is possible to find the right combination, generally this attack is known as a brute force attack. This attack is currently being overcome by applying a captcha after several incorrect combinations, or by temporarily blocking it. While the results from XXS show that the entered playload is not executed by the Website, which indicates that the Website is safe from XSS attacks. Then based on Analysis. Website vulnerabilities carried out using OWASP, the results obtained from the ZAP Report process indicate that the Website of SMP Negeri 3 Semarapura has a risk percentage or vulnerability level of Low and Medium. This is indicated by the web alerts found in the Medium, Low and Informational categories.

So, overall here the author tries to provide input to the West Lampung regency website to improve security on its website. The vulnerability was discovered due to a security flaw in the Lampung Barat district website, so researchers could easily crack the vulnerability without the slightest obstacle to enter the website.

II. RESEARCH METHODS

The main problems of information system security can be summarized into two things, namely: [2]:

1. Threats

Threats come from three main issues, namely:

1. Natural disasters (tsunami, earthquake, fire, landslide, volcanic eruption)
2. Humans (sabotage, hackers, viruses and the environment)
3. pollution, chemical effect, power reduction.

2. CIA or commonly known as Confidentiality (confidentiality), Integrity (integrity) and Availability (availability) is one of the parameters that is often used when analysing security vulnerabilities, and has become a reference for website security [12]. This parameter is used as standard and reference for evaluating network security.

The author conducted a research design using the flow that can be seen in Figure 2.

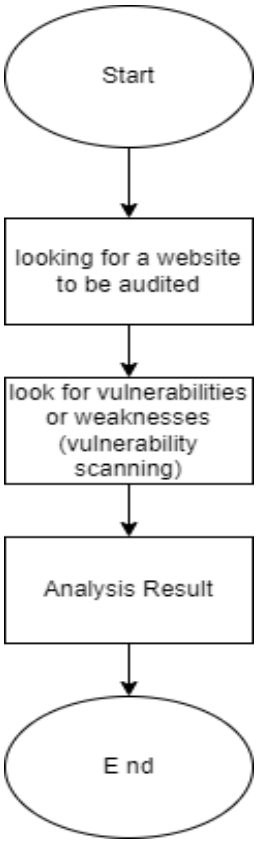

Fig. 2. Research Flowchart

1. Looking for a website that will be security audited

The website can be said as an information medium used for disseminating information on the internet because with the need for information, it is easier to get anywhere and anytime [4][13]. At the initial stage, you must first look for websites that have weaknesses according to the method we use. After doing a website search, it was found that the selected website for the West Lampung district was used as a penetration testing experiment. This is because this website has several important assets related to the West Lampung government district. Government websites should have a good level of security compared to other websites.

2. Look for vulnerabilities or weaknesses (Vulnerability Scanning)

Vulnerability is a security gap in the system that makes the system vulnerable to attack [14]. Some terms related to computer system security are threats, assets, mitigation, security gaps, mitigation, and risk. The more security holes that exist in the computer system, the higher the protection needed [15]. Techniques used to protect the system are called countermeasures [7]. There are several examples of tools that can be used for scanning, including The Harvester, Nmap, and Masscan [6]. In the second stage, the scanning stage is carried out to find security holes using OWASP ZAP tools. OWASP ZAP (Zed Attack Proxy) is an application used to perform penetration testing to find website vulnerabilities or security vulnerabilities. ZAP provides scanner automatically [2].

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1393, Copyright ©2022
Submitted : April 23, 2022; Revised : July 27, 2022; Accepted : August 30, 2022; Published : August 31, 2022

3. Analysis Results

In the last stage, after attacking the website of the Lampung Barat district using Cross-Site Request Forgery (CSRF), it was found that the results of the trial were expected to provide a solution for the CSRF method at this low level. Cross-Site Request Forgery or CSRF is one of the attacks carried out on websites based on input loopholes on the website. The security vulnerability occurs because there is a gap in the form on the website, so from here the attacker can make a request to the original form with the script that has been prepared [16]. Several approaches can be taken to overcome CSRF attacks, namely by using CSRF token [17]. At the time of submitting the form, the CSRF token will be inserted. When the request is made, then the backend will be checked to see if the CSRF sent is valid or not. CSRF token contains a random string that degenerates every form that appears on the website page. Every time a post request is made, the token will be placed as a header or it can also be a query string [18].

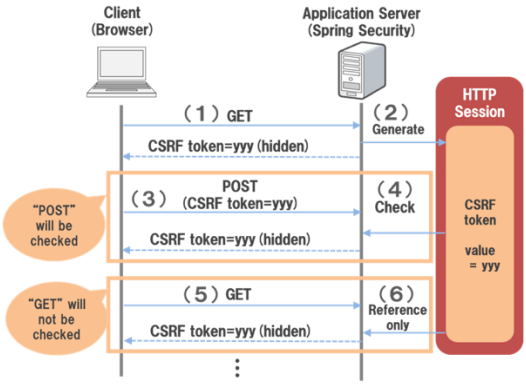

Fig. 1. Illustration from CSRF Attack

III. RESULT AND DISCUSSION

In this section, we will discuss the results of the observations and the results of the analysis carried out by the author.

A. Observation Result

The initial stage is a penetration experiment on the https://www.lampungbaratkab.go.id/ website using OWASP ZAP tools. The results of the image evidence the author scanned on the West Lampung regency website using the OWASP ZAP tools can be seen in Figure 3.

Fig. 3. Observations using OWASP ZAP

Figure 4 is the process of observing the results of scanning vulnerabilities on the website of the West Lampung Regency.

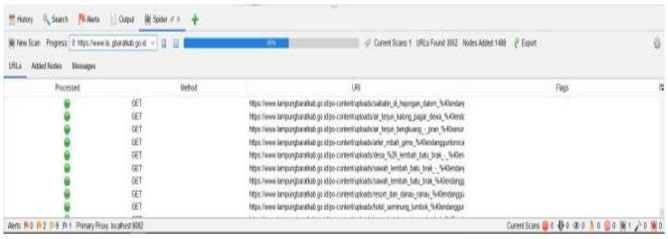

Fig. 4. Observation result (2)

The scan results in Figure 5 show that there are 12 alerts on the website from low-risk threats. Based on the 12 existing alerts, an experiment will be conducted focusing on low-risk alerts, namely using Cross Site Request Forgery (CSRF).

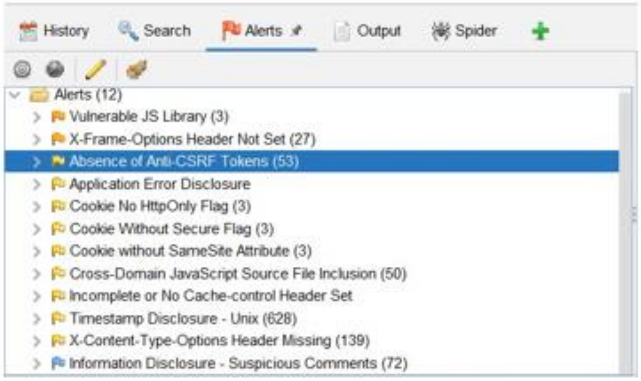

Fig. 5. Observation result (3)

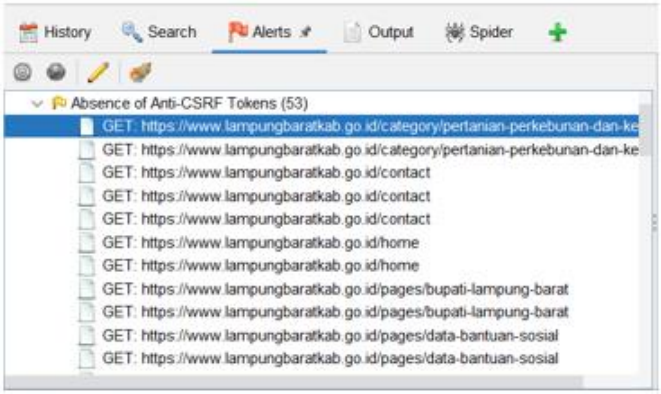

Fig. 6. Observation result (4)

Figure 6 above is a collection of various Uniform Resource Locators (URLs) which are scanned using the OWASP ZAP tool using the GET method, namely contact, home, category, page, and so on with a total of 53 obtained.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1393, Copyright ©2022
Submitted : April 23, 2022; Revised : July 27, 2022; Accepted : August 30, 2022; Published : August 31, 2022

Fig. 7. Observation result (5)

Figure 7 above is the CSRF source code which in this task focuses on form tags. The source code above is obtained from the link obtained from the previous figure 5, which is from GET: https://www.lampungbaratkab.go.id/category/pertanian-perkebunan-dan-kehutanan

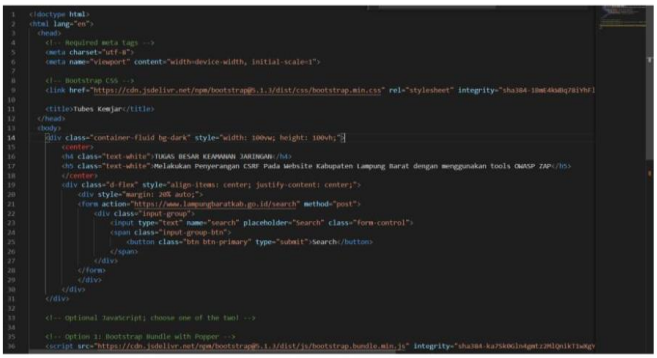

Fig. 8. Observation result (6)

Figure 8 above is a collection of lines of HTML source code that aims to display the form. Then, next we input with certain keywords. Then, if you press the search button, it will automatically lead to line 21, namely <form action= https://www.lampungbaratkab.go.id/search method=”post”>. Finally, this source code is built with CSS and bootstrap.

Fig. 9. Observation result (7)

Figure 9 above is the output in the form of a display that has been made by the development team, which comes from the source code of Figure 8.

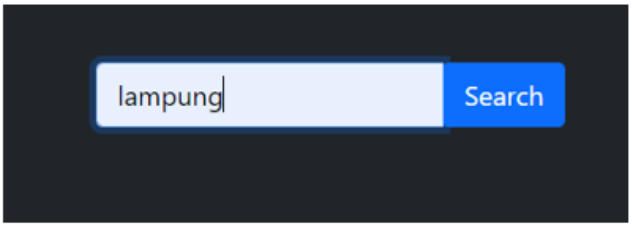

Fig. 10. Observation result (8)

Figure 10 above is a display of the search feature that the author has made. Then, after that input with the keyword "Lampung" then press the search button. Then, the keyword value will be stored as input value which will be sent to https as the keyword you want to search for.

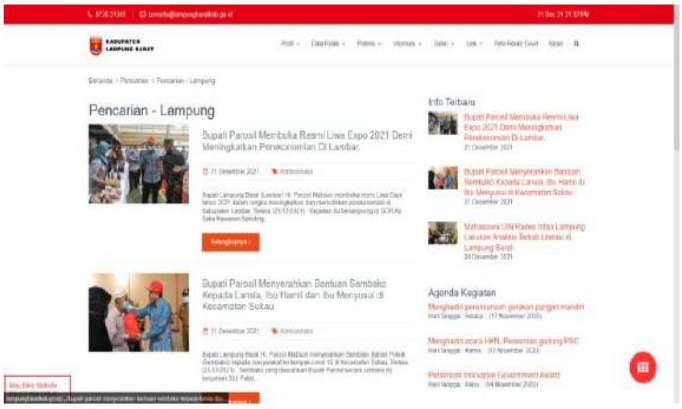

Fig. 11. Observation result (9)

Figure 11 above is the output display after we enter or input keywords and press the search button. Then it will go directly to the website page of the West Lampung Regency.

Fig. 12. Observation result (10)

Figure 12 above is the Uniform Resource Locator (URL) of our HTML index, if successful, it will go to the new direct.

B. *Observation Analysis*

At this stage, an analysis of the observations that have been made previously will be carried out. The steps for it will be described as follows.

1. OWASP ZAP has detected a weakness on the website: https://www.lampungbaratkab.go.id/ which has low risk as shown below.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1393, Copyright ©2022
Submitted : April 23, 2022; Revised : July 27, 2022; Accepted : August 30, 2022; Published : August 31, 2022

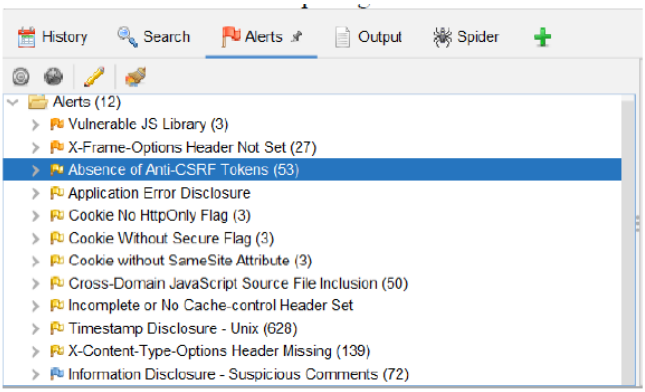

Fig. 13. Observation Analysis (1)

After OWASP ZAP has detected every weakness on the website, then we can attack according to the weakness.

2. The Absence of Anti-CSRF Tokens section (53) at the URL https://www.lampungbaratkab.go.id/ has a weakness so that attackers can carry out attack techniques using the CSRF method, allowing attackers to enter a certain script on the URL to perform his attack. It can be seen in Figure 14.

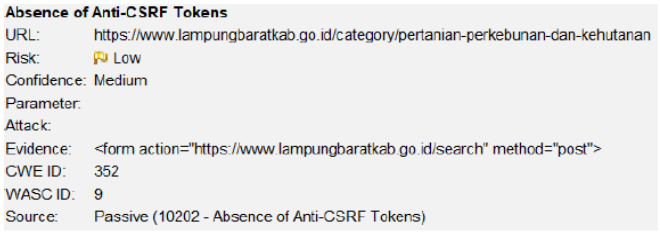

Fig. 14. Observation Analysis (2)

3. In Figure 15, there is a collection of source code that explains how to input data in the form of a form, which later this source code in the form tag will be used as the basic material for carrying out CSRF attacks.

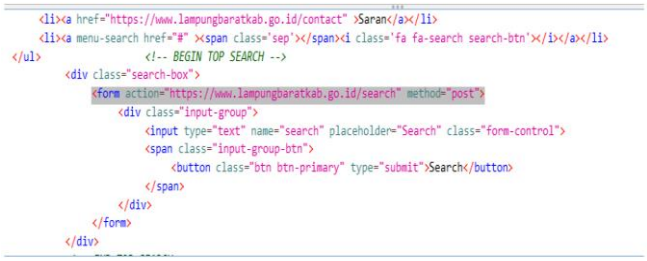

Fig. 15. Source code for CSRF attacks

4. The source code below is a duplicate of the form on the official website which aims to manipulate or defraud data sent from outside the official website. This manipulation form will lead to https://www.lampungbaratkab.go.id/search with the "POST" method.

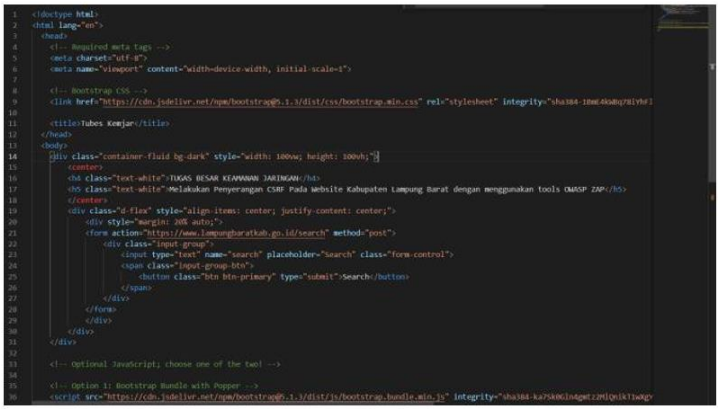

Fig.16. Source code duplication form attachment

C. *Evaluation Result*

Based on the results of previous observations, the writer then recaps the data from the observations and analyzes the observations.

TABLE I. Observation Results Table

Alert	Risk			Analysis result
	High (If the risk of attack is large and is the most important asset)	Medium (If the risk of attack is moderate and is the most important asset)	Low (If the risk of attack is not dangerous and is not a major asset)	
Cross Site Request Forgery (CSRF)			✓	The scanning results obtained from OWASP ZAP show that there are 53 URLs or links that are vulnerable to attack with low level CSRF.

From the observations, it was found that there are about 53 URLs from the https://www.lampungbaratkab.go.id/ domain.

D. *Mitigation Suggestions*

Based on the results of observations and analysis of observations made in the previous stage, to overcome CSRF attacks it is necessary to carry out mitigation as shown in Table II.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1393, Copyright ©2022
Submitted : April 23, 2022; Revised : July 27, 2022; Accepted : August 30, 2022; Published : August 31, 2022

TABLE II. Mitigation Suggestions

Alert	The Number of Vulnerability	Recovery Recommendation
Cross Site Request Forgery (CSRF)	53	Recommendations for improvement or handling are recommended using the Laravel Framework, because it has an Anti-CSRF feature because it is useful for anticipating data transmission from outside the website.

IV. CONCLUSIONS

Based on the results of observations and analysis of research that has been done, it can be concluded that: Security vulnerabilities in websites can be subject to various attack techniques. From the results of observations and analysis, it is found that there are 53 URL pages that are vulnerable to being attacked by CSRF. From the observations, it is found that the type of risk for attacks that occur on this website is low level.

REFERENCES

[1] I. F. Ashari, "Implementation of Cyber-Physical-Social System Based on Service Oriented Architecture in Smart Tourism Case Study : Bandung Natural Tourism," *J. Appl. Informatics Comput.*, vol. 4, no. 1, pp. 66–73, 2020.

[2] S. S. Wanda, "Efektivitas Pemanfaatan Website Dalam Rangka Promosi Produk dan Peningkatan Penjualan Studi Kasus PT Amonindo Utama," *PROSISKO (Jurnal Pengemb. Ris. dan Obs. Sist. Komputer)*, vol. 4, no. 2, pp. 107–117, 2017, [Online]. Available: https://repository.nusamandiri.ac.id/index.php/repo/viewitem/14763.

[3] I. F. Ashari, R. Banjarnahor, and D. R. Farida, "Application of Data Mining with the K-Means Clustering Method and Davies Bouldin Index for Grouping IMDB Movies," vol. 6, no. 1, pp. 7–15, 2022.

[4] I. F. Ashari, M. D. Satria, and M. Idris, "Parking System Optimization Based on IoT using Face and Vehicle Plat Recognition via Amazon Web Service and ESP-32 CAM (Case Study : Institut Teknologi Sumatera)," vol. 11, no. 2, pp. 137–153, 2022.

[5] I. F. Ashari, "The Evaluation of Image Messages in MP3 Audio Steganography Using Modified Low-Bit Encoding," *Telematika*, vol. 15, 2021.

[6] R. Makalalag *et al.*, "Kajian Implementasi Cross Site Request Forgery (Csrf) Pada Celah Keamanan Website," *J. Tek. Inform.*, vol. 12, no. 1, 2017.

[7] Y. Putra, Y. Yuhandri, and S. Sumijan, "Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting," *J. Sistim Inf. dan Teknol.*, vol. 3, pp. 56–63, 2021, doi: 10.37034/jsisfotek.v3i2.44.

[8] Rusdiana, C. Banta, and Sanusi, "Analisa Keamanan Website Terhadap Serangan Cross-Site Request Forgery (CSRF)," *KANDIDATJurnal Ris. dan Inov. Pendidik.*, vol. 1, no. 1, pp. 21–29, 2019.

[9] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *J. Komtika (Komputasi dan Inform.*, vol. 5, no. 1, pp. 35–42, 2021, doi: 10.31603/komtika.v5i1.5134.

[10] D. Aryanti and J. N. Utamajaya, "ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA," *J. Nas. Indones.*, vol. 1, no. 3, p. 6, 2021.

[11] D. Dwi Cahyani, L. P. Windy Puspita Dewi, K. D. Rama Suryadi, and I. M. Edy Listartha, "Analisis Kerentanan Website Smp Negeri 3 Semarapura Menggunakan Metode Pengujian Rate Limiting Dan Owasp," *Inser. Inf. Syst. Emerg. Technol. J.*, vol. 2, no. 2, p. 106, 2022, doi: 10.23887/insert.v2i2.42936.

[12] I. F. Ashari, "Graph Steganography Based On Multimedia Cover To Improve Security and Capacity," in *2018 International Conference on Applied Information Technology and Innovation (ICAITI)*, 2018, no. April 2019, pp. 194–201.

[13] I. F. Ashari, A. J. Aryani, and A. M. Ardhi, "DESIGN AND BUILD INVENTORY MANAGEMENT INFORMATION SYSTEM," vol. 9, no. 1, pp. 27–35, 2022.

[14] K. Subandi and V. I. Sugara, "Analisa Serangan Vulnerabilities Terhadap Server Selama Periode WFH di Masa Pandemi Covid-19 Sebagai Prosedur Mitigasi," in *Seminar Nasional Sains dan Teknologi*, 2021, no. November.

[15] I. F. Ashari, M. F. Zuhdi, M. T. Gagaman, and S. T. Denira, "Kolepa Mobile Application Development Based on Android Using SCRUM Method (Case Study : Kolepa Minigolf and Coffe Shop)," vol. 6, no. 1, pp. 104–112, 2022.

[16] I. F. Ashari, M. Alfarizi, M. N. K, and M. A. H, "Vulnerability Analysis and Proven On The neonime . co Website Using OWASP ZAP 4 and XSpear," *J. Teknol. Komput. dan Sist. Inf.*, vol. 5, no. 2, pp. 75–81, 2022.

[17] Y. Mulyanto and E. Haryanti, "ANALISIS KEAMANAN WEBSITE SMAN 1 SUMBAWA MENGGUNAKAN METODE VULNERABILITY ASESEMENT," *Jinteks*, vol. 3, no. 3, pp. 394–400, 2021, [Online]. Available: https://smanika-sumbawabesar.sch.id.

[18] Sahren, R. Ashari Dalimuthe, and M. Amin, "Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus," in *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, 2019, no. September, pp. 994–1001.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1393, Copyright ©2022
Submitted : April 23, 2022; Revised : July 27, 2022; Accepted : August 30, 2022; Published : August 31, 2022