p–ISSN: 2723 - 6609 e-ISSN: 2745-5254
Vol. 5, No. 5 May 2024 http://jist.publikasiindonesia.id/

Cross-site scripting (XSS) vulnerability in the Cirebon District Health Service web system

Isma Elan Maulani[1*], Siti Ainul Kholipah[2], Mamduh Rihadatul Aisy[3]
Universitas Muhammadiyah Cirebon, Indonesia[1], Politeknik Siber Cerdika Internasional Cirebon, Indonesia[2,3]
Email: ismaelanmaulani068@gmail.com[1*], nengiip30@gmail.com[2], aisyimel@gmail.com[3]

*Correspondence

Keywords: Information Security; Cross-Site Scripting (XSS); VulnerabilityCirebon District Health Service; Web Search; Sanitation Input.

ABSTRACT

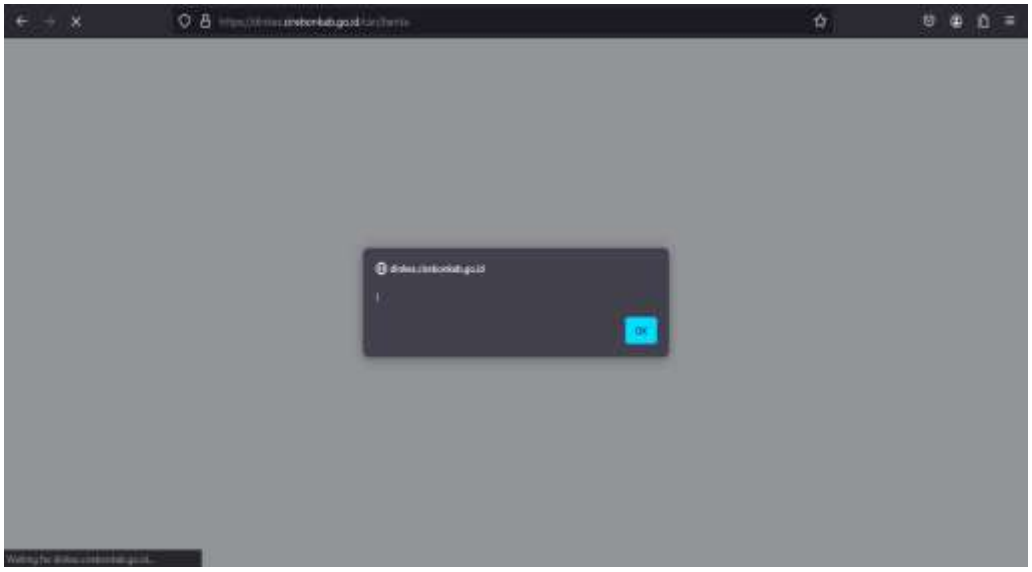
In an era of rapid growth in information technology, the enormous benefits generated are also accompanied by significant security risks. This research was conducted by an independent security researcher, Isma Elan Maulani, to identify and analyse security vulnerabilities on the Cirebon District Health Service website. The focus of the research centred on the "Search" page, where the main finding was the presence of a Cross-Site Scripting (XSS) vulnerability. XSS opens up the potential for attackers to insert and execute JavaScript scripts within web pages, threatening the security and integrity of data. Tests involving custom input proved that JavaScript scripts could be executed without sanitisation or protection. These findings show the urgency of improving the security of the Cirebon District Health Service website. Recommended remedial steps involve implementing adequate input sanitation, more rigorous user input data validation, and stricter security policies. Collaboration with authorities and cybersecurity researchers is recommended to gain additional insights and comprehensive solutions. Digital security is not only the responsibility of developers but also a collective obligation to create a safer and more secure online environment for all users.

Introduction

The growth of information technology brings great benefits but also raises security risks that need serious attention (Malhotra et al., 2021). In this context, I, Isma Elan Maulani, as an independent security researcher, have discovered a vulnerability that can significantly impact a website's security. On this occasion, I would like to share my findings regarding the Cirebon District Health Service website.

My research focused on the "Search" page on the Cirebon District Health Service website (Herawati & Sunjaya, 2022). In the initial stages of the research, I managed to identify and analyse the presence of XSS (Cross-Site Scripting) security vulnerabilities.

This vulnerability allows attackers to insert and execute JavaScript scripts within page content, opening the opportunity for attacks and data misuse (Rodríguez et al., 2020). Through testing by entering input `'"</img> <audio src=1 href=1 onerror="javascript:alert(1)".



Documentation

I discovered that those JavaScript scripts were executed without any sanitisation or protection. Malicious parties can exploit this weakness to carry out XSS attacks, which can harm site users in various ways (Rodríguez et al., 2020). These findings underscore the urgency of improving the security of the Cirebon District Health Service website. By understanding the risks involved, I hope these findings can serve as a basis for overall security improvements.

Recommended remediation steps include updating input sanitisation mechanisms, rigorously validating user input data, and implementing stricter security policies (Krichen, 2023). Collaboration with security researchers or cybersecurity experts is also recommended to gain additional insights and comprehensive solutions. It is important to remember that digital security is a shared responsibility (Trim & Lee, 2021). By taking concrete steps now, we hope to create a safer, more trusted and protected online environment for all users.

Research Methods

A quantitative approach is used in information security research regarding Cross-Site Scripting (XSS) vulnerabilities in the Cirebon District Health Service web system. In the initial stage, relevant quantitative parameters are identified to measure how the vulnerability affects the system (Kampova et al., 2020). These parameters include the number of vulnerabilities, the risk level of each vulnerability, the time required for detection and mitigation, and several other quantitative factors (Mishra et al., 2020). Data

is collected through thorough penetration testing, with each vulnerability discovered recorded along with related information, such as complexity and severity (Upadhyay & Sampalli, 2020). The time required to detect and resolve each vulnerability is also carefully recorded. Statistical analysis using various statistical tools, such as mean and median, is applied to detail and process the collected data (Mertler et al., 2021).

In risk measurement, information security metrics are used to calculate the risk value associated with each vulnerability (Ganin et al., 2020). The next step is to compare the metric and statistical results obtained with applicable security standards to assess how much the system security complies with the established standards (Philippou et al., 2020). After implementing an XSS prevention solution, its effectiveness is measured quantitatively by comparing the number of vulnerabilities before and after the implementation of the solution. Satisfaction and awareness surveys are conducted through questionnaires and interviews to obtain a qualitative perspective that can complement the quantitative data (Wipulanusat et al., 2020). Data visualisation using graphs and diagrams helps present findings clearly and easily understood. The overall research method is designed to provide robust empirical data, support XSS vulnerability analysis, and evaluate the effectiveness of preventive measures implemented on the Cirebon District Health Service web system.

Results and Discussion

The research results related to the security of the Cirebon District Health Service website show an XSS (Cross-Site Scripting) vulnerability, which can seriously impact site security. Identification was performed on the "Search" page, where it was found that JavaScript scripts could be inserted and executed without any sanitisation or protection. A concrete example of this vulnerability is seen when testing using the input `"</img> <audio src=1 href=1 onerror=" javascript: alert(1)"` in the Search field, resulting in the execution of a script that creates an alert message with value 1. Potential impacts may include XSS attacks, theft of user information, or content manipulation. Incompatibilities in input sanitation were highlighted, where existing mechanisms could not address unsafe input, allowing script execution directly within the page content. As a solution, it is recommended to immediately implement adequate input sanitation and update security policies on the site.

The growth of information technology brings tremendous benefits in terms of information availability and accessibility (Chen et al., 2020). However, security risks also grow with these advances, requiring serious attention. As an independent security researcher, my travels led me to an alarming discovery regarding the Cirebon District Health Service website. My research focused on the "Search" page, a crucial feature on the site. To thoroughly understand the site's security, I conducted a series of tests to identify potential vulnerabilities (Zhang et al., 2020). As a result, an XSS vulnerability was revealed that could give attackers access to insert and execute JavaScript scripts in page content without adequate sanitation.

In this in-depth exploration, I chose to use the input `"</img> <audio src=1 href=1 onerror=" javascript: alert(1)"` in the Search column as a test. The goal is to see how far the system can respond to unsafe input. The results show that the inserted JavaScript script executed without a hitch, raising a warning message (alert) with a value 1. This vulnerability raises the potential for significant impact, especially in the context of an XSS attack. Given this vulnerability, an attacker could execute malicious scripts, steal user information, or even replace page content with false or malicious information (Usha et al., 2020).

A more profound weakness was revealed when I noticed a lack of adequate sanitation or protection of user input. Mechanisms that are supposed to mitigate security risks do not function properly, enabling potential attacks that can compromise the integrity and security of the site. To provide a more complete picture of these findings, updating input sanitisation mechanisms and validating user input data more closely is recommended. Additionally, strengthening website security policies, such as adding additional layers of security and adopting security best practices, needs to be implemented immediately.

Regarding follow-up, collaboration with site management is crucial. In this case, the Cirebon District Health Service was invited to be involved in dialogue and joint action. Given the urgency of these findings, this collaboration can speed up the remediation process and ensure a better understanding of the security aspects that need improvement. Next, consider involving security researchers or cybersecurity experts who can provide further insight. This kind of collaboration will allow relevant parties to gain a more in-depth view of these findings and the corrective steps that can be taken.

It is important to remember that digital security is not just the responsibility of developers or researchers but is also the shared responsibility of the entire internet user community. These findings create a more profound awareness of the importance of security in website management, especially in the healthcare context. In conclusion, immediate improvements and efforts to strengthen the security of the Cirebon District Health Service website are crucial to creating a safe and reliable online environment for all users. Through collaboration, deep understanding, and appropriate action, it is hoped that this site will face digital security challenges better in the future.

A Cross-Site Scripting (XSS) vulnerability on the Cirebon District Health Service web system is a severe security problem, allowing attackers to insert and execute malicious scripts within the web page. XSS occurs when a web application does not correctly validate or filter input, allowing users to insert script code later executed by other users' browsers.

The following are several discussion points regarding XSS vulnerabilities on the Cirebon District Health Service web system:

1. Penetration via Forms and User Input:

   Attackers can exploit input forms on web pages to insert malicious scripts. This may occur if user input is not correctly validated or filtered before being saved or displayed.

2. Impact on End Users:

Inserted scripts can affect end users' access to the web page. They can steal session cookies, redirect users to phishing sites, or harvest users' personal information.

3. Insecurity in JavaScript Scripts:

If a web page uses JavaScript scripts without adequate security controls, the inserted script may be executed automatically by the user's browser. Therefore, it is essential to sanitise input and use correct coding methods.

4. Impact on Data Security:

XSS can be used to insert scripts that access or modify sensitive data, compromise data integrity, or even cause leaks of confidential information.

5. XSS Prevention:

Implementing a content security policy (CSP) can help prevent XSS by limiting the types of resources a web page can load. Validating and sanitising user input before saving or displaying it on a web page is crucial to preventing XSS attacks. Use proper encoding functions when inserting dynamic data into HTML or JavaScript.

6. Security Monitoring and Auditing:

Routinely monitor and audit web system security to detect potential vulnerabilities and address security issues that may arise.

7. Security Development:

Always follow security development best practices, including selecting a secure framework, regularly updating it, and using automated security tools.

It is essential to immediately address and repair XSS vulnerabilities in the Cirebon District Health Service web system so that the data and information stored therein remain safe from security threats. These improvements should include implementing good development security practices and regularly monitoring system security.

The Cirebon District Health Service web system faces serious security challenges due to Vulnerability Cross-Site Scripting (XSS), which allows attackers to insert and execute malicious web pages. In this situation, the primary risks involve potential theft of sensitive information, data alteration, and even potential harm to end users by manipulating script execution in the browser. To overcome this problem, it is necessary to take comprehensive preventive measures, including strict validation of user input, use of output encoding techniques, and implementation of a Content Security Policy (CSP) to limit web pages' resources.

XSS vulnerability prevention and remediation efforts also include education of development teams, implementation of security protocols such as HTTPS, and regular system updates. Additional security measures, such as using a Web Application Firewall (WAF), regular penetration testing, and effective monitoring and logging, become an integral part of the security strategy. Thus, the Cirebon District Health Service can minimise security risks and protect their data and web system integrity from XSS threats through this holistic approach.

To complete the security strategy against Vulnerability Cross-Site Scripting (XSS) on the Cirebon District Health Service web system, it is necessary to emphasise the need

to implement additional security policies. Using security headers such as Strict-Transport-Security (HSTS), X-Content-Type-Options, and X-Frame-Options can improve the security of web applications by reducing the risk of exploitation.

In addition, regular security audits are an essential step to detect and address potential security vulnerabilities proactively. Security teams must monitor developments in information security and ensure that systems are kept up to date with the latest updates. Continuous education for end users is also integral to the overall strategy to increase security awareness and prevent social engineering attacks.

In this context, collaboration with cybersecurity experts and local authorities can provide additional insight and resources to confront evolving security threats. By adopting this holistic approach, the Cirebon District Health Service can strengthen the security defences of its web systems and maintain the integrity and confidentiality of vital health information.

Conclusion

Overall, successfully overcoming the Cross-Site Scripting (XSS) Vulnerability in the Cirebon District Health Office's web system requires a holistic and integrated approach to security. Preventive measures involving input validation, output encoding, and implementing a Content Security Policy (CSP) are critical. Education and engagement of the development team and using security protocols such as HTTPS strengthen the security layer. Monitoring and rapid response to threats are recognised through Web Application Firewall (WAF), periodic penetration tests, and effective monitoring and logging. Additional security policies such as Strict-Transport-Security (HSTS) and cooperation with cybersecurity experts are essential to improving security defences. In addition, security awareness for end users and collaboration with authorities can strengthen health data and information protection efforts. With this approach, the Cirebon District Health Office can reduce the risk of XSS, ensure the integrity of the web system, and maintain the security of critical health information.

Bibliography

Chen, Peng Ting, Lin, Chia Li, & Wu, Wan Ning. (2020). Extensive data management in healthcare: Adoption challenges and implications. *International Journal of Information Management*, *53*, 102078.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, Dayton, & Linkov, Igor. (2020). A multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183–199.

Herawati, Dewi Marhaeni Diah, & Sunjaya, Deni Kurniadi. (2022). Implementation Outcomes of National Convergence Action Policy to Accelerate Stunting Prevention and Reduction at the Local Level in Indonesia: A Qualitative Study. *International Journal of Environmental Research and Public Health*, *19*(20), 13591.

Kampova, Katarina, Lovecek, Tomas, & Rehak, David. (2020). A quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic—International *Journal of Critical Infrastructure Protection*, *30*, 100376.

Krichen, M. (2023). Formal methods and validation techniques for ensuring automotive systems security. *Information*, *14*(12), 666.

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. Kumar, & Hong, Wei Chiang. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors*, *21*(5), 1809.

Mertler, C. A., Vannatta, Rachel A., & Lavenia, Kristina N. (2021). *Advanced and multivariate statistical methods: Practical application and interpretation*. Routledge.

Mishra, S., Anderson, K., Miller, B., Boyer, K., & Warren, Adam. (2020). Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. *Applied Energy*, p. *264*, 114726.

Philippou, E., Frey, S., & Rashid, Awais. (2020). Contextualising and aligning security metrics and business objectives: A GQM-based methodology. *Computers & Security*, p. *88*, 101634.

Rodríguez, Germán E., Torres, Jenny G., Flores, Pamela, & Benavides, Diego E. (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. *Computer Networks*, *166*, 106960.

Trim, Peter R. J., & Lee, Yang Im. (2021). The global cyber security model: counteracting cyber-attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing*, *5*(3), 32.

Upadhyay, D., & Sampalli, Srinivas. (2020). SCADA (Supervisory et al.) systems: Vulnerability assessment and security recommendations. *Computers & Security*, p. *89*, 101666.

Usha, G., Kannimuthu, S., Mahendiran, P. D., Shanker, Anusha Kadambari, & Venugopal, Deepti. (2020). Static analysis method for detecting cross-site scripting vulnerabilities. *International Journal of Information and Computer Security*, *13*(1), 32–47.

Wipulanusat, Warit, Panuwatwanich, Kriengsak, Stewart, Rodney A., & Sunkpho, Jirapon. (2020). Applying mixed methods sequential explanatory design to innovation management. *The 10th International Conference on Engineering, Project, and Production Management*, 485–495. Springer.

Zhang, Xiong, Xie, Haoran, Yang, Hao, Shao, Hongkai, & Zhu, Minghao. (2020). A general framework to understand vulnerabilities in information systems. *IEEE Access*, *8*, 121858–121873.