PUBLISHED BY
JR
EDUCATION

Available online at http://ijite.jredu.id

IJITE

International Journal of Information Technology and Education (IJITE) 1(3), (June 2022) 103 - 111

International Journal of Information Technology and Education (IJITE)

http://ijite.jredu.id

Cross-site Scripting Reflected as A Risk High-Level Attack on University Website

Olivia E.S Liando, Johan Reimon Batmetan, Dina Meri Demhi·

Departement of Information and Communication Techonology Education, Universitas Negeri Manado

*Corresponding author : 20208106@unima.ac.id

ARTICLE INFO

Article history:

Received: 20 March 2022; Received in revised form: 29 April 2022; Accepted: 20 June 2022;

Available online: 30 Juli 2022; Handling Editor: Fabiola Natasya Wauran

ABSTRACT

The era of digitalization is an era where information can be exchanged quickly and easily. This has contributed to improving the standard of human life for the better in all areas of life. The web is a technological innovation that changes the provision of information, services, and displays significantly. This allows for better interaction between service providers and their users. In general, universities use the website as a medium of information and media to support lecture activities and as campus promotions. However, many websites at universities do not yet have a strong level of security or protection, giving rise to opportunities for theft and manipulation of university data. XSS is an attack by inserting malicious code in the form of javascript through the input form that aims to steal cookies and then use these cookies to enter the web legally. The purpose of this study is to find out what risks will be posed by XSS to the website, especially the website used by Manado State University. This research method is carried out in 4 stages, namely software installation, vulnerability testing, presentation of the results of testing and solutions for website vulnerabilities.The results obtained through this study contained several vulnerabilities on Manado State University website which were obtained using OWASP tools. In addition to obtaining vulnerabilities on the website, solutions are also provided to overcome these vulnerabilities.

Keywords : Cross-site scripting, University, Manado State University

INTRODUCTION

The era of digitalization is an era where information can be exchanged quickly and easily. This has contributed to improving the standard of human life for the better in all areas of life. Internet service users today have different educational backgrounds and ages. With the more widespread use, the more vulnerable network security is to attacks(Nagarjun & Ahamad, 2020). To avoid unexpected conditions, it is necessary to monitor and disseminate good information for internet service users. One of the concerns of researchers is that some attacks are carried out in a simple way but result in very large losses for other parties and users(Hartono & Triloka, 2021). Thus, site organizers need to take precautions to avoid these security holes. The web is a technological innovation that changes the provision of information, services, and displays significantly(Wibowo & Sulaksono, 2021). This allows for better interaction between service providers and their users. By utilizing this technology, it will be easier for service users to obtain information or access the required features. When accessing a web page, it will be associated with cookies. Cookies are data files that are written to the hard disk by the Web Server to identify the user on the site so that when the user returns to visit the site, the site will recognize it. In general, universities use the website as a medium of information and media to support lecture activities and as campus promotions. However, many websites at universities do not yet have a strong level of security or protection, giving rise to opportunities for theft and manipulation of university data(Hakim, Cahyanto, & Aziza, 2020).

XSS is an attack by inserting malicious code in the form of javascript through the input form that aims to steal cookies and then use these cookies to enter the web legally. XSS has 3 categories including, DOM-Based XSS how it works by utilizing javascript to manipulate model objects, the next Stored On Presistent XSS works by injecting javascript into the server and stored permanently in the database and the last using the technique of reflecting malicious code to the browser used by the victim, this method is called Refected Non-Persistent XSS. If this is allowed, it will have a bad impact on the website and university, because university data is leaked to irresponsible parties.

The purpose of this study is to find out what risks will be posed by XSS to the website, especially the website used by Manado State University. And what steps can be used to deal with these attacks.

METHOD

This research method is carried out in 4 stages, namely software installation, vulnerability testing, presentation of the results of testing and solutions for website vulnerabilities. Software installation is a process to prepare tools used in research (Riadi, Umar, & Lestari, 2020). Vulnerability testing to find out vulnerabilities on the website. After knowing the vulnerability on the website, then the results of the test are described. The last step is to provide solutions for dealing with the vulnerabilities encountered. The schematic can be seen in the following figure.

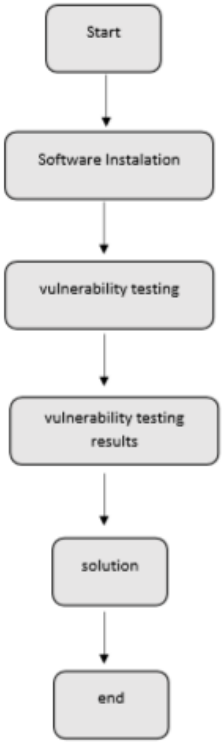

Figure 1. Vulnerability Test Flow

RESULTS AND DISCUSSION

Manado State University website has several security vulnerabilities, where these vulnerabilities were obtained using the OWASP ZAP Here are the test results.

POST:
http://192.100.0.65/gtadmisi/index.php?act=view&mod=home&sub=homeDaftar&typ=ht ml

Risks that occur with medium confidence with active sources that occur in Email

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtadmisi/index.php?act=view&mod=home&sub=homeDaftar&typ=html
Risiko: High
Keyakinan: Medium
Parameter: email
Serangan: "><img src=x onerror=prompt()>
Bukti: "><img src=x onerror=prompt()>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 2. Email Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtadmisi/index.php?act=view&mod=home&sub=homeDaftar&typ=ht ml

Risks that occur with medium confidence with active sources that occur in Nama

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtadmisi/index.php?act=view&mod=home&sub=homeDaftar&typ=html
Risiko: High
Keyakinan: Medium
Parameter: nama
Serangan: "><img src=x onerror=prompt()>
Bukti: "><img src=x onerror=prompt()>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 3. "Nama" Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtadmisi/index.php?act=view&mod=home&sub=homeDaftar&typ=ht ml

Risks that occur with medium confidence with active sources that occur in noHp

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtadmisi/index.php?act=view&mod=home&sub=homeDaftar&typ=html
Risiko: High
Keyakinan: Medium
Parameter: noHp
Serangan: "><img src=x onerror=prompt()>
Bukti: "><img src=x onerror=prompt()>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 4. “noHp” Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtadmisi/index.php?act=view&mod=login_default&sub=pengumuma n&typ=html

Risks that occur with medium confidence with active sources that occur in Test Number

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtadmisi/index.php?act=view&mod=login_default&sub=pengumuman&typ=html
Risiko: High
Keyakinan: Medium
Parameter: noTest
Serangan: "><img src=x onerror=prompt()>
Bukti: "><img src=x onerror=prompt()>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 5. “noTest” Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtriset_portal/index.php?act=view&mod=agenda&sub=Agenda&typ= html

Risks that occur with medium confidence with active sources that occur in keywords

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtriset_portal/index.php?act=view&mod=agenda&sub=Agenda&typ=html
Risiko: High
Keyakinan: Medium
Parameter: keyword
Serangan: "><img src=x onerror=prompt()>
Bukti: "><img src=x onerror=prompt()>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 6. keyword Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtriset_portal/index.php?act=view&mod=home&sub=home&typ=ht ml

Risks that occur with medium confidence with active sources that occur in the tahun_mulai

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtriset_portal/index.php?act=view&mod=home&sub=home&typ=html
Risiko: High
Keyakinan: Medium
Parameter: tahun_mulai
Serangan: </script><img src=x onerror=prompt()><script>
Bukti: </script><img src=x onerror=prompt()><script>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 7. "tahun_mulai" Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtriset_portal/index.php?act=view&mod=home&sub=home&typ=ht ml

Risks that occur with medium confidence with active sources that occur in the tahun_selesai

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtriset_portal/index.php?act=view&mod=home&sub=home&typ=html
Risiko: High
Keyakinan: Medium
Parameter: tahun_selesai
Serangan: </script><img src=x onerror=prompt()><script>
Bukti: </script><img src=x onerror=prompt()><script>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 8. "tahun_selesai" Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtriset_portal/index.php?act=view&mod=login&sub=login&typ=html

Risks that occur with medium confidence with active sources that occur in pword

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtriset_portal/index.php?act=view&mod=login&sub=login&typ=html
Risiko: High
Keyakinan: Medium
Parameter: pword
Serangan: ';alert(1);'
Bukti: ';alert(1);'
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 9. pword Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtriset_portal/index.php?act=view&mod=login&sub=login&typ=html

Risks that occur with medium confidence with active sources that occur in uname

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtriset_portal/index.php?act=view&mod=login&sub=login&typ=html
Risiko: High
Keyakinan: Medium
Parameter: uname
Serangan: ';alert(1);'
Bukti: ';alert(1);'
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 10. uname Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtriset_portal/index.php?act=view&mod=lpm_tema&sub=Tema&typ =html

Risks that occur with medium confidence with active sources that occur in combo_jenis

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtriset_portal/index.php?act=view&mod=lpm_tema&sub=Tema&typ=html
Risiko: High
Keyakinan: Medium
Parameter: combo_jenis
Serangan: "><img src=x onerror=prompt()>
Bukti: "><img src=x onerror=prompt()>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 11. "combo_jenis" Parameter Vulnerability Testing

POST:
http://192.100.0.65/gtriset_portal/index.php?act=view&mod=lpm_tema&sub=Tema&typ =html

Risks that occur with medium confidence with active sources that occur in keywords

Cross Site Scripting (Reflected)
URL: http://192.100.0.65/gtriset_portal/index.php?act=view&mod=lpm_tema&sub=Tema&typ=html
Risiko: High
Keyakinan: Medium
Parameter: keyword
Serangan: "><img src=x onerror=prompt()>
Bukti: "><img src=x onerror=prompt()>
CWE ID: 79
WASC ID: 8
Sumber: Aktif (40012 - Cross Site Scripting (Reflected))

Figure 12. keyword Parameter Vulnerability Testing

Based on OWASP to address the vulnerabilities found on the Manado State University website, the following recommendations are given.

1. Check Site Security
To maintain the security of your website application, you need to ensure that pages that generate dynamic content do not support unwanted tags, such as filtering, validation, and encoding. Not only that, website owners can use a website vulnerability scanner, such as Sucuri or VirusTotal to analyze the security of the site. By doing this method, website owners can find out complete information about the weaknesses and security vulnerabilities that exist in the site.

2. Adopt Crossing Boundaries Policy
The existence of a crossing boundaries policy allows users to enter login information as a form of authentication. Not only that, website owners can also reset and ask users to enter their credentials on certain website pages.

3. Adding SDL
The existence of a crossing boundaries policy allows users to enter login information as a form of authentication. Not only that, website owners can also reset and ask users to enter their credentials on certain website pages.

CONCLUSION

The results obtained through this study contained several vulnerabilities on Manado State University website which were obtained using OWASP tools. The vulnerabilities found include the parameters Email, Name, noHp, noTest, keyword, year_start, year_finished and several vulnerabilities in other features. In addition to obtaining vulnerabilities on the website, solutions are also provided to overcome these vulnerabilities.

REFERENCES

Dwi Cahyani, D., Windy Puspita Dewi, L. P., Rama Suryadi, K. D., & Edy Listartha, I. M. (2022). Analisis Kerentanan Website Smp Negeri 3 Semarapura Menggunakan Metode Pengujian Rate Limiting Dan Owasp. *INSERT : Information System and Emerging Technology Journal*, *2*(2), 106. https://doi.org/10.23887/insert.v2i2.42936

Firmansyah, R., & Prasetya, W. S. (2018). Pencegahan Serangan Cross Site Scripting dengan Teknik Metacharacter pada Sistem e-Grocery. *Jurnal ENTER*, *1*, 294–306.

Hakim, A. S., Cahyanto, T. A., & Aziza, H. A. F. (2020). *Serangan Cross-Site Scripting (Xss) Berdasarkan Base*.

Hartono, H., & Triloka, J. (2021). Method for Detection and Mitigation Cross Site Scripting Attack on Multi-Websites. *International Conference on Information Technology and Business (ICITB)*, 26–32.

Kurniawan, A. (2019). Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based. *Jurnal Telematika*, *14*(1), 9–18. Retrieved from https://journal.ithb.ac.id/telematika/article/view/267%0Ahttps://journal.ithb.ac.id/telematika/article/download/267/281

Hakim, A. S., Cahyanto, T. A., & Aziza, H. A. F. (2020). *Serangan Cross-Site Scripting (Xss) Berdasarkan Base*.

Hartono, H., & Triloka, J. (2021). Method for Detection and Mitigation Cross Site Scripting Attack on Multi-Websites. *International Conference on Information Technology and Business (ICITB)*, 26–32.

Nagarjun, P. M. D., & Ahamad, S. S. (2020). Cross-site scripting research: A review. *International Journal of Advanced Computer Science and Applications*, *11*(4), 626–631. https://doi.org/10.14569/IJACSA.2020.0110481

Putra, Y., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. *Jurnal Sistim Informasi Dan Teknologi*, *3*, 56–63. https://doi.org/10.37034/jsisfotek.v3i2.44

Riadi, I., Umar, R., & Lestari, T. (2020). Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *5*(3), 146–152. https://doi.org/10.14421/jiska.2020.53-02

Wibowo, R. M., & Sulaksono, A. (2021). Web Vulnerability Through Cross Site Scripting (XSS) Detection with OWASP Security Shepherd. *Indonesian Journal of Information Systems*, *3*(2), 149–159. https://doi.org/10.24002/ijis.v3i2.4192