DOI: https://doi.org/10.33197/justinfo.v2i1.1806 ISSN: 3031-3449

Analysis of Website Vulnerability to Defacement Attacks

[1]Fatharani Eka Putri, [2]Fairuz Zahrah An Nibras
[1]Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, fatharani.eka@widyatama.ac.id
[2]Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, fairuz.zahrah@widyatama.ac.id

ABSTRACT

The development of information technology and the internet has become integrated into people's lives. The accessibility of the internet has provided fast access for people to connect globally for communication and sharing information. However, this development has also created vulnerabilities in security systems, including website defacement attacks. Website defacement is a hacking technique used to modify or inject files into a server, performed by hackers to alter or damage a website's appearance. These attacks can be carried out without requiring full access rights. Such actions are taken to tarnish the reputation of individuals or organizations by exploiting vulnerabilities in security systems. Addressing this issue comprehensively, this article examines website defacement attacks by exploring attack techniques. It focuses on the types of defacement attacks, attack techniques, and ways to prevent website defacement attacks to protect individuals and organizations.

Keywords: Defacement Attacks, Information and Internet Security, Website.

Corresponding Author:

Fatharani Eka Putri
Information Systems, Faculty of Engineering, Widyatama University
Bandung, Indonesia
fatharani.eka@widyatama.ac.id

INTRODUCTION

The development of information technology and the internet has transformed the way people interact. Information technology has integrated into people's lives, encompassing communication, commerce or business, information and service provision, and education. The availability of the internet and various online platforms has opened doors for people to connect globally quickly, allowing them to access information, services, and resources that were previously difficult to find.

One of the most significant platforms available on the internet is the website. Websites are a vital digital asset in this digital era, serving as platforms for various activities, including business transactions, information dissemination, and social interactions. However, amidst all its benefits, websites are vulnerable to cyber-attacks, one of which is defacement attacks.

Defacement is a form of cybercrime that alters the web pages of others without the owner's permission [1]. Individuals who perform defacement are called defacers. Defacers engage in activities to exploit security vulnerabilities in websites to deface them. They often replace the website's appearance with messages or images they desire, such as hacker group logos, political messages, or even pornographic content [2]. These attacks not only tarnish the image and reputation of the website owner but can also cause financial losses and leakage of sensitive data. Defacement attacks commonly occur on government websites, such as those of the Ministry of Communication and Information Technology, the General Election Commission, the Ministry of Health, BSSN, and others.

The purpose of this research is to comprehensively analyze website vulnerabilities to defacement attacks. By understanding the types of vulnerabilities, their causes, and prevention methods, website owners can take proactive steps to enhance security and prevent defacement attacks. This study aims to provide a detailed examination of the nature of defacement attacks, the techniques used by defacers, and the best practices for safeguarding websites against such threats.

LITERATURE REVIEW

Defacement attacks have become a significant cybersecurity threat to websites worldwide, including in Indonesia. Defacers exploit various vulnerabilities in website security systems to alter the interface without the owner's permission, often to embarrass the website owner, spread specific messages, or even steal data. Understanding these vulnerabilities is crucial to improving website security and preventing defacement attacks.

Several studies have identified various types of website vulnerabilities that are susceptible to defacement attacks. One such study by Alzahrani (2018) used the Nessus application to identify vulnerabilities in university websites. The study found several vulnerabilities, such as SQL injection, cross-site scripting (XSS), and insecure configurations, which can be exploited by defacers.

Dewanto (2018), in his research using penetration testing methods on the domain UII.AC.ID, also found similar vulnerabilities. This study emphasized the importance of regular security testing to identify and fix vulnerabilities before they can be exploited by defacers.

Additionally, Suhendi (2020) discussed the impact of defacement attacks on website performance and organizational reputation. The study showed that defacement attacks could cause financial losses and loss of customer trust, further highlighting the importance of prevention and mitigation efforts.

The Open Web Application Security Project (OWASP), an organization focused on web application security, also publishes a list of the top 10 web application security risks (OWASP Top 10). This list includes various vulnerabilities that can be exploited by defacers, such as SQL injection, XSS, and insecure configurations [6].

The National Cyber and Crypto Agency (BSSN) in Indonesia regularly publishes reports on the cybersecurity situation in Indonesia. The 2023 report indicated that defacement attacks remain one of the top cybersecurity threats faced by websites in Indonesia [7].

These studies and resources highlight the importance of understanding and addressing website vulnerabilities that are susceptible to defacement attacks. With strong knowledge of these vulnerabilities, website owners and administrators can take steps to strengthen their website security and prevent defacement attacks.

METHODOLOGY

This research adopts a deep qualitative-descriptive approach to understand the inherent vulnerabilities in websites that are susceptible to defacement attacks. The qualitative approach allows researchers to explore deeper aspects, enabling a comprehensive understanding of the dynamics of these vulnerabilities.

The data underlying this research were collected from reliable sources, such as research reports and publications in verified academic journals. Careful and reliable data collection is a crucial foundation for producing credible and comprehensive analysis.

Once the data were collected, the analysis process was carried out using thematic analysis techniques. This technique allows researchers to identify patterns, themes, and relevant information combinations from the existing data. Through this step, the research can detail various types of vulnerabilities in websites that have the potential to be exploited by defacement attacks and understand their root causes more deeply [8].

RESULTS AND DISCUSSION

Defacement is a method to alter, insert, defame, or delete files on a server, main page, index file, or other pages linked to the website through a URL. This method is carried out due to weaknesses in the application or website security system. Defacement is an attack aimed at changing the appearance of a website. Additionally, website defacement is conducted to perform initial security testing of the website. Web defacement aims to obtain important information through data theft, voice political issues, and damage the reputation of individuals or organizations.

Types of Defacement

Defacement is divided into two types based on the impact of the defacement attack on the website.

Full Defacement

Full defacement is a type of defacement aimed at changing the entire website (full page defacement), i.e., completely altering the appearance of a page or index file. In doing so, a defacer directly interacts with the application or website security system, such as root accounts or administrator accounts, allowing the defacer to control the index file entirely. The following are techniques used in full defacement:

1. SQL Injection: SQL injection is an attack technique where hackers insert a website parameter or query that exploits security gaps in the database layer to obtain user data.
2. Brute Force Attack: Brute force attack is a technique to gain access to user accounts by guessing all possible common usernames and passwords. This technique relies on computer processing power rather than human intelligence.
3. Cross-Site Scripting (XSS) Attacks: Cross-site scripting (XSS) attacks involve inserting scripts or codes into the application or website security system, which can be either harmless or harmful. XSS attacks occur when a hacker initiates an attack using a website to send malicious code to users and persuades them to access the application or website.
4. Malware Cybersecurity: Malware cybersecurity involves sending files or codes that infect, explore, steal, or attack through networks, emails, insecure links, or infected applications. Types of malware attacks include computer viruses, worms, trojan horses, ransomware, and spyware.

Partial Defacement

Partial defacement is a type of defacement that involves finding script weaknesses and exploiting bugs on the website. Additionally, vulnerabilities can be found on websites built with Content Management Systems (CMS). This type of defacement impacts part of the website's pages, causing visitors to refrain from accessing the website.

Causes of Defacement

In a case discussed in the journal titled “Risk Measurement of Library Information Systems Using the National Institute of Standard and Technology SP 800-30 Framework” by Megawati et al. (2020), UNILAK (Lancang Kuning University) had a library information system that experienced defacement, resulting in changes to the system's appearance, but the attacker was unknown. This defacement was caused by negligence from the Public Relations and Library UPT of UNILAK. Other causes of defacement include a lack of security awareness and the absence of activity log audits or trails [9].

Another case discussed in the journal titled “Handling Website Security Vulnerabilities with Ethical Hacking and Issaf Using Acunetix Vulnerability (Case Study at Bkpsdmd Kabupaten Kerinci)” by Kestina et al. (2023), indicates that web defacement can occur due to security issues, which are a crucial part of an information system. Government institutions are particularly vulnerable to cyber-attacks because they often fail to manage information security effectively. Many government institutions use pirated installations or applications, making them easy targets for cyber-attacks, including web defacement. Another cause of defacement is the use of non-original or pirated installations or applications [10].

According to the journal titled “Implementation and Modification of WebShell for Monitoring Website-Based Attacks” by Gumilang and Chandra (2021), defacement is carried out by hackers by planting backdoors using various methods. A backdoor is a code commonly used by hackers to gain illegal access to a website. The backdoor is then used by hackers to gain access. Gaining access is an attempt to gain access to a system as a regular user. This attack cannot be detected quickly and may take months to realize that a backdoor has been planted on the website due to the difficulty of identifying backdoor files. This indicates that awareness of information technology security or IT Security is still low, necessitating increased awareness of cybersecurity. Another cause of defacement is the difficulty in identifying backdoor files in defacement attacks [11].

Another cause of defacement, cited from the journal “Designing, Creating, and Managing School Websites for Teachers and Educational Staff at SMAN 11 Sidenreng Rappang” by Rakib et al. (2023), shows that problems can arise when a website has difficulty synchronizing with the web hosting provider. This can lead to defacement due to the inability to provide adequate security levels to protect the website [12].

From the various cases and explanations discussed from various journal sources above, the authors conclude that defacement can occur due to several factors. Some causes of defacement include:

1. Low security awareness.
2. Lack of activity log audits or trails.
3. Use of non-original or pirated installations or applications.
4. Difficulty in identifying backdoor files in defacement attacks.
5. Inability of web hosting providers to synchronize properly.

CONCLUSION

Defacement attacks are a method used to alter the appearance of a website with the aim of obtaining important information through data theft. Based on the impact of defacement attacks, they are divided into two types: full defacement and partial defacement.

There are significant differences between full defacement and partial defacement. Full defacement aims to change the entire appearance of a website. Full defacement employs several techniques, including SQL Injection, Brute Force Attack, Cross-Site Scripting (XSS) Attacks, and Malware Cybersecurity. On the other hand, partial defacement aims to find weaknesses in scripts and exploit bugs on the website.

Several factors can cause defacement attacks, one of which is low security awareness. This can be prevented by using software that functions to protect the web server from defacement attacks. Additionally, the role of the web admin is crucial in continuously monitoring the use of the web server to quickly detect if a defacement attack occurs.

This journal aims to help readers better understand defacement attacks on websites, the forms of defacement attacks, and the types of defacement attacks. Furthermore, this journal provides explanations related to the occurrence of defacement and ways to prevent defacement that readers can implement.

REFERENCES

[1] A. Setiawan and E. Yulianto, Keamanan Dalam Media Digital. Bandung: Informatika Bandung, 2020.

[2] M. S. Hasibuan and L. M. Gultom, "Analisis Serangan Deface Menggunakan Backdoor Shell Pada Website," Techno.Com, vol. 17, no. 4, pp. 415–423, 2018. doi: 10.33633/tc.v17i4.1887.

[3] M. E. Alzahrani, "Auditing Albaha University Network Security Using In-House Developed Penetration Tool," Journal of Physics: Conference Series, vol. 978, p. 012093, 2018. doi: 10.1088/1742-6596/978/1/012093.

[4] A. P. Dewanto, "Penetration Testing Pada Domain uii.ac.id Menggunakan OWASP 10," Undergraduate thesis, Universitas Islam Indonesia, 2018. [Online]. Available: https://dspace.uii.ac.id/bitstream/handle/123456789/11281/13523025-Adetya%20Putra%20D-laporan%20skripsi.pdf

[5] S. Suhendi, "Analisis Tingkat Kerentanan Keamanan Pada Website Simpabu Sistem Monitoring Penyuluhan Agama Buddha Non Pns Kantor Wilayah Kementerian Agama Provinsi Kepulauan Riau Dengan Metode Penetration Testing Execution Standard (PTES)," Undergraduate thesis, Universitas Internasional Batam, 2020. [Online]. Available: https://repository.uib.ac.id/3277/

[6] "OWASP Top Ten," OWASP Foundation. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed: Jan. 13, 2024].

[7] BSSN, "Monitoring Keamanan Siber 2022," Www.Bssn.Go.Id, 2022. [Online]. Available: https://www.bssn.go.id/monitoring-keamanan-siber-2022/. [Accessed: Jan. 13, 2024].

[8] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications, 2017.

[9] K. Megawati, I. Kurniawan, I. Maita, and N. Yanti, "Pengukuran Risiko Sistem Informasi Perpustakaan Menggunakan Framework National Institute of Standard and Technology SP 800-30," in Seminar Nasional Teknologi Informasi, Komunikasi Dan Industri (SNTIKI), 2020.

[10] L. Kestina, Y. Yuhandri, and G. W. Nurcahyo, "Penanganan Celah Keamanan Website Dengan Ethical Hacking Dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus Di Bkpsdmd Kabupaten Kerinci)," Innovative: Journal Of Social Science Research, vol. 3, no. 4, pp. 9192–9203, 2023. doi: 10.31004/innovative.v3i4.4357.

[11] P. M. R. Gumilang and D. W. Chandra, "Implementasi Dan Modifikasi WebShell Untuk Monitoring Serangan Berbasis Website," AITI, vol. 18, no. 1, pp. 54–68, 2021. doi: 10.24246/aiti.v18i1.54-68.

[12] M. Rakib, V. Aris, A. Isma, and N. Halim, "Merancang, Membuat, Dan Mengelola Website Sekolah Bagi Guru-Guru Dan Tenaga Kependidikan Di SMAN 11 Sidenreng Rappang," in Seminar Nasional Pengabdian Kepada Masyarakat, vol. 10, pp. 1072–1078, 2023.

[13] M. Albalawi, R. Aloufi, N. Alamrani, N. Albalawi, A. Aljaedi, and A. R. Alharbi, "Website Defacement Detection and Monitoring Methods: A Review," Electronics, vol. 11, no. 21, p. 3573, 2022. doi: 10.3390/electronics11213573.

[14] I. Mantra, "Indonesia Web Defacement Attacks Analysis for Anti Web Defacement," Jurnal TICOM, vol. 3, no. 3, 2015.