|Jurnal Jaringan Komputer dan Keamanan |JJKK|Vol. 5| No. 2|June|Year 2024|

The Crime of SQL Injection in the Service System at Bina Insan University Lubuklinggau

Erwinsusanto[1*], Edi Surya Negara[2]

Abstract

The rapid progress of contemporary technology significantly aids in the execution of work. The internet, as one of the most developed technologies, facilitates communication, access to stored data, and generally simplifies professional tasks. However, this convenience is accompanied by criminal threats targeting internet users, with phishing (or SQL Injection, according to the Indonesian text) being a particularly damaging offense. Phishing is defined as a threat employing social engineering techniques to deceive users by impersonating an authorized entity. This type of attack is prevalent across various industrial sectors, including corporate, banking, and education. Key factors contributing to phishing in online banking services involve users' limited knowledge, psychological vulnerabilities, and social networking privacy issues. Therefore, securing computer networks is essential for the prevention of phishing (or SQL Injection) attacks. This study employs a qualitative research methodology with descriptive techniques.

Keywords

Phishing, Internet, Research Methods

Article History

Received 27 March 2024
Accepted 21 June 2024

How to Cite

Erwinsusanto & Negara, E.S. (2024). The Crime of SQL Injection in the Service System at Bina Insan University Lubuklinggau. ***Jurnal Jaringan Komputer dan Keamanan****, 5*(2), 72-80.

[1*] Universitas Bina Darma, Indonesia, Corresponding email: erwinsusanto@gmail.com
[2] Science Technology, Universitas Bina Darma, Indonesia

Introduction

The rapid expansion of internet access has transformed how individuals interact, communicate, and complete daily tasks. The increasing reliance on internet-connected systems has made digital services—especially those operated by educational institutions—more vulnerable to various forms of cyber threats. One pressing concern is the prevalence of cyberattacks targeting web-based systems, which store large volumes of sensitive data. As users increasingly depend on online platforms to retrieve, process, and manage information, the security of these systems becomes a critical consideration for protecting user data and ensuring service continuity.

Among the cyber threats that have emerged, SQL Injection stands out as one of the most dangerous and destructive. SQL Injection is a technique used by attackers to manipulate and infiltrate a database by inserting malicious SQL queries through input fields or URL parameters. If exploited successfully, attackers can bypass authentication mechanisms, steal confidential data, alter system operations, or even destroy entire databases. These intrusions pose severe risks to institutions, including data theft, service disruption, and reputational damage. In educational institutions that manage student records, financial information, and administrative data, the consequences can be particularly harmful.

In addition to SQL Injection, phishing attacks also represent a significant cybercrime technique that targets users through social engineering and technical deception. Phishing typically involves fraudulent emails that imitate legitimate business communications, tricking victims into accessing deceptive websites designed to steal identities, login credentials, or financial information. Technical subterfuge often involves the installation of malware or "crimeware" on a victim's computer to monitor activities, steal passwords, or redirect users to attacker-controlled proxy servers. Both SQL Injection and phishing exploit human and technical vulnerabilities, making them prevalent and highly damaging.

The social engineering aspects of phishing further complicate cybersecurity challenges within organizations. Fraudulent emails, fake portals, and deceptive websites often appear legitimate, making it difficult for users to distinguish malicious attempts from authentic communication. These conditions potentially expose staff and students to identity theft, credential compromise, and unauthorized access. Such risks highlight the necessity of evaluating whether such attacks have occurred within university service systems and whether staff possess adequate awareness and preparedness.

The widespread nature of phishing and SQL Injection crimes underscores the importance of conducting systematic studies within public service sectors, including higher education environments. Universities, with their broad user base and extensive digital services, are often prime targets for cyberattacks. Their service systems typically handle high volumes of private data, making them vulnerable if security measures are not properly implemented. For this reason, analyzing the presence and potential impact of SQL Injection attempts becomes crucial in maintaining system integrity and safeguarding sensitive information.

Based on these considerations, this research focuses specifically on investigating SQL Injection crimes targeting public service systems at Universitas Bina Insan Lubuklinggau. Through direct interviews with service staff, the study seeks to identify whether phishing or

SQL Injection incidents have occurred within university services, assess staff awareness of cyber threats, and evaluate the security posture of institutional information systems. The findings are expected to contribute to improved cybersecurity practices, stronger system resilience, and better protection of user data within higher education institutions.

Methodology

Within this context, the study examines cybercrime as a broad category of offenses committed through the virtual environment, encompassing activities that target computer infrastructure, information systems, websites, and internet-based platforms. Since cybercrime has grown in parallel with advancements in digital, communication, and information technologies, understanding its evolving characteristics is essential for identifying the risks faced by institutional service systems. The investigation highlights unauthorized access, data manipulation, and digital fraud as examples of cyber-attacks that may threaten university systems.

A significant focus is directed toward the practice of hacking, defined as a technical activity performed by individuals such as hackers, crackers, intruders, or attackers to compromise a system, network, or application. Hacking techniques allow perpetrators to bypass authentication mechanisms, exploit system vulnerabilities, or gain control of sensitive information. In the context of this research, hacking is examined not only as a technical action but also as an indicator of potential system weaknesses within the university's public service platform.

To address more specific forms of attack, the study centers on SQL Injection as the primary threat under investigation. SQL Injection is a cybercrime technique used to insert malicious SQL commands into an input field or URL parameter, allowing attackers to access, manipulate, or retrieve confidential data without authorization. As noted in the conceptual reference, SQL Injection is often used to steal User IDs, PINs, bank account numbers, or credit card information. Attackers may exploit this stolen data to commit fraudulent transactions or deceive users into transferring money under false pretenses.

The research design includes qualitative data collection through interviews with service staff at Universitas PGRI Silampari, who are directly involved in operating and maintaining the affected service system. These interviews aim to explore staff awareness, identify whether past incidents resemble SQL Injection or phishing attacks, and assess institutional readiness to handle such threats. Complementing these interviews, documentation analysis is conducted to review system structures, security configurations, and potential vulnerabilities within the university's web-based services.

Finally, the collected data is analyzed using a descriptive-qualitative method to interpret patterns, assess institutional risks, and evaluate whether the system shows signs of SQL Injection vulnerabilities. The analysis seeks to determine the extent to which cyber threats have affected the institution and to provide recommendations for strengthening information system security. This methodological approach ensures that the study not only identifies existing problems but also contributes practical solutions for mitigating cybercrime risks in university service environments.

.

Research Methods

The research methodology is the approach employed to solve the problems investigated throughout the study. The researchers utilized a specific research method in the writing of this article. Qualitative research focuses on the quality or the most essential aspects inherent in the nature of an item or object. In the context of goods or services, the most crucial element, which can be a valuable lesson for developing theoretical concepts, is the meaning underlying the event/phenomenon/social symptom. Therefore, the specific qualitative approach used is descriptive research utilizing a literature review method. Literature review is a research method performed to critically examine and evaluate the issues under investigation. The researchers employed secondary data sources obtained from documents, archives, books, papers, articles, and other research findings. For data analysis, Milles and Huberman (1984) proposed a sequence of steps: data reduction, data display, and inference or validation.

Conceptual Freamwork

The conceptual framework for this research is illustrated in Figure 1 , depicting the following sequential process:

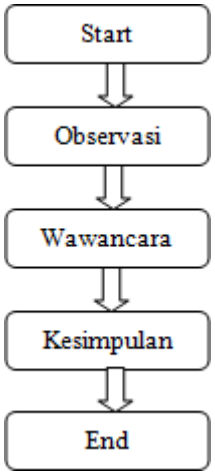

Figure 1. Research Framework

Data Collection Tecniques

Data collection was conducted directly at Universitas Bina Insan Lubuklinggau, located at Jl. HM Soeharto No. Kel, Lubuk Kupang, Kec. Lubuk Linggau Sel. I, Kota Lubuklinggau, South Sumatra 31626. The techniques used were:

- Observation Method: Direct observation was carried out at Universitas Bina Insan Lubuklinggau, where the researchers met with the Head of the Library and the Head of ICT at Universitas PGRI Silampari.
- Interview Method: Direct interviews were conducted with the Head of the Library and the Head of ICT at Universitas Bina Insan Lubuklinggau.

- Documentation: Data collection included photographs, journals, books, documents, and data on the staff members of the Musi Rawas Ministry of Religious Affairs.

Results

The evolution of cyber-attacks is accelerating and expanding rapidly. The proliferation of smartphone users, automatically connected to the internet, has not been matched by a sufficient level of understanding regarding the filtering of information, activities, or the criminal acts that can occur online, particularly via social networks. Furthermore, technological advancements have transformed crime from direct attacks on physical objects to remote attacks utilizing the internet. This remote method is used to gather detailed information on targets, with SQL Injection being one such technique.

Phishing was first introduced in 1995. According to James (2005), the initial method used by phishers was an algorithm that generated random credit card numbers. These random numbers were used to create AOL accounts , which were then exploited for sending spam and other purposes. Specialized programs like AOHell were used to simplify this process. AOL ended this practice in 1995 by implementing security measures to prevent the successful use of random credit card numbers.

Phishing, also referred to as "Brand Spoofing" or "Carding," is a deceptive service that falsely assures users that their data is legal and secure. Spoofing, as defined by Felten et al. (1997), is a technique used to gain unauthorized access to a computer or information where the attacker communicates with a user while pretending to be a trusted host.

Phishing in public services is a threat that uses social engineering to deceive users (customers). Users are lured by offers via emails, text messages, or phone calls from criminals impersonating company officials. The general public often refers to this as SQL Injection. The term phishing originates from the English word "fishing". Phishing is a form of fraud carried out by falsifying data to deceive the victim. The objective of SQL Injection (phishing) is to obtain the victim's information, ranging from passwords to credit card details, by impersonating a trustworthy person or business in an official electronic communication, such as email or instant message. This is why it is called "fishing"—luring for users' financial information and passwords.

Discussion

How Phishing Works

Phishing involves an attacker obtaining a user's sensitive information using fraudulent emails and websites that are meticulously designed to resemble the actual, official website in look and feel. The phisher uses emails, banners, or pop-ups to trick the user into being redirected to a fake webpage where they are asked to provide personal information. Phishers exploit users' lack of attention and negligence on these fake networks to obtain the information. Aspects of the threat infected by the phishing "virus" include:

1. Link Manipulation: Some phishing methods involve manipulating the link to appear as the address of the authentic institution. Common tricks used by phishers include broken URLs or the use of subdomains, for example: www.micosoft.com.
2. Filter Evasion: Phishers use images instead of text to compel users to disclose their private information. This is why services like Gmail or Yahoo disable images for incoming emails by default. To enhance the legitimacy of phishing emails, the phisher/fraudster includes:
    - Links that appear to lead to a legitimate webpage but actually direct to a phishing webpage.
    - Pop-ups that are exact replicas of the official page.

Cyber Crime Techniques Employed by Phishes

A phisher executes cybercrime using several techniques, including:

- Email Spoofing: This technique involves a phisher sending broadcast emails to millions of users, purportedly from an official institution, urging them to perform an action. The emails typically request a credit card number, password, or the uploading of a specific form.

- Web-Based Delivery: This is one of the most sophisticated phishing techniques, known as a "man-in-the-middle" attack, where the phisher positions himself between the original website and the phishing system.

- Instant Messaging (Chatting): In this method, the user receives a message containing a link that directs them to a fake website with an identical appearance. This leads the user to believe they are accessing the official and legitimate website, when it is, in fact, fraudulent.

- Trojan Hosts: The phisher attempts to log in to the user's account to gather credentials via the local machine. The acquired information is then sent to the phisher.

- Link Manipulation: A technique where the phisher sends a link to a website. If the user clicks on the link, they are redirected to the phisher's website instead of the actual, legitimate website.

- Malware Phishing: Fraudulent activity involving malware that runs on the user's computer. This malware is usually attached to an email sent by the phisher. Once the victim clicks the link, the malware is activated. The malware is sometimes included in a downloadable file.

Case Study: Website Compromise at Universitas Bina Insan Lubuklinggau Using the Phishing Technique

In 2022, the website of Universitas Bina Insan Lubuklinggau was compromised by an unknown hacker. The hacker manipulated a link to a website. When the website administrator of Universitas Bina Insan clicked on this link, the administrator's account data was captured by the phisher. Consequently, the phisher obtained the admin's username and password for the Universitas Bina Insan Lubuklinggau website. The phisher then proceeded to alter the website's front page, modify the menus, and extract data from the Universitas Bina Insan Lubuklinggau website. To resolve this, the website developer changed the admin account details (both username and password). The developer also repaired the damage, restored the front-page view and menus that had been corrupted by the hacker/phisher, and restored the lost website data. Following the recovery, the developer implemented a firewall system to enhance the security of the Universitas Bina Insan Lubuklinggau website.

Scenario of the Website Compromise at Universitas Bina Insan Lubuklinggau Using the Phishing Technique

The perpetrator sent a link to a fake free hosting service website to the email of the Universitas Bina Insan Lubuklinggau website administrator. The administrator subsequently clicked on this link.

Impact of Phishing on the Universitas Bina Insan Lubuklinggau Website

The impact of SQL Injection (phishing) on the Universitas Bina Insan Lubuklinggau website was that the website was taken over by a phisher. The phisher gained unrestricted control, altering the front-page display and the menus on the Universitas PGRI Silampari website, and was able to extract data from the Universitas Bina Insan Lubuklinggau website.

Resolution of the Phishing Impact on the Universitas Bina Insan Lubuklinggau Website

Upon the change in the website's appearance, the administrator recognized that the website had been hacked. Since the administrator could no longer access the admin account, the developer was contacted. The developer immediately checked the website, analyzing that it had been hacked using the phishing method to trap the administrator, thereby acquiring the admin account credentials. The solution involved the developer changing the administrator's username and password to block the hacker's access. The developer also restored the website's original appearance, including the front page and other pages, and repaired the menus. Additionally, the developer restored the data that had been stolen by the hacker and installed a new firewall to mitigate future attacks.

Case Study: SQL Injection on the Digital Library Website of Universitas Bina Insan Lubuklinggau

In 2021, an SQL Injection incident occurred on the Digital Library website. A phisher created a duplicate website that was an exact replica of the Digital Library website of Universitas Bina Insan Lubuklinggau. The phisher then distributed the link to users of the

Universitas PGRI Silampari Digital Library website, resulting in the successful hacking of the Universitas Bina Insan Lubuklinggau Digital Library website.

Scenario of the Digital Library Website Compromise at Universitas Bina Insan Lubuklinggau Using the Phishing Technique

A phisher created a nearly identical duplicate website of the Universitas Bina Insan Digital Library and disseminated the link to the users of the Universitas PGRI Silampari Digital Library. When a user clicked on the link provided by the phisher, the phisher was immediately able to obtain the user's data and could also hack the original Universitas Bina Insan Digital Library website.

Impact of Phishing on the Universitas Bina Insan Lubuklinggau Website

The SQL Injection attack on the Universitas Bina Insan Lubuklinggau Digital Library website resulted in a complete takeover by the phisher. The phisher gained unrestricted control, changing the front-page display and menus, and modifying the overall structure of the Digital Library website. Consequently, the website administrator could no longer log in to the admin account.

Resolution of the Phishing Impact on the Universitas Bina Insan Lubuklinggau Website

Following the successful takeover and alteration of the website's appearance and structure, the administrator of the Digital Library contacted the developer for repairs. The developer addressed the issue by closing the phisher's access to the website, preventing further control or modification. The developer subsequently repaired the website's appearance and installed a firewall to ensure it would not be easily hacked or phished again.

Conclusion and Recommendations

The analysis concludes that phishers execute cyber-attacks by creating a duplicate website and distributing its link to genuine website users. When the original website user clicks the link, the phisher can easily steal the user's data and potentially take control of the original website itself. Phishing is an activity of cybercrime that utilizes social engineering and technical deception to steal identity data and financial account credentials. As a highly detrimental cybercrime, phishing allows the phisher to steal all of the victim's data.

Disclosure Statement

No potential conflict of interest was reported by the authors.

Acknowledgments

This research was part of the Teachers' Training for Teaching Democracy program administered by the Paramadina Institute for Education Reform (PIER), funded by Konrad Adenauer Stiftung (KAS) Indonesia. We, therefore, gratefully acknowledge KAS Indonesia for providing funds for this research project.

References

N. Widya Ramailis, "Cyber Crime Dan Potensi Munculnya Viktimisasi Perempuan Di Era Teknologi Industri 4.0," Sisi Lain Realita, vol. 5, no. 01, pp. 1–20, 2020, doi: 10.25299/sisilainrealita.2020.vol5(01).6381.

A. R. Kelrey and A. Muzaki, "Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan," Cyber Secur. dan Forensik Digit., vol. 2, no. 2, pp. 77–81, 2019, doi: 10.14421/csecurity.2019.2.2.1625.

B. Suharto and A. B. Kurniawan, "Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (SQL Injection)," JHP 17 (Jurnal Has. Penelitian), vol. 5, no. 2, pp. 57–61, 2020, [Online]. Available: http://jurnal.untag-sby.ac.id/index.php/jhp17

Muftiadi A, Putri Mulyani Agustina T, and Evi M, "Studi kasus keamanan jaringan komputer: analisis ancaman SQL Injectionterhadap layanan online banking," J. Ilm. Tek., vol. 1, no. No. 2, Agustus 2022, pp. 60–65, 2022.

Z. Efendy, I. E. Putra, and R. Saputra, "Analisis Serangan Web Phishing pada Layanan E-commerce dengan Metode Network Forensic Process," J. Terap. Teknol. Inf., vol. 2, no. 2, pp. 135–146, 2019, doi: 10.21460/jutei.2018.22.103.

W. Candraditya Pamungkas and F. Trimuti Saputra, "Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling," J. Ris. Komputer), vol. 7, no. 4, pp. 2407–389, 2020, doi: 10.30865/jurikom.v7i4.2304.

T. Rompi and H. S. Muaja, "Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan," Lex Priv., vol. IX, no. 4, pp. 183–192, 2021, [Online]. Available: https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33358

D. Irawan, "Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook Dengan Metode SQL Injection," JIKI (Jurnal llmu Komput. lnformatika), vol. 1, no. 1, pp. 43–46, 2020, doi: 10.24127/jiki.v1i1.671.

D. N. Hidayat, "Metodologi Penelitian dalam Sebuah Multi-Paradigm Science," Mediat. J. Komun., vol. 3, no. 2, pp. 197–220, 2002.

M. R. Fadli, "Memahami desain metode penelitian kualitatif," Humanika, vol. 21, no. 1, pp. 33–54, 2021, doi: 10.21831/hum.v21i1.38075.

R. S. P. Selfi Fitria Sari, "Literature Review Sistem Pengelolaan Arsip Di Kantor Kelurahan Keboledan Kecamatan Wanasari Kabupaten Brebes," J. Ekon. dan Akunt., vol. 2, no. 1, pp. 116–126, 2022.