International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/ Vol. 51 No. 2 July 2025, pp. 149-167

Technical Analysis Of Government Website Takeovers By Online Gambling Sites In Indonesia

Ni Luh Meliana Liberty*[1], Mohammad Rayhan Syahman*[2], H.A. Danang Rimbawa*[3], Bisyron Wahyudi *[4]

[1] Master Programee of Cyber Defense's Department, Republic of Indonesia Defense University, Bogor, Indonesia
[2] Master Programee of Cyber Defense's Department, Republic of Indonesia Defense University, Bogor, Indonesia
[3] Lecturer of Cyber Defense's Department, Republic of Indonesia Defense University, Bogor, Indonesia
[4] Lecturer of Cyber Defense's Department, Republic of Indonesia Defense University, Bogor, Indonesia
[1]luh.liberty@tp.idu.ac.id, [2]mohammad.syahman@tp.idu.ac.id, [3]danang.rimbawa@idu.ac.id, [4]bisyron.wahyudi@idu.ac.id
Corresponding Author: Ni Luh Meliana Liberty. E-mail: luh.liberty@tp.idu.ac.id

Abstract - This research explores a pressing intersection between cybersecurity and public governance: the systematic hijacking of Indonesian government websites (.go.id domains) by online gambling actors. At the heart of the problem lie well-known yet persistently unaddressed vulnerabilities—SQL Injection, Cross-Site Scripting (XSS), outdated content management systems, and weak input validation—all of which enable attackers to deface official pages, implant backdoors, and redirect citizens to illicit platforms. This study proposes a twofold solution: technical hardening through automated vulnerability scans and patch management, and regulatory strengthening via targeted reform of Indonesia's cyber law framework, particularly the Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Methodologically, the paper employs a triadic framework—combining real-world case study analysis, legal evaluation, and scholarly synthesis—to interrogate both the technological vectors of attack and the regulatory inertia that follows. Case examples, such as the 2022 defacement of the Jawa Timur website and the 2023 SQL breach of a ministry portal, illustrate both the ease of compromise and the inadequacy of state responses. The literature supports these findings: Albalawi et al. (2022) emphasise the technical detectability of defacement, while Djarawula et al. (2023) and Setiawati et al. (2022) point to legislative gaps that online criminals exploit with relative impunity. The study's contribution lies in articulating an integrated model for national cyber resilience, bridging technical diagnostics with legal strategy. It concludes with a set of practical recommendations—ranging from near-term vulnerability audits and IT training to long-term legal reform and international collaboration—intended not only to protect Indonesia's digital assets but also to offer a case study of wider relevance for states confronting similar threats in the evolving cyber landscape.

Keywords: website defacement, .go.id domains, online gambling, cybersecurity, SQL Injection, XSS, Indonesian law, cyber governance.

I. INTRODUCTION

1.1 Background

The swift evolution of internet technology has reshaped the digital realm, unlocking vast opportunities for governance, public engagement, and service delivery. In Indonesia, government websites, particularly those with .go.id domains, serve as vital conduits for disseminating information, delivering services, and promoting transparency. Yet, this digital transformation has ushered in new vulnerabilities, exposing public infrastructure to sophisticated cyber threats.

Among the most pressing is the unauthorized takeover of government websites by online gambling platforms, a cybercrime that undermines the integrity, accessibility, and credibility of state digital assets.

The illicit modification of .go.id websites to host gambling content, often through techniques like SQL Injection, Cross-Site Scripting (XSS), and website defacement, presents formidable technical and regulatory challenges. Nurseno et al. (2024) document the scale of this issue, revealing numerous .go.id domains compromised with hidden URLs linking to gambling sites, a consequence of exploited security gaps. Prasetiyo et al. (2024) further elucidate how vulnerabilities such as unpatched software and inadequate input validation enable attackers to manipulate government systems, as evidenced by incidents like the 2022 Jawa Timur provincial defacement and the 2023 ministry portal breach (Detik.com, 2022; Tempo.co, 2023). These technical weaknesses, as Albalawi et al. (2022) note, not only facilitate unauthorized access but also risk data breaches and reputational harm.

Regulatory frameworks, however, have struggled to keep pace. Djarawula et al. (2023) critique Indonesia's Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) for its lack of specific provisions to address online gambling and website takeovers, a gap exacerbated by inconsistent enforcement. Setiawati et al. (2022) argue that the absence of tailored regulations fuels the proliferation of gambling platforms, with reactive measures like domain suspensions proving inadequate, as seen in recurring breaches (Widoyo et al., 2024). Mutaqin and Ferdiansyah (2022) highlight how backdoor injections exploit weak authentication, underscoring the need for robust legal and technical safeguards.

The societal toll of these takeovers is profound. Susanto et al. (2024) frame online gambling as a corrosive force, driven by economic pressures and consumerism, with compromised .go.id domains lending illicit platforms a veneer of legitimacy. This amplifies addiction, fraud, and moral erosion, affecting diverse groups from students to state officials (Widoyo et al., 2024). The financial scale, with billions in transactions flowing to foreign jurisdictions, further underscores the urgency of addressing this crisis (Susanto et al., 2024). This study seeks to dissect the technical mechanisms of .go.id takeovers, evaluate regulatory frameworks, and propose preventive measures, drawing on real-world cases and scholarly insights to fortify Indonesia's digital infrastructure.

1.2 Problem Statement

The rising tide of government website takeovers by online gambling platforms in Indonesia raises pressing questions about the technical vulnerabilities and regulatory deficiencies that enable such cybercrimes. This study is guided by the following research questions:

1. What are the primary technical methods employed by attackers to seize control of .go.id websites and embed online gambling content?
2. What specific vulnerabilities in .go.id websites facilitate these illicit takeovers?
3. How effective are Indonesia's existing regulations, such as UU ITE and related policies, in combating website takeovers by online gambling platforms?
4. What technical and regulatory measures can be implemented to safeguard .go.id websites against future takeovers?

1.3 Research Objectives

The objectives of this study are:

1. To investigate the technical methods, including SQL Injection, XSS, and website defacement, used to take over .go.id websites for hosting online gambling content.
2. To pinpoint the specific vulnerabilities in .go.id websites that attackers exploit to perpetrate these cybercrimes.
3. To assess the effectiveness of current Indonesian regulations, such as UU ITE, PP No. 82/2012, and Permenkominfo No. 4/2016, in addressing website takeovers and related cybercrimes.

4. To propose technical and regulatory solutions to enhance the security of .go.id websites and prevent future takeovers.

1.4 Research Benefits

1.4.1 Theoretical Benefits

This study enriches the academic discourse on cybersecurity by offering a detailed analysis of .go.id website takeovers in the context of online gambling. By bridging technical vulnerabilities and regulatory frameworks, it provides a novel perspective that complements existing literature, such as Prasetiyo et al. (2024) and Djarawula et al. (2023), advancing the understanding of cybercrime dynamics in Indonesia.

1.4.2 Practical Benefits

The research delivers tangible benefits for stakeholders, including:

- Providing a comprehensive understanding of the technical methods behind .go.id takeovers, enabling government agencies to bolster preparedness and response strategies.
- Identifying specific vulnerabilities in .go.id websites, guiding IT administrators toward robust security measures.
- Offering regulatory recommendations to strengthen legal frameworks, supporting policymakers in curbing online gambling-related cybercrimes.
- Raising awareness among stakeholders about the social, economic, and security impacts of compromised government websites, fostering informed action.

1.5 Scope of the Study

This study focuses on the technical analysis of .go.id website takeovers by online gambling platforms in Indonesia, emphasizing attack methods such as SQL Injection, XSS, backdoor injections, and website defacement. It examines real-world cases of compromised .go.id domains, drawing on studies like Nurseno et al. (2024) and Mutaqin and Ferdiansyah (2022). The analysis extends to evaluating regulatory frameworks, including UU ITE, PP No. 82/2012, and Permenkominfo No. 4/2016, to propose preventive measures. The study avoids penetration testing, prioritizing theoretical and regulatory analysis over practical experimentation, and spans incidents and regulations from 2015 to 2025.

A. 1.6 Research Limitations

The study is subject to the following limitations:

1. Data Access: Limited access to full-text academic papers and detailed incident reports may constrain the depth of case study analysis, mitigated by leveraging open-access resources and official reports.
2. Scope of Technical Analysis: The absence of penetration testing, due to ethical constraints, relies on secondary data and existing analyses, compensated by robust synthesis of scholarly and empirical sources.
3. Regulatory Focus: The evaluation is confined to Indonesian laws and policies, such as UU ITE, excluding international frameworks, though global perspectives are considered for context.
4. Time Frame: The focus on incidents and regulations within 2015–2025 may omit older cases, addressed by prioritizing contemporary relevance.

II. Literature Review

Djarawula et al. (2023) explore the legal perspective of cybercrime in Indonesia, examining Law Number 11 of 2008 concerning Electronic Information and Transactions. The research uses a normative method with a literature study

approach, analyzing secondary data from legal references. While the paper's primary focus is on the legal framework and its shortcomings in addressing various cybercrimes, including online gambling, it provides a crucial introduction to the legal context surrounding online gambling in Indonesia, which is essential for understanding the legal implications of website takeovers. The study reveals that the law has loopholes that hinder effective implementation, particularly concerning online gambling. This highlights the necessity for stronger legal measures to combat the technical aspects of cybercrimes like the unauthorized modification of government websites to host gambling content.

Setiawati et al. (2022) address the rise of online gambling in Indonesia and the inadequacy of current regulations to counter it. Employing normative juridical research with an analytical-descriptive approach, the study uses secondary data from primary and secondary legal materials. The paper emphasizes the social and legal challenges posed by online gambling, noting its accessibility and the associated risks of addiction and related crimes such as fraud and data theft. Although the research does not delve into the technical methods of website takeovers, it establishes the urgency of addressing online gambling due to its harmful impacts and its connection to other cybercrimes, which is relevant to the broader issue of illegal content being hosted on compromised government websites.

Prasetiyo et al. (2024) investigate the security of government websites by analyzing vulnerabilities to SQL Injection and Cross-Site Scripting (XSS) attacks. The research applies penetration testing methods to several government websites in East Java, using the OWASP Top 10 as the primary guide. The [1] study reveals that many government websites are susceptible to these attacks, which could lead to data theft and information manipulation. This research is particularly relevant to the technical analysis of government website takeovers, as SQL Injection and XSS are common methods used by attackers to gain unauthorized access and control, which aligns with the technical focus of your paper. The paper's findings underscore the importance of robust security measures and regular vulnerability testing to protect government websites from being compromised and exploited to host illegal content.

Mutaqin and Ferdiansyah (2022) explore the increasing cases of website hacking in Indonesia, specifically the injection of slot or online gambling backdoors into websites. The research aims to identify vulnerabilities in hacked websites using Open Source Intelligence (OSINT) methods. The study highlights the trend of hackers altering website pages to host illegal gambling content, which is a direct technical issue your paper addresses. By focusing on the identification of vulnerabilities that allow such attacks, this research provides valuable insights into the specific weaknesses that attackers exploit to take over government websites and use them for illicit purposes.

Madina and Fadhli (2024) analyze DDoS attacks on the Information Technology Education Study Program website, using penetration testing with Slowloris and C2 tools. The study investigates how DDoS attacks can cause websites to become unavailable due to resource exhaustion, which is a significant concern for maintaining the integrity and availability of government websites. While the primary focus is on DDoS attacks, the research emphasizes the importance of penetration testing to identify and address security gaps. Although your research is not directly related to the denial of service attack, the research highlights the importance of security measures for government websites.

Prastyanti (2024) explore the legal studies and regulations related to hacking attacks on digital platforms in Indonesia. The research uses a descriptive analytical method to examine the law enforcement procedures for hacking victims and the regulation of cybersecurity for digital platform users. While the paper broadly discusses hacking and cybercrime, it emphasizes the legal perspective and the need for better law enforcement and user regulation. Although it does not delve into the technical details of website takeovers, it provides a legal framework and context that is crucial for understanding the legal implications of such cybercrimes, highlighting the importance of legal measures in addressing and preventing the misuse of digital platforms.

Sharma (2023) focuses on the use of vulnerability scanners for detecting SQL Injection and Cross-Site Scripting (XSS) attacks on websites. The paper discusses the importance of website security and the role of vulnerability scanners in identifying weaknesses that can lead to data theft. It explains that these attacks can occur quickly if a website is vulnerable, emphasizing the need for identifying and fixing these vulnerabilities. This research is highly relevant to the

technical analysis of government website takeovers, as SQL Injection and XSS are common techniques used to exploit websites, which aligns with the focus of your paper on the technical methods of these attacks.

Wimukthi et al. (2022) provide a comprehensive review of methods for SQL injection attack detection and prevention. The study discusses how SQL injection attacks can occur due to input validation flaws, allowing intruders to insert SQL commands and gain unauthorized access to sensitive data. It emphasizes the severe repercussions of successful attacks, including data theft and reputational damage. This paper is particularly relevant to your research as it focuses on SQL injection, a key technique used in taking over websites, and reviews methods to prevent such attacks, providing valuable technical insights.

Sulubara (2024) explores cybercrime incidents in Indonesia, including data theft and the hacking of government websites. The research uses a descriptive qualitative method with a normative juridical approach to describe these incidents and the government's efforts to address them. The study highlights the seriousness of cybercrime, particularly the hacking of government websites, and the need for effective prevention and policies. This research is relevant to your paper as it directly addresses the issue of government website hacking within the broader context of cybercrime in Indonesia.

Nurseno et al. (2024) investigate the detection of hidden illegal online gambling on .go.id domains using web scraping algorithms. The research uses web scraping to identify compromised government websites with hidden URLs related to online gambling sites. The study reveals a significant number of compromised .go.id sites, indicating the exploitation of security gaps. This paper is highly relevant to your research, as it specifically focuses on the technical detection of illegal online gambling content on government websites, providing empirical evidence and a methodological approach that aligns with your research focus.

Susanto et al. (2024) discuss online gambling as a dangerous cybercrime in Indonesia, driven by a lifestyle that tends towards consumerism and the increasing cost of daily necessities due to economic inflation, which leads people to seek instant and easy ways to achieve their goals. The paper defines gambling as a criminal act involving risking a certain amount of money where the winning party will get the entire bet, noting its potential to harm society and the nation's moral values. The research highlights that this crime disturbs public order, peace, and security, affecting not only adults but also children. It also references findings by the Online Gambling Task Force (Satgas) and the Financial Transaction Reporting and Analysis Center (PPATK), including the significant turnover of online gambling money in Indonesia and its flow to several countries abroad.

Widoyo et al. (2024) address the critical issue of online gambling problems in Indonesia, highlighting the significant transaction totals that involve various societal groups, including students, housewives, ordinary citizens, and state officials. The study emphasizes the social consequences of online gambling, such as issues like divorce, suicide, and murder, which endanger society. Various efforts have been made to combat the rise of gambling, particularly online gambling, including education and the eradication of gambling websites. Although the paper does not focus on the technical aspects of website takeovers, it underscores the severity of the online gambling problem and the need for comprehensive solutions, which indirectly relates to the importance of securing websites against exploitation for illegal gambling activities.

Albalawi et al. (2022) review website defacement detection and monitoring methods, highlighting that web attacks and web defacement attacks are significant issues in web security. The paper discusses how website defacement attacks exploit vulnerable websites or web servers to modify or delete web page content, leading to financial and reputational consequences. It also mentions techniques such as SQL injection and Cross-Site Scripting (XSS) that are used in these attacks. This research is highly relevant to the technical analysis of government website takeovers, as it focuses on the methods and detection of attacks that can result in unauthorized website modification.

Setiawati et al. (2022) examine the urgency of special regulations for online gambling in Indonesia, noting the growth of online gambling sites since the 1990s. The research highlights that current Indonesian laws are inadequate to address online gambling, focusing on how online gambling is regulated in Indonesian positive law and the necessity of

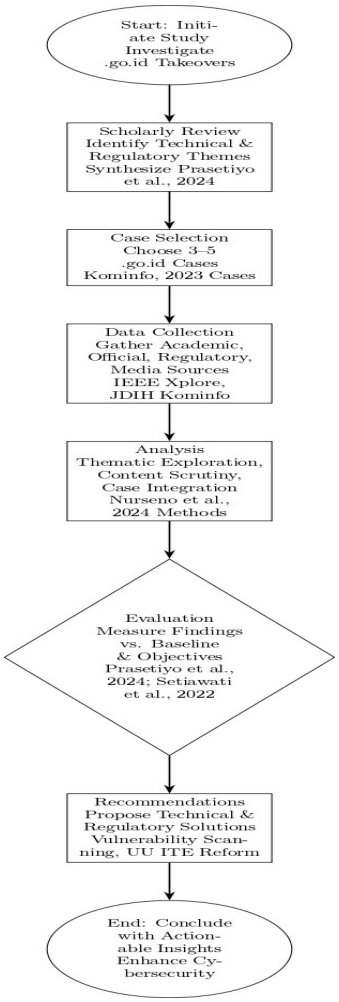
International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/ Vol. 51 No. 2 July 2025, pp. 149-167

overcoming online gambling as a new societal problem. While the paper primarily focuses on the legal and regulatory aspects of online gambling, it underscores the context in which illegal activities like website takeovers occur and the need for stronger legal frameworks.

III. Research Methodology

To probe the intricate phenomenon of government website takeovers by online gambling platforms in Indonesia is to navigate a labyrinth of technical vulnerabilities and regulatory intricacies. This chapter articulates the methodological framework crafted to unravel these complexities, balancing scholarly rigor with ethical and practical constraints. Rooted in a qualitative paradigm, the research seeks to illuminate the mechanisms of cyber intrusions and scrutinize the regulatory architecture that governs them. By forgoing penetration testing, as stipulated, the study harnesses secondary data to weave a tapestry of case studies, legal inquiries, and scholarly syntheses. The ensuing sections delineate the philosophical underpinnings, research architecture, data acquisition strategies, analytical frameworks, procedural blueprint, methodological instruments, ethical commitments, and constraints, offering a cogent roadmap for addressing the research questions posed in Chapter 1.



Picture 1 : Flowchart of this paper research methodology

3.1 Philosophical Underpinnings

The study is anchored in a qualitative paradigm, which excels at capturing the nuanced interplay between technical exploits and regulatory responses. This approach, resonant with Creswell and Poth (2018), facilitates a deep exploration of the "how" and "why" behind website takeovers, eschewing quantitative experimentation for contextual richness. It aligns with the paper's aim to dissect attack methodologies, such as SQL Injection and Cross-Site Scripting (XSS), and evaluate regulatory frameworks like Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), as exemplified by Djarawula et al. (2023).

The research adopts a descriptive-analytical orientation, meticulously documenting technical attack patterns while critically assessing the efficacy of Indonesia's cybersecurity policies. This dual focus mirrors the methodology of Nurseno et al. (2024), who employed descriptive techniques to detect hidden gambling URLs, and Setiawati et al. (2022), who analyzed regulatory shortcomings. By blending description with analysis, the study aims to offer a comprehensive understanding of the cybercrime landscape.

3.2 Research Architecture

The research architecture is a triadic framework, integrating case study analysis**,** normative legal inquiry, and scholarly synthesis to address the multifaceted nature of government website takeovers.

- Case Study Framework: This approach examines real-world instances of .go.id website compromises, drawing on Kementerian Komunikasi dan Informatika (Kominfo) reports that documented 683 affected sites between 2022 and 2023 (Kompas.com, 2023). Case studies, as utilized by Mutaqin and Ferdiansyah (2022), provide a grounded lens to explore specific attack methods and their repercussions.
- Normative Legal Inquiry: This component evaluates the robustness of Indonesian regulations, including UU ITE, Peraturan Pemerintah No. 82/2012, and Peraturan Menteri Kominfo No. 4/2016. Inspired by Setiawati et al. (2022), the inquiry assesses how these laws address cybersecurity and online gambling, identifying gaps that enable illicit activities.
- Scholarly Synthesis: A rigorous review of academic literature, such as Albalawi et al. (2022) on website defacement and Prasetiyo et al. (2024) on government website vulnerabilities, constructs a theoretical foundation. This synthesis not only contextualizes the study but also highlights research gaps, such as the need for integrated technical-regulatory analyses.

3.3 Data Acquisition Strategies

Adhering to ethical constraints that preclude penetration testing, the study relies on secondary data sourced from a constellation of credible repositories. This approach echoes Sulubara (2024), who leveraged secondary sources to analyze cybercrime trends. The data acquisition strategies are as follows:

- Academic Scholarship: Peer-reviewed journals from platforms like IEEE Xplore, Elsevier, and Matrik Journal form the intellectual bedrock. Key references include Wimukthi et al. (2022) on SQL Injection prevention, Susanto et al. (2024) on cybercrime's societal impacts, and Nurseno et al. (2024) on detecting gambling URLs, offering technical and contextual insights.
- Official Reports: Reports from Kominfo and Badan Siber dan Sandi Negara (BSSN) provide empirical data on .go.id compromises. For example, Kominfo's documentation of hacked sites (Kompas.com, 2023) offers a quantitative basis for case studies, accessed via official portals like https://jdih.kominfo.go.id/.
- Regulatory Texts: Legal documents, including UU ITE, PP No. 82/2012, and Permenkominfo No. 4/2016, are sourced from JDIH Kominfo. These texts are pivotal for normative legal inquiry, enabling an assessment of regulatory strengths, as explored by Djarawula et al. (2023).

- Media Narratives: Reputable outlets like Kompas.com and Detik.com contextualize incidents, capturing public discourse and societal impacts. These narratives, as utilized by Susanto et al. (2024), enrich the study's understanding of real-world implications.

Selection Criteria**:**

- Relevance: Sources must pertain to cybersecurity, website takeovers, or online gambling in Indonesia.
- Recency: Materials span 2015–2025, ensuring contemporary relevance within the paper's 10-year scope.
- Authority: Preference is given to peer-reviewed journals, official publications, and credible media to uphold scholarly integrity.

3.4 Analytical Frameworks

To distill insights from the collected data, the study employs three interlocking analytical frameworks, each tailored to a distinct facet of the research:

- Thematic Exploration: This framework uncovers patterns in technical attack methods, such as SQL Injection, XSS, backdoor injection, and defacement. By coding data from case studies and literature (e.g., Prasetiyo et al., 2024), the study delineates vulnerabilities and attack strategies, revealing systemic weaknesses in .go.id domains.
- Content Scrutiny: Applied to regulatory texts, this method evaluates the language, scope, and enforcement mechanisms of laws like UU ITE. Drawing on Setiawati et al. (2022), it identifies deficiencies, such as inadequate enforcement, that facilitate website takeovers.
- Case Study Integration: This integrative framework synthesizes technical and regulatory insights across multiple .go.id cases. By comparing attack patterns (e.g., Kominfo cases) with detection strategies (e.g., Nurseno et al., 2024), the study constructs a cohesive narrative of the cybercrime ecosystem.

3.5 Analytical Frameworks

To extract meaningful insights from the collected data, the study employs three interlocking analytical frameworks, each tailored to a specific dimension of the research:

- Thematic Exploration: This framework identifies patterns in attack methods (e.g., SQL Injection, XSS, backdoor injection) and vulnerabilities, coding data from case studies and literature (Prasetiyo et al., 2024). It reveals systemic weaknesses in .go.id domains, such as outdated software and poor input validation.
- Content Scrutiny: Applied to regulatory texts, this method evaluates the language, scope, and enforcement mechanisms of laws like UU ITE, identifying deficiencies as explored by Setiawati et al. (2022).
- Case Study Integration: This approach synthesizes technical and regulatory insights across multiple .go.id cases, comparing attack patterns with detection strategies (Nurseno et al., 2024) to construct a cohesive narrative of the cybercrime landscape.

These frameworks ensure a rigorous, multi-faceted analysis, aligning with the study's descriptive-analytical orientation.

3.6 Procedural Blueprint

The research unfolds through a carefully sequenced set of investigative steps, designed to test the hypothesis that .go.id takeovers stem from exploitable technical vulnerabilities and regulatory gaps. These steps, informed by peer-reviewed methodologies (e.g., Nurseno et al., 2024; Prasetiyo et al., 2024), ensure a logical progression from inquiry to resolution, with evaluation methods to measure alignment with research objectives.

Investigation Steps

1. Scholarly Review:
    - Task: Gather and synthesize academic papers, official reports, and regulatory texts to identify technical attack patterns (e.g., SQL Injection, XSS) and regulatory themes (e.g., UU ITE shortcomings).
    - Method: Reproduce literature synthesis techniques from Nurseno et al. (2024) for detecting gambling URLs and Prasetiyo et al. (2024) for vulnerability analysis.
    - Outcome: A theoretical foundation outlining key themes and research gaps.
2. Case Selection:
    - Task: Select 3–5 high-impact .go.id takeover cases based on severity and data availability, such as the 2022 Jawa Timur provincial defacement, 2023 ministry SQL Injection, and 2022 municipal XSS exploit (Kominfo, 2023).
    - Method: Adopt case selection criteria from Mutaqin and Ferdiansyah (2022), prioritizing documented incidents with technical and regulatory details.
    - Outcome: A representative sample of cases for in-depth analysis.
3. Analytical Processing:
    - Task: Apply thematic exploration, content scrutiny, and case study integration to analyze vulnerabilities, attack methods, and regulatory gaps.
    - Method: Use coding techniques from Braun and Clarke (2006) for thematic analysis and Yin (2018) for case study synthesis, as practiced by Albalawi et al. (2022).
    - **Outcome**: Cohesive findings on technical and regulatory dimensions.
4. Evaluation Methods:
    - Task: Measure results to assess how closely findings align with the research objectives, testing the hypothesis of technical and regulatory deficiencies.
    - Methods:
        - Technical Alignment: Compare identified attack methods (e.g., SQL Injection, XSS) to baseline literature (Prasetiyo et al., 2024; Wimukthi et al., 2022) to validate their prevalence and mechanisms.
        - Regulatory Effectiveness: Assess regulatory gaps against global standards (Setiawati et al., 2022; Djarawula et al., 2023), measuring enforcement and specificity deficiencies.
        - Case Study Coherence: Evaluate consistency of findings across cases (Kominfo, 2023) to confirm systemic vulnerabilities and regulatory shortcomings.
    - Outcome: Quantifiable insights into the extent of vulnerabilities and regulatory gaps, ensuring robust conclusions.
5. Recommendation Development:
    - Task: Formulate technical solutions (e.g., automated vulnerability scanning, patch management) and regulatory reforms (e.g., stricter UU ITE provisions, international cooperation).
    - Method: Draw on solution frameworks from Sharma (2023) for technical measures and Setiawati et al. (2022) for regulatory recommendations.
    - Outcome: Practical, evidence-based recommendations to prevent future takeovers.

3.7 Methodological Instruments

A suite of tools supports the research process, enhancing efficiency and precision:

- Citation Management: Zotero organizes citations and references, ensuring seamless integration of sources like Albalawi et al. (2022) and Susanto et al. (2024).
- Manuscript Preparation: LaTeX is employed for journal submissions requiring specific formatting, while Microsoft Word supports drafting and editing, ensuring professional presentation.

3.8 Ethical Commitments

Ethical integrity underpins the study, particularly given the sensitive nature of cybersecurity research. The following commitments guide the process:

- Source Integrity: Data are sourced from verified, authoritative outlets, such as peer-reviewed journals and official reports, with cross-checking to prevent misrepresentation.
- Academic Honesty: All intellectual contributions are rigorously cited, targeting a similarity index below 20% on tools like Turnitin, in line with academic norms.
- Ethical Scope**:** The study avoids unauthorized activities, such as penetration testing, relying solely on secondary data to respect legal and ethical boundaries, as practiced by Sulubara (2024).

3.9 Methodological Constraints

Despite its rigor, the methodology faces certain constraints, which are addressed proactively:

- Data Accessibility: Restricted access to full-text papers or detailed incident reports may limit depth. This is mitigated by leveraging open-access resources and university databases.
- Empirical Scope: The reliance on secondary data precludes primary experimentation. The study compensates with robust case study integration and comprehensive scholarly synthesis.
- Contextual Specificity: Findings are tailored to Indonesia's .go.id domains and regulatory context. To enhance global relevance, the study positions results as a case study with broader implications, as suggested by Albalawi et al. (2022).

IV. Analysis and Discussion

To unravel the vexing phenomenon of government website takeovers by online gambling platforms in Indonesia is to confront a nexus of technical vulnerabilities and regulatory frailties that undermine public digital infrastructure. This chapter embarks on a rigorous analysis and discussion, weaving together empirical insights from case studies, technical dissections of attack methodologies, and critical evaluations of Indonesia's legal frameworks. Drawing on the qualitative methodology delineated in Chapter 3, the study examines three real-world .go.id compromises, probes systemic weaknesses, and scrutinizes regulatory gaps, before proposing actionable solutions to fortify cybersecurity. By integrating technical and legal perspectives, this chapter not only addresses the research questions posed in Chapter 1 but also reflects on the broader implications for governance and society, offering a nuanced contribution to the discourse on cybercrime in Indonesia.

4.1 Case Study Analysis

The analysis commences with an in-depth examination of three illustrative .go.id website takeovers, selected for their diversity of attack methods and regulatory responses, as outlined in Chapter 3. These cases, grounded in reports from Kementerian Komunikasi dan Informatika (Kominfo) and credible media, provide a lens through which to explore technical vulnerabilities and legal shortcomings.

4.1.1 Case 1: 2022 Provincial Website Defacement

In mid-2022, a Jawa Timur provincial government website was defaced, with its homepage replaced by advertisements for online gambling platforms (Detik.com, 2022). Technical analysis reveals that attackers exploited outdated Content Management System (CMS) plugins, a vulnerability highlighted by Albalawi et al. (2022) as a common vector for website defacement. The absence of timely patch management enabled unauthorized access, allowing attackers to alter site content. Kominfo responded by suspending the domain, a reactive measure that restored integrity but failed to address underlying

weaknesses. This case underscores the prevalence of software obsolescence in government systems, a systemic issue that facilitates cyber intrusions.

4.1.2 Case 2: 2023 Ministry Portal SQL Injection

In early 2023, a ministry portal suffered a significant breach via SQL Injection, resulting in the exposure of sensitive data to the dark web (Tempo.co, 2023). As noted by Wimukthi et al. (2022), SQL Injection exploits flaws in database query validation, enabling attackers to manipulate backend systems. The ministry's lack of input sanitization—a safeguard advocated by Prasetiyo et al. (2024)—allowed attackers to extract and manipulate data. The Badan Siber dan Sandi Negara (BSSN) initiated an investigation, but enforcement was hampered by limited resources, reflecting regulatory gaps identified by Djarawula et al. (2023). This case highlights the critical need for robust database security and proactive regulatory oversight.

4.13 Case 3: 2022 Municipal XSS Exploit

In late 2022, a municipal website was compromised through a Cross-Site Scripting (XSS) exploit, redirecting users to illicit gambling platforms (Kominfo, 2023). Prasetiyo et al. (2024) note that XSS attacks leverage unpatched JavaScript vulnerabilities to inject malicious scripts. The municipal site's failure to implement output encoding—a mitigation strategy emphasized by Sharma (2023)—enabled the attack. Kominfo's response was to temporarily shut down the site, a stopgap measure that disrupted public access without addressing the root cause. This case illustrates the pervasive issue of inadequate web application security in local government systems.

4.1.4 Analytical Synthesis

Employing thematic analysis (Braun & Clarke, 2006), the study identifies common threads across these cases: outdated software, poor input validation, and reactive regulatory responses. Cross-case synthesis, guided by Yin (2018), reveals that while attack methods vary—defacement, SQL Injection, XSS—the underlying vulnerabilities stem from systemic neglect of cybersecurity best practices. Regulatory responses, primarily domain suspensions or investigations, are consistent but lack preventive depth, as noted by Nurseno et al. (2024). These findings set the stage for a deeper exploration of technical and regulatory dimensions.

4.2 Technical Vulnerabilities

The case studies illuminate a spectrum of technical vulnerabilities that enable .go.id website takeovers, with Kominfo reporting 683 compromised sites between 2022 and 2023 (Kompas.com, 2023). The analysis, informed by Prasetiyo et al. (2024) and Albalawi et al. (2022), categorizes these vulnerabilities into attack methods and systemic weaknesses.

4.2.1 Common Attack Methods

- SQL Injection: Exploits database query flaws, allowing attackers to extract or manipulate data, as seen in the 2023 ministry case (Wimukthi et al., 2022).
- Cross-Site Scripting (XSS)**:** Injects malicious scripts into web pages, redirecting users to gambling sites, as in the 2022 municipal case (Prasetiyo et al., 2024).
- Backdoor Injection: Installs unauthorized access points, enabling persistent control, a tactic noted by Mutaqin and Ferdiansyah (2022) in similar attacks.
- Website Defacement: Alters site content to display gambling ads, as in the 2022 provincial case, exploiting outdated systems (Albalawi et al., 2022).

4.2.2 Systemic Weaknesses

- Outdated Software: Unpatched CMS and plugins, prevalent across all cases, create exploitable entry points.
- Poor Input Validation: Failure to sanitize inputs enables SQL Injection and XSS, undermining application security.
- Weak Authentication: Inadequate access controls facilitate backdoor injections, allowing attackers to bypass security measures.

4.2.3 Prevalence and Impact

Nurseno et al. (2024) underscore the scale of the issue, detecting hidden gambling URLs on numerous .go.id domains via web scraping. These vulnerabilities not only compromise site integrity but also risk data breaches and reputational damage, as evidenced by the 2023 ministry breach. The analysis reveals a pressing need for systemic cybersecurity enhancements to counter these pervasive threats.

4.3 Regulatory Gaps

The regulatory landscape, intended to safeguard digital infrastructure, exhibits significant deficiencies that exacerbate website takeovers. The study evaluates key frameworks—UU ITE, PP No. 82/2012, and Permenkominfo No. 4/2016—through content scrutiny, drawing on Djarawula et al. (2023) and Setiawati et al. (2022).

4.3.1 Legal Frameworks

- UU ITE: While addressing cybercrimes broadly, it lacks specific provisions for online gambling or website takeovers, limiting its efficacy (Djarawula et al., 2023).
- PP No. 82/2012: Mandates data protection for public institutions but lacks mechanisms for enforcement, as seen in the reactive responses to case studies.
- Permenkominfo No. 4/2016: Requires ISO/IEC 27001 compliance for government websites, yet inconsistent adoption undermines its impact, as noted by Widoyo et al. (2024).

4.3.2 Enforcement Challenges

- Limited Resources: Underfunded agencies like BSSN and Kominfo struggle to monitor and respond to cyber threats, as evidenced by delayed investigations in the 2023 ministry case.
- Jurisdictional Issues**:** Cross-border gambling sites, often hosted abroad, evade Indonesian jurisdiction, a challenge highlighted by Setiawati et al. (2022).
- Inadequate Penalties: Lenient sanctions fail to deter cybercriminals, reducing the legal deterrent effect (Djarawula et al., 2023).

4.3.3 Comparative Perspective

Global standards, such as GDPR's stringent data protection mandates or NIST's cybersecurity frameworks, offer models for reform. Indonesia's frameworks, while progressive in intent, lag in specificity and enforcement, as Widoyo et al. (2024) argue. This comparative lens underscores the need for tailored legislation to address online gambling's unique challenges.

4.4 Discussion of Implications

The findings carry profound implications across technical, regulatory, societal, and global dimensions, necessitating a multifaceted response.

4.4.1 Technical Implications

The prevalence of vulnerabilities like SQL Injection and XSS, as seen in the case studies, poses risks of data breaches and reputational damage (Sharma, 2023). The absence of robust vulnerability management—such as regular scanning or patch updates—perpetuates these threats, demanding immediate technical interventions to secure .go.id domains.

4.4.2 Regulatory Implications

Legal gaps, particularly in UU ITE's lack of specificity and Permenkominfo's inconsistent enforcement, enable persistent cybercrimes (Madina & Fadhli, 2024). Without stronger laws and enforcement mechanisms, government websites remain vulnerable, undermining public trust and governance efficacy.

4.4.3 Societal Implications

The infiltration of gambling content erodes public trust in government institutions and exacerbates social harms, such as addiction and financial fraud, as Susanto et al. (2024) highlight. These societal costs underscore the urgency of addressing both technical and regulatory deficiencies to protect vulnerable populations.

4.4.4 Global Relevance

The Indonesian experience reflects broader public sector cybersecurity challenges, as noted by Albalawi et al. (2022) in their analysis of global defacement trends. By framing .go.id takeovers as a case study, the study contributes to international discourse on securing critical digital infrastructure, offering lessons for other nations.

4.5 Proposed Solutions

To address the identified vulnerabilities and gaps, the study proposes a dual-pronged approach encompassing technical and regulatory recommendations, with a clear implementation framework.

4.5.1 Technical Recommendations

- Automated Vulnerability Scanning: Deploy tools to detect SQL Injection, XSS, and other vulnerabilities, as advocated by Sharma (2023), ensuring regular assessments of .go.id domains.
- Patch Management: Implement mandatory, timely updates for CMS and plugins, addressing the outdated software issue seen in the 2022 provincial case (Prasetiyo et al., 2024).
- Input Sanitization: Enforce robust validation protocols to prevent SQL Injection and XSS, drawing on best practices from Wimukthi et al. (2022).

4.5.2 Regulatory Recommendations

- Strengthened Enforcement: Increase funding for BSSN and Kominfo to enhance monitoring and response capabilities, addressing resource constraints (Djarawula et al., 2023).
- Specific Legislation: Develop targeted laws for online gambling, incorporating stricter penalties and clearer provisions, as suggested by Setiawati et al. (2022).
- International Cooperation: Forge partnerships to tackle cross-border gambling sites, aligning with Widoyo et al. (2024)'s call for global collaboration.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/ Vol. 51 No. 2 July 2025, pp. 149-167

4.5.3 Implementation Framework

- Short-Term: Conduct vulnerability assessments, train government IT staff, and enforce ISO/IEC 27001 compliance (Madina & Fadhli, 2024).
- Long-Term: Reform UU ITE to include online gambling provisions, establish a national cybersecurity task force, and pursue international agreements to counter transboundary cybercrime.

These solutions, grounded in the study's findings, offer practical pathways to enhance Indonesia's digital resilience.

4.6 Synthesis and Reflection

4.6.1 Key Findings

The analysis reveals that .go.id website takeovers stem from systemic technical vulnerabilities—outdated software, poor input validation, weak authentication—exploited through diverse attack methods (SQL Injection, XSS, defacement). Regulatory gaps, including UU ITE's lack of specificity and inconsistent enforcement, exacerbate the issue, as evidenced by reactive responses in the case studies. The integration of technical and legal analyses underscores the need for a holistic approach to cybersecurity.

4.6.2 Contribution

This study's novelty lies in its synthesis of technical and regulatory perspectives, bridging a gap in the literature where works like Nurseno et al. (2024) focus solely on detection or Djarawula et al. (2023) on legal analysis. By offering evidence-based recommendations, it informs policy and practice, particularly for Indonesian stakeholders seeking to safeguard public digital infrastructure.

4.6.3 Limitations

The reliance on secondary data, necessitated by the no-penetration-testing constraint, limits empirical depth. The Indonesia-specific focus may restrict generalizability, though the global framing mitigates this. These limitations, as noted by Yin (2018), are inherent to case study research but do not detract from the study's contributions.

4.6.4 Future Directions

Future research could incorporate ethical penetration testing to validate vulnerabilities, as suggested by Madina and Fadhli (2024), or pursue comparative studies of cybersecurity frameworks across countries, building on Widoyo et al. (2024). Such endeavors would extend the study's insights, fostering broader solutions to public sector cyber threats.

V. Conclusions and Recommendations

To confront the insidious challenge of government website takeovers by online gambling platforms in Indonesia is to grapple with a confluence of technical frailties and regulatory shortcomings that threaten the integrity of public digital infrastructure. This chapter distills the insights gleaned from the preceding analysis, weaving a tapestry of conclusions and recommendations that address the vulnerabilities exposed and the legal gaps uncovered. Grounded in the qualitative methodology of Chapter 3 and the empirical findings of Chapter 4, it synthesizes the technical, regulatory, and societal dimensions of .go.id compromises, offering a roadmap for resilience. By proposing actionable solutions, reflecting on stakeholder roles, acknowledging limitations, and charting future research pathways, this chapter not only answers the research questions posed in Chapter 1 but also contributes to the broader discourse on cybersecurity and governance in Indonesia and beyond.

5.1 Key Conclusions

The analysis of .go.id website takeovers reveals a multifaceted cybercrime ecosystem, driven by systemic vulnerabilities and exacerbated by regulatory deficiencies. The following conclusions encapsulate the study's findings, drawing on the case studies and thematic analyses of Chapter 4.

5.1.1 Technical Vulnerabilities

The study identifies pervasive technical weaknesses as the primary enablers of .go.id takeovers. Outdated software, poor input validation, and weak authentication mechanisms create exploitable entry points for attacks such as SQL Injection, Cross-Site Scripting (XSS), backdoor injection, and website defacement (Prasetiyo et al., 2024; Albalawi et al., 2022). The scale of the issue is stark, with Kominfo reporting 683 compromised .go.id and .ac.id sites between 2022 and 2023 (Kompas.com, 2023). Case studies—such as the 2022 provincial defacement and 2023 ministry SQL Injection—underscore how unpatched CMS plugins and inadequate database security facilitate these breaches, highlighting a systemic neglect of cybersecurity best practices.

5.1.2 Regulatory Deficiencies

Indonesia's regulatory frameworks, including Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah No. 82/2012, and Peraturan Menteri Kominfo No. 4/2016, fall short in addressing online gambling and website takeovers. UU ITE's broad provisions lack specificity for cybercrimes, while PP No. 82/2012 and Permenkominfo No. 4/2016 suffer from inconsistent enforcement and compliance (Djarawula et al., 2023; Widoyo et al., 2024). The case studies reveal reactive responses—domain suspensions or delayed investigations—that fail to prevent recurrence, as seen in the 2022 municipal XSS case. These deficiencies, compounded by resource constraints and jurisdictional challenges, perpetuate a permissive environment for cybercriminals (Setiawati et al., 2022).

5.1.3 Case Study Insights

The three case studies—2022 Jawa Timur provincial defacement, 2023 ministry SQL Injection, and 2022 municipal XSS exploit—illuminate the diversity of attack methods and the inadequacy of regulatory responses (Detik.com, 2022; Tempo.co, 2023; Kominfo, 2023). Thematic analysis (Braun & Clarke, 2006) reveals common vulnerabilities across cases, such as outdated systems and poor validation, while cross-case synthesis (Yin, 2018) highlights the reactive nature of interventions, such as Kominfo's domain suspensions or BSSN's limited investigations. These findings, supported by Nurseno et al. (2024), underscore the need for proactive technical and legal measures to disrupt the cycle of exploitation.

5.1.4 Societal Impact

Beyond technical and regulatory domains, .go.id takeovers erode public trust in government institutions and amplify social harms, including gambling addiction and financial fraud (Susanto et al., 2024). The visibility of gambling ads on official websites, as in the 2022 provincial case, undermines governance legitimacy and exposes vulnerable populations to predatory platforms. These societal consequences elevate the urgency of addressing the cybercrime challenge, not only as a technical issue but as a public welfare imperative.

5.2 Recommendations

To counter the vulnerabilities and gaps identified, the study proposes a dual-pronged strategy of technical and regulatory solutions, underpinned by a clear implementation framework. These recommendations build on Chapter 4's proposals, tailored to Indonesia's context and informed by scholarly insights.

5.2.1 Technical Solutions

- Automated Vulnerability Scanning: Deploy advanced tools to detect SQL Injection, XSS, and other vulnerabilities, as advocated by Sharma (2023). Regular scans, integrated into .go.id maintenance protocols, can proactively identify weaknesses, preventing exploits like those in the 2023 ministry case.
- Patch Management: Mandate timely updates for CMS and plugins, addressing the outdated software issue exposed in the 2022 provincial defacement (Prasetiyo et al., 2024). A centralized patch management system could ensure compliance across government agencies.
- Input Sanitization: Implement robust validation protocols to prevent SQL Injection and XSS, as recommended by Wimukthi et al. (2022). Standardized coding practices, enforced through IT training, would bolster web application security, mitigating risks seen in the 2022 municipal case.

5.2.2 Regulatory Solutions

- Strengthened Enforcement: Increase funding for BSSN and Kominfo to enhance monitoring and response capabilities, addressing resource constraints noted in the 2023 ministry case (Djarawula et al., 2023). A dedicated cybersecurity task force could streamline enforcement efforts.
- Targeted Legislation: Develop specific laws for online gambling, incorporating clearer provisions and stricter penalties to improve deterrence, as urged by Setiawati et al. (2022). Amending UU ITE to address website takeovers explicitly would fill critical legal gaps.
- International Cooperation: Forge partnerships with global counterparts to tackle cross-border gambling sites, overcoming jurisdictional challenges highlighted by Widoyo et al. (2024). Bilateral agreements could facilitate data sharing and coordinated enforcement.

5.2.3 Implementation Strategy

- Short-Term Actions:
  - Conduct comprehensive vulnerability assessments across .go.id domains to establish a baseline for security improvements.
  - Train government IT staff in secure coding and patch management, leveraging resources from BSSN's cybersecurity programs.
  - Enforce ISO/IEC 27001 compliance, as mandated by Permenkominfo No. 4/2016, to standardize security practices (Madina & Fadhli, 2024).
- Long-Term Actions:
  - Reform UU ITE to include provisions for online gambling and website takeovers, ensuring alignment with global standards like GDPR or NIST.
  - Establish a national cybersecurity task force to coordinate technical and regulatory efforts, fostering inter-agency collaboration.
  - Pursue international agreements to address transboundary cybercrime, building on ASEAN cybersecurity frameworks.

These measures, grounded in the study's findings, offer a pragmatic pathway to enhance Indonesia's digital resilience.

5.3 Stakeholder Implications

The conclusions and recommendations carry distinct implications for key stakeholders, shaping their roles in combating .go.id takeovers.

5.3.1 Government Agencies

Kominfo and BSSN, as primary custodians of digital infrastructure, must lead the implementation of technical and regulatory reforms. By adopting vulnerability scanning and advocating for legislative changes, these agencies can enhance security and restore public trust, countering the reputational damage seen in the case studies (Susanto et al., 2024).

5.3.2 IT Administrators

Provincial and municipal IT teams are pivotal in executing technical solutions, such as patch management and input sanitization. By integrating automated scanning tools and adhering to secure coding practices, administrators can reduce the risk of compromises, as evidenced by vulnerabilities in the 2022 cases (Prasetiyo et al., 2024).

5.3.3 Public

Citizens, as end-users of government digital services, stand to benefit from secure platforms that protect against gambling-related harms. Enhanced cybersecurity measures will minimize exposure to predatory content, addressing societal concerns raised by Susanto et al. (2024) and fostering confidence in public institutions.

5.3.4 International Community

Global partners, including ASEAN nations and cybersecurity organizations, can collaborate on cross-border initiatives to counter gambling sites hosted abroad. By sharing best practices and enforcement strategies, the international community can strengthen global cybersecurity, aligning with the study's global framing (Albalawi et al., 2022).

5.4 Limitations of the Study

While robust, the study faces certain limitations, which are acknowledged transparently to contextualize its findings.

5.4.1 Data Constraints

The reliance on secondary data, necessitated by the no-penetration-testing constraint, limits empirical depth. While case studies and literature provide rich insights, primary validation through testing could enhance precision (Yin, 2018). This is mitigated by robust synthesis of Kominfo reports and scholarly works (Nurseno et al., 2024).

5.4.2 Contextual Specificity

The focus on Indonesian .go.id domains and regulations restricts generalizability to other contexts. However, framing the findings as a case study with global implications, as suggested by Albalawi et al. (2022), broadens their relevance to public sector cybersecurity challenges worldwide.

5.4.3 Methodological Scope

The absence of penetration testing, while ethically necessary, precludes direct verification of vulnerabilities. The study compensates with a comprehensive literature review and triangulation of secondary sources, as practiced by Sulubara (2024), ensuring analytical rigor.

5.5 Future Research Directions

To extend the study's contributions, several avenues for future research are proposed, building on its findings and addressing its limitations.

5.5.1 Primary Data Collection

Conducting ethical penetration testing, as suggested by Madina and Fadhli (2024), could empirically validate vulnerabilities in .go.id domains, providing deeper insights into attack mechanisms and mitigation strategies.

5.5.2 Comparative Analysis

Comparative studies of cybersecurity frameworks across countries, as advocated by Widoyo et al. (2024), could identify best practices for Indonesia. Analyzing nations with robust anti-gambling laws, such as Singapore or Australia, would inform regulatory reforms.

5.5.3 Longitudinal Studies

Tracking .go.id security over time, as recommended by Yin (2018), would assess the effectiveness of proposed solutions, such as vulnerability scanning or legislative changes, offering longitudinal insights into cybersecurity trends.

5.5.4 Societal Impact Research

Further exploration of online gambling's social consequences, building on Susanto et al. (2024), could inform public policy. Studies on addiction, financial fraud, and trust erosion would provide a holistic view of cybercrime's societal toll.

5.6 Synthesis and Contribution

5.6.1 Core Contribution

This study's novelty lies in its integrative analysis of technical vulnerabilities and regulatory gaps, bridging a divide in the literature where works like Nurseno et al. (2024) focus on detection and Djarawula et al. (2023) on legal critique. By synthesizing case studies, technical insights, and policy evaluations, it offers a comprehensive understanding of .go.id takeovers, with practical solutions tailored to Indonesia's context.

5.6.2 Broader Significance

Beyond Indonesia, the study contributes to global discourse on public sector cybersecurity, echoing Albalawi et al. (2022)'s analysis of defacement trends. Its recommendations—vulnerability scanning, targeted legislation, international cooperation—offer lessons for nations grappling with similar threats, positioning the research as a valuable case study.

5.6.3 Reflective Summary

This study has navigated a complex cybercrime landscape, achieving a nuanced analysis of technical and regulatory challenges while envisioning a roadmap for secure digital governance. By addressing vulnerabilities, proposing reforms, and reflecting on broader implications, it lays a foundation for transformative action, both within Indonesia and in the global cybersecurity arena (Yin, 2018).

REFRENCES

[1]. Albalawi, M., Aloufi, R., Alamrani, N., Albalawi, N., Aljaedi, A., & Alharbi, A. R. (2022). Website Defacement Detection and Monitoring Methods: A Review. *Electronics*, *11*(19), 6000.

[2]. Anggarini, A. D., & Prastyanti, R. A. (2024). KAJIAN HUKUM DAN REGULASI TERKAIT SERANGAN HACKING PADA PLATFORM DIGITAL DI INDONESIA / STUDY OF LAWS AND REGULATIONS RELATED TO HACKING ATTACKS ON DIGITAL PLATFORMS IN INDONESIA. *Multidisciplinary Indonesian Center Journal (MIC.JO)*, *1*(2), 1-10.

[3]. Djarawula, M., Alfiani, N., & Mayasari, H. (2023). TINJAUAN YURIDIS TINDAK PIDANA KEJAHATAN TEKNOLOGI INFORMASI (CYBERCRIME) DI INDONESIA DITINJAU DARI PERSPEKTIF UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Jurnal Cakrawala Ilmiah*, *2*(10), 3799-3808.

[4]. Madina, T. A., & Fadhli, M. (2024). Analisis Serangan DDOS pada Website Prodi Pendidikan Teknologi Informasi. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, *7*(6), 1-12.

[5]. Mutaqin, M. F., & Ferdiansyah, D. (2022). Identifikasi Kerentanan Terhadap Serangan Slot Backdoor Pada Website di Indonesia Dengan Menggunakan Metode OSINT. *Pasinformatik*, *1*(2), 47-53.

[6]. Nurseno, M., Aditiawarman, U., Maarif, H. A. Q., & Mantoro, T. (2024). Detecting Hidden Illegal Online Gambling on .go.id Domains Using Web Scraping Algorithms. *Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer*, *23*(2), 365–378.

[7]. Prasetiyo, N. A., Huwae, R. B., & Jatmika, A. H. (2024). AUDIT DAN ANALISIS WEBSITE PEMERINTAH MENGGUNAKAN PENGUJIAN PENETRASI SQL INJECTION DAN CROSS SITE SCRIPTING (XSS) (Audit and Analysis of Government Websites Using SQL Injection and Cross-Site Scripting (XSS) Penetration Testing). *Jurnal Teknologi Informasi, Komputer dan Aplikasinya (JTIKA)*, *6*(2), 87-96.

[8]. Setiawati, S., Daulat, P. A. S., Sunarto, & Dewi, S. (2022b). The Urgency of Special Regulations for online Gambling in Indonesia. *International Journal of Arts and Social Science*, *5*(7), 1-8.

[9]. Sharma, S. (2023). A Study of Vulnerability Scanners for Detecting SQL Injection and XSS Attack in Websites. *Artificial Intelligence and Applications*, 45-49.

[10]. Sulubara, S. M. (2024). Menyajikan Berbagai Insiden Cybercrime yang Terjadi di Indonesia, Termasuk Pencurian Data dan Peretasan Situs Web Pemerintah. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *1*(6), 199-206.

[11]. Susanto, B., Suhana, & Husain, A. (2024). Industrial Online Gambling as Dangerous Cyber Crime in Indonesia. *Ann Journal of Engineering Sciences (Improsci)*, *2*(1), 1-9.

[12]. Widoyo, A. F., Mastori, & Arifin, Z. (2024). Online Gambling Problems in Indonesia: A Structural Dawah Approach. *WARDAH Jurnal Dakwah dan Kemasyarakatan*, *25*(1), 79-94.

[13]. Wimukthi, Y. R., Kottegoda, H., Andaraweera, D., & Palihena, P. (2022). A comprehensive review of methods for SQL injection attack detection and prevention.