ROUTERS: Jurnal Sistem dan Teknologi Informasi
Vol. 1, No. 1, Juli 2022, pp. xx-xx
ISSN: xxxx-xxxx, DOI: 10.xxxxx/routers.v0i0.xxxx

Exploring the Risk and Impact of Insufficiently Protected Credentials and Directory Listing Exposure on Web Application

Toni Montana [1], Festy Winda Sari [2]
[1] Informatic Engineering, Batam State Polytechnic

ARTICLE INFO

Received [DD/MM/YY]
Revised [DD/MM/YY]
Published [DD/MM/YY]

Keyword:

Web Security, Credential Protection, Directory Listing, Vulnerability Assessment, Cybersecurity Risks, Data Breach, Information Security, Quantitative Research

ABSTRACT

This study examines the risks and impacts of two fundamental web security vulnerabilities: insufficiently protected credentials and directory listing exposure. A Quantitative methods approach was employed, combining analysis of user behavior through questionnaires and technical demonstrations using Dirsearch on a designated target website. The results indicate that students majoring in Cyber Security Engineering at Batam State Polytechnic demonstrate a high level of awareness and understanding of credential protection practices, reflecting effective user education. However, significant risks remain due to vulnerabilities in server configurations that allow directory listing exposure, which could facilitate unauthorized data access. Collectively, these issues elevate the likelihood of data breaches and unauthorized access. The findings highlight the urgent need for proactive mitigation focusing on system hardening alongside continued user education.

Corresponding Author:

Toni Montana, Festy Winda Sari S.Tr. Kom., M.Sc.
Email: toni.montana3@students.polibatam.ac.id

1. INTRODUCTION

In the rapidly evolving digital landscape, web security remains a critical foundation underpinning the trust and continuous functionality of modern online systems. Web applications have become fundamental components of the digital ecosystem, managing diverse operational aspects ranging from financial transactions and business communications to sensitive data storage. However, the widespread adoption and dependency on web applications have brought serious consequences in the form of increasing cyber security threats that can exploit various weaknesses in system implementations.

Recent data reveals that cyber security incidents have experienced significant increases over the past several years. According to the IBM Cost of a Data Breach Report 2025, the global average cost of a data breach reached $4.44 million in 2025, with the United States recording the highest cost at $10.22 million per incident [1]. More concerning, data breaches involving stolen or compromised credentials require an average of 292 days to identify and contain [2], demonstrating the complexity and long-term impact of vulnerabilities related to credential management.

In the context of web application security, the Open Web Application Security Project has identified various categories of the most critical and commonly found vulnerabilities. The OWASP Top 10 2021 positions Identification and Authentication Failure as one of the most serious threats, encompassing various weaknesses in authentication mechanism implementation and credential management [3]. This category is directly related to the concept of Insufficiently Protected Credentials, defined by MITRE Corporation in the Common Weakness Enumeration as system weaknesses in protecting authentication credentials from unauthorized access or interception [4].

The magnitude of credential exposure in recent years has reached unprecedented levels, demonstrating the systemic failure of credential protection mechanisms across industries globally. In 2024 alone, the United States documented 3,158 data compromises including data breaches, exposures, and leaks affecting over 1.35 billion individuals [5]. This represents a staggering 312% increase in victim notifications compared to 2023, where 419 million individuals were impacted [6]. The dramatic escalation underscores not only the increasing frequency of security incidents but also the growing scale of individual breaches, with six data compromises in 2024 each exceeding 100 million exposed records [6].

The credential-specific dimension of these breaches reveals particularly concerning patterns. Analysis indicates that stolen or compromised credentials served as the initial access vector in 22% of all non-error, non-misuse data breaches in 2025 [7], making credential abuse the single most common attack methodology employed by threat actors. More alarmingly, research by Check Point Security identified a 160% surge in compromised credentials circulating in underground markets during 2025 compared to previous periods [8], with approximately 14,000 employee credential exposures documented in a single month alone [8]. These credentials, once exposed, become commodities traded on dark web marketplaces, enabling subsequent attacks across multiple organizations and platforms through credential stuffing and account takeover campaigns.

Beyond credential protection failures, directory listing exposure represents another frequently overlooked vulnerability with significant potential security implications. Directory listing exposure, classified as CWE-548 by MITRE Corporation, occurs when web servers are misconfigured to display directory contents in the absence of default index files [9]. While often categorized as an information disclosure vulnerability with lower immediate severity compared to authentication failures, directory listing can provide attackers with valuable reconnaissance data about system architecture, file structures, and potentially sensitive resources that should remain concealed from unauthorized access. Information disclosed through directory enumeration enables attackers to identify backup files, configuration files potentially containing hardcoded credentials, temporary development artifacts, and other resources that may facilitate subsequent exploitation attempts [10]

This study adopts a quantitative research methodology to systematically investigate the prevalence, characteristics, and technical impact of insufficiently protected credentials and directory listing exposure on web security. This methodological approach is essential for generating objective, measurable data that enables robust statistical analysis and comparative risk assessment. The research design is fundamentally descriptive

and analytical, aiming to characterize the extent of these vulnerabilities through precise technical measurement, assess knowledge levels among cybersecurity students, and correlate these findings with established global risk metrics and industry standards.

This research employs two complementary quantitative methods operating in parallel tracks. The first track utilizes structured questionnaires distributed to Cyber Security Engineering students at Batam State Polytechnic to capture authentic data regarding their knowledge levels, awareness, and understanding of insufficiently protected credentials and directory listing vulnerabilities. The questionnaire employs multiple-choice formats and Likert scales to generate quantifiable responses amenable to statistical analysis, enabling measurement of knowledge gaps and identification of specific areas requiring enhanced pedagogical attention.

The second track implements systematic technical assessment through controlled vulnerability scanning of sample web applications. This technical evaluation specifically targets directory listing exposure using specialized security assessment tools to identify, document, and quantify instances where web server misconfigurations enable unauthorized directory enumeration. Each identified vulnerability is catalogued according to standardized parameters including directory path, exposed file types, accessibility level, and potential sensitivity of disclosed information. Subsequently, severity assessment is conducted using the Common Vulnerability Scoring System version 4.0, providing standardized, reproducible risk ratings that facilitate comparison with broader vulnerability trends and enable evidence-based prioritization of remediation efforts.

The research phase was carefully orchestrated through parallel execution of these quantitative tracks. Following the initiation of the formal research agenda and precise definition of research questions and objectives, both tracks proceeded simultaneously to optimize data collection efficiency. The questionnaire track involved meticulous instrument design incorporating validated measurement scales, pilot testing with a subset of the target population to ensure clarity and reliability, formal distribution to the complete target demographic, systematic collection of responses, and rigorous statistical analysis combining descriptive statistics and inferential techniques to identify patterns and correlations.

Concurrently, the technical assessment track entailed identification and selection of appropriate sample web applications representing realistic deployment scenarios, establishment of controlled testing environments adhering to ethical penetration testing standards, systematic execution of directory listing scans using Dirsearch and complementary reconnaissance tools, comprehensive documentation of identified vulnerabilities including screenshots and technical details, and quantitative analysis of findings including prevalence rates, common misconfiguration patterns, and severity distributions.

Both tracks converged in an integrated results and discussion phase where findings from knowledge assessment and technical vulnerability analysis were synthesized. This convergence enabled derivation of holistic insights regarding the current state of understanding among emerging cybersecurity professionals relative to the actual prevalence and characteristics of these vulnerabilities in real-world contexts. The synthesis ultimately guided the formulation of comprehensive conclusions and actionable recommendations addressing both educational enhancement opportunities and technical mitigation strategies, thereby contributing to improved cybersecurity education outcomes and more secure web application deployments.

Through this comprehensive quantitative investigation combining knowledge assessment and technical vulnerability analysis, this research aims to contribute meaningfully to both cybersecurity education improvement and practical enhancement of web application security postures.

2. THEORETICAL FRAMEWORK

This research, focused on the risks and impacts of insufficiently protected credentials and directory listing exposure on web security, is grounded in several established theories and concepts within cybersecurity. These theoretical foundations provide a conceptual lens through which the study systematically analyzes observed phenomena, facilitating valid interpretation and practical implications for both educational and practical cybersecurity contexts.

2.1. Literature Review

The security vulnerabilities examined in this research represent fundamental weaknesses in web application security that have been extensively documented in academic literature and industry practice. Understanding the theoretical underpinnings and empirical evidence surrounding these vulnerabilities is essential for contextualizing this study's contributions and establishing its relevance within the broader cybersecurity research landscape.

The systematic risks associated with weak authentication mechanisms have been increasingly recognized as critical attack vectors in contemporary cyber threat environments. Kim et al. developed PassREfinder, a novel framework employing graph neural networks to predict credential stuffing risks by modeling password reuse relationships between websites [11]. Their research, conducted on a large-scale dataset comprising credential breaches affecting 360 million accounts across 22,378 websites, demonstrated that users exhibit predictable patterns in password reuse behavior, creating exploitable vulnerabilities across interconnected web platforms. The study achieved an F1-score of 0.9153 in predicting password reuse relations, providing empirical validation that password reuse constitutes a systemic rather than isolated security concern [11]. This work substantiates the theoretical premise that credential protection failures extend beyond individual authentication events to create network effects wherein a breach at one service amplifies risk across the entire ecosystem of accounts maintained by affected users.

Further empirical evidence supporting the severity of credential-based attacks emerges from research by Pal et al. who developed neural network-based password similarity models to analyze attack strategies beyond simple credential stuffing [12]. Their work at the 2019 IEEE Symposium on Security and Privacy demonstrated that attackers employ sophisticated techniques to generate password variations based on leaked credentials, exploiting users' tendencies to create predictable modifications of existing passwords across different services. The research revealed that similarity-based password guessing attacks achieve success rates significantly higher than traditional brute-force approaches, particularly when leveraging machine learning models trained on large-scale breach datasets [12]. These findings underscore that insufficiently protected credentials create vulnerabilities not only through exact password reuse but also through predictable password derivation patterns, expanding the threat landscape beyond what traditional password policy enforcement mechanisms can effectively address.

The authentication security challenge is further compounded by findings from Rees-Pullman, whose analysis in Computer Fraud & Security examined whether credential stuffing represents the contemporary equivalent of phishing as a primary attack vector [13]. The research documented that credential stuffing attacks have become increasingly automated and scalable, with attackers deploying sophisticated botnet infrastructure capable of testing millions of stolen credential pairs across numerous target services within hours. This industrialization of credential-based attacks transforms what might appear as isolated account compromises into systematic campaigns threatening organizational security at scale [13]. The study emphasizes that credential protection represents not merely a technical implementation challenge but a fundamental security posture issue requiring comprehensive approaches encompassing user education, technical controls, and continuous monitoring.

Server Misconfigurations and Information Disclosure

Complementing the credential security research, literature examining web server misconfigurations provides critical context for understanding directory listing exposure as a persistent vulnerability category. Acunetix's technical analysis comprehensively documented directory listing as a prevalent misconfiguration resulting from inadequate server hardening practices [14]. The research identified that directory listing vulnerabilities commonly expose backup files with extensions such as .bak, .old, or

.backup, configuration files including environment variables and database connection strings, FTP logs containing usernames and IP addresses, and complete directory structure information revealing the organization of web hosting systems [14]. This systematic cataloging of exposed information types demonstrates that directory listing represents not a singular disclosure but rather a gateway through which multiple categories of sensitive data become accessible to unauthorized parties.

The security implications of directory listing extend beyond mere information disclosure to encompass its role as a reconnaissance enabler in multi-stage attack chains. Invicti Security's comprehensive research on information disclosure vulnerabilities positioned directory listing within the broader context of attack surface expansion [15]. Their analysis revealed that even when individual exposed files do not contain immediately exploitable content, the aggregate intelligence gained through directory enumeration significantly reduces attacker effort in subsequent exploitation phases. The research documented cases where exposed directory structures revealed administrative panel locations, backup file naming conventions, technology stack versions, and application architecture patterns. All information assets that informed more targeted and effective secondary attacks [15]. This contextual framing supports the research premise that directory listing exposure warrant systematic investigation not as an isolated low severity finding but as a critical component in understanding comprehensive web application security postures.

2.2. Quantitative Method

This study adopts a Quantitative Method to systematically investigate the prevalence and technical impact of insufficiently protected credentials and directory listing exposure on web security. This methodology is essential for generating objective, measurable data that allows for robust statistical analysis and comparative risk assessment. The research design is fundamentally descriptive and comparative, aiming to characterize the extent of these vulnerabilities through precise technical measurement and link these findings to established global risk metrics.

The first quantitative method utilizes structured questionnaires as the primary instrument for data collection, specifically designed to assess the knowledge levels, awareness, and understanding of Cyber Security Engineering students at Batam State Polytechnic regarding insufficiently protected credentials. The questionnaire employs standardized measurement scales primarily Likert scales and multiple-choice formats to quantify respondents' comprehension of authentication security principles, credential protection mechanisms, attack vectors including credential stuffing, password spraying, and brute force attacks.

The second quantitative method implements systematic technical assessment through controlled vulnerability scanning to empirically measure the prevalence, characteristics, and severity of directory listing exposure vulnerabilities in sample web applications. This method employs Dirsearch a specialized command line tool designed for directory and file enumeration to systematically probe web servers for accessible directories lacking proper index files or exhibiting enabled directory listing functionality. The tool automates the process of sending HTTP requests to potential directory paths, analyzing server responses, and identifying instances where directory contents are disclosed to unauthorized requesters.

The technical assessment generates quantifiable data including the number of exposed directories identified, types of sensitive files or resources disclosed through directory listing, accessibility levels of exposed resources, and technical characteristics of identified vulnerabilities. Each discovered vulnerability is systematically documented and subjected to severity assessment using the Common Vulnerability Scoring System, which provides standardized numerical scores ranging from 0.0 to 10.0 reflecting vulnerability exploitability and potential impact across confidentiality, integrity, and availability dimensions. This scoring methodology enables objective comparison of vulnerability severity, risk-based prioritization of remediation efforts, and benchmarking against industry vulnerability data.
The framework employed herein aligns with modern methodologies for technical security analysis by focusing on data quantization and validation.

2.3. Confidentiality, Integrity, and Availability

The Confidentiality, Integrity, and Availability (CIA) Triad represents the foundational model in information security, serving as the cornerstone for understanding and implementing security measures across diverse technological environments [11]. This model consists of three fundamental principles that collectively define the objectives of information security practice.

1. **Confidentiality** addresses protection of information against unauthorized access and disclosure. Within this research context, insufficiently protected credentials directly compromise confidentiality by facilitating illicit access to sensitive systems and data [11]. When authentication mechanisms fail to adequately safeguard user credentials through proper encryption, robust hashing, or effective access controls, confidential information becomes vulnerable to unauthorized viewing, copying, or exfiltration by malicious actors.

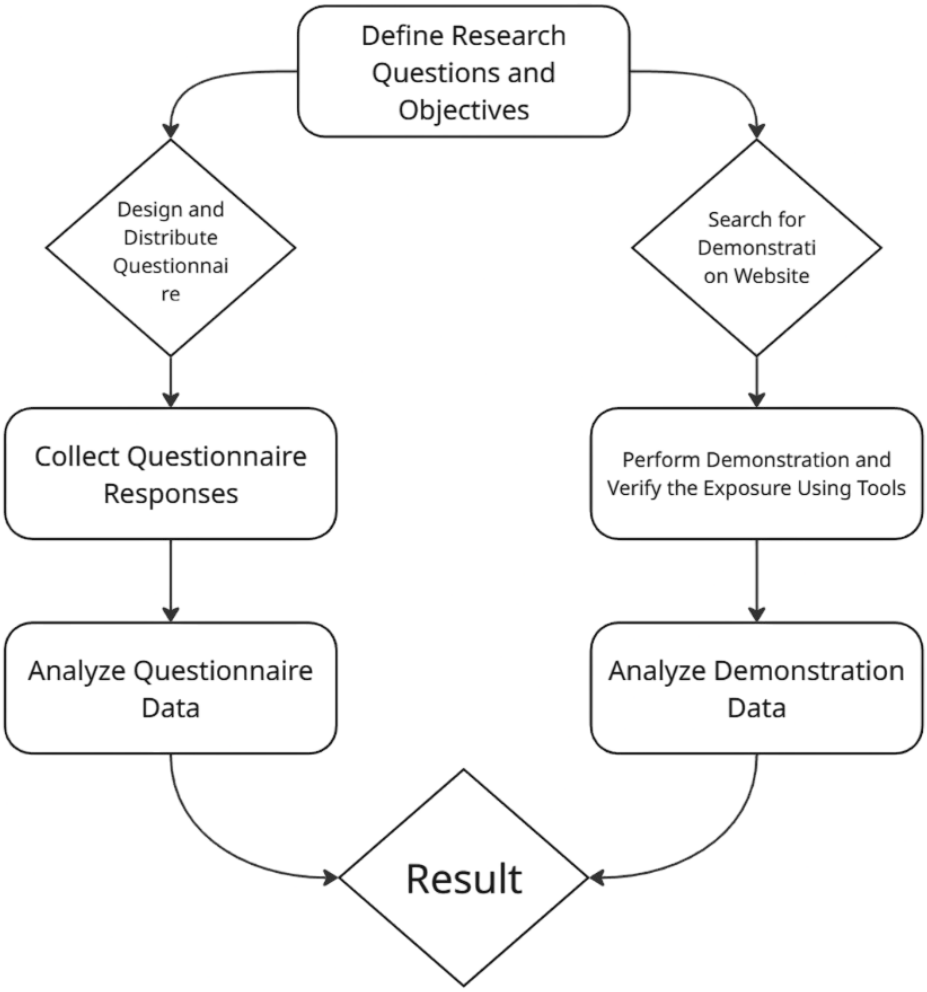
2. **Integrity** ensures the accuracy, completeness, and trustworthiness of data and processing methods throughout information lifecycles [11]. Vulnerabilities such as exposed directory listings can undermine integrity by revealing system architecture and file structures, potentially enabling unauthorized file modification, corruption, or deletion. When attackers gain insight into application internal structures through directory listing exposure, they can identify specific files to target for tampering, thereby compromising the reliability and authenticity of information assets.

3. **Availability** guarantees that authorized users maintain timely and uninterrupted access to information and systems when needed [11]. While connections may appear less direct than confidentiality or integrity breaches, successful exploitation stemming from credential compromise or information disclosure can result in system downtime, resource exhaustion, or denial-of-service conditions. For instance, repeated brute-force attempts against inadequately protected authentication systems can consume substantial computational resources, while attackers gaining unauthorized access through compromised credentials might deliberately disrupt services as part of extortion or sabotage campaigns.

This study directly examines how failures in credential protection and directory management systematically undermine the confidentiality and integrity aspects of the CIA Triad. The cumulative impact of these failures ultimately degrades and affects the overall security posture of web applications.

3. RESEARCH METHODOLOGY

This research adopts a quantitative approach focused on the systematic measurement and statistical analysis of web security vulnerabilities, specifically insufficiently protected credentials and directory listing exposures in web applications. The quantitative method was chosen due to its strength in providing objective, reproducible, and generalizable results through the use of numeric data and standardized instruments. The detailed breakdown of tools and techniques employed at each phase is presented in Picture 1 below.



Picture 1 Research Phase

3.1. Research Phase

The research phase in this study was carefully orchestrated as visualized in the accompanying flowchart, depicting the parallel execution of quantitative tracks under a quantitative design. The process commenced with the initiation of the formal research agenda, followed by the precise definition of research questions and objectives to provide clear direction for all subsequent activities.

On the left side, a questionnaire was meticulously designed and directly distributed to the target demographic of informatics students, capturing authentic responses regarding user behavior, password practices, and perceptions of credential security. The collected questionnaire responses then became the primary material for a thorough analysis, combining thematic exploration of narrative answers and descriptive statistical scrutiny of behavioral patterns. The online questionnaire was administered over a ten-day period, spanning from September 23, 2025 to October 2, 2025. A total of 52 respondents participated in the survey during this timeframe. Following a rigorous data validation process to ensure response quality and completeness, 50 respondents were determined to have provided valid responses with complete and accurate personal information.

On the right side, the methodology entailed careful search for, and construction of a demonstration website purposely configured for security assessment. Upon establishing this controlled environment, a demonstration was performed and exposure to directory listing was systematically verified using specialized penetration testing tools. The resulting dataset, consisting of raw findings on the number, type, and severity of directory exposures, was then subjected to quantitative analysis. Target xyz.com was chosen because the website is still active and well-maintained, and also because it has a login page, which means that the website has a database.

Both tracks converged in the result and discussion phase, this synthesis enabled the derivation of holistic explanations for the prevalence and risks of insufficiently protected credentials and directory listing exposures within the context of web security, ultimately guiding the discussion to comprehensive conclusions and actionable recommendations that address both human and technical aspects of vulnerability. The entire methodological cycle was thus implemented as a coherent, stepwise process, faithfully reflecting the phases delineated in the research flowchart and ensuring the integrity of the mixed methods paradigm.

4. RESULT AND DISCUSSION

This section presents the key findings derived from the quantitative analysis of website scans and discusses their implications in the context of web security. The results shed light on the prevalence of insufficiently protected credentials and directory listing exposure, along with their observed correlations with security incidents.

4.1 Vulnerabilities Findings

Data collection was executed by distributing a questionnaire to 50 respondents drawn from the Cybersecurity Engineering program. The selection of the Cybersecurity Engineering program was specifically informed by the need to ensure that each respondent possessed a foundational understanding of the insufficiently Protected Credentials vulnerability from the user behavior, authentication and application flaws, credential storage and protection, and attack types and mechanism.

1. **Insufficiently Protected Credentials**

   From User Awareness and Behavior, out of 50 respondents, 41 reported using a random combination of uppercase and lowercase letters, numbers, and symbols when creating passwords for their important accounts. Among these 41 respondents, 15 indicated that they use a unique password for each of their accounts and out of the 41 respondents, 37 reported being aware of and actively using multi-factor authentication (MFA) or two-step verification across many of their accounts, while 13 indicated its use only on select critical accounts. Additionally, all 37 of these respondents identified the primary benefits of MFA as providing an additional security layer in the event of password compromise and protecting accounts from unauthorized login attempts.

   In the context of Authentication and Application Flaws

   Out of 50 respondents, 24 expressed hesitation and were likely to avoid registering or using websites requiring passwords consisting solely of 6 lowercase characters. These respondents also recognized default passwords on new devices or applications as a security weakness, given attackers can easily discover them online. Furthermore, 22 of these 24 respondents were aware that specific error messages, such as "Username not found or incorrect password for this username," assist attackers in confirming valid usernames and facilitating subsequent attack escalation.

   In the context of Credential Storage and Protection

   Out of 50 respondents, 41 identified the use of strong one-way hash functions as the most effective practice for protecting credentials during storage. Among these 41 respondents, 38 further emphasized that hashing functions incorporating salt and high iteration counts are essential for secure credential storage. Additionally, 29 of the 41 respondents demonstrated understanding of salt in the context of credential protection, while 19 recognized that fast hashing algorithms like MD5 and SHA-1 are unsuitable due to their vulnerability to brute-force and rainbow table attacks. Finally, 40 of the 41 respondents acknowledged that the greatest risk of using weak encryption for password storage is that attackers can readily decrypt credentials if the encryption key is compromised.

   In the context of Attack Types and Mechanism

   Among 50 respondents, 49 were aware of what Credential Stuffing is, and 46 of them indicated that implementing multi-factor authentication (MFA) is the most critical measure to prevent such attacks. Furthermore, 32 of those 46 respondents recognized that password spraying is an effective attack on authentication systems because it targets multiple accounts using the most common passwords. Additionally, 43 out of these 46 respondents understood that protecting against brute force attacks is crucial in the context of insufficiently protected credentials, as these attacks systematically and automatically try all possible passwords.

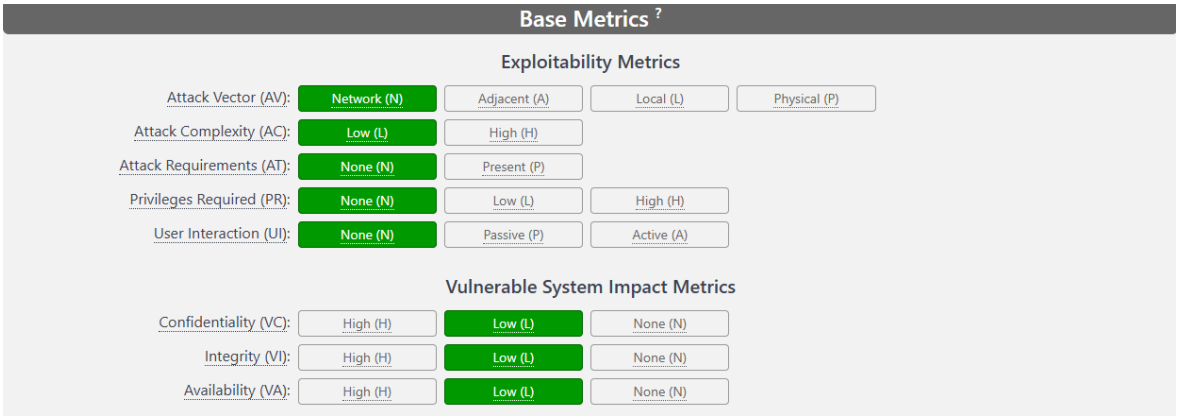
2. Directory Listing Exposure

The demonstration website scan discovered 3 directories with exposed listings, verified through Dirsearch. The Common Vulnerability Scoring System (CVSS) is used to measure the severity of these directories are presented in Table below.

Table 1. Directory Listing Exposure

Directory	Severity	Score
/assets	High	8.7
/controlpanel	Medium	6.9
/webmail	Medium	6.9

CVSS v4.0 Base Score calculation incorporates eleven distinct metrics organized into two primary categories: Exploitability Metrics and Impact Metrics [17]. The Exploitability Metrics assess the characteristics of the vulnerability itself and the conditions required for successful exploitation, including Attack Vector (AV) which specifies the context from which exploitation is possible (Network, Adjacent, Local, or Physical), Attack Complexity (AC) describing the difficulty of exploitation beyond normal user actions (Low or High), Attack Requirements (AT) identifying prerequisites such as deployment or execution conditions (None or Present), Privileges Required (PR) quantifying the authentication level necessary to exploit the vulnerability (None, Low, or High), and User Interaction (UI) indicating whether exploitation requires action from a user other than the attacker (None, Passive, or Active) [17]. The Impact Metrics evaluate the consequences of successful exploitation across the fundamental security objectives embodied in the CIA Triad, The architectural composition and hierarchical relationships of these eleven metrics within the CVSS v4.0 scoring framework are graphically represented in Picture 2 below.



Picture 2 Common Vulnerability Scoring System

4.2 Discussion of Implications

The questionnaire results revealing that Cyber Security Engineering students at Batam State Polytechnic demonstrate substantial understanding of Insufficiently Protected Credentials (IPC) concepts present an encouraging finding regarding the effectiveness of current cybersecurity curriculum implementation. This positive outcome suggests that theoretical instruction in authentication security, credential management, and password protection has successfully translated into comprehensible knowledge frameworks among students. The students' ability to recognize IPC-related risks, identify vulnerable authentication mechanisms, and articulate appropriate countermeasures indicates that foundational cybersecurity education objectives are being met with respect to credential security awareness.

4.3 Conclusions

This research investigated the risks and impacts of insufficiently protected credentials and directory listing exposure within web security contexts, employing a quantitative methodology combining knowledge assessment and technical vulnerability evaluation. The study addressed two primary research objectives: first,

assessing the knowledge levels of Cyber Security Engineering students at Batam State Polytechnic regarding these fundamental vulnerability categories; and second, conducting empirical technical assessment to identify and characterize actual directory listing exposures using standardized severity metrics.

Knowledge Assessment Results: The questionnaire-based evaluation revealed that students demonstrate substantial understanding of insufficiently protected credentials concepts, including recognition of credential-based attack vectors, awareness of secure credential storage mechanisms and comprehension of authentication security principles. This finding validates the effectiveness of current cybersecurity curriculum components addressing authentication security and suggests that theoretical instruction in credential protection has achieved meaningful knowledge transfer among students.

Technical Vulnerability Assessment: The systematic directory enumeration assessment using Dirsearch identified three significant exposures requiring remediation:

1. Administrative Control Panel Exposure (/control-panel/): Discovery of cPanel login interface through directory listing, assessed at CVSS v4.0 This finding represents the most severe identified vulnerability, as cPanel access provides comprehensive server administration capabilities including file system access, database management, email account control, and service configuration. The high subsequent system impact ratings reflect that successful compromise following administrative panel discovery could result in complete system control, enabling data exfiltration, system modification, and service disruption.

2. Webmail Interface Exposure (/webmail/): Identification of webmail login page accessibility through directory enumeration, assessed at CVSS v4.0 This exposure creates targeted attack opportunities against email accounts, potentially compromising sensitive communications, enabling phishing campaigns from legitimate organizational addresses, and facilitating password reset attacks against other services. The high confidentiality impact rating reflects the sensitivity of email content and authentication credentials.

3. Digital Signature File Exposure (/assets/): Discovery of principal's digital signature file in accessible assets directory, assessed at CVSS v4.0 This exposure enables potential document forgery, impersonation, and unauthorized use of administrative authority. While the vulnerable system impact is limited to confidentiality, subsequent system impacts on other organizational processes reflect the potential for misuse in creating fraudulent official documents.

4.4 Recommendations

Based on the research findings, analysis, and identified implications, this study proposes recommendations organized across three primary stakeholder categories: educational institutions and cybersecurity programs, organizational security practitioners, and future research directions.

1. Recommendations for Educational Institutions and Cybersecurity Programs
   Cybersecurity curricula should incorporate structured laboratory exercises requiring students to conduct actual vulnerability assessments using industry-standard tools such as Dirsearch, Nikto, Burp Suite, NMAP, and OWASP ZAP against controlled test environments. Rather than analyzing pre-identified vulnerabilities in classroom scenarios, students should experience the complete assessment process including reconnaissance, enumeration, vulnerability identification, documentation, and severity assessment using frameworks such as OWASP TOP 10. This practical orientation complements theoretical vulnerability knowledge with operational competencies required in professional practice.

2. Recommendations for Organizational Security Practitioners
   The identification of critical-severity misconfigurations suggests that security awareness should extend beyond dedicated security teams to encompass all personnel involved in system development, configuration, and deployment. Regular security training, secure coding guidelines, and integration

of security considerations into performance evaluations can cultivate organizational cultures where security is a shared responsibility rather than solely a security team concern.

REFERENCES

[1] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2025," IBM Corporation, 2025.

[2] Varonis, "Data Breach Statistics & Trends 2025," Varonis Systems, 2025.

[3] OWASP Foundation, "A07:2021 – Identification and Authentication Failures," OWASP Top Ten 2021, 2021.

[4] MITRE Corporation, "CWE-522: Insufficiently Protected Credentials," Common Weakness Enumeration, 2024.

[5] Statista, "Annual number of data compromises and individuals impacted in the United States from 2005 to 2024," Identity Theft Resource Center, Feb. 2025.

[6] HIPAA Journal, "More Than 1.7 Billion Individuals Had Personal Data Compromised in 2024," Identity Theft Resource Center 2024 Annual Data Breach Report, Apr. 2025.

[7] Huntress, "90 Business-Critical Data Breach Statistics [2025]," Verizon Data Breach Investigations Report 2025, 2025.

[8] IT Pro, "Credential theft has surged 160% in 2025," Check Point Research, Aug. 2025.

[9] MITRE Corporation, "CWE-548: Exposure of Information Through Directory Listing," Common Weakness Enumeration, 2024.

[10] PortSwigger Ltd., "Directory Listing Vulnerability," PortSwigger Web Security Academy, 2024.

[11] J. Kim, D. Kim, S. Han, D. Yun, S. Shin, and S. Kang, "PassREfinder: Credential Stuffing Risk Prediction by Representing Password Reuse between Websites on a Graph," in Proc. 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2024, pp. 1-18. doi: 10.1109/SP54263.2024.00140

[12] B. Pal, T. Daniel, R. Chatterjee, and T. Ristenpart, "Beyond Credential Stuffing: Password Similarity Models Using Neural Networks," in Proc. 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2019, pp. 417-434. doi: 10.1109/SP.2019.00056

[13] S. Rees-Pullman, "Is credential stuffing the new phishing?" Computer Fraud & Security, vol. 2020, no. 7, pp. 16-19, Jul. 2020. doi: 10.1016/S1361-3723(20)30076-2

[14] Acunetix, "Why Is Directory Listing Dangerous?" Acunetix Security Blog, Jan. 2024.

[15] Invicti Security, "Information Disclosure Attacks in Web Applications," Invicti Security Blog, 2024.

[16] L. Samonas and D. Coss, "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security," Journal of Information System Security, vol. 10, no. 3, pp. 21-45, 2014

[17] FIRST.Org, Inc., "Common Vulnerability Scoring System version 4.0: User Guide," Forum of Incident Response and Security Teams (FIRST), Nov. 2023

APPENDIX

User Awareness & Behaviors

Bagaimana biasanya kamu membuat kata sandi untuk akun - akun penting kamu?			
Menggunakan kata kata umum atau frasa sederhana	Menggunakan informasi pribadi yang mudah diingat (tanggal lahir, tanggal nikah, nama hewan, dll)	Menggunakan kombinasi acak antara huruf besar dan kecil, angka, dan simbol	Menggunakan Password Manager atau Generator kata sandi
0	0	41	9

Apakah Anda menggunakan kata sandi yang sama atau sangat mirip untuk beberapa akun yang berbeda?			
Ya, untuk Sebagian besar akun	Ya, untuk beberapa akun penting	Terkadang, untuk akun tidak penting	Tidak, saya menggunakan kata sandi unik di setiap akun
8	8	10	15

Apakah Anda familiar dengan istilah "Otentikasi Multi - Faktor (MFA)" atau "Verifikasi Dua Langkah (2FA)"?			
Ya, saya tahu dan aktif menggunakannya di banyak akun	Ya, saya tahu tapi hanya menggunakannya di beberapa akun penting	Ya, saya tahu tapi tidak menggunakan nya sama sekali	Tidak, saya tidak tahu apa itu
37	13	0	0

Menurut anda apa manfaat utama dari otentikasi Multi-Faktor?			
Membuat kata sandi lebih mudah diingat	Memberikan lapisan keamanan tambahan jika kata sandi saya bocor	Melindungi akun saya dari Upaya login tidak sah	Tidak terlalu penting, hnaya menambah kerepotan
0	37	37	0

Authentication & Application Flaws

Apa yang akan Anda lakukan jika sebuah situs web meminta Anda untuk membuat kata sandi yang hanya terdiri dari 6 karakter huruf kecil?			
Saya akan tetap menggunakannya karena situs yang memintanya	Saya akan mencoba membuat yang sekompleks mungkin dalam batas itu	Saya akan ragu dan mungkin tidak jadi mendaftar/menggunakan situs tersebut	Saya tidak terlalu memikirkannya, yang penting bisa login
4	21	24	1

Mengapa penggunaan kata sandi default pada perangkat atau aplikasi baru dianggap sebagai kelemahan keamanan?			
Karena kata sandi default seringkali tidak dicatat	Karena tidak ada system yang menggunakan kata sandi default	Karena kata sandi default sangat Panjang dan sulit diingat	Karena penyerang dapat dengan mudah menemukannya secara online.
0	0	0	24

Bagaimana reaksi Anda jika sebuah situs web menampilkan pesan kesalahan login yang spesifik, seperti "Username tidak ditemukan atau password salah untuk username ini"?			
Itu membantu saya mengetahui apa yang salah	Saya tidak terlalu memikirkannya	Saya tahu itu bisa membantu penyerang mengidentifikasi Username valid	Saya merasa informasi itu tidak relevan
2	0	22	0

Apakah Anda menyadari risiko keamanan dari sistem yang tidak memiliki pembatasan percobaan login? (mencoba login dengan password yang salah berulang kali tanpa di blokir)			
Ya, saya tau itu rentan terhadap brute-force	Tidak terlalu, saya tidak memikirkannya	Tidak, saya bahkan tdak tahu itu adalah suatu masalah keamanan	Tidak, saya piker itu untuk memudahkan user yang lupa dengan akun nya
24	0	0	0

Credential Storage & Protection

Praktik apa yang paling efektif untuk melindungi kredensial saat disimpan?			
Menggunakan fungsi hash satu arah yang kuat	Menggunakan fungsi hash satu arah yang kuat, mengenkripsi dengan kunci statis	Mengenkripsi kredensial dengan kunci statis	Menggunakan fungsi hash lemah tanpa salt
41	1	7	1

Fungsi apa yang harus digunakan untuk menyimpan kredensial dengan aman?			
Fungsi hashing satu arah dengan salt dan jumlah iterasi yang tinggi	Fungsi hashing satu arah yang cepat dan tidak disarankan	Algoritma hashing yang lemah tanpa salt	Algoritma enkripsi dua arah dengan kunci statsi
38	0	0	3

Apa itu ‘salt’ dalam konteks perlindungan kredensial?			
Sebuah bahan kimia yang digunakan untuk membersihkan kredensial	Kunci enkripsi yang digunakan untuk mendekripsi kredensial	Sebuah nilai acak yang ditambahkan ke kata sandi sebelum di-hash	Sebuah hash yang kuat untuk melindungi kata sandi
0	10	29	2

Mengapa penggunaan fungsi hashing yang cepat seperti MD5 dan SHA-1 tidak disarankan untuk kredensial?			
Karena mereka mudah dikembalikan ke teks biasa	Karena kecepatan eksekusinya yang sangat lambat	Karena fungsi tersebut sudah usang dan tidak kompatibel dengan system modern	Karena mereka rentan terhadap serangan brute-force dan rainbow table yang efisien
9	2	11	19

Apa risiko terbesar dari penggunaan enkripsi yang tidak kuat (weak encryption) untuk menyimpan kata sandi?			
Sistem akan melambat secara signifikan	Penyerang dapat dengan mudah mendekripsi kredensial jika kunci enkripsi diketahui	Kredensial akan menjadi terlalu Panjang	Pengguna akan lupa kata sandi mereka
1	40	0	0

Attack Types & Mechanisms

Apa yang dimaksud dengan Credential Stuffing?			
Membuat banyak akun palsu secara otomatis	Menghapus kredensial pengguna secara massal	Menggunakan kembali kredensial yang dicuri dari satu layanan untuk mencoba login ke layanan lain.	Mengisi formulir login dengan data yang tidak relevan.
1	0	49	0

Tindakan apa yang paling penting untuk mencegah serangan Credential Stuffing?			
Menerapkan otentikasi Multi-Factor	Mewajibkan pengguna untuk menggunakan kata sandi yang sama di semua situs	Menyimpan kata sandi pengguna dalam teks biasa	Menggunakan fungsi hash MD5
46	3	0	0

Mengapa password spraying menjadi serangan yang efektif terhadap system otentikasi?			
Karena ini memanfaatkan kata sandi yang mudahh ditebak	Karena ini mencoba banyak kata sandi pada satu akun secara berurutan	Karena ini menyasar beberapa akun menggunakan kata sandi yang paling umum	Karena ini mengeksploitasi kelemahan dalam fungsi hash
5	8	32	1

Dalam konteks Insufficiently Protected Credentials, mengapa perlindungan terhadap serangan brute force penting?			
Karena brute-force tidak dapat dicegah	Karena ini hanya menyerang system yang tidak menggunakan enkripsi	Karena serangan brute-force adalah satu – satunya serangan yang memungkinkan	Karena serangan ini mencoba semua kemungkinan kata sandi secara sistematis.
0	0	3	43