International Journal of
Technology, Law, and Economic Management Systems
Vol. 1, No. 1, June 2025, pp. 01-14 DOI. 10.22437/ijstphas.vxix.xxx

Research Article

PTES-Based Security System for Personal Data Protection of Rural Area Websites

Muhammad Edwin Firjatulloh[1], Rahmalia Syahputri[2]
[1,2] Institut Informatika dan Bisnis Darmajaya, Bandar Lampung, Indonesia
ORCIDs:
Second AUTHOR: https://orcid.org/0000-0002-8509-5517
Corresponding author email: rahmalia@darmajaya.ac.id

Article Info
Recieved:
Revised:
Accepted:
OnlineVersion:

Abstract
The use of digital systems like XYZ for managing data in rural areas plays a critical role in improving the efficiency and effectiveness of development programs. This study investigates security weaknesses in the login system of the XYZ platform through a structured penetration testing approach, guided by the Penetration Testing Execution Standard (PTES). A mockup environment was developed using tools such as Visual Studio Code, XAMPP, MySQL, PHPMailer, Twilio, and Hydra to safely simulate attacks without affecting the live system. The assessment revealed that the platform relies solely on password-based authentication, making it highly vulnerable to brute-force and hybrid attacks, especially when users use weak or outdated passwords. These vulnerabilities pose serious risks to the confidentiality and availability of sensitive user data. To mitigate these threats, the study proposes implementing two-factor authentication (2FA), one-time passwords (OTP), account lockout mechanisms, and brief delay periods after failed login attempts. These measures were tested in the mockup environment, and the results showed a significant improvement in system security, with all attack simulations failing to gain access. This research contributes to the broader discourse on cybersecurity in rural informatics by offering practical recommendations for securing digital public service platforms. It emphasises the importance of layered authentication mechanisms and proactive testing to prevent unauthorised access and data misuse, ensuring that community information systems remain both resilient and trustworthy.

Keywords: Information System Security, Penetration Testing Execution Standard, Two-Factor Authentication, One-Time Password, Brute Force Prevention

Ethical Consideration

As this research involves the analysis of an active website, the name and address of the website are intentionally omitted to preserve confidentiality and prevent any potential security or reputational risks. To ensure ethical compliance and avoid disruption to real-world systems, all testing activities and data collection were conducted using a controlled mock-up environment that replicates the original website's structure and functionality. No actual user data or live system components were accessed or

altered during the course of this study. This approach ensures that the integrity, availability, and privacy of the real website and its users remain fully protected. The research strictly adheres to ethical guidelines for cybersecurity testing, prioritising non-invasiveness and the avoidance of any operational impact on production systems.

INTRODUCTION

Protecting the privacy, availability, and integrity of data has become more essential in today's digital landscape. When these principles are compromised, especially within government information systems, the impact can be serious, ranging from unauthorised access and data loss to the disruption of vital public services and a decline in public confidence (Raza, 2024). As governments increasingly rely on digital platforms to deliver services and manage information (Blue et al., 2018; Perwej et al., 2021) secure authentication processes have taken centre stage. These systems act as the first barrier against unauthorised users (Wang et al., 2021), and any weakness in them can open the door to impersonation (Tu et al., 2018) , privilege abuse, or broader system attacks. This is why authentication-focused penetration testing is essential. It allows organisations to safely explore potential vulnerabilities, better understand their risk exposure, and take informed steps to improve security before real threats emerge. For public institutions, this kind of proactive assessment is not just good practice, it is a key part of ensuring that critical systems remain trustworthy, resilient, and aligned with national cybersecurity expectations.

Authentication is one of the key roles that Website XYZ, a digital platform utilised by governments to manage resident data and increase public visibility, plays in the digitisation of public services in rural areas. However, based on the analysis, several vulnerabilities were identified in its authentication mechanism. The current login system on website XYZ only uses single-factor authentication through passwords, without any additional security features. Generally, it is prone to phishing (Alkhalil et al., 2021), dictionary attacks (Fürst & Aßmuth, 2025), hybrid attack (Fa'atulo Halawa et al., 2020), and shoulder surfing (Prabhu & Shah, 2015). Further, it lacks of login attempt limit or a delay mechanism after failed logins, making it vulnerable to brute-force attacks (Fürst & Aßmuth, 2025; Wang et al., 2021) . Furthermore, the presence of publicly visible usernames on the website increases the risk of account compromise (Fürst & Aßmuth, 2025), particularly when combined with weak or rarely updated passwords (Rodrigues et al., 2025). This situation poses a significant threat to the confidentiality of sensitive data. If left unaddressed, such vulnerabilities may also affect Integrity, as unauthorised users could manipulate stored data (Duggineni, 2023), installed ransomware that may against availability (Javaid et al., 2023; Perwej et al., 2021), due to the risk of service disruptions caused by attacks.

The urgency of strengthening system security is further supported by recent national cybersecurity incidents. For instance, the ransomware attack on the National Data Centre (PDN) in June 2024 resulted in encrypted data and financial losses estimated at 6.3 trillion rupiah (MetroTV, 2024; Simorangkir et al., 2024). The attack was attributed to poor password management and the absence of multi-layer authentication mechanisms (KumparanNews, 2024) . These incidents highlight the importance of implementing stricter security protocols, including better password handling and multi-factor authentication (MFA).

To address the weaknesses in single-factor authentication, this study proposes the implementation of Two-Factor Authentication (2FA). 2FA adds a security layer by requiring users to verify their identity through an additional step (Nur et al., 2024; Syahputri et al., 2024)such as an OTP (One-Time Password) (Alkhalil et al., 2021; Ritonga et al., 2025)sent via SMS or email. Although if a password is compromised, the additional verification step helps prevent unauthorised access. Furthermore, implementing login attempt restrictions and delay mechanisms can help mitigate brute-force attacks. These measures aim to protect the three pillars of cybersecurity: Confidentiality, Integrity, and Availability(Harahap et al., 2023).

This research adopts the Penetration Testing Execution Standard (PTES) as its methodological framework. PTES provides a comprehensive and structured approach to identifying and mitigating system vulnerabilities (Zhang, 2023) . The framework consists of seven stages: (1) Pre-Engagement Interactions, (2) Intelligence Gathering, (3) Threat Modelling, (4) Vulnerability Analysis, (5) Exploitation, (6) Post-Exploitation, and (7) Reporting (Abu-Dabaseh & Alshammari, 2018; Haubris & Pauli, 2013; Safitra et al., 2023). By applying this framework, this study aims to assess and improve the

security posture of website XYZ systematically and professionally. The research describes questions related to:

RQ1: How can security vulnerabilities be identified, tested, and addressed using the PTES methodology?

RQ2: What are the impacts of implementing Two-Factor Authentication on user data protection and system resilience?

RESEARCH METHOD

This research adopts the Penetration Testing Execution Standard (PTES) as the primary framework for conducting penetration testing on the authentication system of the website XYZ. PTES is a structured methodology developed to provide comprehensive guidance in identifying, evaluating, and mitigating security vulnerabilities within information systems (Abu-Dabaseh & Alshammari, 2018) . The primary goal of this framework is to ensure system protection against various cyber threats that may compromise the confidentiality, integrity, and availability of data and digital services. The flow of PTES phases is shown in Figure 1.

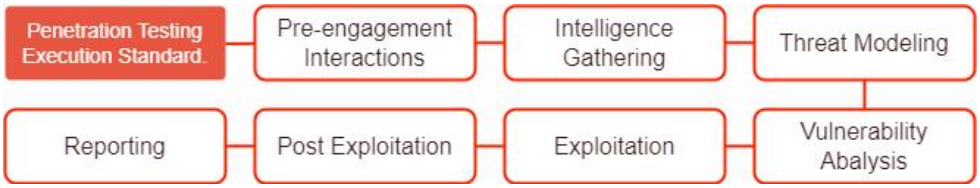

Figure 1. Penetration Testing Execution Standard

1. Pre-Engagement Interactions

The initial phase in this methodology is Pre-Engagement Interactions, which involves identifying the testing scope, defining objectives, and understanding the target system along with its existing security policies. In this study, this phase was carried out through structured interviews with the staff who handle the website.

Interviews revealed several weaknesses in the management of authentication and account security at the local administrative level. There are no specific policies regarding the use of the admin account, password change frequency, or limitations on failed login attempts. These shortcomings indicate insufficient access control, exposing the system to brute force and dictionary attacks. Moreover, the official email is not utilised for account verification processes, reducing the overall security of user authentication. A feature known as the Management Administration (MD) checklist was also found to have no real impact on system functionality or security.

2. Intelligence Gathering

2.1 Registration Page Observation and Password Pattern

Observation of the registration page at xxy.websiterural.com/register.xyz revealed consistent patterns in both usernames and default passwords. Usernames followed a predictable format (name<code>@mailxxxx.id), and default passwords used a similar pattern (administrator<name>@456). These uniform structures significantly increase vulnerability to dictionary and automated brute-force attacks, as they offer minimal variation and can be easily guessed using common wordlists. Table 1 presents sample combinations that illustrate these uniform patterns, further highlighting the system's vulnerability to automated attacks.

Table 1. Sample Observation of Username and Password Formats

No.	Username	Password
1.	name<code>@mailxxxx.id	administratorrural<name>@456
2.	name1234567891@mailxxxx.id	administratorruraljambu@456
3.	name1234567892@mailxxxx.id	administratorruralmangga@456
4.	name1234567893@mailxxxx.id	administratorruralkedondong@456

5.	name1234567894@mailxxxx.id	administratorruralapel@456
6.	name1234567895@mailxxxx.id	administratorruraljeruk@456

2.2 Absence of Multi-Factor Authentication

In Figure 2, the login page at https://xxy.websiterural.com/entry.xyz does not implement Multi-Factor Authentication (MFA). The lack of an additional verification layer significantly increases the risk of unauthorised access. Without MFA, attackers who obtain or guess login credentials can easily access admin accounts, potentially compromising the system. Implementing MFA would mitigate this risk by requiring an additional verification step, making unauthorised access more difficult.

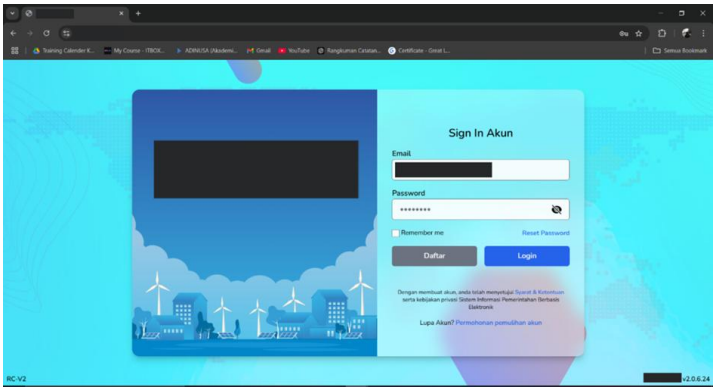

Figure 2. Admin Account Login Page for Rural Area Website

2.3 Absence of Reset Password Feature

The "Reset Password" feature on the login page (Figure 2) was found to be non-functional. As a result, users cannot reset their passwords if forgotten. According to findings from the Pre-Engagement Interaction phase, the rural area must contact the Website XYZ team for manual assistance, which often takes a long time. This lack of functionality not only hinders user access recovery but also poses a security risk; attackers could exploit it to lock users out or manipulate the system further. A reliable password reset feature is essential for secure and controlled account recovery.

3. Threat Modelling

Based on findings from the previous phases, a key threat identified is the risk of brute-force attacks due to the absence of login attempt throttling on the login page. A simulated attack was conducted on a mockup environment to evaluate its potential impact on data security. The results emphasise the system's vulnerability to unauthorised access through repeated login attempts. These threats are further detailed in Table 2, which presents the threat modelling of identified vulnerabilities.

Table 2. Threat Modeling

No.	Threat	Description	Affected CIA Aspect
1.	Insider Attack	Absence of account expiration increases the risk of unauthorised use	Confidentiality, Integrity
2.	Dictionary Attack	Use of weak, guessable passwords	Confidentiality, Integrity, Availability
3.	Brute Force	No login attempt throttling enables repeated automated login attempts	Availability, Confidentiality
4.	Hybrid Attack	Combination of multiple attacks (e.g., Insider + Dictionary)	Confidentiality, Integrity, Availability
5.	Account Lockout Risk	Non-functional "Reset Password" feature hinders	Availability, Confidentiality

		account recovery	

Table 2 illustrates the compromise of different aspects of the system's confidentiality, integrity, and availability. Notably, the table outlines insider attacks, which highlight the risks posed by inactive or unmonitored user accounts that may remain accessible beyond their intended use. It also includes dictionary attacks, which take advantage of weak, guessable passwords commonly observed in earlier assessments. Hybrid attacks are of particular concern, as they combine multiple vectors, such as insider knowledge with predictable credential patterns, to increase the sophistication and impact of intrusions. Additionally, the table draws attention to account lockout risks caused by the absence of functional recovery mechanisms, which can inadvertently affect legitimate users while leaving systems open to denial-of-service scenarios. Together, these identified threats underscore the multifaceted nature of the system's vulnerabilities and the need for comprehensive, layered security controls.

4. Vulnerability Analysis

Building on the threats identified in the previous section (Threat Modelling), this stage focuses on evaluating specific weaknesses in the system that could be exploited to realise those threats. Vulnerability analysis is the process of identifying security flaws in software or services and determining potential attack methods that a penetration tester or attacker might employ. This process may involve both automated techniques, such as vulnerability scanning, and manual approaches, including simulation and direct interaction with the system. For example, tools like Hydra may be used to conduct brute-force simulations, while observations from earlier phases (Pre-Engagement and Intelligence Gathering) inform more targeted testing strategies.

In this study, a manual and observational approach was used to analyse the authentication components of the XYZ system. The vulnerabilities found directly align with the threats modelled in Table 2, including risks related to brute force, insider access, password weaknesses, and account control. The vulnerabilities discovered are detailed in the following subsections:

4.1 Admin Account Vulnerability

Access granted to external parties, such as interns or former employees, with still-active credentials creates a significant vulnerability. Although these individuals no longer manage rural area data, they can still access the system. This may lead to unauthorised data manipulation or deletion, impacting the Confidentiality and Integrity of the information.

4.2 Password Vulnerability

The use of easily guessable default passwords, such as administrator <name>@456, increases the risk of compromise. Since the same pattern is applied across multiple admin accounts, the system becomes highly susceptible to dictionary attacks. Attackers can easily predict the password structure, affecting the Confidentiality, Integrity, and Availability of the system.

4.3 Username Disclosure

On the registration page (Figure 2), usernames follow a visible and predictable format such as administrator<name>@mailxxxx.id, which can be accessed publicly. This leakage allows attackers to identify valid usernames, enabling brute force or dictionary attacks with higher efficiency since no effort is needed to guess valid user IDs.

4.3 Lack of Login Attempt Throttling

The absence of login attempt limits on the login page allows brute-force attacks without restriction. Attackers can repeatedly attempt password combinations using automated tools, especially when usernames and predictable password patterns are already known. This increases the likelihood of unauthorised access and compromises both Availability and Confidentiality.

4.5 Absence of Multi-Factor Authentication (MFA)

Without MFA, the login mechanism lacks an essential layer of identity verification. If login credentials are stolen or guessed, attackers can directly access admin accounts. This leads to heightened risks of data breaches and system compromise, endangering the overall security posture.

RESULTS AND DISCUSSION

This section focuses on exploiting the vulnerabilities previously identified in Section 4 (Vulnerability Analysis), post-exploitation, and mitigating risk (steps 5 to 7 in the PETS framework).

5. Exploitation

The exploitation process includes tests targeting the absence of Multi-Factor Authentication (MFA), lack of login attempt throttling, and a brute force simulation on a mockup system. These tests are described as follows:

5.1 Testing for the Absence of Multi-Factor Authentication (MFA)

As illustrated in Figure 3, a login attempt was conducted using credentials provided by the rural area system operator (XYZ). Consistent with findings in Section 2 (Intelligence Gathering), the login process did not require any additional verification layers beyond the username and password. Upon successful entry of valid credentials, the user was immediately redirected to the admin dashboard.

This confirms the absence of MFA implementation, demonstrating a significant security weakness. Without MFA, attackers who acquire valid login credentials can gain unauthorised access to the system, compromising the confidentiality and integrity of the rural area data.

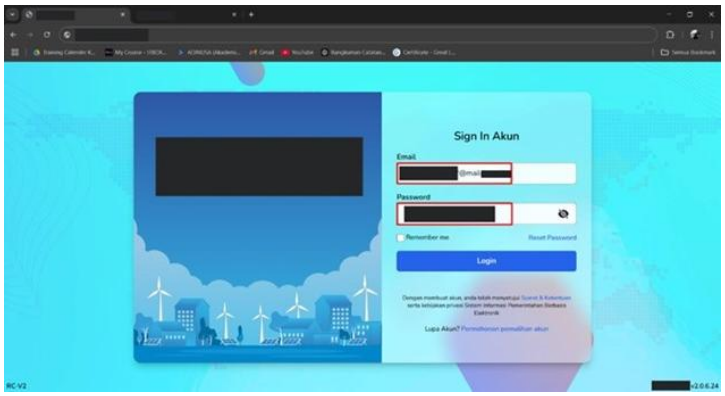

Figure 3. Login Process

5.2 Absence of Login Restrictions

The tester conducted multiple login attempts using usernames discovered from the registration page, following the pattern administrator<name>@mailxxxx.id. Additionally, the tester applied password patterns previously identified, such as administrator<name>@456. Several login attempts were performed using both the discovered pattern and intentionally incorrect combinations to simulate unauthorised access behaviour.

The results revealed that the system lacks any form of login attempt throttling or lockout mechanism. There were no delays, error warnings, or restrictions even after numerous failed login attempts. This absence of login control mechanisms significantly increases the risk of brute force attacks, where attackers can continuously attempt different password combinations until successful access is achieved. The results of this login attempt simulation are summarised in Table 3 below.

Table 3. Login Attempt

No.	Username	Password	Status
1.	name1234567891@mailxxxx.id	administratorruraljambu@456	Success
2.	name1234567892@mailxxxx.id	administratorruralmangga@456	Success
3.	name1234567893@mailxxxx.id	administratorruralkedondong@456	Success

4.	name1234567894@mailxxxx.id	administratorruralapel@456	Success
5.	name1234567895@mailxxxx.id	administratorruraljeruk@456	Success
6.	name1234567891@mailxxxx.id	wrongpassword1@456	Failed
7.	name1234567892@mailxxxx.id	wrongpassword2@456	Failed
8.	name1234567893@mailxxxx.id	wrongpassword3@456	Failed
9.	name1234567894@mailxxxx.id	wrongpassword4@456	Failed
10.	name1234567895@mailxxxx.id	wrongpassword5@456	Failed

5.3 Hydra Testing on Mockup

Hydra was employed to evaluate the system's resistance to automated login attacks by simulating both Dictionary and Hybrid attacks. The target was a mockup environment replicating the actual login system to ensure ethical testing without affecting the production server. Two types of wordlists were used:

1) Username wordlist, derived from the registration page structure observed during the Intelligence Gathering phase.
2) Password wordlists, consisting of dictionary.txt (common passwords) and hybrid.txt (based on insider findings and observed patterns).

Hydra was executed in Kali Linux using the following command structure:
hydra -L username.txt -P hybrid.txt <target IP> https-post-form"/path/login.php:username=^USER^ &password=^PASS^:S=Logout"

Note: The hybrid attack simulates a combination of insider knowledge and dictionary patterns.

Results:

1) Figure 4 shows that the dictionary attack yielded no successful login due to irrelevant password guesses.

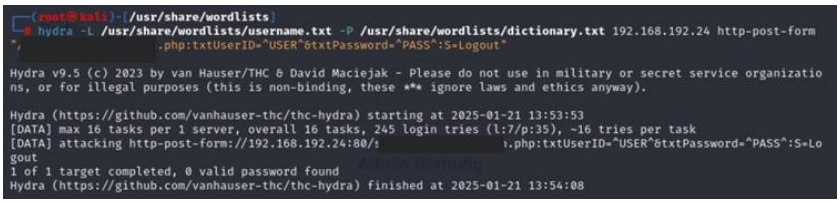

Figure 4. Result of Dictionary Attack

2) Figure 5 presents the result of the hybrid attack, which successfully cracked 6 valid admin credentials out of 42 login attempts.

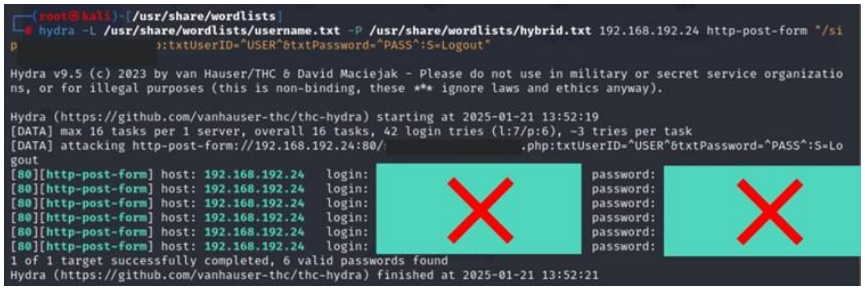

Figure 5. Result of Hybrid Attack

3) Table 4 summarises repeated testing: from 10 iterations, the hybrid attack succeeded 6 times, while the dictionary attack failed entirely.

Table 4. Testing Experiment Using Hydra

No.	Attack Type	Time	Result
1.	Dictionary Attack	00:00:15	0 Valid Password Found

2.	Hybrid Attack	00:00:02	6 Valid Password Found
3.	Dictionary Attack	00:00:14	0 Valid Password Found
4.	Hybrid Attack	00:00:03	6 Valid Password Found
5.	Dictionary Attack	00:00:15	0 Valid Password Found
6.	Hybrid Attack	00:00:03	6 Valid Password Found
7.	Dictionary Attack	00:00:15	0 Valid Password Found
8.	Hybrid Attack	00:00:04	6 Valid Password Found
9.	Dictionary Attack	00:00:15	0 Valid Password Found
10.	Hybrid Attack	00:00:03	6 Valid Password Found

Key Findings:

1. Credential Exposure: Six valid admin accounts were accessed, indicating poor password strength and predictable formatting.
2. Attack Efficiency: Hydra completed the process in a short time, showing a lack of brute force protection mechanisms.
3. Security Weakness: The system lacks login attempt throttling, allowing unlimited login attempts without penalties.

These results strongly suggest that the system is vulnerable to brute force attacks, especially those leveraging predictable credential patterns. Immediate review and enhancement of login security policies are recommended, including password complexity rules and multi-factor authentication.

6. Post-Exploitation

After successful exploitation, the attacker gained administrative-level access, enabling deeper evaluation of system exposure and potential real-world consequences. This stage focuses on assessing the extent of control achievable and the severity of security risks.

Key Findings:

1) Access to Sensitive Citizen Data: Attackers could access confidential data such as family records, phone numbers, emails, national identity numbers, and health insurance numbers. This poses a serious threat to personal privacy and opens the risk of identity theft or fraud.
2) Modification of Public Information: The system allowed the attacker to alter key rural area information (e.g., address, motto, vision/mission, bank details, logo), potentially misleading the public and damaging the rural area's reputation.
3) Full Control Over Admin Accounts: Attackers could change admin passwords and modify admin details, effectively locking out legitimate users and maintaining unauthorised access.
4) Manipulation of Rural Area Official Accounts: Beyond admin access, the attacker was able to manage, edit, and delete subordinate user accounts such as rural area officials, disrupting administrative operations.
5) Unsecured Admin Registration Interface: Although admin accounts are distributed manually by super admins, the presence of an accessible "Admin Registration" page revealed usernames and posed a potential entry point for attackers.

Identified Risks:

1) Privacy Breach: Exposure of citizen data may lead to fraud or misuse.
2) Information Manipulation: Tampering with public-facing data can damage credibility and cause misinformation.
3) System Takeover: Full account control enables attackers to disrupt operations and erase legitimate access.
4) Persistent Threats: Attackers could maintain long-term access by altering credentials and deleting logs.

These findings highlight critical vulnerabilities that jeopardise the integrity, confidentiality, and availability of the system. A thorough security audit and immediate implementation of access controls are urgently recommended.

7. Reporting

This section presents the findings and mitigation strategies resulting from penetration testing conducted on the digital rural area system (xxy.websiterural.com), based on the Penetration Testing Execution Standard (PTES) framework. The assessment focused on the registration page, login mechanism, and administrative features.

7.1 Key Findings

The penetration test identified several critical vulnerabilities, including:

1) Weak Default Credentials: Easily guessed username and password combinations increased the risk of brute-force and dictionary attacks.
2) Absence of Multi-Factor Authentication (MFA): The login system lacked additional verification layers.
3) Non-Functional Password Reset Feature: Users were unable to recover their accounts if their login credentials were forgotten.
4) No Login Attempt Limitation: Unlimited login attempts allowed for brute-force exploitation.
5) Sensitive Data Exposure: Administrative credentials and citizen information were accessible, such as national identity numbers and health insurance numbers, without proper authorisation.
6) Privilege Abuse: Attackers were able to modify and manage sensitive administrative data.

7.2 Potential Impacts

These vulnerabilities could lead to:

1) Privacy Breaches: Unauthorised access to personal citizen data.
2) Operational Disruption: Tampering with administrative data could compromise public trust.
3) Loss of Access Control: Authorised users could be locked out of the system.
4) Reputational Damage: Weak system security undermines credibility and trust in digital services.

7.3 Mitigation Implementation

To address the identified security vulnerabilities, a series of mitigation strategies was implemented in a mockup system developed using PHP, Visual Studio Code, XAMPP, MySQL, PHPMailer, Twilio, and WGET. WGET was used to extract and replicate the front-end of the original system, enabling realistic interface simulation without impacting the production environment. These mitigation strategies were grouped into three categories: Authentication Hardening, Account Management, and User Awareness and Education.

7.3.1 Authentication Hardening

1. Reset Password Feature Fix

The password recovery mechanism was rebuilt to function properly, allowing users to request reset links via email. If the email is registered, the system sends a reset link and enables the user to create a new password.

2. Login Attempt Throttling

A rate-limiting mechanism was introduced to block IP addresses after five failed login attempts, temporarily restricting access for 10 minutes. Accounts experiencing over 10 failed attempts are locked for 5 minutes.

3. Multi-Factor Authentication (MFA)

MFA using OTP (sent via email or SMS) was implemented. After successful credential input, users must verify their identity using a one-time code. This step ensures additional protection, particularly against insider threats.

All authentication-focused mitigations were documented using flowcharts and user interface mockups to support transparency, comprehension, and reproducibility by future system developers.

7.3.2 Authentication Hardening

1. Mandatory Password Change from Default

To eliminate default password reuse, users are forced to change the default password upon first login. The new password must meet defined complexity standards: at least 8 characters including uppercase, lowercase, digits, and symbols. An email verification step finalizes the activation process before full access is granted.

2. Account Expiration for Apparatus Users

Accounts tied to temporary staff or rural area officials were assigned an expiration policy. Once the account validity period ends, login is blocked, ensuring former users cannot access the system post-tenure. This status is configurable via the admin dashboard.

3. Registration Page Hardening

The registration button on the login page was removed, and access to the registration page was masked or renamed to prevent username enumeration. When registration visibility was still required, username masking was applied to obscure identifiers.

4. Activity Logging and Intrusion Detection

A monitoring dashboard was developed for administrators to:

1) Log user activity,
2) Detect and respond to failed login attempts,
3) Block suspicious IP addresses after five consecutive failures,
4) Ensure non-repudiation through comprehensive audit trails.

These account management features not only enhance access control but also mitigate both internal and external threat vectors.

7.3.3 User Awareness and Education

To address the lack of security awareness identified during the Pre-Engagement Interactions phase, a series of educational initiatives were recommended:

1. Security Training for Rural Area Operators
   Although training sessions have been conducted, they have primarily focused on administrative functions, with minimal emphasis on cybersecurity. It is crucial to deliver dedicated sessions that cover account protection practices, threat awareness, and secure system usage.
2. Password Hygiene Education
   Users should be educated about secure password practices, including the importance of using strong, unique passwords and avoiding the sharing of login credentials with others.
3. Role-Based Access and Admin Education
   Specific guidance must be provided to rural area administrators on how to properly manage apparatus-level accounts. It is essential that admin-level credentials are not shared among users

and that only designated individuals retain access to administrative functions. This measure prevents misuse and preserves the integrity of rural area data.

This structured approach to mitigation ensures not only technical reinforcement of the system's defences but also supports long-term resilience through better user behaviour and operational awareness.

7.4 Implementation Notes

The use of a mirrored front-end enabled testing and demonstration without altering the live system. The mockup served as a controlled environment for verifying each mitigation before deployment.

7.5 Post-Mitigation Testing

Following the implementation of mitigation strategies, testing was conducted to evaluate the system's resistance to hybrid brute-force attacks using the Hydra tool. The test results are summarised in Figure 6, and the Mitigation results are in Table 5.

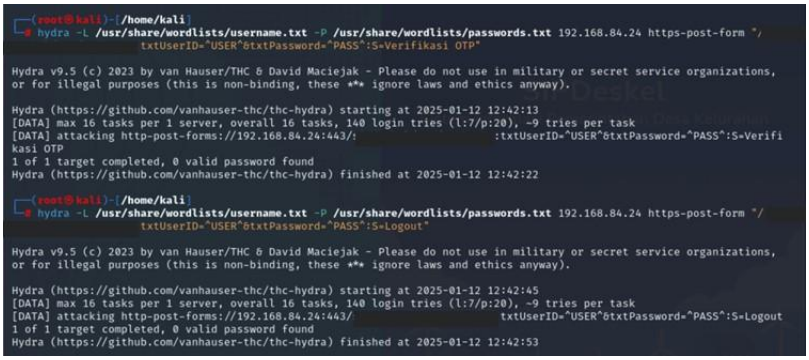

Figure 6. Hybrid Attack Attempt After Mitigation Implementation

A total of 140 login attempts were made using predefined combinations of usernames and passwords. However, no valid passwords were discovered during the attack. This outcome demonstrates that the implemented security features, including multi-factor authentication (MFA) and login throttling, were effective in mitigating both brute-force and hybrid attacks.

Table 5. Mitigation Result

No.	Identified Vulnerability	Recommended Mitigation	Security Improvement Description
1.	No account expiration policy	Establish an account validity period for apparatus-level users	Reduces the risk of inactive accounts being misused after the end of the user's assignment
2.	Weak or predictable default passwords	Enforce mandatory password change with strong password requirements	Increases password strength and reduces the risk of unauthorized access
3.	Lack of login attempt throttling	Implement login rate-limiting and account lockout after failed attempts	Mitigates brute-force attacks by restricting excessive login attempts

4.	Combined insider and dictionary attack possibility	Apply Multi-Factor Authentication (MFA) to the login system	Adds an additional layer of authentication, especially against credential stuffing
5.	Non-functional password reset feature	Repair the password reset function to allow secure account recovery	Ensures that users can regain account access securely and efficiently
6.	Potential information disclosure via the login page	Remove registration links from the login interface if not needed	Prevents attackers from gathering system-related information via exposed UI elements
7.	Visible or guessable usernames	Hide the registration page or apply username masking techniques	Decreases the likelihood of valid usernames being identified and targeted

Table 5 presents the mitigation results derived from the assessment of authentication-related vulnerabilities within the XYZ system. The table outlines seven identified weaknesses and pairs each with a targeted recommendation and corresponding security benefit. Key issues such as the absence of account expiration policies, weak default passwords, and lack of login attempt throttling are addressed through practical measures like setting account validity periods, enforcing password changes with complexity rules, and implementing rate-limiting mechanisms. These actions directly contribute to minimising risks associated with unauthorised access and brute-force attacks.

Further mitigations include the application of Multi-Factor Authentication (MFA) to defend against combined insider and dictionary attacks, and the repair of the password reset function to support secure account recovery. In addition, user interface-based vulnerabilities are addressed by removing unnecessary registration links and applying username masking or hiding techniques. These steps help prevent attackers from identifying valid usernames or collecting system metadata via exposed elements. Collectively, the mitigation strategies detailed in Table 5 aim to strengthen the login system's overall resilience and enhance the confidentiality, integrity, and availability of user data.

Note: This penetration test was conducted without the use of automated scanning tools such as Acunetix. All vulnerabilities were identified manually. While effective for smaller systems, this method may not scale efficiently to larger systems due to the time and effort required.

CONCLUSION

Based on the security assessment conducted on the digital rural area system (XYZ v2.0.6.24) using the Penetration Testing Execution Standard (PTES), several key conclusions can be drawn:

1. The vulnerabilities identified pose significant risks to the confidentiality, integrity, and availability of sensitive data. These include privacy breaches, unauthorised access, loss of system control, operational disruptions, and potential reputational damage, especially concerning personal information of residents stored within the system.
2. To evaluate these risks, a Hybrid Attack—combining insider access and dictionary techniques—was simulated using Hydra during the Exploitation phase. This allowed for a realistic assessment of the authentication system's exposure to coordinated attack vectors.
3. A controlled mockup environment was developed using technologies such as Visual Studio Code, XAMPP, MySQL, PHPMailer, Twilio, and WGET. This testbed enabled detailed vulnerability analysis and mitigation without impacting the live production system, ensuring ethical research conduct.

4. Several mitigation strategies were implemented within the mockup system, including Multi-Factor Authentication (MFA), strengthened account management policies, password reset mechanisms, and user security awareness efforts. Post-mitigation testing confirmed the effectiveness of these countermeasures, with no valid credentials retrieved during follow-up hybrid attack attempts.
5. These findings highlight the broader need for layered authentication security in rural digital platforms. Protecting data in such systems is not only a technical necessity but also essential for maintaining public trust, ensuring uninterrupted access to digital services, and supporting the integrity of rural information infrastructure.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the Informatics Engineering Study Program of IIB Darmajaya for its support throughout this research. We also extend our thanks to all individuals and parties who provided valuable assistance during data collection and simulation activities

AUTHOR CONTRIBUTIONS

The first author contributed to data collection, mockup website development, simulation execution, and drafting of the manuscript. The second author was responsible for conceptualising the research, conducting the literature review, designing the methodology, and co-authoring the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest. This study was conducted independently, and no external funding body influenced the design, implementation, data interpretation, or decision to publish the findings.

REFERENCES

Abu-Dabaseh, F., & Alshammari, E. (2018). *Automated Penetration Testing: An Overview*. 121–129. https://doi.org/10.5121/csit.2018.80610

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*, 563060. https://doi.org/10.3389/FCOMP.2021.563060/BIBTEX

Blue, J., Condell, J., & Lunney, T. (2018). A Review of Identity, Identification and Authentication. *International Journal for Information Security Research (IJISR)*, *8*(2).

Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. *Science and Technology*, *2023*(2), 29–35. https://doi.org/10.5923/j.scit.20231302.04

Fa'atulo Halawa, B., Suwardi, A., Toro, R., & Syahputri, R. (2020). *Analisis Kelemahan Sistem Authentication Pengguna Pada Wireless IEEE 802.11i*. *3*(1), 2020.

Fürst, D., & Aßmuth, A. (2025). *Practical Acoustic Eavesdropping On Typed Passphrases*. http://arxiv.org/abs/2503.16719

Harahap, A. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). *Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder*.

Haubris, K. P., & Pauli, J. J. (2013). Improving the efficiency and effectiveness of penetration test automation. *Proceedings of the 2013 10th International Conference on Information Technology: New Generations, ITNG 2013*, 387–391. https://doi.org/10.1109/ITNG.2013.135

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. In *Cyber Security and Applications* (Vol. 1). KeAi Communications Co. https://doi.org/10.1016/j.csa.2023.100016

KumparanNews. (2024). *Hadi Ungkap Faktor Utak-Atik Password Jadi Penyebab Serangan Ransomware ke PDN*. https://kumparan.com/kumparannews/hadi-ungkap-faktor-utak-atik-password-jadi-penyebab-serangan-ransomware-ke-pdn-232n4xCBOJL/full

MetroTV. (2024). *PDN Diretas, Potensi Kerugian Ekonomi Capai Rp6,3 Triliun*. https://www.metrotvnews.com/play/b2lCVP5y-pdn-diretas-potensi-kerugian-ekonomi-capai-rp6-3-triliun

Nur, R., Radin, H., Aziz, A., Amin, K., & Sukri, M. (2024). Web Based Locker Booking System with Multifactor Authentication for Wajasakti Sdn Bhd. *Applied Information Technology And Computer Science*, *5*(1), 163–181. https://doi.org/10.30880/aitcs.2024.05.01.010

Perwej, D., Qamar Abbas, S., Pratap Dixit, J., Akhtar, N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *2021*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04ï

Prabhu, S., & Shah, V. (2015). Authentication using session based passwords. *Procedia Computer Science*, *45*(C), 460–464. https://doi.org/10.1016/j.procs.2015.03.079

Raza, A. (2024). A Review Of Cybersecurity Threats In E- Government Systems: Towards Secure Digital Governance. *Multidisciplinary Research In Computing Information Systems*, *4*(3). https://mrcis.org/index.php/journal/article/view/74/76

Ritonga, A., Putra, B., Togatorop, D., Ginting, H. B., Laoli, K. M., Tri, M., Sinaga, Y., Amelia, R. I., & Kartini Pangaribuan, W. (2025). Analisis Kombinatorik Dalam Menentukan Keamanan dan Kompleksitas Password dengan Penerapan Teori Kombinatorik. *Katalis Pendidikan: Jurnal Ilmu Pendidikan Dan Matematika*, *2*, 49–64. https://doi.org/10.62383/katalis.v2i2.1463

Rodrigues, G. A. P., Fernandes, P. A. G., Serrano, A. L. M., Filho, G. P. R., Vergara, G. F., Bispo, G. D., Albuquerque, R. de O., & Gonçalves, V. P. G. (2025). From RockYou to RockYou2024: Analyzing Password Patterns Across Generations, Their Use in Industrial Systems and Vulnerability to Password Guessing Attack. *Journal OfInternet Services and Applications*, *16*(1). https://doi.org/10.5753/jisa.2025.5041

Safitra, M. F., Lubis, M., & Widjajarto, A. (2023). Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website. *ACM International Conference Proceeding Series*, 139–145. https://doi.org/10.1145/3592307.3592329

Simorangkir, A., Palangkaraya, U., Sihombing, H., Parhusip, J., Yos, J., Palangka, S., & Kalimantan, R. (2024). Ransomware pada Data PDN: Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber. *Jurnal Sains Student Research*, *2*(6). https://doi.org/10.61722/jssr.v2i6.2966

Syahputri, R., Fa, B., Halawa, atulo, & Trisnawati, S. (2024). FaceVoting: e-Voting Berbasiskan Pengenalan Wajah. *Jurnal Teknik Komputer*, *10*(2), 107–117. https://doi.org/10.31294/JTK.V10I2.21918

Tu, S., Waqas, M., Rehman, S. U., Aamir, M., Rehman, O. U., Jianbiao, Z., & Chang, C. C. (2018). Security in Fog Computing: A Novel Technique to Tackle an Impersonation Attack. *IEEE Access*, *6*, 74993–75001. https://doi.org/10.1109/ACCESS.2018.2884672

Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. In *Journal of Network and Computer Applications* (Vol. 188). Academic Press. https://doi.org/10.1016/j.jnca.2021.103080

Zhang, H. (2023). *Academic Journal of Management and Social Sciences The Innovation of the PEST Analysis Model in Public Sector Strategy Formulation*. *2*(1), 2023. https://doi.org/10.13366/j.dik.2016.04.119