JOURNAL SYNTAX IDEA
p–ISSN: 2723-4339 e-ISSN: 2548-1398
Vol. 6, No. 06, Juni 2024

EVALUATION OF PASSWORD SECURITY COMPLIANCE USING NIST SP 800-63

Mohammad Ghifari Yusuf, Jarot Sembodo Suroso
Bina Nusantara University, Indonesia
Email: mohammad.yusuf001@binus.ac.id, jarot_suroso@binus.ac.id

Abstract

This study aims to investigate password compliance within a web application used by 174 users, following NIST SP 800-63 guidelines. A questionnaire was employed to assess user password attributes aligned with NIST guidelines, using a binary scoring system for compliance. The research findings will unveil strengths and weaknesses in password policies and their implementation within the web application. As a result, the security compliance level of the web application is approximately 28.30%. Based on these findings, recommendations will be provided to enhance the web application’s security

Keywords: password security, compliance scorecard, NIST SP 800-63

INTRODUCTION

In today's digital landscape, the security of user identity and the management of passwords have risen to the forefront as critical concerns (Kennison, Jones, Spooner, & Chan-Tin, 2021). The pervasive issue of weak password practices has escalated into a significant security challenge, resulting in a surge of data breaches and vulnerabilities within digital systems. This predicament not only endangers individual privacy but also poses formidable risks to organizations and society (Hall, Hoppa, & Hu, 2023) . Effectively addressing these challenges is paramount in protecting sensitive information and upholding the integrity of digital environments.

Passwords represent one of the most employed security mechanisms within information systems, safeguarding sensitive data from unauthorized access (Lee, Sjöberg, & Narayanan, 2022). However, many users fail to implement adequate measures to ensure the security of their passwords. Common practices include using easily guessable passwords or employing the same password across multiple accounts (Cazier & Medlin, 2006). These practices undermine the security of stored information. Consequently, the establishment of effective and efficient password security mechanisms is imperative.

A research study underscores weak password usage within information systems (Bonneau, 2012). Their findings reveal that users often opt for easily memorable passwords, such as names or birthdates, rendering passwords susceptible to unauthorized guesses. Additionally, many users employ identical passwords across multiple accounts, heightening the risk of data breaches if one account is compromised (Indonesia, 2017)

How to cite:	Mohammad Ghifari Yusuf, Jarot Sembodo Suroso (2024) Evaluation of Password Security Compliance Using Nist SP 800-63, *(06) 06*, https://doi.org/10.36418/syntax-idea.v3i6.1227
E-ISSN:	2684-883X
Published by:	Ridwan Institute

Avast, a global company specializing in internet security, conducted research that revealed inadequate protection measures for online accounts among Americans. A survey conducted by Avast highlighted that 83% of American users neglect to include a comprehensive combination of elements in their passwords, including numbers, special symbols, and upper and lower case letters, and fail to ensure their passwords are minimal. It's ten characters long. Additionally, the study found that more than half of the participants (53%) repeatedly used the same passwords across accounts, increasing the vulnerability of those accounts to cyber threats (Indonesia, 2003; Yıldırım & Mackie, 2019).

The security audit conducted by Vumetric in collaboration with the game services company revealed several critical findings. Firstly, the audit identified issues with access control, as Developer users could access functions intended only for administrative users. Secondly, the absence of multi-factor authentication left user accounts vulnerable to unauthorized access. Thirdly, the password policy was lacking, increasing the risk of password-related breaches. Additionally, disclosing sensitive technical information in HTTP headers and error messages posed significant security risks, potentially facilitating targeted attacks. These findings underscore the need for immediate action to address these vulnerabilities and enhance the overall security posture of the company's systems (Mayer, Schwartz, & Volkamer, 2018).

Based on these findings, data security remains a pressing concern that demands continuous vigilance. Addressing this issue necessitates the implementation of effective password security measures. For a gaming services company, systems and information security hold paramount importance. Consequently, evaluating user password security compliance using NIST SP 800-63 guidelines on the web application of a game services company is a relevant research topic.

RESEACRH METHOD

This research employed a qualitative method to inspect the company's web application. The overall experiment encompassed the following procedural elements (Hennink, Hutter, & Bailey, 2020).

Sample Population Selection

The research population for this study includes all web application users, specifically employees of the company's clients who possess accounts for logging into the system. The total user population amounts to 308. This sample provides a comprehensive overview of the web application's usage, encompassing a diverse range of user interactions and experiences within the system.

For determining an appropriate sample size, the Slovin formula was applied, which is recommended for research where the population size is known (Siponen & Willison, 2009). The slovin formula can be seen in Figure 1.

$$\mathbf{n} = \frac{\mathbf{N}}{\mathbf{1} + \mathbf{N}\,(\mathbf{e})^{\mathbf{2}}}$$

Figure 1 The Slovin Formula

This formula, with a 5% error tolerance level, calculated the sample size for this study to be 174 respondents. This size ensures a representative sample of the entire user population of the web application, allowing for a comprehensive analysis of user interactions and experiences within the system.

Data Collection

The data collection method employed in this study was a questionnaire. The questionnaire was created based on previously developed indicators and was distributed through a Google Form. Based on this data collection technique, the following indicators and statements will be included in the questionnaire and can be seen in Table 2.

Table 2 Research Questionnaire

No	Question
1.	Does the password have to be at least eight characters?
2.	Is the maximum limit to 64 characters?
3.	Does the password require special characters? (e.g., “?”, “!”, “@”, “#”)
4.	Does the password require a mix of upper and lower case characters?
5.	Does the password require at least one number?
6.	Are there any warnings telling you your password is easy to guess?
7.	Is there a visual guidance that shows the complexity of the password you entered?
8.	When entering an incorrect password, is there a warning about the number of attempts to enter the password?
9.	Have you been told your account will be locked out after an “X” number of attempts?
10.	Are there regular announcements telling you to change your password?
11.	Are you required to prove you are human? (e.g., Captcha)
12.	Are you NOT prompted to create a security question to reset your password? (e.g., your pet's name, your city)
13.	Are you NOT prompted to create a password hint regarding the password you create?
14.	Are you prompted to register for two-factor authentication?
15.	When you click forgot/reset password, is there a code you must enter or a link in the email you must click?

Calculations and Inferences

This study employed a compliance scorecard, utilizing a binary scoring system. Respondents were required to select one of three options for each question, with explanations provided in Table 3.

Table 3 Binary Scoring System

Option	Score	Description
Yes	1	Signifies that the criterion is met and

		the requirement is fulfilled (compliance achieved).
No	0	Indicates that the statement is not met or the requirement is not fulfilled (no compliance).
Unsure	0	Implies uncertainty or lack of knowledge regarding compliance with the statement.

The compliance score was then calculated based on the number of "yes" responses compared to the total number of criteria. This calculation provided an overall compliance percentage or score, clearly indicating the entity's level of compliance.

Variable Operations

Operationalizing variables is one technique that can be used to reduce abstract ideas or concepts into observable research characteristics (Siponen & Willison, 2009).

The variables studied in this research are operationalized, consisting of length (L), character types (CT), truncation (T), screening (S), complexity (C), lockout (LO), expiration (E), knowledge-based authentication (KA), and two-factor authentication (TA). The operationalization of variables can be seen in the following Table 4.

Table 4 Variable Operations

Indicator	Variable
The minimum password length is eight characters.	L1
The maximum password length is 64 characters.	L2
All special characters ("?", "!", "@", "#"), including spaces, are allowed in passwords.	CT1
Passwords must contain both uppercase and lowercase letters.	CT2
Passwords must contain at least one digit.	CT3
There is a warning indicating easily guessable passwords.	S1
There is a visual explanation showing the complexity of created passwords.	C1
When entering the wrong password, there is a remaining attempt warning for incorrect password entry.	LO1
Accounts will be locked or unable to log in after multiple incorrect password attempts.	LO2
There are periodic announcements to change passwords.	E1
There is verification indicating the user is human.	KA1
There are no security questions when	KA2

resetting passwords.	
There is no requirement to provide hints about created passwords.	KA3
Two-factor authentication is mandatory.	TA1
When resetting passwords, a code or link is sent to the email.	TA2

.

RESULTS AND DISCUSSION

In this research, the researcher collected data through a questionnaire distributed to 174 respondents, selected based on specific criteria to ensure diverse perspectives were captured. The questionnaire was meticulously designed to encompass a comprehensive range of questions on the variables under investigation. The respondents were asked to respond based on their experiences and perceptions of the subject matter. The results of the questionnaire analysis yielded several values that reflect various aspects assessed in this study (Fayers & Machin, 2013). These values include numerical scores, percentages, and qualitative insights from respondents' feedback. In this context, the researcher meticulously examined and interpreted the scores and percentages of each respective variable and attribute to derive meaningful conclusions. The detailed questionnaire results, including statistical analyses and graphical representations where applicable, are comprehensively presented in Table 5 for further scrutiny and interpretation.

Table 5 Compliance Scores

Attribute	Variable	Score	%
Length	L1	1	100
	L2	0	0
Character types	CT1	0.9942	99.43
	CT2	1	100
	CT3	0.9885	98.85
Screening	S1	0	0
Complexity	C1	0	0
Lockout	LO1	0	0
	LO2	0	0
Expiration	E1	0	0
Knowledge-based authentication	KA1	0	0
	KA2	0.7298	72.99
	KA3	0.6321	63.22
Two-factor authentication (2FA)	TA1	0	0
	TA2	0.6321	63.22

Based on the available data, involves the assessment of various variables to determine compliance with NIST standards (Hogan, Liu, Sokol, & Tong, 2011). Each variable carries a specific score and corresponding percentage. To calculate the percentage for each attribute, we aggregate the percentages of variables within that attribute and divide by the maximum possible percentage for that attribute. This computation yields the compliance percentage value for each attribute, following the formula:

$$Category\ Percentage = \frac{Sum\ of all\ variable\ percentages}{Maximum\ category\ percentage}$$

To arrive at the total compliance percentage, we sum all the attribute percentages and then divide this sum by the number of categories under assessment (Grassi, Garcia, & Fenton, 2020). The detailed results for each attribute are presented comprehensively in Table 6. This methodology comprehensively evaluates compliance levels across various aspects, offering insights into the web application's adherence to NIST standards.

Table 6 Compliance Scores per Attribute

Attribute	%
Length	50
Character types	98.43
Screening	0
Complexity	0
Lockout	0
Expiration	0
Knowledge-based authentication	45.40
Two-factor authentication (2FA)	31.61
Average	28.30

Consequently, the outcome of our assessment reveals that the security compliance level of the web application stands at approximately 28.30%. This metric is a pivotal indicator, shedding light on the web application's alignment with essential security standards, particularly those outlined in NIST guidelines. The calculated compliance level underscores the significance of further efforts to bolster security measures and enhance the protection of sensitive data within the web application (Shouran, Rokhman, & Priyambodo, 2021). These findings provide a clear baseline for addressing vulnerabilities and implementing necessary security enhancements to fortify the web application's resilience in an ever-evolving digital landscape

CONCLUSSION

The findings of this research reveal that the compliance level of the company's web application security with NIST standards is approximately 28.30%. This indicates that specific aspects require enhancement to achieve higher compliance with NIST security standards. These findings are a foundation for improving security policies for the company's web application and similar applications in the industry, aiming to enhance overall security compliance.

BIBLIOGRAFI

Bonneau, Joseph. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. *2012 IEEE Symposium on Security and Privacy*, 538–552. IEEE.

Cazier, Joseph A., & Medlin, B. Dawn. (2006). Password security: An empirical investigation into e-commerce passwords and their crack times. *Information Systems Security*, *15*(6), 45–55.

Fayers, Peter M., & Machin, David. (2013). *Quality of life: the assessment, analysis and interpretation of patient-reported outcomes*. John wiley & sons.

Grassi, Paul, Garcia, Michael, & Fenton, James. (2020). *Digital identity guidelines*. National Institute of Standards and Technology.

Hall, Robert C., Hoppa, Mary Ann, & Hu, Yen Hung. (2023). An Empirical Study of Password Policy Compliance. *Journal of The Colloquium for Information Systems Security Education*, *10*(1), 8.

Hennink, Monique, Hutter, Inge, & Bailey, Ajay. (2020). *Qualitative research methods*. Sage.

Hogan, Michael, Liu, Fang, Sokol, Annie, & Tong, Jin. (2011). Nist cloud computing standards roadmap. *NIST Special Publication*, *35*, 6–11.

Indonesia, Pemerintah Republik. (2003). *Undang-Undang Republik Indonesia Nomor 17 Tahun 2003 tentang Keuangan Negara*.

Indonesia, Pemerintah Republik. (2017). Kementerian Kesehatan Republik Indonesia. *Republic of Indonesia Law Number 36 of 2014 Concerning Health Workers*.

Kennison, Shelia M., Jones, Ian T., Spooner, Victoria H., & Chan-Tin, D. Eric. (2021). Who creates strong passwords when nudging fails. *Computers in Human Behavior Reports*, *4*, 100132.

Lee, Kevin, Sjöberg, Sten, & Narayanan, Arvind. (2022). Password policies of most top websites fail to follow best practices. *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 561–580.

Mayer, Peter, Schwartz, Christian, & Volkamer, Melanie. (2018). On the systematic development and evaluation of password security awareness-raising materials. *Proceedings of the 34th Annual Computer Security Applications Conference*, 733–748.

Shouran, Zaied Saad, Rokhman, Nur, & Priyambodo, Tri Kuntoro. (2021). System Security Awareness Planning Model Using The Octave Method Approach. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *13*(3), 231–240.

Siponen, Mikko, & Willison, Robert. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270.

Yıldırım, M., & Mackie, Ian. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*, 741–759.

.