Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*College of Cyber Science, Nankai University*
Name of Submitter/POC:	*Wang Ding*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63B	5.1.1.2	15	714-715	Delete the original sentence and replace it with a more scientific one: A website SHALL only reject a password because it is weak (i.e., easily to be guessed), not because of the substrings it contains (e.g., the name of the service). See this suggestion on the upper-right of page 1550 of the following [SEC19] work: [SEC19] Ding Wang, Ping Wang, Debiao He, Yuan Tian. Birthday, Name and Bifacial-security: Understanding Passwords of Chinese Web Users. Proceedings of the 28th USENIX Security Symposium (USENIX Security 2019), pp.1537-1554. https://www.usenix.org/system/files/sec19-wang-ding.pdf	Delete the sentence "Context-specific words, such as the name of the service, the username, and derivatives thereof " , and replace it with a more scientific, actionable guideline: A website SHALL reject a password only because it is easily to be guessed (i.e., rated “weak” by state-of-the-art password strength meters) [SEC19], not because of any substring(s) it contains (e.g., the name of the service, the username, and derivatives thereof). [SEC19] Ding Wang, Ping Wang, Debiao He, Yuan Tian. Birthday, Name and Bifacial-security: Understanding Passwords of Chinese Web Users. Proc. of the 28th USENIX Security Symposium (USENIX Security 2019), pp.1537-1554. https://www.usenix.org/system/files/sec19-wang-ding.pdf
2	63B	5.1.1.2	15	726-728	A non-full-string matching algorithm is necessary for a website that wants to capture trivially modified variants of listed (and potentially very weak) memory secrets. While non-full-string blocklist matching algorithms can provide strong security against guessing attacks, they may seriously impair password-creation usability if used alongside a large blocklist [CCS20]. Therefore, we recommend using both a moderate password blocklist (e.g., 10^6 [CCS20]) and an accurate password-strength meter (e.g., Zxcvbn, fuzzyPSM, and [SEC23]) to detect and prevent weak passwords. [CCS20] Tan, J., Bauer, L., Christin, N., & Cranor, L. F.. Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements. In Proceedings of ACM CCS 2020, pp. 1407-1426. https://dl.acm.org/doi/10.1145/3372297.3417882 [SEC23] Ding Wang, Xuan Shan, Qiying Dong, Yaosheng Shen, Chunfu Jia. No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters. Proceedings of 32nd USENIX Security Symposium (USENIX Security 2023). pp. 1-28. http://wangdingg.weebly.com/uploads/2/0/3/6/20366987/usenix23-n3-fullversion.pdf	Modify: "This is particularly important following the rejection of a memorized secret on the above list as it discourages trivial modification of listed (and likely very weak) memorized secrets." To: "This is particularly important after rejecting memory secrets from the above list, as it discourages selecting passwords rated as weak (including, but not limited to, the listed memory secrets and their trivial modified variants) by an accurate password-strength meter [SEC23]." [SEC23] Ding Wang, Xuan Shan, Qiying Dong, Yaosheng Shen, Chunfu Jia. No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters. Proceedings of 32nd USENIX Security Symposium (USENIX Security 2023). pp. 1-28. http://wangdingg.weebly.com/uploads/2/0/3/6/20366987/usenix23-n3-fullversion.pdf