Investigating the Password Policy Practices of Website Administrators

Sena Sahin† Suood Al Roomi†⋆ Tara Poteat† Frank Li†
†*Georgia Institute of Technology* ⋆*Kuwait University*

***Abstract*—Passwords are the de facto standard for online authentication today, and will likely remain so for the foreseeable future. As a consequence, the security community has extensively explored how users behave with passwords, producing recommendations for password policies that promote password security and usability for users. However, it is the website administrators who must adopt such recommendations to enact improvements to online authentication in practice. To date, there has been limited investigation of how web administrators manage password policies for their sites. To improve online authentication at scale, we must understand the factors behind this specific population's behaviors and decisions, and how to help administrators deploy more secure password policies.**

In this paper, we explore how web administrators determine the password policies that they employ, what considerations impact a policy's evolution, and what challenges administrators encounter when managing a site's policy. To do so, we conduct an online survey and in-depth semi-structured interviews with 11 US-based web administrators with direct experience managing website password policies. Through our qualitative study, we identify a small set of key factors driving the majority of password policy decisions, and barriers that inhibit administrators from enacting policies that are more aligned with modern guidelines. Moving forward, we propose directions for future research and community action that may help administrators manage password policies more effectively.

1. Introduction

Password-based online authentication is ubiquitous, and despite the multitude of drawbacks associated with passwords, this state is unlikely to change in the foreseeable future [1]. As a consequence, the security of the online ecosystem is acutely dependent on how both users and websites manage password authentication. Given the critical importance of passwords, the security research community has extensively explored how users behave with passwords, particularly when interacting with certain password policies [2]–[11]. These user-centric works have shed light on which password policies promote better security and usability for users.

Ultimately though, it is the website administrators who must deploy recommended policies on their websites to enact improvements to authentication security in practice. To date, there has been limited administrator-centric exploration focusing on how website administrators manage password authentication. Several studies have conducted small-scale measurements of the password policies deployed on websites [12]–[18], frequently finding weak policies that do not align with modern password recommendations and guidelines. This line of research does not explicitly explore the human factors involved though, and thus provides limited insights into *why* such password policies remain widespread in practice. Meanwhile, a couple of prior studies have investigated the human factors involved with web developers and how they manage password storage [19], [20]. However, password storage is only one facet of a site's password policy, and the existing literature does not yet account for other important dimensions, especially user-facing policy decisions such as password composition requirements and password change workflows.

It is vital for the security community to develop a more comprehensive and systematic understanding of how web administrators manage password authentication, determining what their mental models are when deciding on and deploying certain password policies, diagnosing the challenges that they encounter and the barriers preventing the adoption of more secure policies, and identifying directions for driving widespread improvements to online authentication. In this work, we take a step towards filling this gap by investigating the password policy practices of web administrators. Specifically, we aim to answer two core research questions, focusing on user-facing aspects of password policies, including password composition requirements, disallowed passwords, password expiration, and password change restrictions:

RQ1. What factors influence the password policies that web administrators deploy?

RQ2. What are the considerations that arise when updating a website's password policy?

To answer these questions, we conduct a user study that integrates an online survey with in-depth semi-structured interviews. Our study involves 11 US-based web administrators who have direct experience with managing website password policies[1]. Through our study, we identify several primary factors behind the password policy decisions of our study participants, including a variety of security and usability concerns, technical dependencies, and adherence to common guidelines and standards. We also find challenges and barriers that web administrators encounter when managing password policies, including uncertainty when determining the design of a suitable policy, competing interests and priorities that inhibit taking actions that may improve a

1. While our study sample is small, it is commensurate with similar qualitative administrator/operator-oriented studies [21]–[27], and our data collection and analysis achieve thematic saturation.

policy, and both technical and logistical hurdles encountered when trying to deploy a new policy.

Ultimately, our evidence-based study extends the research literature on the password policy practices of web administrators, a unique population. In particular, our work makes two primary contributions. First, we provide empirical grounding on how web administrators manage password policies, considering policy aspects beyond prior exploration [19], [20]. Second, drawing from our results, we make grounded recommendations for improving how web administrators manage password policies and propose avenues for driving improved online authentication moving forward.

2. Related Work

Here we survey the prior work that has either investigated the human factors behind website developer and administrator password policy behaviors, or empirically measured the password policies deployed in the wild.

2.1. Web Developer and Administrator Password Policy Studies

To date, there has been limited work exploring how website administrators handle password-related tasks. What work does exist has primarily focused on password storage considerations. Naiakshina et al. [19] combined multiple qualitative methods with computer science students to investigate the rationale behind password storage decisions. They identified that participants concentrated on functionality before security, and that existing security recommendations and standards were not always clear and sometimes conflicting. In follow-on work, Naiakshina et al. [20] conducted a similar study with freelance developers. They found that providing security prompts to the developers could significantly impact whether the participants securely stored their passwords. While password storage is an important aspect of online authentication, it is only one facet. These studies do not encapsulate other key password policy components, particularly user-facing ones such as password composition and password change requirements.

Another related study is that of Gerlitz et al. [28], who qualitatively explored the state of password policies. The study conducted an online survey with 83 German web administrators about their website password policies. They observed a large heterogeneity in policies, with various password length requirements, password expiration periods, and composition rules. Furthermore, they noted that a participant's company size was not significantly correlated with the strength of its password policy. However, this work did not deeply investigate why the administrators chose the policies that they did, and what challenges they encountered while managing password authentication. Through semi-structured interviews with administrators, we expand upon this prior work to investigate the considerations behind the password policies deployed by administrators.

2.2. Password Policies

A handful of studies have empirically measured the password policies of real-world websites [12]–[18], [29]–[32]. Policies were found to vary among websites [15], [29], and policies that modern guidelines consider weak were widespread [15], [29]–[31]. Still, policies were observed evolving over time, such as imposing more complex requirements [12], [31], [32]. Other studies have compared policy strength across German, US, and Chinese websites, finding differences [12], [16]. Florencio et al. observed that a website's monetization potential seemed inversely correlated with its password policy's strength [13]. While these studies have shed light on real-world website password policies, they have not investigated the human facets of why these policies manifest.

3. Methodology

In this study, we explore how web administrators manage password authentication policies in practice, seeking to understand the reasons behind deployed policies and considerations for making changes to policies. In particular, we aim to answer two primary research questions.

RQ1. What factors influence the password policies that web administrators deploy?

RQ2. What are the considerations that arise when updating a website's password policy?

To answer these research questions, we conducted a qualitative study of web administrators who have directly managed password policies for websites. Our study consisted of online surveys paired with semi-structured interviews with 11 administrators. Specifically, our study contained two integrated phases. First, we distributed a short online survey to recruit potential study participants and obtain basic information about their demographics and the password policies deployed on a website they have directly managed. Second, we conducted semi-structured interviews with survey respondents, allowing us to deeply investigate their experiences managing a website's password policy. For each participant, our interview questions were specifically customized to align with the information provided via the survey. Together, the surveys and interviews allow us to identify the policies deployed by participants, the reasons behind those policies, and the factors at play in updating those policies in the future.

3.1. Recruitment

Prior work [33]–[35] found that recruiting security-related professionals for qualitative studies is very challenging, and our study is no exception. We not only require participants with real-world experience managing a website, but those who have directly handled a site's password policy. Thus, our pool of prospective study candidates is a significantly smaller subset of the web administrator population. While we could have recruited administrators without experience engaging with website password policies, we would then be restricted to inquiring about hypothetical scenarios rather than real-world ones, limiting the ecological validity of our findings. Instead, we focus on participants who self-identify as web administrators with password policy experience in practice. Our study is further restricted to those over 18 years old residing in the United States.

To recruit such web administrators, we created advertisement posters and text blurbs providing information about our study and its goals, and included a link to our online survey (discussed more in § 3.2). (An example recruiting message is in the Appendix.) Note that while we linked to a survey, our recruiting text clearly stated that the study would involve an interview, and that interested individuals should complete the survey first, and then we would contact them for the interview. From November 2021 through April 2022, we distributed the posters and blurbs through a diverse set of communication channels, including social media outlets such as Twitter, LinkedIn, Facebook, and online web administrator forums. We also identified multiple public Slack workspaces serving web administrator groups and posted about our study on appropriate public Slack channels. We further advertised our study in a university cybersecurity-related newsletter. We additionally manually searched GitHub for web development projects and emailed contributors with public contacts. Finally, we reached out through personal social networks. For anyone we engaged with during the recruiting process, including those who did not ultimately participate in our study, we employed snowball sampling [36] by requesting that they share our study information with others who may be relevant. Throughout our study (including the survey and interview component), we did not offer compensation as administrators are already well-paid, similar to prior administrator-oriented works [23], [28], [37]–[44].

Through our extensive and lengthy recruiting effort, we directly interacted with a total of 41 individuals. The majority of individuals were not suitable for our study though (e.g., no experience with password policies), and in the end, we interviewed 11 administrators. (We note that the small portion of contacted individuals that yielded interviews demonstrates the challenges in recruiting such study participants.) Overall, our interview participants were recruited through Slack channels (N=5), social networks (N=4), and the newsletter (N=2). While our study sample size is relatively small, it is commensurate with similar qualitative studies of administrators, developers, and other specialized populations [21]–[27]. Furthermore, our analysis of our collected interview data achieves thematic saturation, indicating our data collection was conducted to an appropriate scale.

Pilot Participants. In §§ 3.2 and 3.3, we will discuss the details of the surveys and interviews conducted with recruited participants. To evaluate the quality of our instrument design, we first conducted a pilot study, where we monitored the quality of responses to our questions and solicited feedback on our instruments from our first three participants. We received valuable feedback that resulted in the removal of a few redundant interview questions. However, we did not identify further changes required, and subsequently transitioned from the pilot phase to the full study. As the data collected from pilot participants is a superset of that collected from the remaining study participants, we include pilot participants in our final study sample.

3.2. Phase 1: Survey

The first phase of our study was an online survey hosted on our university's Qualtrics platform. The survey contained up to 26 questions in total (some questions were presented depending on prior question answers), consisting primarily of yes/no, multiple-choice, and numerical answer questions (as listed in the Appendix). Prospective interview participants completed this survey by providing basic information about their demographics and the password policies of a website that they managed, as well as contact information for scheduling the subsequent interview (Phase 2).

Our use of an online survey in this first phase of the study was both for recruitment (obtaining contact information for interested interview participants) and for collecting information to customize the subsequent interview. For example, by identifying the specific policy parameters employed by a participant, we could ask interview questions about how those parameters were chosen, and bypass allocating a portion of the interview to determining what those parameters were or asking about irrelevant policy aspects. Furthermore, we believe that a participant may be able to provide more accurate information about their site's password policy through the survey compared to the interview, as a participant can search for and identify details about their policy offline, whereas they may struggle to recall during a live discussion.

In total, our survey was started 44 times, although only 13 individuals completed the survey. We contacted all such respondents and identified that 11 were suitable for interviews (in subsequent communication, we identified that the other two survey respondents lacked direct experience with password policy management). On average, the survey took 7 minutes to complete.

3.3. Phase 2: Semi-Structured Interview

The second phase of our study consisted of semi-structured interviews with web administrators to discuss their experiences managing website password policies. In pursuit of our first research question, we first asked participants about how they determined their site's password policy along the following user-facing dimensions:

- Password composition requirements
- Disallowed passwords
- Password expiration
- Password change restrictions

To explore our second research question, we then asked participants about how their site's password policy could be updated. Specifically, we asked about:

- Potential reasons behind enacting a policy change
- What the policy update process would entail, including organizational and implementation aspects
- Challenges encountered during a policy update

Finally, we asked participants to expand on their experience and education in managing password authentication.

The interview guide consisted of 47 potential questions (as shown in the Appendix). However, prior to each interview, we determined the relevant subset of questions based

ID	Age	Edu	Yrs	Org Size	Org Sector	# Users
P1	30-49	B.S.	15	10-50	Logistics	>1M
P2	30-49	M.S.	13	10-50	-	-
P3	50-69	B.S.	18	>250	Education	>100K
P4	18-29	B.S.	8	10-50	eCommerce	>6K
P5	50-69	B.S.	14	>250	Education	>100K
P6	30-49	B.S.	18	10-50	IT Support	∼100
P7	50-69	M.S.	5	>250	Education	-
P8	30-49	A.S.	8	0-9	-	-
P9	-	Ph.D.	-	-	Business	-
P10	30-49	Ph.D.	10	50-249	Education	>2K
P11	30-49	B.S.	23	>250	Legal	-

TABLE 1. SUMMARY OF PARTICIPANT DEMOGRAPHICS. ALL WERE MALE EXCEPT P7. (YRS = YEARS OF ADMINISTRATOR EXPERIENCE)

on the participant's survey responses. For example, if one participant indicated that they disallowed users from using common passwords, we asked the participant about their considerations behind doing so and how they implemented this policy. However, if another participant did not employ such a policy, we would instead ask about their opinions on such policies and why they might not deploy them. As our interviews were semi-structured, the interviewer adjusted the questions asked and made follow-on inquiries as necessary.

From November 2021 to April 2022, we conducted interviews with 11 suitable respondents to our Phase 1 survey. (As discussed in § 3.1, we used the first three participants for a pilot study, and included their collected data as we did not identify consequential changes to our study instruments.) One researcher conducted all interviews for consistency. The interviews were conducted and recorded using an online video conference platform of the participant's choosing, lasting 45 minutes on average.

3.4. Data Analysis

We transcribed all recorded interviews and analyzed the data using inductive thematic analysis [45]. For each of the four question sections of the interview, two researchers independently developed a set of codes across the responses from all participants and met to converge on a codebook. Then, each researcher independently coded all participant responses using the finalized codebook. To evaluate the consistency of the coding process, we compute the Kupper-Hafner inter-rater reliability scores [46] (other scoring calculations are less suitable when multiple codes are assigned per response [47]), finding an average agreement of 0.89, indicative of highly consistent coding between the coder pairs. Subsequently, the two researchers met to converge on the final codes assigned to each participant's response. Throughout the analysis process, all team members met to discuss points of disagreement and ensure that the resulting themes discussed in the paper are in line with all coders' interpretations of the data. In §§ 4 and 5, we list the primary themes identified with bolded paragraph labels.

3.5. Participants

In total, our study consists of 11 US-based participants. Table 1 lists those participants and their demographic information. Our sample is male-dominated, with only one female participant, similar to prior works [22], [33]. All participants had some higher education: 1 had an associate degree, 6 had a bachelor's degree, and four held a graduate degree. On average, our participants had 13 years of web administration experience, ranging from 5 to 23 years. Our participants span a variety of both smaller and larger organizations. While we solicited information about participants' websites, we made responding optional (as we identified during our pilot study that such information could be sensitive). As a result, we only collected partial information, although we observe participant websites in different sectors with user bases ranging from hundreds to millions of users.

3.6. Limitations

Due to our qualitative study method and participant sample, our study exhibits several important limitations.

1) Our study bears the same limitations as other interview-based qualitative research, such as social desirability bias (where participants respond in the fashion that they believe to be more socially acceptable, especially in a security/privacy context) and recall bias (where participants fail to correctly recall details about their experiences).
2) As web administrators are often paid well, we did not provide compensation. Rather, those who participated in our study are more likely to be ideologically motivated.
3) Due to our recruitment method, our study participants may not be representative of web administrators in general. For example, we did not study individuals who resided outside of the United States, so our findings may not generalize globally. Similarly, our participant sample skews towards certain demographics (e.g., males) and our results reflect our study's sample. However, we note that our sample exhibits diversity in education/experience.
4) Our sample size was sufficient for reaching thematic saturation, affording a qualitative analysis. Prior administrator-oriented studies have also been conducted at similar scales [21]–[27]. However, our results should not be interpreted quantitatively, and sample proportions are not reliable indicators of real-world prevalence. We also cannot assume that because a respondent did not discuss a theme, it does not apply, as the participant may have focused on other topics.
5) This study is ultimately an exploratory one, focusing on key factors and considerations when managing website password policies. However, we do not investigate all aspects of password policies in depth (e.g., password meters, textual password guidance). We also do not deep dive into the mental models and workflows of web administrators. Moving forward, our study can help inform the design of follow-on qualitative and quantitative explorations of these other password policy dimensions.

3.7. Ethical Considerations

Our full study was approved by our university's Institutional Review Board (IRB). We obtained consent in both study phases and informed participants that they need not answer questions they were not comfortable with and could halt participation at any time. We also informed the

participants and obtained approval to record the interviews. All collected data was anonymized and stored securely, with access restricted to our research team.

4. RQ1: Factors Influencing Password Policies

In this section, we consider our first research question (RQ1) on the factors influencing the password policies deployed by web administrators. Specifically, we look at four core aspects of password policies that affect the construction of and updates to passwords: 1) password composition requirements, 2) disallowed passwords, 3) password expiration and 4) password change restrictions.

4.1. Password Composition Requirements

We asked participants about the factors influencing their site's password composition requirements, specifically focusing on password length constraints, required character classes, and allowed password characters.

System Compatibility. A widely discussed factor (7 out of 11 participants) affecting password composition requirements was compatibility with existing system constraints.

Password Length. For 2 participants, compatibility concerns affected the maximum password length allowed (we note that participants did not mention this factor as affecting minimum password lengths). For example, P3 stated that *"Our database table limits the password length"*, demonstrating how the configuration of their password storage system impacted the maximum password length.

Character Classes Required. Two administrators mentioned that compatibility aspects influenced which character classes they required in their password composition policy. For example, P5 described how their underlying password storage did not support some special characters, so they required only three character classes. Thus, compatibility issues could reduce the set of required character classes.

Disallowed Characters. Seven participants highlighted compatibility issues as a key reason behind which characters were disallowed in passwords. As an example, P10 described how certain special characters require careful encoding for their authentication software to handle correctly, and chose not to support such characters to avoid errors. Meanwhile, P1 disallowed passwords with certain special characters (e.g.,*"&"*, *"?"*) as they observed a common issue where their users would copy/paste passwords from other locations (e.g., password managers) during login, but for certain user environments, these special characters would not copy/paste correctly, resulting in failed login attempts. Similarly, P2 indicated that *"We're only accepting English characters. That's because our program understands only those right."* We note that such policies constrain password selection for non-English speaking users (although P2 did not explicitly mention issues with international users). Overall, such compatibility concerns limited the characters allowed in passwords.

Security Concerns. Security considerations were another common factor in the design of our participants' password composition policies, mentioned by 6 participants.

Password Length. Three participants mentioned security as a key factor in requiring longer passwords. For example, P2 chose a minimum password length of 8, arguing that *"If you have 8 characters...cracking the password is kind of harder."* Overall, participants generally considered longer passwords more secure, aligning with modern NIST guidelines [48] and research recommendations [8], [49], [50].

P3 was an interesting case where security considerations led to shorter password requirements, so long as two-factor authentication (2FA) was enabled. They said that *"We looked at the security benefit of two-factor and felt like we could maintain the same security with fewer characters because the password was less important to the overall scheme of security. Thus, reducing length from 11 to 8 seemed like a good balance and also kind of a carrot to encourage people to sign up for two-factor."*

Character Classes Required. Five participants discussed requiring passwords to contain multiple character classes to make them more secure. For example, P8 required passwords to contain one of each character class (lowercase letters, uppercase letters, digits, and special characters), justifying this decision as *"Just trying to be as secure as possible really and the more options you have character type-wise, the more chances [a password] could be safer."*

Disallowed Characters. We did not observe security concerns relevant to disallowing certain password characters.

Usability Concerns. Usability considerations were as prominently discussed by our study participants as security issues, mentioned by 6 out of 11 interview subjects.

Password Length. We observed 5 participants selecting password length requirements partly due to usability reasons. For P2, usability factors led them to limit passwords to 16 characters. They stated that even though having a long password is more secure, limiting the password length was necessary because users often forgot long passwords. In the opposite direction, P6 and P9 did not limit password lengths to allow users to pick long passwords if they choose to, such as if they rely on password managers or random password generators. For example, P6's view was *"hey if you want a really long one [password], go ahead."*

Character Classes Required. Two participants indicated that they considered usability aspects in deciding character class requirements, particularly for limiting the number of required classes. For example, P9 avoided even more extensive character class requirements because *"we don't want to limit the style of passwords...by dictating that there's too many of any one character [type]."*

Disallowed Characters. We observed 4 participants disallowing certain characters to promote authentication usability. As an example, P3 disallowed special characters in passwords to better support international users, saying that *"One of the challenges is with international users who do not speak English as a first language. We wanted to be able to set passwords that we could read to them [users] over the phone, because we do lots of phone support. So getting into the punctuation marks...would be hard."* P6 similarly disallowed spaces in passwords because *"I think most people are not familiar with using spaces, and so not allowing it just*

makes things easier." These opinions are counter to modern guidance on giving users maximum flexibility in selecting their passwords to promote usability [48].

Guidelines/Standards. Many participants (5 out of 11) mentioned that industry standards and the policies of other trusted websites influenced their own site's policy. P11 said that *"Our initial password composition requirements were primarily selected based on information security standards like this special publication, NIST 800-63B."* Meanwhile, P4 and P6 indicated that they took guidance from the policies of popular websites like Facebook and Google. Participants also discussed obtaining information from other sources such as technical papers and security blogs.

Other Factors. Three administrators indicated that their password composition policies were influenced by external stakeholders, such as users or customers. For example, P10 managed an elementary school website and had initially deployed a more complex password policy. However, parents of the students requested a simpler password policy because students had trouble creating and remembering the more complex passwords. P10 obliged, saying that they felt that their system's data was not particularly sensitive but would likely have pushed back against the change otherwise.

Three administrators additionally discussed how their policies followed the defaults in the software they used. For example, P10 said that by default, their software *"requires at least one lower letter, one upper letter, a digit, and a special character combination."*

P3 and P11 also discussed how different password policies were deployed based on the account type. P11 said *"We have different systems that serve different types of clients. So the system we have that serves more security-sensitive clients has a higher default standard based on the password requirements...I believe for our least security-sensitive instance, you will only have a length requirement, and there are no composition requirements. For our more secure instances where we have some external compliance requirements, we do require a different composition of characters."* Interestingly, NIST's latest authentication guideline [48] suggests that the most secure password composition policy only requires sufficiently long passwords without further compositional constraints (although NIST recommends further password checks, discussed in § 4.2), which actually matches P11's policy for less security-sensitive clients.

4.2. Disallowed Passwords

Beyond password composition requirements, websites may disallow the use of certain passwords, checking for repetitive/sequential patterns in passwords (e.g., *aaaa*, *1234*), passwords with personal information (PII), commonly used passwords, passwords with common dictionary words, or breached passwords. These checks are widely recommended, such as by NIST's latest password guideline [48]. We explored why participants do or do not deploy these checks, and how such checks are implemented.

4.2.1. Deploying Password Checks

We first assess the factors that contributed to deploying such password checks.

Security Concerns. All 8 participants deploying password checks brought up security concerns as motivation. Four participants who disallowed passwords with repeating/sequential patterns argued that such passwords were simpler and easy to guess. For example, P2 said *"Let's say "aaaa". It is too obvious...so we don't allow any types of things that the people can crack easily."* According to 5 participants who disallowed passwords containing PII, such passwords are similarly straightforward to attack. P9 exemplified this, saying that *"It seems pretty easy, just a simple brute force attack to copy-paste the username."* Three participants also discussed similar security benefits from preventing common passwords, as did the two participants blocking breached passwords and the one participant blocking passwords with dictionary words. These administrators said that there are many public datasets to find such passwords, which are often used in brute-force attacks.

Software Defaults. Three participants indicated that they employed certain password checks, as they were enabled by default through their software systems. For example, P10 mentioned that their authentication process relied on Windows Active Directory, which provides some password checks automatically. In another case, P9 said that their authentication system integrates with a third-party tool that automatically disallows common passwords. These cases highlight how existing software support for these checks reduces the barriers to adoption, resulting in broader use of such password checks (which are widely recommended, such as by NIST's 2017 guidelines [48]).

Guidelines/Standards. Two participants mentioned that they followed common industry standards or guidelines when deciding to employ password checks. For example, P2 mentioned that most companies follow similar guidelines, structures, and rules when disallowing repetitive/sequential passwords and passwords with PII.

4.2.2. Passwords to Check Against

For participants who employed password checks, we asked about how they determined the list of passwords to check against, particularly for dictionary words, common passwords, and breached passwords.

Online Resources. Six participants indicated that there are many online resources for passwords to block. For example, P9 mentioned that breached passwords are distributed (sometimes even sold) online, and they update their set of disallowed passwords with new breached datasets. Similarly, P1 said *"From reading blog posts, I enlarged my list."*

Personally Curated Lists. Three participants mentioned that their lists of blocked passwords were curated over time, through their prior experiences. For example, P2 mentioned that they maintained their checklist throughout their career.

Analysis of User Behavior. Three participants indicated that they monitor the passwords chosen by their users and identify popular passwords to potentially block. For example, P2 mentioned that if they noticed easy-to-guess

passwords being commonly used in their system, they added them to their list of blocked passwords, forcing password changes for existing users. Similarly, P7 recalled blocking a password because *"there was one [password] that people were using a lot because there was a really popular song."*

4.2.3. Not Deploying Password Checks

While most of our participants employed some form of password checking, none applied all of the password checks that we explored. When a participant did not implement a check, we investigated the reasons behind such a decision.

Implementation Challenges. Five participants mentioned that they did not add password checks because of technical limitations. For example, P1 said that they found it hard to implement leaked password checks because it would require significant technical work, which they were not prepared for. P9 and P10 similarly discussed how implementing the remaining checks would be complex, but both indicated that they would have applied these checks if their software supported it already by default.

Competing Priorities. Five participants explained that they did not implement certain password checks because they had to focus on other competing priorities. For example, P3 believed that their password policy was secure enough, particularly with two-factor authentication (2FA), and implementing all of these checks was not a priority. They said *"It [password policy] is not an area that we try to make more secure very often. We've been working on things [2FA] that make a bigger difference."* Similarly, P8 mentioned that they had not yet implemented password checks because they had to prioritize other website administrative aspects.

Usability Concerns. Two participants brought up usability concerns when employing password checks. P2 did not block dictionary words in passwords to avoid overly constraining user password choices. We note that P2 did block breached passwords, but limited the set of blocklisted passwords to only top leaked passwords, explaining that millions of passwords have been breached in recent years, and they did not want to prevent users from using all of those passwords. Meanwhile, P3 only prevented passwords with PII, explaining that they did not implement other checks because providing clear information about rejected passwords can be challenging, and existing standards (e.g., NIST's 2017 guidelines [48]) do not provide guidance on presenting users with feedback.

4.3. Password Expiration

While no longer recommended [48], websites often force their users to periodically change their passwords, expiring their passwords after a period. We asked our participants about whether they enforced password expiration, and the factors behind their decisions.

4.3.1. Deploying Password Expiration

In total, 7 of our participants still enforced such a policy. We asked these participants why they chose to do so.

Security Concerns. Six participants employed password expiration due to security concerns. For example, P2 stated that they required users to change their passwords every six months to combat frequent password sharing among users. In addition, P2 indicated that expiring passwords allowed them to combat vulnerable passwords by enforcing checks on the newly chosen passwords. Similarly, P10 mentioned that if a password is compromised, changing it frequently could be a way to reduce the risk of the account being hijacked, saying *"As a webmaster, you have maybe millions of users. You cannot guarantee that users are storing their passwords securely. It can be compromised. But if you force them to change it, the attacker can not access this website."*

Guidelines/Standards. Six participants said that requiring password expiration is standard practice. For example, P11 discussed how they followed an older version of NIST's password guidelines [51] when designing their authentication system. This case highlights the staying power of older recommendations, as the newer NIST 2017 guidelines explicitly recommend avoiding password expiration [48].

4.3.2. Expiration Period

We asked our participants who expired passwords about how they determined the expiration period.

Guidelines/Standards. Six participants selected a 90-day password expiration period, saying that they took guidance from existing standards (such as the outdated NIST authentication guideline [51]).

Other Factor. The remaining participant, P7, managed a school website and chose to expire passwords each term.

4.3.3. Not Deploying Password Expiration

For the four participants who did not use password expiration, we asked them why.

Usability Concerns. All four participants mentioned usability concerns with password expiration. For example, P8 said that while password expiration might provide security benefits, it would come with usability costs. They said that with forced password changes, *"it's harder for people to remember their logins and stuff, and not everybody likes to use password management tools."* Similarly, P9 said that forced password changes are annoying for users. Even though P11 did employ password expiration, they had usability concerns too, saying that *"They [users] may be inclined to choose poor passwords if they are being rotated all the time because they are sort of put on the spot to come up with a new password."*

Limited Benefits. Three participants indicated that they felt password expiration would provide limited benefits. P4 and P6 said that their authentication system was secure enough without forced password resets. P9 believed that they did not require password expiration because if an account's password is not in a known breach and meets the site's standard for being a strong password, then the risk of cracking the password is low.

4.4. Password Change Restrictions

When passwords are expired (or users choose to update their passwords), websites may employ policies preventing the new password from matching or being similar

to old passwords, and limiting how frequently users can change passwords. We asked our participants whether they employed such policies and why. In total, 7 participants disallowed choosing old passwords, 2 prevented the use of similar ones, and 4 rate-limited password changes.

4.4.1. Deploying Password Change Restrictions

We asked participants who deployed password change restrictions about the factors that affected their decisions.

Security Concerns. Six participants indicated that they disallowed users to reuse their old passwords during password changes because of security concerns. P10 and P11 mentioned that such a policy helped prevent compromised passwords from reappearing in their systems. As an example, P11 said that *"If someone is cycling through a small number of passwords and one of them were to be compromised, and we did not know about it, then there is a reasonable chance that the person would just switch back to that password that had been compromised, and then it would no longer be securing access to the account."* P2 and P4 were the only two participants also checking the similarity between a newly selected password and an old password. They described security benefits from doing so. For example, P2 said that if an attacker had an account's old password and wanted to gain access using that, it would be hard to guess the account's new password if similar passwords were not allowed.

Security concerns were also the primary driver behind limiting how frequently passwords could be changed, as discussed by all four participants doing so. One case is where rate limiting is tied to disallowing old passwords. For example, P3 implemented both policies to dissuade users from just initiating a sequence of password changes that allowed them to return back to their original old password. Another case is limiting password changes to combat compromise. For example, P11 said that they only allowed users to change their passwords once daily because if a user conducts a password reset to protect their account, an attacker could not quickly change the password again as well. P11 explained *"If someone's password reset operation was compromised, then an attacker would immediately try to reset [the password] to persist access to that account with some password that the attacker knows."* P11 did bring up that if users wanted to change their passwords more than once a day, they could contact customer support to verify their identity.

Guidelines/Standards. Four participants said that they employed password change restrictions as they were recommended by common guidelines and standards. For example, P11 mentioned that such restrictions are recommended by Microsoft and NIST. Two administrators also drew inspiration from other popular websites with similar policies.

Other Factors. P10 mentioned that their software implemented password change restrictions by default, so they simply kept the default configuration. Meanwhile, P5 explained that they rate limited to ensure that password changes would have enough time to fully propagate across their backend authentication systems.

4.4.2. Deciding Password Change Policy Parameters

We asked our participants who employed password change restrictions about how they chose the length of password history to track and the password change rate limit.

Guidelines/Standards. Four participants indicated that they followed common guidelines or standards in selecting password change policy parameters. For example, P11 indicated that their password history consists of a user's previous 24 passwords and users could change passwords once a day, as these parameters are recommended by Microsoft [52]. Two additional participants mentioned deciding on parameters based on the policies they observed on other secure sites (such as financial institutions).

Usability Concerns. Three participants discussed usability aspects affecting their password change policy. For example, P1 said that users would need to remember more passwords if they extended their password history beyond 3 previous passwords. P2 mentioned that when considering the balance between usability and security, they did not want to overly burden users by requiring them to remember more passwords or disallowing frequent password updates.

Other Factors. As P10's software supported password change restrictions by default, they just used the default parameters. Meanwhile, P5 selected a password change rate limit that ensured password changes would propagate through their systems.

4.4.3. Not Deploying Password Change Restrictions

For participants who did not deploy certain password change restrictions, we asked them why they chose not to.

Implementation Challenges. Four participants mentioned that they did not implement certain password change restrictions (particularly similar password checks) due to implementation challenges. Three of these participants said that implementing such restrictions would require non-trivial engineering effort, although they would deploy them if their software already supported such features.

Limited Benefits. Three participants discussed how they saw little value in enforcing password change restrictions. P4 considered their authentication system secure enough, without needing to limit password changes. Meanwhile, P9 and P11 both did not believe that the similarity checks are meaningful because the primary threat to accounts is credential stuffing attacks, where attackers only automatically test the exact passwords from data leaks, so similar passwords would not be successfully targeted. In particular, P9 argued that their deployment of breached password checking was sufficient, countering the primary credential stuffing threat. However, modern guidelines [48] recommend both password checks and change restrictions.

Other Factors. Two participants (P5 and P6) mentioned that they did not employ password similarity checks for usability reasons. P5 stated that they wanted to make it easy for users to remember their passwords. Meanwhile, P6 indicated that providing clear feedback to users about the similarities between old and new passwords is challenging, saying *"I think people will wonder what makes this password similar to the old one."* An additional two participants

(P7 and P8) indicated that they had not been aware of such policies and their security benefits. P7 at least indicated that learning about such policies was informative and that they may implement such restrictions in the future.

5. RQ2: Considerations for Updating Policies

In this section, we tackle our second research question (RQ2) which investigates the considerations that arise when making changes to a website's password policy. In particular, we explore why changes could be initiated, what the modification process entails, and what challenges administrators might face during the update process.

5.1. Update Reasons

We first asked our participants about what reasons could drive changes to their website's password policy.

Security Concerns. Eight participants discussed security concerns as motivation for updating a site's policy. For example, P1 and P10 both recalled switching their password policy in the past to a more secure one when they faced security issues. P1 said that *"At the beginning of my career, I adopted a less secure password policy, but after a few years, we faced some security issues and we changed our password policy to a more secure one."* Meanwhile, P10 mentioned previously detecting unauthorized users in their system and subsequently updating their website's password policy to one they believed was more secure. While P6 had not experienced a security incident themselves, they said that if a major security event occurred, such as a significant data breach, they would re-evaluate their password policy and consider updating it as necessary.

Staying Modern. Another common factor, also discussed by eight participants, was updating policies to keep them relevant. One dimension was in keeping policies sufficient against current threats. For example, P2 said that they might strengthen their policy as passwords were easier to crack, since *"the computing powers of processors are better now."* P5 and P10 similarly highlighted how modern CPUs and GPUs made brute-force password attacks much more effective, and subsequent developments in attacking passwords could spur them to change their policy (particularly in increasing password length minimums). Another dimension was in keeping policies aligned with modern recommendations. P11 said that *"I mentioned that we are not currently up to date with the latest NIST recommendations, and I think it would be great for us to get onto that."* Similarly, P9 said that changes to the standard that they adhere to would result in their policy being updated to remain in compliance.

Usability Concerns. Three participants discussed usability concerns as a driver behind policy updates. For example, P3 argued that they should make their policy more usable, as they employed 2FA, which provides adequate security. Meanwhile, P11 mentioned that they would like to eliminate password expiration to improve usability. Similarly, as discussed in § 4.1, P10 had previously simplified their password composition policy to make it more usable for their site's users (i.e., students).

User Requests. Three participants discussed updating policies in response to user feedback or requests. For example, P2 stated that they would evaluate external requests to update a password policy against industry standards, trying to keep usability and security balanced. Similarly, P8 said that *"If people want them [the password policies] to be updated, that would be a reason for me."*

Other Factors. P5 indicated that implementation changes could support changes to their password policy. Specifically, if they switched away from their current authentication software, which limits passwords to 64 characters, they would select a new software that would allow them to increase their maximum password length. Another implementation-related aspect was discussed by P3, who had previously explained that they applied different policies to different accounts. P3 said that they may further update their policies as they extend their classification of accounts to new user categories (e.g., administrators, test users).

5.2. Policy Updating Process

We next asked participants about the process for enacting a password policy update. Specifically, we investigated the organizational aspects of the update process and what would be involved when rolling out a new policy.

5.2.1. Organizational Logistics

We asked participants about the organizational facets of the password policy updating process, focusing on who would make decisions during the process and how the update was coordinated.

Initiating the Update Process. We asked our participants about who in their organization would initiate the password policy update process. The most common response from our participants (7 out of 11) was that the organization's management or leadership would officially initiate the updating process. Four of these participants explicitly indicated that they could suggest a policy update to their managers, but it was ultimately management that decided whether to start the process. The remaining four participants indicated that they could initiate the process as administrators, although others in the organization would be involved.

Decision Making during the Update Process. We asked participants about who made password policy decisions during the update process. Five participants described a top-down organization at their company, where management/leadership would make the final decisions on the password policy changes, and administrators or developers would implement the changes. As an exemplar of this model, P1 described their decision-making workflow as *"It is a top to bottom approach. First, the manager decides to move to a more secure point. Then the analyst decides when to implement the password policy, and what's the new password policy. And the developer implements the policy."* This workflow was particularly prominent when a participant's organization aimed to comply with a security standard, as the organization management had to satisfy the security requirements. This was the case for P3, who explained, *"Auditors came and reviewed our compliance...They wrote*

in a report somewhere that we have a password history of four, and the requirements are to have a password history of five. So security shared that with our director, and our director told us to fix that and so we went through change management and fixed it." Similarly, P5 said that their management could mandate a new policy, and that they would need to implement it then.

The remaining 6 participants described the decision-making process as collaborative, where they converged on decisions with other stakeholders (including management). For example, P9 described working with others before making changes, saying *"I do need to make sure that people are informed and it's also within my responsibilities to consult with people before I do it."* Similarly, P8 explained that the decision-making process involved themselves and management, indicating that *"we typically will talk through it together."* P11 said that the amount of collaboration varies and *"will depend a little bit on the scope of the change"*, where for a minor change, they would *"just make the change, roll it out"*, but for larger changes, *"teams or individuals across the company are going to be involved in the decision-making process."*

Coordination between Stakeholders. We asked participants about how the password policy update process was coordinated between stakeholders. Five participants mentioned that they would form a team of stakeholders while deciding on password policy updates, and discuss the changes with team members. For instance, P4 said that when they went through the policy update process in the past, they would create different teams to handle different aspects of the update process: *"there was a design team and a development team."* Meanwhile, P11 described engaging with the team of stakeholders, saying *"I get all team members' opinions...So we discuss it together and decide."* P1 discussed communicating between the different stakeholders: *"We have meetings before the implementation...If there is a challenge while implementing, we communicate with each other through Slack channels or reschedule more meetings."* P5 also said that *"Meetings are held between the teams and there may be either email or documentation shared."*

5.2.2. Deploying the New Policy

Finally, we asked our participants about what their process was for rolling out a new policy. We observed several common topics, including testing the policy before deployment, implementing the policy, and handling old passwords that no longer satisfy the new policy. We also note that the majority (9 out of 11) of our participants employed involved updating processes (e.g., implementing new code), as only two participants (P9 and P10) described simpler deployment methods centered on configuring through user interfaces.

Testing. Five participants indicated that they had a testing stage as part of their deployment process, allowing them to check that the changes did not negatively affect their authentication system's implementation. For example, P1 explained that they first deployed an updated policy to their test systems, then tested it using demo users and passwords. They manually performed general user activity workflows, such as logging into the system and changing passwords, to self-evaluate the usability and security of the system. P11 mentioned that password policy changes could potentially cause significant disruption to their authentication workflow, so they also used a testing phase. Describing a past update, P11 said *"We got a test group of users, sort of early adopters, who volunteered to try that [the updated policy] out first. Then we worked with them to collect feedback on how well it was working, any challenges that they ran into, and smooth out some of the bumps. After we had completed the test group and captured that feedback, then we went ahead with a broader rollout."* Three administrators said that they test the security of their password policies. While P1 self-assessed their policy's security through their test system, P9 and P10 used penetration tests for evaluation. None of the other participants discussed any empirical assessments of password policy security.

Implementation. We asked participants about the password policy implementation process. All of our participants said that many changes could be straightforward to deploy, particularly if the new policy is similar to the old one but just with different parameter values (e.g., different password length requirements). For example, P9 and P10 both mentioned that they could just use their authentication system's administrative interface to reconfigure policy parameters and push out the new policy. Specifically, P9 said that *"I'd log into the administrative console and go to the password policy settings, change, then press save. Done."* Meanwhile, P6 explained that many changes *"would be relatively quick, can be done in a day. A lot of it is just front-end, changing the validation checks."* Similarly, P4 said *"We just change the requirements by writing regexes and we can test. It's really easy. It's just one line of code."*

However, many of these participants indicated that more complex changes would require more effort and time. For example, P3 said that *"It's a very small fraction of the effort to tweak a policy than it is to put in a completely different check that we haven't built the plumbing for."* Meanwhile, P5 thought that changes affecting their backend password storage could be more significant, saying that *"It depends on the change and if it is something that affects the technical aspects of the password store or not."*

Handling Old Passwords. One particularly tricky aspect of updating a password policy is how to handle user passwords that no longer satisfy the new policy. We asked our participants about how they handled this situation.

Notifications. Before a new password policy is deployed, nine of our participants explicitly discussed notifying users to change their passwords to comply with the new policy. These notifications could also explain why the new policy was being put in place. For example, P4 said *"We can send alert notifications or these type of things to change their [users'] passwords."*

Forcing Password Resets. Eight participants said that one option they would consider is forcing password resets for their users, requiring them to select new passwords that comply with the updated password policy. P1 described their process as *"After deploying the change, we force the users*

to change their passwords. During the password change, we enforce the new policy." Similarly, P9's method was *"An email is sent to the user, their account is suspended immediately, pending a password recovery or change."* P3 also forced users to change their passwords, but did so gradually by starting with small subsets of users before resetting passwords for larger groups of users. They explained that this strategy avoided having too many users change their passwords in a short period of time, while also potentially allowing them to catch deployment issues early on.

Natural Decay. Five of our participants said that they would consider letting non-compliant passwords gradually fade over time. Two of them (P5 and P11) also indicated that they would consider forcing password resets, but only in security-critical situations (e.g., a major data breach), thus illustrating that the method deployed depended on the reason behind the policy update. Notifications were paired with this natural decay approach, where the administrators hoped that many users would update their passwords once given notice. As password expiration was broadly used by our participants (§ 4.3), many users would need to eventually change their passwords to conform with the new policy. For example, P5 said that they *"let the passwords age out and then we know within a while of implementing [the policy] that technically people will evolve to comply with it."* Similarly, P11 said *"you allow people to continue using their non-compliant password until the next time that they change the password and then you require them to change it to something that follows the new password policy."*

5.3. Challenges

Finally, we asked our study's administrators about challenges faced while deploying an updated password policy.

Technical Challenges. Broadly across our participants (7 out of 11), we heard of potential technical challenges when implementing a new password policy. For example, three participants indicated that adding a check disallowing breached passwords would be difficult. P5 also described how changes affecting password storage would be complicated to resolve, saying *"We knew that 64 characters were the maximum for the password store. If we wanted to change it to 68, well, then we would have to find some way of making our password store support that change."* Similarly, as authentication systems can entail multiple components, ensuring that an update is fully propagated across an entire system can be challenging. P10 exemplified this case by highlighting how there were multiple dependencies on their authentication API, and certain policy updates (e.g., password expiration periods) required changes at dependent components, otherwise authentication errors could occur.

User Backlash. Six of our participants described user backlash against a new policy as a difficult situation to handle. For instance, P5 said that if they deployed a more complex password policy, *"we would get some pushback from people, like why do we have to do that?"* Similarly, P10 got user complaints about their password policy in the past, and simplified the policy as a result. In this case, P10 said that this was acceptable as their system's data was not very sensitive, otherwise they would not have simplified.

Organizational Hurdles. Several participants described various challenges that arose through implementing the policy update as part of an organization. For instance, P7 mentioned that their team lacked the budget to implement features (specifically breached password checks). Meanwhile, P6 indicated that converging on policy changes as a team was an involved task, saying *"I think that will take the longest part of deciding...multiple meetings over the course of weeks, to finalize like okay this is what we want for our policy."* P11 believed that changing certain policy parameters away from what their organization management requested would be hard, saying that such changes *"would not be quick. We would have to go through some sort of exception process to get approval."*

6. Concluding Discussion

Through our study of website administrators and their management of online password policies, we identified the key factors that influence policy decisions (RQ1) and the considerations that arise when updating policies (RQ2). In this section, we conclude by summarizing our findings, synthesizing the lessons learned, providing grounded recommendations for the research community to better support the activities of web administrators, and suggesting directions for future research.

6.1. Study Summary

We first summarize our study's core findings.

6.1.1. Key Factors Affecting Password Policy Decisions

While our study found many factors involved in password policy decisions, we observed four recurrent factors.

Security. One common factor that affected many password policy decisions was security concerns. Those concerns influenced administrators when deciding on various policy parameters, such as the minimum password length, required character classes, disallowing certain passwords, expiring passwords, and applying restrictions during password changes (§§ 4.1, 4.2.1, 4.3.1 and 4.4.1). In some cases, administrators did not employ a certain policy because they believed it would provide limited security benefits. For example, as discussed in § 4.3.3, three participants did not believe that password expirations provided security benefits. We also note that in §§ 4.1 and 4.3.1, we found that some administrators implemented policies that they believed were most secure, but which modern guidelines no longer recommend (e.g., requiring multiple character classes).

Usability. Our participants were well-aware of and deeply considered usability aspects in their password policy design, particularly when determining password lengths, character type requirements, disallowed characters, disallowed passwords, password expiration, and password change restrictions (§§ 4.1, 4.2.3, 4.3.3, 4.4.2 and 4.4.3). In many cases, participants chose not to enforce a policy to reduce user burden/friction, such as our participant disallowing special characters in passwords to facilitate phone

support for international users (§ 4.1). We also observed cases where users could influence a policy based on their behavior or feedback, such as in § 4.1, where a participant adjusted their password policy to be more amenable to their specialized user base (elementary school children).

System Influences. The password policy design is entangled with the underlying system implementation, which we observed manifesting in multiple ways throughout our study. In § 4.1, we observed system compatibility issues constraining the choice of maximum password lengths, required character classes, and allowed password characters. For example, we saw that database configurations could constrain the maximum password length. Implementation challenges also prevented some administrators from disallowing certain passwords and enforcing password change restrictions (§§ 4.2.3 and 4.4.3). In the opposite direction, we observed that software support and defaults facilitated the deployment of password composition policies and restrictions on allowed passwords and password changes (§§ 4.1, 4.2.1 and 4.4.1).

Guidelines/Standards. We observed guidelines and standards as key factors in all facets of password policy decisions. Web administrators relied upon this guidance when determining password composition policies, disallowed passwords, password expiration, and password change restrictions (§ 4). In § 4.3, we did observe several cases where administrators seemed to adhere to more dated guidelines rather than modern ones. We also observed shortcomings of current standards, where some participants did not block certain types of passwords because they lacked guidance on how to provide meaningful feedback to the user (§§ 4.2.3 and 4.4.3).

6.1.2. Challenges With Managing Password Policies

We observed various challenges experienced by our study participants, falling into three broad categories.

Design Challenges. Throughout our study, our participants identified the importance of both security and usability considerations in the design of password policies. However, they often highlighted that there exists a tension between the two facets, and that it could be difficult to decide how to balance the two. As a consequence, administrators often sought guidance, although we observed that information could come from a large and diverse set of sources. In several cases, administrators had to proactively seek out such information, and we did not observe a single central authority for password policy guidance (§§ 4.1, 4.2.1, 4.3.1, 4.3.2, 4.4.1 and 4.4.2). We did find that many participants relied on common industry guidelines and standards, such as those of NIST and prominent technology companies (e.g., Microsoft). However, several participants discussed challenges with keeping up with modern recommendations (§ 5.3), and we noted that many administrators demonstrated mental models aligned with the older recommendations (§§ 4.1 and 4.3.1), illuminating how there exist barriers to incorporating more up-to-date guidance.

Competing Interests. Our study observed that administrator priorities are pulled in various directions beyond their own volition, sometimes preventing them from managing their website's password policies as they would like. This includes needing to focus on other non-password policy tasks as part of their responsibilities as web administrators (e.g., implementing 2FA, as discussed by a participant in § 4.2.3), as well as often adhering to the decisions put forth by their organization's management (§§ 5.2.1 and 5.3). We also observed that in many cases, the management of password policies required input from various other stakeholders, including potentially the feedback from the site's users (§§ 4.1, 5.1 and 5.2).

Deployment Challenges. Our participants highlighted that they frequently encountered implementation and deployment hurdles when managing password policies. These challenges include technical barriers, such as those preventing the implementation of certain policies and dealing with system inconsistencies (§§ 4 and 5). As discussed in § 5.2.1, logistical difficulties also occur, particularly when communicating and coordinating a new policy deployment. For example, when deploying a new policy, administrators need to carefully plan out some process of rolling non-conformant passwords to the new policy (§ 5.2.2).

6.2. Lessons Learned and Recommendations

Based on the challenges that we observed web administrators encountering when managing password policies, as well as the reasons behind their decisions, we distill lessons learned and recommendations for the research community, including directions for future work.

Need for better software support and defaults. Our study found that the software used by web administrators can heavily influence the password policies they employ. Several administrators deployed certain policy components, such as checks for disallowed passwords or password history tracking, as they were supported either by default or as an available feature of their software (§§ 4.1, 4.2.1, 4.4.1 and 4.4.2). Many of our participants also discussed encountering challenges with implementing such functionalities, whether due to technical hurdles/limitations (§ 5.3) or needing to prioritize other efforts instead (§ 6.1.2), with several participants explicitly saying that they would have deployed certain password policy functionality had their software already supported it. Related, our study identified that many web administrators rely on their software's default configurations for selecting password policy parameters.

These cases highlight the value of providing recommended password policy features in common software that are used by web administrators today. Many websites are constructed using popular tools (e.g., content management systems like WordPress, Drupal, or Joomla) or software frameworks/libraries (e.g., Python's Django, Ruby on Rails). We recommend that the web development community integrates these password policy features (with recommended configurations for these features as defaults) into these widely-used software systems (ideally enabling the features by default). Such integration could help significantly broaden adoption, driving wider use of more secure and usable password policies.

Need for outreach and education. We observed throughout our study that many administrators exhibit outdated mental models about secure and usable password policies. For example, while modern password policy guidelines [48] and research [49] push for longer passwords with flexible composition requirements, checks against common and breached passwords, and no password expiration [48], [49], many of our participants deployed policies enforcing password complexity requirements and password expiration (§§ 4.1 and 4.3), likely influenced by dated recommendations (e.g., NIST's older 2004 guidelines [51]). We also found cases where some of our participants were unaware of recommended password policy actions, such as applying restrictions to password changes (§ 4.4.3). Furthermore, in § 5.2, we observed that password policy decisions often came from an organization's leadership or management, so it is likely that leadership/management individuals exhibit similarly dated perspectives about password policies.

We also found that our participants often still sought information from various other sources (§ 4). While our study did not investigate why this is the case (which future work could explore), we hypothesize that it could be partially due to difficulties with digesting modern standards. Password policies are complex, with various dimensions (as we saw throughout our study). Existing standard documents are often long and detailed [48], potentially making it challenging for administrators to digest and readily enact recommended policies. Exploring other formats for presenting guidelines, such as presenting details at different levels of granularity (e.g., a summary table of recommended password policy parameters versus detailed justifications) may assist administrators in better absorbing modern guidelines.

Together, these discrepancies between what web administrators (and managers) *believe* are secure and usable policies, and what is currently recommended [48], [49] highlight that updated recommendations are not enough on their own. There is a need for outreach and education efforts to better inform administrators and other stakeholders about modern password policy guidelines. One approach could be to directly notify administrators of websites employing weaker policies, communicating what the best practices today are. Prior work on security-related notifications [53]–[56] has found some value in such outreach efforts to administrators, although ultimately reaching most administrators remains a challenge. Another potential vector for outreach is through the various platforms that our participants often relied on for password policy guidance (§ 4), including developer-oriented forums and blogs (e.g., Stack Overflow), documentation released by popular websites and software vendors (e.g., Microsoft, Github), and social media outlets (e.g., LinkedIn, YouTube). Future efforts can evaluate the impact of information from these platforms on password policy decisions, and how best to drive the adoption of modern guidelines.

Need for expanded guidelines. Our findings reveal multiple areas for improving the existing authentication guidelines. One dimension is in providing guidance on handling different contexts, such as varying types of users and data stored for a site. In § 4.1, we observed administrators catering their policies to specialized populations (e.g., international users, children), often following their own intuition on policy decisions as existing standards only provide general guidance. Some administrators also felt that they did not need as secure of policies if their site managed less sensitive data. Research is needed into how password policies should be adapted for different situations, such as for less security-sensitive scenarios or certain subpopulations (e.g., children, elderly, or less-abled users). Overall, while existing guidelines provide flexibility in policy design, there is limited guidance on how to navigate these design decisions, especially when balancing usability versus security tradeoffs across varying contexts (e.g., 2FA is generally recommended, but may be less suitable for certain subpopulations, such as children or the elderly).

Moreover, we also found some confusion by administrators about the interplay between different authentication mechanisms. For example, some administrators incorrectly assumed that checking for breached passwords made password similarity and history checks irrelevant (§ 4.4.3). In other cases, we saw participants who modified their policy configurations when 2FA was used (§§ 4.1 and 5.1). While existing evaluations of the security and usability of password policies typically consider individual policy parameters in isolation, future work is needed to evaluate policies more holistically. Such exploration would support guidelines that better inform administrators about the interactions and overlap between various authentication layers.

Another dimension where guidelines can be expanded is in how administrators evaluate their policy, both in terms of usability and security, as existing standards (e.g., NIST [48], [51], Microsoft [52]) lack such guidance. In § 5.2.2, we observed few administrators providing any self-assessment of their site's policy. However, information on empirically assessing parameter values would help inform administrators on how best to determine usable and secure password policies for their specific environments.

Finally, we observed in §§ 4.2.3 and 4.4.3 that some administrators struggled with conveying clear, actionable feedback to users on their password policy decisions. This issue was particularly prominent for password checks, which several of our participants avoided employing as they did not know how to explain to users why a check failed. Prior work [57] identified that such feedback can drive users towards stronger passwords, but more investigation is warranted into how best to design the feedback interface, which would provide guidance to administrators on fully implementing such authentication mechanisms.

7. Acknowledgements

We thank our study participants for their contributions to this research, and the anonymous reviewers for their constructive feedback. This work was supported in part by the National Science Foundation award CNS-2055549. The opinions expressed in this paper do not necessarily reflect those of the research sponsors.

References

[1] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in IEEE Symposium on Security and Privacy (S&P), 2012.

[2] D. Florencio and C. Herley, "A Large-Scale Study of Web Password Habits," in International World Wide Web Conference (WWW), 2007.

[3] A. Hanamsagar, S. S. Woo, C. Kanich, and J. Mirkovic, "Leveraging Semantic Transformation to Investigate Password Habits and Their Causes," in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2018.

[4] P. G. Inglesant and M. A. Sasse, "The True Cost of Unusable Password Policies: Password Use in the Wild," in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2010.

[5] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of Passwords and People: Measuring the Effect of Password-Composition Policies," in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2011.

[6] M. Wei, M. Golla, and B. Ur, "The Password Doesn't Fall Far: How Service Influences Password Choice," Who Are You?! Adventures in Authentication Workshop (WAY), 2018.

[7] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering Stronger Password Requirements: User Attitudes and Behaviors," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2010.

[8] R. Shay, S. Komanduri, A. L. Durity, P. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Can Long Passwords Be Secure and Usable?" in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2014.

[9] R. Shay, L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, M. L. Mazurek, W. Melicher, S. M. Segreti, and B. Ur, "A Spoonful of Sugar?: The Impact of Guidance and Feedback on Password-Creation Behavior," in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2015.

[10] E. Stobert and R. Biddle, "The Password Life Cycle: User Behaviour in Managing Passwords," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2014.

[11] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, "Do Users' Perceptions of Password Security Match Reality?" in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2016.

[12] P. Mayer, J. Kirchner, and M. Volkamer, "A Second Look at Password Composition Policies in the Wild: Comparing Samples from 2010 and 2016," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2017.

[13] D. Florêncio and C. Herley, "Where Do Security Policies Come From?" in USENIX Symposium on Usable Privacy and Security (SOUPS), 2010.

[14] S. Preibusch and J. Bonneau, "The Password Game: Negative Externalities from Weak Password Practices," in International Conference on Decision and Game Theory for Security (GameSec), 2010.

[15] J. Bonneau and S. Preibusch, "The Password Thicket: Technical and Market Failures in Human Authentication on the Web," in Workshop on the Economics of Information Security (WEIS), 2010.

[16] D. Wang and P. Wang, "The Emperor's New Password Creation Policies," in European Symposium on Research in Computer Security (ESORICS), 2015.

[17] T. Seitz, M. Hartmann, J. Pfab, and S. Souque, "Do Differences in Password Policies Prevent Password Reuse?" in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2017.

[18] R. Dudheria, "Assessing password practices of mobile apps," International Journal of Computers and Applications, vol. 44, no. 1, pp. 64–82, 2022.

[19] A. Naiakshina, A. Danilova, C. Tiefenau, M. Herzog, S. Dechand, and M. Smith, "Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study," in ACM Conference on Computer and Communications Security (CCS), 2017.

[20] A. Naiakshina, A. Danilova, E. Gerlitz, E. Von Zezschwitz, and M. Smith, ""If you want, I can store the encrypted password": A Password-Storage Field Study with Freelance Developers," in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2019.

[21] H. Assal and S. Chiasson, "Security in the Software Development Lifecycle," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2018.

[22] R. Balebako, A. Marsh, J. Lin, J. I. Hong, and L. F. Cranor, "The Privacy and Security Behaviors of Smartphone App Developers," in Usable Security and Privacy Symposium (USEC), 2014.

[23] S. Bartsch, "Practitioners' Perspectives on Security in Agile Development," in International Conference on Availability, Reliability and Security (ARES), 2011.

[24] M. Christakis and C. Bird, "What Developers Want and Need from Program Analysis: An Empirical Study," in IEEE/ACM International Conference on Automated Software Engineering (ASE), 2016.

[25] S. Turpe, L. Kocksch, and A. Poller, "Penetration Tests a Turning Point in Security Practices? Organizational Challenges and Implications in a Software Development Team," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2016.

[26] A. Poller, L. Kocksch, S. Türpe, F. A. Epp, and K. Kinder-Kurlanda, "Can Security Become a Routine?: A Study of Organizational Change in an Agile Software Development Group," in ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW), 2017.

[27] M. Hilton, N. Nelson, T. Tunnell, D. Marinov, and D. Dig, "Trade-Offs in Continuous Integration: Assurance, Security, and Flexibility," in Joint Meeting on Foundations of Software Engineering (ESEC/FSE), 2017.

[28] E. Gerlitz, M. Häring, and M. Smith, "Please do not use!?_ or your License Plate Number: Analyzing Password Policies in German Companies," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2021.

[29] S. Furnell, "An assessment of website password practices," Computers & Security, vol. 26, no. 7-8, pp. 445–451, 2007.

[30] M. Mannan and P. C. Van Oorschot, "Security and Usability: The Gap in Real-World Online Banking," in Workshop on New Security Paradigms (NSPW), 2008.

[31] B. T. Kuhn and C. Garrison, "A Survey of Passwords from 2007 to 2009," in Information Security Curriculum Development Conference (InfoSecCD), 2009.

[32] S. Furnell, "Assessing password guidance and enforcement on leading websites," Computer Fraud & Security, vol. 2011, no. 12, pp. 10–18, 2011.

[33] T. W. Thomas, M. Tabassum, B. Chu, and H. Lipford, "Security During Application Development: an Application Security Expert Perspective," in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2018.

[34] C. Stransky, Y. Acar, D. C. Nguyen, D. Wermke, D. Kim, E. M. Redmiles, M. Backes, S. Garfinkel, M. L. Mazurek, and S. Fahl, "Lessons Learned from Using an Online Platform to Conduct Large-Scale, Online Controlled Security Experiments with Software Developers," in USENIX Workshop on Cyber Security Experimentation and Test (CSET), 2017.

[35] S. Fahl, M. Harbach, H. Perl, M. Koetter, and M. Smith, "Rethinking SSL Development in an Appified World," in ACM Conference on Computer and Communications Security (CCS), 2013.

[36] L. A. Goodman, "Snowball Sampling," The Annals of Mathematical Statistics, vol. 32, no. 1, pp. 148–170, 1961.

[37] J. M. Haney, M. Theofanos, Y. Acar, and S. S. Prettyman, ""We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2018.

[38] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. L. Mazurek, and C. Stransky, "Comparing the Usability of Cryptographic APIs," in IEEE Symposium on Security and Privacy (S&P), 2017.

[39] Y. Acar, C. Stransky, D. Wermke, M. L. Mazurek, and S. Fahl, "Security Developer Studies with GitHub Users: Exploring a Convenience Sample," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2017.

[40] E. Derr, S. Bugiel, S. Fahl, Y. Acar, and M. Backes, "Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android," in ACM Conference on Computer and Communications Security (CCS), 2017.

[41] A. Voronkov, L. A. Martucci, and S. Lindskog, "System Administrators Prefer Command Line Interfaces, Don't They? An Exploratory Study of Firewall Interfaces," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2019.

[42] C. Dietrich, K. Krombholz, K. Borgolte, and T. Fiebig, "Investigating System Operators' Perspective on Security Misconfigurations," in ACM Conference on Computer and Communications Security (CCS), 2018.

[43] J. M. Haney and W. G. Lutters, ""It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2018.

[44] P. L. Gorski, L. L. Iacono, D. Wermke, C. Stransky, S. Möller, Y. Acar, and S. Fahl, "Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic API Misuse," in USENIX Symposium on Usable Privacy and Security (SOUPS), 2018.

[45] V. Braun and V. Clarke, Thematic Analysis. American Psychological Association, 2012.

[46] L. L. Kupper and K. B. Hafner, "On Assessing Interrater Agreement for Multiple Attribute Responses," Biometrics, vol. 45, no. 3, pp. 957–967, 1989.

[47] D. Armstrong, A. Gosling, J. Weinman, and T. Marteau, "The Place of Inter-Rater Reliability in Qualitative Research: An Empirical Study," Sociology, vol. 31, no. 3, pp. 597–606, 1997.

[48] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, and M. F. Theofanos, "NIST Special Publication 800-63b: Digital Identity Guidelines," National Institute of Standards and Technology (NIST), 2017.

[49] J. Tan, L. Bauer, N. Christin, and L. F. Cranor, "Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements," in ACM Conference on Computer and Communications Security (CCS), 2020.

[50] R. Shay, S. Komanduri, A. L. Durity, P. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Designing Password Policies for Strength and Usability," ACM Transactions on Information and System Security (TISSEC), vol. 18, no. 4, pp. 1–34, 2016.

[51] W. Burr, D. Dodson, and W. T. Polk, "NIST Special Publication 800-63-2: Electronic Authentication Guidelines," National Institute of Standards and Technology (NIST), 2014.

[52] Microsoft, "Enforce password history," https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/enforce-password-history, 2021.

[53] B. Stock, G. Pellegrino, F. Li, M. Backes, and C. Rossow, "Didn't You Hear Me? Towards More Successful Web Vulnerability Notifications," in Network and Distributed System Security Symposium (NDSS), 2018.

[54] F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey, D. McCoy, S. Savage, and V. Paxson, "You've Got Vulnerability: Exploring Effective Vulnerability Notifications," in USENIX Security Symposium, 2016.

[55] F. Li, G. Ho, E. Kuan, Y. Niu, L. Ballard, K. Thomas, E. Bursztein, and V. Paxson, "Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension," in International World Wide Web Conference (WWW), 2016.

[56] B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, "Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification," in USENIX Security Symposium, 2016.

[57] B. Ur, F. Alfieri, M. Aung, L. Bauer, N. Christin, J. Colnago, L. F. Cranor, H. Dixon, P. Emami Naeini, H. Habib, N. Johnson, and W. Melicher, "Design and Evaluation of a Data-Driven Password Meter," in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2017.

Appendix

Recruitment Text

We are researchers at *UNIVERSITY*, doing a research study to investigate the password practices of web administrators/web developers. Our motivation is to understand the reasons behind deploying certain password policies.

We are looking for web administrators/developers who have managed a website and its password policies to participate in a short survey (<5 min) followed by an approximately 30-45 minutes interview. Your participation would be very valuable to us. Please consider taking part in our study and/or forwarding our invitation to one of your colleagues who might be interested!

If interested in participating, please fill out the short pre-interview survey here (*LINK*), and we will reach out to you using your preferred email address for the interview.

Survey Questions

Please think about one of your websites that you have managed and its password policy, and answer the following survey questions about that site's password policy.

1) What are the minimum and maximum password lengths allowed on your website?
   a) Minimum length: ___ b) Maximum length: ___
   c) No minimum length d) No maximum length
2) What are the minimum numbers of uppercase, lowercase, digits, and/or special characters required in your password policy?
   a) Minimum uppercase: _ b) Minimum lowercase: _
   c) Minimum digit: _ d) Minimum special characters: _
3) What do you consider to be special characters? Please list those characters below. _____
4) Do you disallow any character types in passwords? Please check all that apply and specify what characters you disallow.
   a) Disallow certain symbol characters b) Disallow non-ASCII characters (e.g., non-English characters) c) Disallow emojis d) Disallow spaces e) Other: ___
5) Do you prevent users from using repetitive (e.g., ddd, 000) and/or sequential patterns (e.g., abc, 123) in their passwords?
   a) Disallow only repetitive patterns b) Disallow only sequential patterns c) Disallow both d) Disallow neither

6) Do you prevent users from using personal identification information (e.g., username, first/last name) in their passwords? a) Yes b) No
7) Do you prevent users from choosing a password (or a part of the password) that is a common word in a dictionary? a) Yes b) No
8) Do you prevent users from choosing passwords that are one of the most popular passwords? (For example, some of the most popular passwords include "123456" and "password".) a) Yes b) No
9) Do you prevent users from choosing passwords found in password leaks/breaches from other websites? (For example, using compromised password lists or services like "haveibeenpwned.com") a) Yes b) No
10) Do you ever require users to change their passwords? a) Yes b) No
11) Do you prevent users from reusing an old/previously chosen password? a) Yes b) No
12) How many old passwords do you keep track of?
Number of old passwords: ___
13) When a user selects a new password, do you check the similarity between the current (or past) password and the new password? a) Yes b) No
14) Is there a limit to how frequently users can change their passwords? (For example, once an hour, or once a day.) a) Yes b) No

At the beginning of the survey, we asked you to answer the survey questions about one specific site's password policy. Please answer the following job-related questions based on when you were managing that specific website.

15) Are you currently managing that specific website? a) Yes b) No
16) Please specify your current job title. ___
Please specify your job title while managing that specific website. ___
17) How many employees are at your company?
a) 0-9 b) 10-49 c) 50-249 d) >250 e) Not part of a company (e.g., freelancer/contractor)
18) Are you managing your website by yourself or with a team? If with a team, what is the number of employees on your team? a) by myself b) with a team
Number of employees on the team: ___
19) How long have you managed websites before managing this specific website? ___
20) How long have you managed this specific website? ___
21) What industry/sector is this specific website in, and about how many website users do you have? ___
22) Have you had any certificate/training for webmaster proficiency? a) Yes b) No
23) Did you have any certificate/training for webmaster proficiency while you were managing that specific website? a) Yes b) No
24) Please specify the gender with which you most closely identify.
a) Male b) Female c) Other d) Prefer not to say
25) Please specify your age.
a) 18-29 b) 30-49 c) 50-69 d) >70 e) Prefer not to say
26) Please specify the highest degree or level of education that you have completed.
a) Less than high school b) High school graduate c) Some college d) 2-year degree e) 4-year degree f) Professional degree g) Doctorate

Thank you for answering all the questions in this short survey. To reach out to you for setting up the interview, please provide an email address we can contact you at _____

Interview Questions

■ Understanding Password Requirements

1) You mentioned that your password composition policy allows passwords between length ____ and ____. How did you decide on those?
2) You mentioned that your password composition policy requires ____ number of ____ characters. How did you decide on those?
3) You mentioned that you forbid some character types. Why are those specific characters disallowed? Why do you limit the character types?
4) You mentioned that you disallow passwords with repetitive/sequential patterns in your policy. What are those repetitive or sequential patterns? How do you decide on those? Why do you disallow them?
5) You mentioned that you disallow selected passwords that contain personal identification information. What is personal identification information for you? How did you decide to disallow passwords with PII?
6) You mentioned that you disallow selected passwords with a dictionary word. How do you determine the list of dictionary words? Does the list of dictionary words evolve over time? Why does/doesn't the list of dictionary words evolve over time?
7) You mentioned that you compare selected passwords with a list of common passwords. What are the reasons that you do this check? How do you determine the list of common passwords? How large is your common password list? Does the list of common passwords change over time? Why does/doesn't the list of common passwords change over time?
8) You mentioned that you don't compare selected passwords with a list of common passwords. Do you think it is a good idea to compare selected passwords with a list of common passwords? If so, what are the reasons that you don't make this comparison?
9) You mentioned that you compare selected passwords with a list of breached passwords. What are the reasons that you do this check? How do you determine the list of leaked passwords from a breach at another website? Does the list of leaked passwords evolve/change over time? Why does/doesn't the list of leaked passwords evolve/change over time? How do you link the compromised password with the user?
10) You mentioned that you don't compare selected passwords with a list of breached passwords. Do you think it is a good idea to compare selected passwords with a list

of breached passwords? What are the reasons that you don't make this comparison?
11) Are there any other composition policies/password requirements of your website that we didn't cover?
12) Beyond the considerations you have already discussed, are there other factors that affect your composition policy (e.g., company policy, password storage, 2FA, password strength, customer pressure)?

■ Understanding Password Changes
13) You mentioned that you require users to change their passwords. When do you require users to change their passwords (e.g., changing if there is evidence of compromise, changing every X days)? What are the reasons that you require changing passwords every X days? How do you decide on X?
14) You mentioned that you don't require users to change their passwords. Do you think there might be cases in which you should require users to change their passwords? What are the reasons that you don't require changing passwords?
15) You mentioned that you don't prevent users from reusing an old password. Do you think it is a good idea to prevent users from reusing an old password? If so, what are the reasons that you don't do this prevention?
16) You mentioned that you prevent users from reusing an old password and block X number of the old passwords. How did you choose that threshold? What are the reasons for doing this?
17) You mentioned that you don't check the similarity between current (or past) and new passwords. Do you think it is a good idea to check the similarity between current (or past) and new passwords? If so, what are the reasons that you don't do this check?
18) You mentioned that you check the similarity between current (or past) and new passwords. While checking similarity, do you use the hashed version of the passwords, plaintext versions, or something else? How do you measure similarity? What are the reasons that you do this check?
19) You mentioned that you have a limit on how frequently users can change their passwords. What is that limit, and why did you pick that limit? What is your policy if the password is compromised/forgotten within this time frame?
20) Are there any differences between your password creation and password recovery policies? If so, what is different? What are the reasons that make password creation and password recovery policies different?
21) Are there any other password change policies on your website that we didn't cover?

■ Understanding Policy Updates
* Initiating Password Policy Changes
22) Do you know who would decide to change the password policy of your (organization) website? If so, who would be the one to make the decision if the password policy of your (organization) website should be updated?
23) What would be the potential reasons for updating the password policy?
24) Please tell me about the possible policy updating decision-making process in terms of management structure (e.g., chain of command, communication between and within departments)
25) Please tell me about the possible policy updating decision-making process in terms of information sources (e.g., outsourcing company suggestions, forum discussions, news).
26) Do you think the password policy must be changed over time? If yes, when do you think the password policy must be changed?
27) What are your thoughts on your current password policy in terms of satisfying your intended security and usability objectives?

* Designing The New Password Policy
28) What would be your role, if you were involved with constructing a new password policy for your current organization/website (e.g., policy designer, implementer, consultant)?
29) Would you work alone while constructing new password policies, or would you work with a team?
30) If you were to work on improving your current password policy, what would be the changes? Why would you change those? Where and how would you/your team gather the information to create the new password policies?
31) Please tell me more about the dynamics in your team while deciding password policies (e.g. chain of command directly influences the design, discussions within and between departments, limitations of other departments).
32) Do the people responsible for the policy design need the approval of someone before changing the policies?

* Deciding to Deploy
33) Does your company or team evaluate the strengths and weaknesses of the new password policy?
34) If so, how does your company/team evaluate the strengths or weaknesses of the changes in the password policy? If not, why?
35) Does your company/team evaluate the feasibility of implementing the new password policy?
36) If so, how does your company/team evaluate the feasibility of the changes in the password policy? How does your company/team evaluate the possible technical challenges before deployment? How does your company/team assess the possible post-deployment issues? If not, why?
37) Who would be responsible for implementing the new password policy on your website?
38) Are the password policy design team and the password policy implementation team the same? If not, please tell me how they communicate about their technical abilities to implement the new policies.

* Deploying the New Policy
39) If you want to change the password policies of your

website, is it quick/possible to deploy new password policies? If you were to change the minimum and/or maximum password length requirements, would that be quick/possible? What would the process involve? If you were to add a breached password and/or common password check, would that be quick/possible? What would the process involve? Are there any challenges that you may face while deploying new password policies? Please walk me through the process you would follow to implement the new password policy.

40) If you were to change your password policy, what types of changes in the password policy would cause more or fewer issues for implementing, deploying, or post-deployment?
41) What would you do if the changed policy and users' current passwords no longer comply?
42) How does the organization impact your decisions for more secure password policies?

* Job Responsibilities and Processes

43) Do you check for the most recent password guidelines and best practices? If so, where do you get the most recent information for the best password practices?
44) You mentioned that you had certification/training for webmaster proficiency. What kind of information related to password and password policy is part of that?
45) Have you had any other training on secure password authentication?
46) You mentioned that you had training on secure password authentication. Please tell me more about it.
47) What are your thoughts and objectives toward your team's awareness of the most recent password policy guidelines?

		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
Length Requirements	Min Length	6	8	8	8	8	8		10	8	8	8
	Max Length	20	16	64	255	64						
	No Min							✓				
	No Max						✓	✓	✓	✓	✓	✓
Required Character Classes	Uppercase Letter	1	1	1	1	1	1		1	1	1	1
	Lowercase Letter	1		1	1	1			1	1	1	1
	Digit	1	1	1	1	1	1		1	1	1	1
	Special Characters	1	1		1				1	1	1	1
Disallowed Character Types	Certain Special Characters	✓	✓	✓	✓						✓	
	Non-ASCII Characters		✓	✓	✓	✓	✓	✓				
	Emojis		✓	✓	✓	✓	✓	✓	✓			
	Spaces		✓	✓	✓	✓	✓	✓	✓			
Disallowed Passwords	Repetitive Pattern Check	✓	✓		✓						✓	
	Sequential Pattern Check		✓		✓						✓	
	PII Check		✓	✓	✓	✓		✓		✓	✓	
	Dictionary Word Check				✓							
	Popular Password Check	✓	✓		✓			✓		✓	✓	
	Leaked Password Check		✓							✓		
Password Expiration and Password Change Restrictions	Password Expiration	✓	✓	✓		✓		✓			✓	✓
	Track Old Passwords	✓	✓	✓	✓	✓					✓	✓
	Password History Length	3	4	4	1	4					8	24
	Password Similarity Check		✓									
	Rate-Limiting Password Changes			✓		✓		✓				✓

TABLE 2. THE PASSWORD POLICIES ON WEBSITES MANAGED BY OUR STUDY PARTICIPANTS, BASED ON OUR SURVEY DATA.