İmamoğlu, M.B. & Eser, A. (2025). Bilişsel uyumsuzluk ve parola güvenliği: Kullanıcı eğilimlerinin analizi. Gümüşhane Üniversitesi Sosyal Bilimler Dergisi, 16(3), 1187-1203.

Bilişsel Uyumsuzluk ve Parola Güvenliği: Kullanıcı Eğilimlerinin Analizi

Cognitive Dissonance and Password Security: Analysis of User Trends

Mustafa Bilgehan İmamoğlu[1], Aleyna Eser[2]

Öz

Günümüzde dijitalleşmenin hızla artmasıyla birlikte parola güvenliği, bireylerin ve kurumların bilgi güvenliğini sağlamasında kritik bir unsur haline gelmiştir. Kullanıcıların sıklıkla basit, tekrar eden ve kolay hatırlanabilir parolalar tercih etmeleri, ciddi güvenlik açıklarına yol açmaktadır. Bu çalışma, kullanıcıların bilişsel parola eğilimlerini analiz eden ve güçlü-zayıf parola ayrımına dayalı olarak kullanıcıya anlık geri bildirim sağlayan web tabanlı bir sistem geliştirmeyi amaçlamaktadır. React kütüphanesi kullanılarak geliştirilen sistem, kullanıcıların parola oluşturma süreçlerinde yaşadıkları bilişsel zorlukları ve geri bildirime verdikleri tepkileri incelemektedir. Çalışma, bilişim alanındaki bölümlerden lisans eğitimi almış 50 gönüllü katılımcı ile çevrimiçi ortamda gerçekleştirilmiştir. Katılımcıların parola oluşturma süresi, tercih ettikleri karakter türleri ve parola güç seviyeleri analiz edilmiştir. Bulgular, yönergelerle desteklenen kullanıcıların daha güçlü parolalar oluşturduğunu ve parola oluşturma süresi ile parola gücü arasında pozitif bir ilişki bulunduğunu göstermektedir. Geliştirilen sistem, bireysel ve kurumsal düzeyde parola güvenliğini artırmaya yönelik uygulanabilir bir model sunmaktadır.

Anahtar Kelimeler: *Parola Gücü, Bilişsel Uyumsuzluk, Siber Saldırı, Kullanıcı Eğilimleri, Bilgi Güvenliği.*

Abstract

With the rapid rise of digitalization, password security has become a critical element in ensuring the information security of individuals and organizations. The frequent use of simple, repetitive, and easily guessable passwords by users poses significant security vulnerabilities. This study aims to develop a web-based system that analyzes users' cognitive tendencies in password creation and provides real-time feedback based on the strength-weakness classification of passwords. The system, built using the React framework, examines users' cognitive difficulties during password creation and their responses to feedback. The experimental study was conducted online with 50 voluntary participants who held undergraduate degrees in information and communication technology-related fields. Throughout the process, participants' password creation times, character preferences, and password strength levels were recorded and analyzed. The findings indicate that users who received guidance through visual and written cues created significantly stronger passwords, and a positive correlation was observed between password creation time and password strength. The developed system offers a practical model for enhancing password security at both individual and organizational levels.

Keywords: *Password Strength, Cognitive Dissonance, Cyber Attack, User Trends, Information Security*

JEL Codes: *M15, M30, M31, L86.*

Araştırma Makalesi [Research Paper]

Submitted: 13 / 02 / 2025
Accepted: 23 / 09 / 2025

[1]Dr. Öğr. Üyesi, Karadeniz Teknik Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü Öğretim Üyesi, Trabzon, Türkiye, bilgehan@ktu.edu.tr, ORCID: https://orcid.org/0000-0002-3496-2959.
[2]Karadeniz Teknik Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü Yüksek Lisans Öğrencisi, Trabzon, Türkiye, aleynaeseer@gmail.com, ORCID: https://orcid.org/0009-0001-7263-2352.

Giriş

Dijitalleşmenin hayatımızın her alanına nüfuz ettiği günümüzde, bireylerin ve kurumların güvenliğini sağlamak adına parola kullanımı her zamankinden daha büyük bir önem taşımaktadır. İnternet tabanlı hizmetlerin yaygınlaşmasıyla birlikte, kullanıcılar günlük yaşamlarında birçok farklı platforma giriş yapmakta ve bu platformlarda kişisel, finansal ve kurumsal bilgilerini saklamaktadır. Ancak, siber tehditlerin giderek karmaşık hale gelmesi, parola güvenliğini sağlamayı zorunlu kılmaktadır. Buna rağmen, kullanıcıların büyük bir kısmı hala güvenli parola oluşturma konusunda bilinçsiz hareket etmekte ve basit, kolay tahmin edilebilir parolalar tercih etmektedir. Özellikle mobil bankacılık, sosyal medya hesapları ve e-posta hizmetleri gibi kişisel ve finansal bilgilerin depolandığı platformlarda parola güvenliği, kullanıcıların kimlik hırsızlığı, veri ihlali ve diğer siber saldırılara karşı korunmasında kritik bir rol oynamaktadır. Kullanıcılar, çoğu zaman birden fazla platform için aynı parolayı kullanarak güvenlik açıklarını daha da artırmaktadır. Bunun temel nedenlerinden biri, bireylerin her platform için farklı ve karmaşık parolalar oluşturmayı zahmetli ve hatırlaması güç bulmasıdır. Mobil bankacılık gibi kritik platformlarda bile kullanıcıların parolalarını belirlerken hatırlaması kolay, ancak güvenlik açısından riskli parolalar tercih ettikleri görülmektedir. Bu durum, sadece bireylerin değil, aynı zamanda kurumların da ciddi güvenlik açıklarına maruz kalmasına neden olmaktadır (Florencio, D. & Herley, C., 2007).

Bireyler genellikle güçlü ve karmaşık parolalar oluşturmak yerine, hatırlaması kolay ve kısa süreli kullanımda pratik olan parolalar seçme eğilimindedir. Doğum tarihleri, basit sıralamalar (örneğin "123456") veya kişisel bilgiler (örneğin, bir aile üyesinin adı) gibi unsurlar sıklıkla parolalarda yer almaktadır. Bu eğilimlerin arkasında yatan temel nedenleri anlamak için Bilişsel Uyumsuzluk Teorisi'nden faydalanılabilir. Bilişsel Uyumsuzluk Teorisi, bireylerin inançları ile davranışları arasında bir uyumsuzluk olduğunda rahatsızlık hissettiklerini ve bu rahatsızlığı azaltmak için çeşitli stratejiler geliştirdiklerini öne sürer (Festinger, 1957). Bireyler, karmaşık ve hatırlaması zor parolalar oluşturmanın güvenli olduğunu bilseler dahi, bunu yapmaktan kaçınabilirler. Çünkü bu davranış günlük rutinlerine ve kolaylık beklentilerine ters düşer. Sonuç olarak, kullanıcılar güvenliğe dair bilgilerle kendi alışkanlıkları arasında bir çatışma yaşar ve bu çatışmayı azaltmak adına güvensiz, ancak hatırlaması kolay parolalar oluşturmayı tercih ederler. Aynı zamanda, kullanıcıların parola oluşturma ve değiştirme süreçlerinde bir başka eğilim daha dikkat çekicidir: tekrar eden parola kullanımı. Çalışmalar, kullanıcıların birden fazla platformda aynı parolayı kullanma eğiliminde olduğunu göstermektedir. Bunun altında yatan bilişsel neden, hem hatırlamanın kolay olması hem de parola oluşturma işlemini hızlı bir şekilde tamamlamaya duyulan ihtiyaçtır. Ancak, bu durum, bir platformda yaşanan veri ihlalinin diğer tüm hesapları da risk altına sokmasına neden olarak ciddi bir güvenlik açığı yaratmaktadır (Shay vd., 2010).

Bu çalışmada, kullanıcıların parola oluşturma davranışlarını analiz eden web tabanlı bir sistem geliştirilecektir. Facebook tarafından geliştirilen açık kaynaklı bir JavaScript kütüphanesi olan React kullanılarak hazırlanan model sistem, kullanıcıların parola oluşturma eğilimlerini analiz edecek ve güçlü parola oluşturma sürecini teşvik eden bir geri bildirim mekanizması sağlayacaktır.

Bu kapsamda, kullanıcıların:

- Güçlü parola oluşturma sürecinde yaşadığı bilişsel zorluklar,
- Güçlü parola oluşturma ipuçlarına karşı verdiği tepkiler,
- Parola oluşturma süresince yapılan denemeler ve bu denemelerin sonuçları

ölçülecek ve değerlendirilecektir. Bu analizler ile, hem kullanıcı davranışlarının daha iyi anlaşılması hem de güvenli parola oluşturma süreçlerinin iyileştirilmesine yönelik önerilerin sunulması hedeflenmektedir. Kullanıcıya verilen geri bildirimler sayesinde, parola oluşturma sürecindeki bilişsel eğilimlerin anlaşılması sağlanacak ve güçlü parola oluşturma davranışlarının geliştirilmesi için yönlendirme yapılacaktır. Bu uygulamalı çalışmada, kullanıcıların bilişsel zorlukları, parola güvenliği kriterlerine uyum dereceleri ve bu süreçte verilen geri bildirimlere karşı gösterdikleri tepkiler analiz edilmiş olacaktır. Web tabanlı sistemin kullanıcı eğilimlerini değerlendirerek parola güvenliğini artırmaya yönelik rehberlik sunduğu bu etkileşimli entegrasyonun detayları açık erişime sunulmuştur. Çalışmanın temel araştırma problemi, "Kullanıcıların parola oluşturma sürecindeki bilişsel eğilimleri, güçlü parola oluşturma davranışlarını ne ölçüde etkilemektedir?" sorusu çerçevesinde şekillenmiştir. Bu doğrultuda, bilişsel uyumsuzluk kuramı ve kullanıcı davranışlarına ilişkin literatür temel alınarak üç hipotez ortaya konmuştur. Birinci hipotez, kullanıcıların görsel ve yazılı yönergelerle desteklendiğinde daha güçlü parolalar oluşturma eğiliminde olduklarını öne sürmektedir. İkinci hipotez, güçlü parola oluşturmanın daha uzun bilişsel işlem süresi gerektirdiğini, dolayısıyla parola oluşturma süresi ile parola gücü arasında pozitif bir ilişki olduğunu varsaymaktadır. Üçüncü hipotez ise, kullanıcıların sistemden "zayıf parola" uyarısı aldıklarında bu durumu fark edip davranışlarını değiştirerek daha güçlü parolalar üretmeye yönelip yönelmediklerini incelemektedir. Bu hipotezler, hem kullanıcı davranışlarının dinamik analizine olanak tanımakta hem de parola güvenliği alanında bireysel bilişsel tepkilerin değerlendirilmesini mümkün kılmaktadır.

1. Literatür

Parola güvenliği, bireylerin ve organizasyonların dijital ortamlardaki güvenliğini sağlamak adına kritik bir unsur olarak öne çıkmaktadır. Kullanıcıların parola oluşturma tercihlerini ve davranışlarını anlamaya yönelik yapılan çalışmalarda, özellikle bilişsel faktörlerin, kullanıcı deneyimlerinin ve kullanıcı farkındalığını artırmaya yönelik mekanizmaların belirleyici rol oynadığı vurgulanmaktadır. Bu bağlamda, literatürdeki çalışmalar temelde üç ana tema altında gruplanabilir: (1) görsel ve bilişsel işleme dayalı parola sistemleri, (2) bireysel ve bilişsel farklılıkların etkisi, ve (3) parola güvenliğini artırmaya yönelik rehberlik ve oyunlaştırma yaklaşımları.

Parola güvenliği ile görsel bilgi işleme süreçleri arasındaki ilişkiyi ele alan çalışmalar, kullanıcıların geleneksel alfasayısal parolalar yerine görsel bileşenler içeren sistemlerde daha iyi performans gösterdiğini ortaya koymaktadır. Jha ve arkadaşları (2022), JavaScript ile geliştirilen grafik tabanlı bir parola doğrulama sistemi önererek, kullanıcıların görselleri alfasayısal ifadelere göre daha kolay hatırladığını göstermiştir. Benzer şekilde, Katsini vd. (2019) çalışmasında da Alan Bağımlılığı-Bağımsızlığı kuramı çerçevesinde, kullanıcıların görsel bilgi işleme stratejilerinin parola gücü ile doğrudan ilişkili olduğu, özellikle alan bağımsız bireylerin daha güçlü parolalar oluşturduğu ancak bu süreçte daha fazla bilişsel efor sarf ettiği tespit edilmiştir. Bu çalışmalar, görsel ögelerin kullanıcı davranışlarını şekillendirmedeki rolünü ve parola sistemlerinin bilişsel özelliklere duyarlı olarak tasarlanmasının önemini vurgulamaktadır.

İkinci olarak, kullanıcıların bireysel ve bilişsel özelliklerinin parola oluşturma davranışlarına etkisini ele alan araştırmalar, kişilik yapısı, bilişsel motivasyon düzeyi ve metabilişsel inançların belirleyici olduğunu ortaya koymuştur. Kennison vd. (2023), güçlü bilişsel işleme motivasyonuna (Need for Cognition) sahip bireylerin daha güvenli parola tercihleri yaptığını, hafıza kaybı yaşayan kullanıcıların ise daha zayıf parolalar oluşturduğunu bildirmiştir. Choudhary vd. (2021) ise, kullanıcıların metabilişsel inançlarının parola seçiminde etkili olduğunu ve hatırlanabilir parolaların daha az güvenli olduğuna inanmanın bilişsel uyumsuzluk yarattığını belirtmektedir. Bu bağlamda, parola güvenliği uygulamalarında kullanıcıların bilişsel profillerinin ve zihinsel eğilimlerinin dikkate alınmasının kritik olduğu anlaşılmaktadır.

Üçüncü grup çalışmalar ise, parola güvenliğini artırmaya yönelik sistematik rehberliklerin ve oyunlaştırma tekniklerinin etkisini incelemektedir. Shay vd. (2010), kullanıcıların karmaşık parola oluşturma kurallarını çoğu zaman gereksiz ve zorlayıcı bulduğunu, bu nedenle güvenli olmayan parolalar tercih ettiklerini ifade etmiştir. Bonneau vd. (2012), kullanıcı dostu rehberlik mekanizmalarının parola güvenliğini artırmada etkili olabileceğini vurgulamış ve bu mekanizmaların kullanım kolaylığı ile güvenlik arasında bir denge kurabileceğini savunmuştur. Bu çalışmaların devamı niteliğinde olan araştırmalarda, gerçek zamanlı geri bildirim sağlayan parola ölçüm sistemlerinin kullanıcıyı daha güçlü parola oluşturmaya yönlendirdiği gösterilmiştir. Öte yandan, Scholefield ve Shepherd (2019) tarafından geliştirilen Android tabanlı bir RPG uygulamasında, oyunlaştırma yoluyla parola güvenliği bilincinin artırıldığı, kullanıcıların güvenlik bilgilerini eğlenceli bir şekilde öğrenerek içselleştirdiği sonucuna ulaşılmıştır.

Literatürdeki bulgular parola güvenliğinin yalnızca teknik bir konu olmadığını, aynı zamanda kullanıcı davranışları, bilişsel süreçler ve kullanıcıya sunulan etkileşimli sistemlerle doğrudan ilişkili olduğunu göstermektedir. Bu bağlamda geliştirilen yeni nesil parola güvenliği sistemlerinin hem kullanıcı odaklı hem de bilişsel temelli olması gerektiği açıktır.

2. Bilişsel Uyumsuzluk ve Parola Gücü İlişkisi

Bilişsel uyumsuzluk, bireylerin inançları, tutumları ve davranışları arasında bir çelişki algıladıklarında hissettikleri psikolojik rahatsızlık durumudur. Festinger (1957) tarafından ortaya konan bu teori, bireylerin bu rahatsızlığı azaltmak için bilişsel uyarlamalar yaptıklarını öne sürmektedir. Bu kuramsal çerçeve, parola güvenliği davranışlarının analizinde de açıklayıcı bir rol üstlenmektedir. Kullanıcılar güçlü parola oluşturmanın öneminin farkında olmalarına rağmen, çoğu zaman hatırlanması kolay ve basit parolaları tercih etmektedir. Bu tercih, güvenlik bilgisinin gerekleriyle kişisel rahatlık ve kullanım kolaylığı arasındaki çelişkinin bir sonucu olarak değerlendirilmekte, bilişsel uyumsuzluk ile açıklanmaktadır (LastPass, 2020; Perez, 2021).

Bu bağlamda yapılan çalışmalar, kullanıcıların bilişsel eğilimleri ile parola oluşturma davranışları arasındaki ilişkileri ortaya koymaktadır. Di Campi (2021), kullanıcıların dilsel alışkanlıkları, çevresel faktörler ve bilişsel basitlik arayışı doğrultusunda tahmin edilmesi kolay parolalar seçme eğiliminde olduğunu göstermiştir. Bu tür parolalar, saldırganlar için öngörülebilir zayıflıklar oluşturmakta ve güvenlik risklerini artırmaktadır. Choudhary ve arkadaşları (2021) ise, metabilişsel inançların parola seçimindeki etkisini inceleyerek, kullanıcıların hatırlanabilirliğin güvenlikten daha önemli olduğunu düşündüklerinde bilişsel uyumsuzluk yaşadıklarını ve bu durumu gerekçelendirme eğiliminde olduklarını ifade etmiştir.

Bilişsel uyumsuzluğun ötesinde, kullanıcı alışkanlıkları ve parola davranışlarına odaklanan çalışmalar da parola güvenliğinin çok boyutlu bir yapı arz ettiğini göstermektedir. Florêncio ve Herley (2007), kullanıcıların parolaları birden

fazla platformda yeniden kullanma eğiliminde olduklarını ve bu davranışın güçlü parola oluşturma motivasyonunu azalttığını tespit etmiştir. Choong ve Theofanos (2015) tarafından gerçekleştirilen geniş ölçekli bir çalışmada ise, çalışanların kurumsal parola politikalarına yönelik olumlu tutumlarının, daha güçlü parola tercihleri ile ilişkili olduğu; bu bireylerin parola yönetiminde daha az hata yaptığı ve sistem güvenliğine daha fazla önem verdiği belirlenmiştir. Di Campi ve Luccio (2024) tarafından yürütülen bir diğer araştırma ise, teknik geçmişe sahip kullanıcıların dahi zayıf parola oluşturma eğiliminde olduklarını ortaya koyarak, bilgi birikiminin davranış değişikliği için yeterli olmadığını vurgulamıştır.

Parola oluşturma sürecinde kullanıcıya sağlanan rehberlik ve geri bildirim mekanizmalarının da davranışları olumlu yönde etkilediği gösterilmiştir. Ur ve arkadaşları (2015), kullanıcıların gerçek zamanlı parola analizine dayalı görsel geri bildirim aldıklarında daha güçlü parolalar oluşturduklarını tespit etmiştir. Geri bildirim sistemlerinde kullanılan renk kodlamaları (örneğin, yeşil: güçlü, kırmızı: zayıf) kullanıcıların bilinçli tercihler yapmalarını kolaylaştırmaktadır. Ancak bu tür sistemlerin etkinliği, kullanıcıya verilen bilginin doğruluğu ve tutarlılığı ile doğrudan ilişkilidir. Bu çerçevede, Carnavalet ve Mannan (2014), parola güçlendirme araçlarının çoğunun kullanıcıya çelişkili geri bildirimler sunduğunu ve bunun güvenlik algısını olumsuz etkileyebileceğini belirtmiştir.

Güvenlik davranışlarını desteklemek üzere oyunlaştırma temelli yaklaşımlar da önemli bir alan olarak öne çıkmaktadır. Kostić ve Saveljić (2023), geliştirdikleri "Lockedout: Password Defense" isimli oyun ile kullanıcıların parola güvenliği bilincini artırmayı başarmış ve oyunlaştırma tekniklerinin güçlü parola oluşturma alışkanlıklarını desteklemede etkili olduğunu göstermiştir. Bu bulgu, kullanıcıların bilişsel motivasyonlarını artırmak için sadece bilgi vermenin değil, aynı zamanda etkileşimli ve motive edici yöntemlerin de önemli olduğunu ortaya koymaktadır.

Son olarak, parola kalıpları ve saldırı yüzeyleri üzerine yapılan teknik çalışmalar, kullanıcı davranışlarının güvenlik açıklarıyla nasıl kesiştiğini göstermektedir. Li, Romdhani ve Buchanan (2016), kullanıcıların öngörülebilir şifre kalıpları oluşturduğunu ve bunun parola tahmini yapan sistemler için büyük avantaj yarattığını belirlemiştir. Bu durum, bireysel alışkanlıkların sadece kişisel bir tercih değil, sistemsel bir güvenlik zafiyetine dönüşebileceğini göstermektedir.

Tüm bu bulgular birlikte değerlendirildiğinde, bilişsel uyumsuzluk, alışkanlıklar, metabilişsel inançlar ve kullanıcıya sunulan yönlendirmelerin parola güvenliği üzerinde güçlü etkiler yarattığı söylenebilir. Bu nedenle, parola güvenliğini artırmayı hedefleyen sistemlerin yalnızca teknik olarak değil, kullanıcı davranışları ve psikolojik süreçler açısından da bütüncül bir yaklaşımla tasarlanması gerekmektedir. Kullanıcı eğilimlerini doğru analiz eden ve bu analizleri rehberlik sistemleriyle destekleyen çözümler, dijital güvenliğin sürdürülebilirliği açısından kritik bir rol üstlenmektedir.

3. Yöntem

Deneysel desen kullanılarak yürütülen bu nicel araştırma kapsamında kullanıcıların parola oluşturma davranışlarını analiz etmek amacıyla web tabanlı bir sistem geliştirilmiştir. Yazılım süreçlerinde kullanılan React, kullanıcı arayüzleri geliştirmek için kullanılan açık kaynaklı Javascript kütüphanesidir. Facebook firması tarafından geliştirilmiş ve 2013 yılında açık kaynak olarak yayımlanmıştır. Hazırlanan sistem, kullanıcıların güçlü parola oluşturma süreçlerinde karşılaştıkları bilişsel zorlukları, verilen ipuçlarına gösterdikleri tepkileri ve deneme süreçlerini analiz etmek üzere yapılandırılmıştır. Bu bölümde, çalışmada kullanıcıların parola oluşturma davranışlarını analiz etmek için kullanılan yöntem, çalışmanın bağımlı ve bağımsız değişkenleri, amaç ve kapsamı, çalışma modeli ve hipotezleri açıklanacaktır.

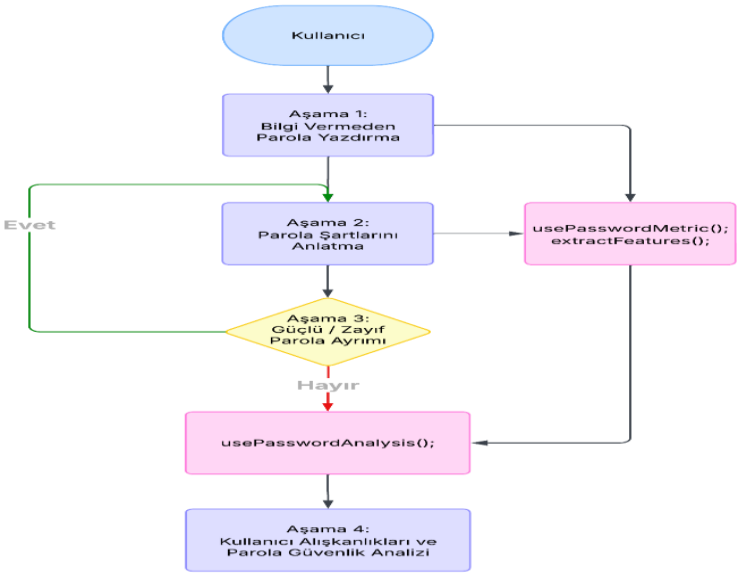
3.1. Bağımlı ve Bağımsız Değişken

Kullanıcıların parola oluşturma davranışlarını analiz etmek ve güçlü parola oluşturma süreçlerini teşvik etmek amacıyla bağımlı ve bağımsız değişkenler parola güvenliği çalışmalarında yaygın olarak kullanılan metriklerden (Morph1Max, 2021; Bonneau et al., 2012) ve parola karmaşıklığı ölçüm kriterlerinden yararlanılarak belirlenmiştir. Bağımlı değişken, parolaların güvenlik seviyesi (strength) olarak tanımlanmıştır. Parolaların güçlü, orta veya zayıf olarak sınıflandırılmasını ifade eder ve kullanıcıların oluşturduğu parolaların güvenliğini ölçmek için temel metrik olarak kullanılır. Bağımsız değişkenler ise parolaların güvenlik seviyesini etkileyen çeşitli faktörlerden oluşmaktadır. Bunlar; parolaların uzunluğu, küçük harf, büyük harf, rakam ve özel karakter içerme durumu, paroladaki bilgi entropisi ve karakter çeşitliliği gibi yapısal özelliklerden oluşur. Ayrıca, parolanın yaygın kullanımı ve sözlük kelimesi içerip içermemesi de bağımsız değişkenler arasında yer alır. Ek olarak kullanıcıların parola oluşturma süreleri de bu bağlamda bilişsel eğilimlerin değerlendirilmesine olanak sağlamaktadır. Bu değişkenler arasındaki ilişki, kullanıcıların güçlü parola oluşturma eğilimlerini anlamak ve daha güvenli parola politikaları geliştirmek için analiz edilecektir

3.2. Çalışma Modeli

Çalışmada kullanıcıların parola oluşturma süreçlerini analiz etmek ve güçlü-zayıf parola ayrımını değerlendirmek amacıyla, literatürde yer alan parola güvenliği özellikleri dikkate alınmıştır. Kobelev Maxim'in "Password Security: Sber Dataset" isimli veri seti, bu özelliklerin belirlenmesinde önemli bir referans kaynağı olarak kullanılmıştır (Morph1Max,

2021). Şekil 1'de gösterilen çalışma modeli, güçlü-zayıf parola analizine dair süreçleri görselleştirmektedir. Kullanıcıların parola oluşturma süreci boyunca ihtiyaç duyulan özellikler ve bu özelliklerin güvenlik değerlendirmelerine etkisi sistematik bir şekilde ele alınmıştır.



Şekil 1. Uygulama Çalışma Modeli

Parolaların güvenlik düzeylerini değerlendirmek için Maxim'in veri setinde yer alan özellikler, sistem tasarımımıza entegre edilmiştir. Kullanılan ana özellikler Tablo 1'de yer almaktadır. Bu özellikler, kullanıcıların bilişsel parola eğilimlerini analiz etmek ve parolaların güvenlik düzeylerini değerlendirmek amacıyla geliştirilen React tabanlı sistemimize entegre edilmiştir. Sistem, kullanıcı tarafından girilen parolaların bu kriterlere göre anlık olarak değerlendirilmesini ve geri bildirim sağlanmasını mümkün kılmıştır. Verilerin analizi sırasında bu özellikler hem bağımsız değişkenler hem de parola güvenliğini belirleyici faktörler olarak ele alınmıştır.

Söz konusu veri seti, kullanıcıların parola oluşturma süreçlerindeki eğilimlerini ve davranışlarını incelemek için zengin bir analiz imkânı sunmaktadır. Parola uzunluğu, harf çeşitliliği, entropi ve diğer faktörler, güçlü parola oluşturmayı teşvik eden algoritmaların geliştirilmesine katkı sağlamaktadır.

Tablo 1. Parola Değerlendirme Veri seti Özellikleri

Özellik	Açıklama
Id	Aşama seviyesi.
Password	Parola metni.
Strength	Parolanın güvenlik seviyesi (0: zayıf, 1: orta, 2: iyi, 3: güçlü).
Value	Parola güç karşılığı.
Length	Parolanın karakter uzunluğu.
HasLowerCase	Parola küçük harf içeriyor mu? (True/False).
HasUpperCase	Parola büyük harf içeriyor mu? (True/False).
HasSpecialChars	Parola özel karakter içeriyor mu? (True/False).
IsCommonPassword	Parola yaygın bir parola mı? (True/False). Bu özellik belirlenirken ilgili parola Top 10 Million Passwords listesiyle karşılaştırılmıştır (Joakim, 2023).
ContainsDictionaryWord	Parola bir sözlük kelimesi içeriyor mu? (True/False).
NumLowercase	Paroladaki küçük harf sayısı.
NumUppercase	Paroladaki büyük harf sayısı.
NumDigits	Paroladaki rakamların sayısı.

NumSpecialChars	Paroladaki özel karakter sayısı.
NumSpaces	Paroladaki boşluk karakter sayısı.
ConsecutiveChars	Art arda tekrar eden karakter sayısı.
CharacterDiversity	Paroladaki farklı karakter türlerinin sayısı.
Entropy	Parolanın güvenlik seviyesini ölçen bilgi entropisi.

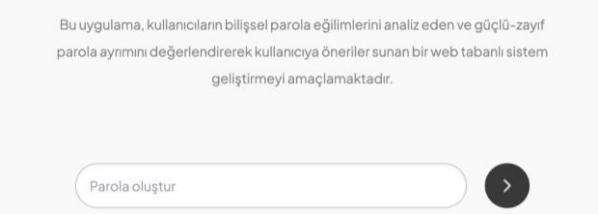
Çalışma, bilişim alanındaki lisans programlarından mezun olmuş gönüllü katılımcılarla çevrimiçi ortamda gerçekleştirilmiştir. Katılımcılar, araştırma çağrısına yanıt veren ve sistemin test edilmesine katkı sunmayı kabul eden 50 gönüllü bireyden oluşmaktadır. Katılımcılar herhangi bir ödül veya teşvik almadan, tamamen gönüllü esasına göre çalışmaya dâhil edilmiştir. Yaş ve cinsiyet gibi demografik bilgiler toplanmamış, veri yalnızca parola oluşturma davranışları ve sistem etkileşimleriyle sınırlı tutulmuştur.

Katılımcılar uygulamanın çalışma modelini oluşturan dört aşamayı tamamlamış; her aşamada parola girişleri, parola oluşturma süresi, karakter türleri ve kullanıcı kararları otomatik olarak sistem tarafından kaydedilmiştir. Katılımcıların sisteme erişimi ve veri üretimi bireysel olarak gerçekleştirilmiş, harici bir gözlemci ya da müdahale yapılmamıştır. Uygulama süreci kullanıcı başına ortalama 5–7 dakika sürmüştür.

Pilot bir kullanıcı testi gerçekleştirilmemiş fakat sistemin uygulanabilirliğini sağlamak amacıyla geliştirilen React tabanlı uygulama, farklı kullanıcı senaryoları üzerinde detaylı bir şekilde test edilmiştir. Parola giriş ekranları, geri bildirim mekanizmaları ve veri kayıt sistemleri yazılım geliştirme süreci boyunca defalarca simüle edilmiş, kullanılabilirlik açısından açık kaynak parola güvenlik ölçütleriyle entegrasyonu sağlanmıştır. Böylece, kullanıcı deneyimi ile ilgili olası sorunlar önceden yazılım seviyesinde giderilmiştir.

3.2.1. Aşama 1: Bilgi Vermeden Parola Yazdırma

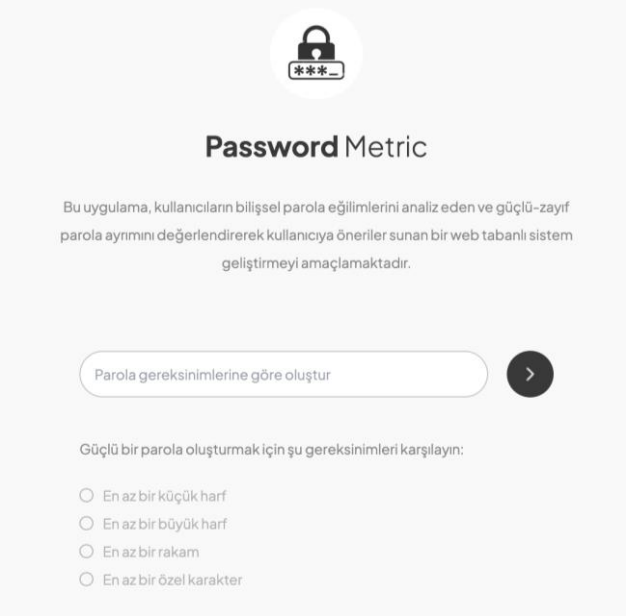
İlk aşamada, kullanıcılara parola oluşturma hakkında herhangi bir bilgi verilmeden Resim 1'deki uygulama ekranında parolasını oluşturması istenir. Bu aşama, kullanıcının doğal eğilimlerini gözlemlemek ve parola oluşturma alışkanlıklarını anlamak için kullanılır. Kullanıcı, parola oluşturma sürecini kendi başına tamamlar ve bu süreçte müdahale edilmez. Bu sayede kullanıcıların ilk parola oluşturma eğilimlerini analiz etmek için temel veriler elde edilmiş olur.



Resim 1. Birinci Aşama Uygulama Ekranı

3.2.2. Aşama 2: Parola Şartlarını Anlatma

İkinci aşamada, Resim 2'deki uygulama ekranıyla kullanıcılara güçlü bir parola oluşturmak için gerekli şartlar (uzunluk, büyük/küçük harf, rakam, özel karakter) açıklanır. Kullanıcılara, güçlü bir parola oluşturabilmek için bu kriterleri dikkate almaları gerektiği bildirilir. Bu aşama, parola güvenliği hakkında verilen bilgilerin kullanıcılar tarafından nasıl uygulandığını gözlemeyi amaçlar. Verilen bilgilerin ardından kullanıcının tekrar parola oluşturması istenir. Böylece kullanıcıların verilen bilgileri nasıl uyguladıklarını ve parola güvenliği hakkında edindikleri bilgilerin ne kadar etkili olduğunu analiz edilir.

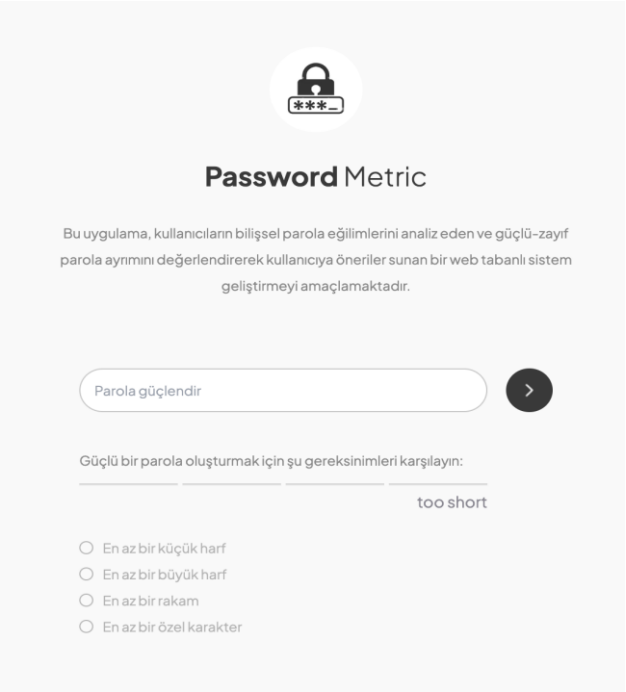


Resim 2. İkinci Aşama Uygulama Ekranı

3.2.3. Aşama 3: Güçlü / Zayıf Parola Ayrımı

Bu aşamada, kullanıcı oluşturduğu parolanın güvenlik seviyesini değerlendirir. Kullanıcının belirlediği parolanın güç (strength) özelliği hesaplanır. Parolanın güç değeri 3 (güçlü) ise, bu parola kabul edilir ve süreç tamamlanır. Eğer 3 den düşük bir seviyedeyse kullanıcının karar verme yetisine bırakılır ve böylece kullanıcının zayıf olarak girdiği parolayı kabul etme yetisi öğrenilir. Kullanıcı dilerse daha güçlü bir parola oluşturmayı seçebilir. Resim 3 ve Resim 4'de ekran görüntüleri verilen bu aşama, güçlü ve zayıf parolaların analizini yaparak, kullanıcı davranışlarını gözlemlemeyi amaçlar.

Resim 3. Üçüncü Aşama Karar Ekranı



Resim 4. Üçüncü Aşama Sonrası İkinci Aşama Uygulama Ekranı

3.2.4. Aşama 4: Kullanıcı Alışkanlıkları ve Parola Güvenlik Analizi

Son aşama, kullanıcının parola oluşturma alışkanlıklarını, bilişsel uyumsuzluklarını ve parola güvenliği üzerindeki gelişimini daha ayrıntılı olarak analiz eder. Bu aşamada, kullanıcılara önceki parola denemeleri üzerinden geri bildirim verilerek, güçlü parola oluşturma alışkanlıkları ve parola güvenliğine dair davranışları incelenir. Kaydedilen veriler, iki ana sınıflamada ele alınır: Parola Özelliği ve Kullanıcı Tutumu.

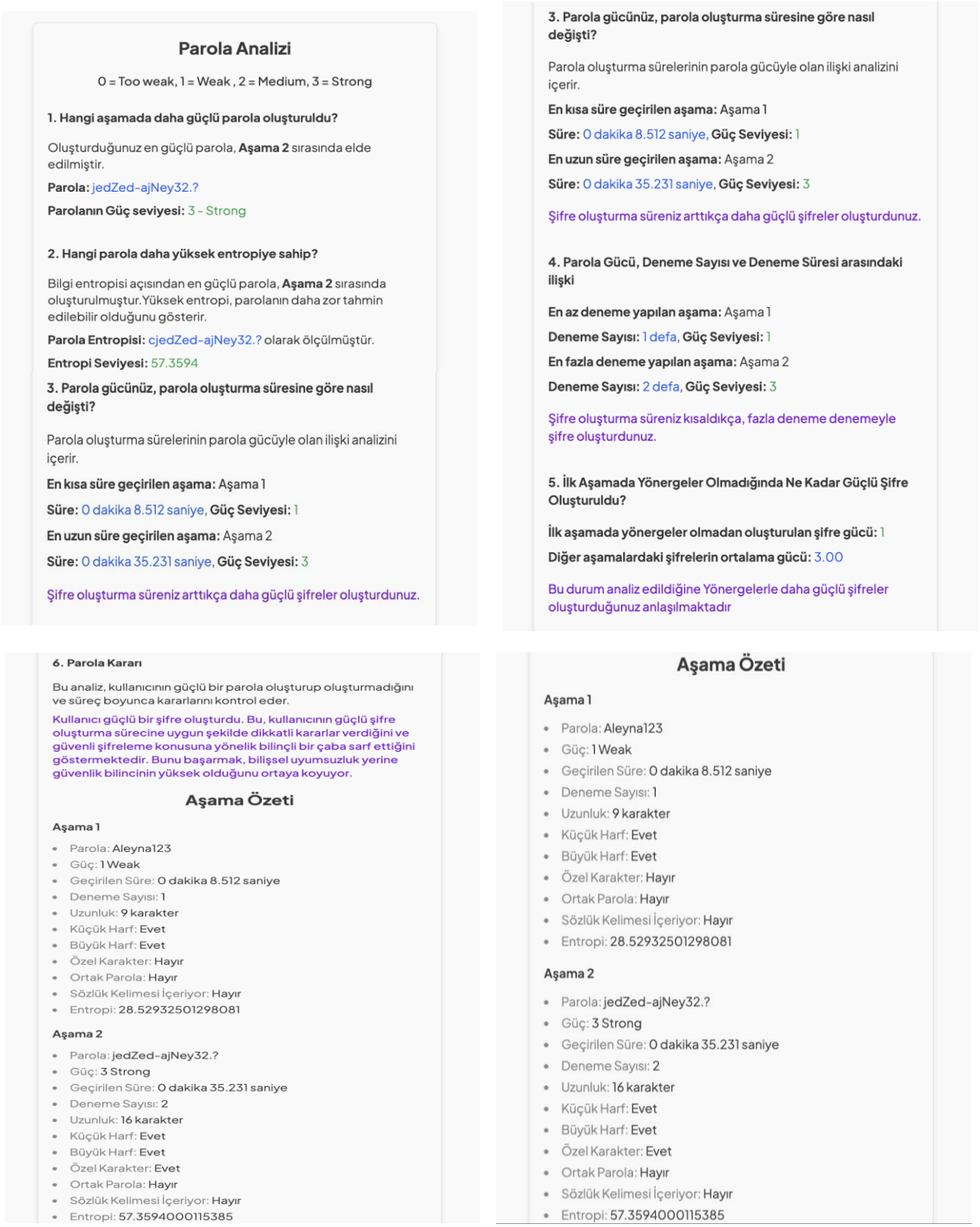
Parola Özelliği: Her aşamada kullanıcı tarafından oluşturulan parola, belirlenen özelliklere göre analiz edilir ve bir veri satırı olarak kaydedilir. Parolanın güvenlik seviyesi ve kullanıcının parola oluşturma eğilimleri hakkında bilgi veren özellikler şöyledir;

- Parola Güçlülüğü ve Entropisi: Parolanın güvenlik seviyesi ve entropi değeri hesaplanarak kaydedilir.
- Kullanıcının Tercih Ettiği Karakter Türleri: Kullanıcıların parola oluştururken tercih ettiği karakter türleri (küçük harf, büyük harf, rakam, özel karakter) kaydedilir.
- Parolanın Uzunluğu, Özelliği ve İçerdiği Karakter Türleri: Parolanın uzunluğu ve içerdiği karakter türleri ile birlikte parolanın oluşturulma biçimi kaydedilir.

Kullanıcı Tutumu: Aşamalar boyunca kullanıcının gösterdiği davranışlar ve bilişsel uyumsuzluklar detaylı bir şekilde analiz edilir. Bu analizlerde aşağıdaki kriterler göz önünde bulundurulur:

- Kullanıcı Parola Oluşturma Süresi ve Denemeleri: Yönergelerle ve görsel açıklamalarla parola oluşturma süresi arasındaki ilişki analiz edilir. Kullanıcının parola oluşturma süresi, parola güçlülüğüne göre nasıl değişiyor? Görseller ve açıklamalar parola oluşturma sürecinde ne kadar etkili oluyor? Bu veriler, kullanıcıların parola oluşturma hızını ve güvenlik seviyesiyle ilişkisini anlamaya yardımcı olur.
- Kullanıcı Parola Güçlülüğü Karar Verme Yetisi: Kullanıcıya parolanın güçlülüğü sunulduğunda, kullanıcının bu bilgiyi nasıl algıladığı ve ne kadar süreyle parola oluşturmayı sürdürdüğü analiz edilir. Kullanıcı, zayıf olduğunu bildiği bir parolayı kabul mü ediyor, yoksa güçlü olması için çaba sarf ediyor mu? Görsel olarak parolanın kırmızı (zayıf) ve yeşil (güçlü) renklerle belirtildiği durumlarda, kullanıcının parola gücüne karşı tepkisi değişiyor mu? Kullanıcının bu davranışı, bilişsel uyumsuzluk ve karar verme süreçlerini gözler önüne sermektedir.

Bu aşamada, kullanıcıların parola oluşturma süreçleri ve parola güvenliği konusundaki tutumları analiz edilir. Kullanıcılara parolaların gücü hakkında görsel geri bildirim verilir ve bunun parola oluşturma süreci üzerindeki etkileri gözlemlenir. Ayrıca, kullanıcıların parola oluşturma süresi, tercih ettikleri karakter türleri ve parola oluşturma alışkanlıkları gibi verilerle parola güvenliğine dair karar verme süreçleri incelenir. Son olarak, kullanıcıların bilişsel uyumsuzlukları ve geri bildirimlere verdikleri tepkiler değerlendirilerek, Resim 5'te gösterildiği gibi, parola güvenliği konusundaki tutumları derinlemesine analiz edilir.



Resim 5. Son aşama Parola Güvenlik Analiz Ekranları

3.3. Hipotezler

Çalışmada, kullanıcıların parola oluşturma süreçlerinde yönlendirme ve geri bildirim mekanizmalarının güçlü parola tercihleri üzerindeki etkisi ile oluşturma süresi ile parola gücü arasındaki ilişki test edilmiştir. Hipotezler, istatistiksel analiz yapılabilirliği gözetilerek hem yokluk (H_0) hem de araştırma (H_1) hipotezleri biçiminde formüle edilmiştir.

Hipotez 1: Yönergelerle Desteklenen Parola Oluşturma Süreci

H_0 (Yokluk Hipotezi): Kullanıcılara sistem tarafından görsel ve yazılı yönergeler verilmesi, oluşturdukları parolaların güvenlik seviyesi üzerinde anlamlı bir etki yaratmaz.

H_1 (Araştırma Hipotezi): Kullanıcılara sistem tarafından görsel ve yazılı yönergeler verilmesi, oluşturdukları parolaların güvenlik seviyesini anlamlı düzeyde artırır.

Bu hipotez, kullanıcıların parola oluşturma sürecinde sistem tarafından sağlanan yönlendirmelerle (örneğin, güçlü parola kriterleri, renk kodlamaları, "zayıf–orta–güçlü" uyarıları) daha güvenli parolalar üretip üretmediklerini test etmeyi amaçlamaktadır. Parola gücü, 0'dan 3'e kadar puanlayan bir metrik olan check-password-strength bileşeni aracılığıyla ölçülmekte ve bu sayısal skor analizde bağımlı değişken olarak kullanılmaktadır. Katılımcıların ilk aşamada (yönerge verilmeden) ve ikinci aşamada (yönergeyle) oluşturduğu parolalar karşılaştırılarak analiz edilmektedir.

Literatürdeki çalışmalarda, kullanıcıların parola güvenliği davranışlarını güçlendirmek için sağlanan görsel ve yazılı yönergelerin etkili olduğu gösterilmiştir. Ur vd. (2015), gerçek zamanlı parola analizine dayalı görsel geri bildirimlerin kullanıcıların daha güçlü parolalar oluşturmasını sağladığını ortaya koymuştur. Benzer şekilde Shay vd. (2010), kullanıcıların parola kurallarına ilişkin yönlendirmeleri içselleştirerek güvenli davranış geliştirdiklerini rapor etmiştir. Ayrıca Jha vd. (2022) görsel ipuçlarının bilişsel yükü azalttığını ve kullanıcıların daha güçlü parola üretme eğilimini artırdığını belirtmiştir.

Hipotez 2: Parola Oluşturma Süresi ile Güç Düzeyi Arasındaki İlişki

H_0 (Yokluk Hipotezi): Kullanıcıların parola oluşturma süresi ile oluşturdukları parolaların güvenlik seviyesi arasında anlamlı bir ilişki yoktur.

H_1 (Araştırma Hipotezi): Kullanıcıların parola oluşturma süresi ile oluşturdukları parolaların güvenlik seviyesi arasında anlamlı ve pozitif yönde bir ilişki vardır.

Bu hipotez, güçlü parola oluşturma davranışının daha uzun sürede ve daha fazla bilişsel çaba ile gerçekleştiği varsayımına dayanmaktadır. Parola oluşturma süresi bağımsız değişken, parola güvenlik skoru ise bağımlı değişken olarak değerlendirilmiştir. Bu iki değişken arasındaki ilişki analiz edilerek, güçlü parola oluşturma sürecinin bilişsel yoğunluğa bağlı olup olmadığı test edilmiştir.

Önceki çalışmalar, kullanıcıların güçlü parolalar oluştururken daha fazla bilişsel çaba harcadığını göstermektedir. Florêncio ve Herley (2007), karmaşık parola seçimlerinin daha uzun süre aldığını belirtmiştir. Kennison ve Chan-Tin (2023), güçlü bilişsel işleme motivasyonuna sahip bireylerin daha güvenli parolalar ürettiklerini ve bu sürecin daha fazla zaman gerektirdiğini ortaya koymuştur. Ayrıca Shay vd. (2010), güçlü parola oluşturma davranışlarının genellikle daha dikkatli ve uzun sürede gerçekleştiğini vurgulamaktadır.

Hipotez 3: Bilişsel Uyumsuzluk Temelli Davranışsal Uyarlama

H_0 (Yokluk Hipotezi): Zayıf parola oluşturduğunu bildiği hâlde aynı parolayı kabul eden kullanıcıların oranı ile daha güçlü parola oluşturan kullanıcıların oranı arasında anlamlı bir fark yoktur.

H_1 (Araştırma Hipotezi): Zayıf parola oluşturduğunu bildiği hâlde aynı parolayı kabul eden kullanıcıların oranı, güçlü parola oluşturmak için davranışını değiştiren kullanıcıların oranından anlamlı düzeyde farklıdır.

Bu hipotez, kullanıcıların sistem tarafından "zayıf parola" uyarısı almasına rağmen bu parolayı kabul edip etmedikleri davranışlarını analiz etmektedir. Hipotez, kullanıcıların bilişsel uyumsuzluk farkındalığına göre davranışlarını değiştirip değiştirmediklerini test etmeyi amaçlamaktadır. Kullanıcılara zayıf parola ile karşılaştıklarında yeni parola denemesi sunulmuş ve kararları sistem tarafından kaydedilmiştir. Bu iki grup arasındaki fark, Pearson χ^2 testi ile analiz edilmiştir.

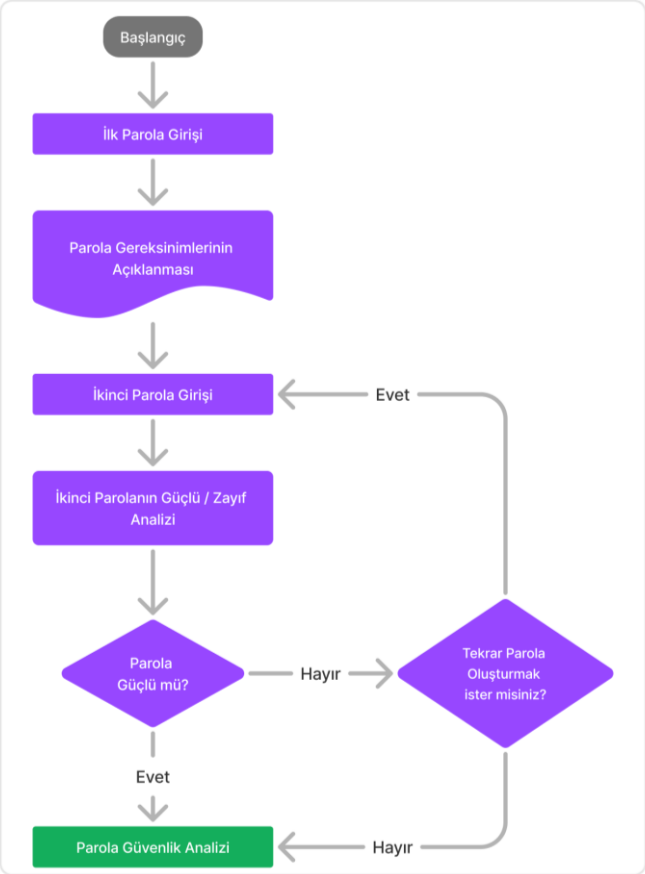
Bilişsel Uyumsuzluk Teorisi (Festinger, 1957), bireylerin inançları ve davranışları arasında çelişki algıladıklarında bu uyumsuzluğu azaltmak için davranışlarını değiştirme eğiliminde olduklarını savunmaktadır. Parola güvenliği bağlamında yapılan çalışmalar da bu teoriyi destekler niteliktedir. Choudhary vd. (2021), kullanıcıların hatırlanabilirlik ile güvenlik arasındaki çelişkiden dolayı bilişsel uyumsuzluk yaşadıklarını ve bu durumda güvenlik tercihlerinde değişikliğe gidebildiklerini göstermiştir. Ayrıca Kostić ve Saveljić (2023), oyunlaştırma yoluyla kullanıcılara verilen geri bildirimlerin davranışsal uyumu artırdığını rapor etmiştir.

Hipotezler, React tabanlı sistemin kullanıcı davranışlarını gözlemlemeye ve güvenli parola oluşturma sürecine yönelik davranışsal eğilimleri istatistiksel olarak analiz etmeye olanak sağlayan ölçümler üzerinden yapılandırılmıştır. Bu sayede, kullanıcı yönlendirmelerinin etkisi ve bilişsel sürecin güvenlik tercihlerine etkisi bilimsel olarak test edilebilir hale getirilmiştir.

4. Uygulama

JavaScript kütüphanesi olan React kullanılarak hazırlanan model sistem, kullanıcıların parola oluşturma eğilimlerini analiz edecek ve güçlü parola oluşturma sürecini teşvik eden bir geri bildirim mekanizması sağlayacaktır. Böylece sistem, kullanıcıların parola oluşturma süreçlerindeki bilişsel tepkilerini ve tercihlerini analiz etmektedir.

Uygulamanın temel akışının özetlendiği Şekil 2'deki akış diyagramı, kullanıcıların güçlü bir parola oluşturma sürecini yönlendiren bir sistemin işleyişini göstermektedir. Süreç, kullanıcıdan ilk parola girişinin alınmasıyla başlar. Ardından, parola gereksinimleri kullanıcılara açıklanır. Kullanıcı ikinci kez parola girişi yaptığında, sistem bu parolanın güçlü ya da zayıf olduğunu analiz eder. Eğer parola zayıf bulunursa, kullanıcıya yeni bir parola oluşturma seçeneği sunulur ve kullanıcı isteğine göre tekrar parola oluşturur. Güçlü bir parola oluşturulduğunda ise süreç tamamlanarak parola güvenlik analizi gerçekleştirilir.



Şekil 2. Parola Gücü ve Kullanıcı Eğilimleri Akış Diyagramı

Uygulama kapsamında gerekli analizlerin sağlanması için hook yapısından faydalanılmıştır. Hook, bir React projesinde bileşenler arasında durum ve mantık paylaşımını kolaylaştırarak yeniden kullanılabilirlik sağlamaktadır. Bu bağlamda projede usePasswordMetric ve usePasswordAnalysis hook'ları oluşturulmuştur. İlk olarak, usePasswordMetric hook'u kullanılarak parolayla ilgili özellikler, belirlenen veri seti parametrelerine göre analiz edilmiştir. Bu analiz sürecinde farklı görevleri yerine getiren yardımcı fonksiyonlar ile parola özellik değerleri hesaplanmıştır.

Kullanılan yardımcı fonksiyonlardan ilki extractFeatures isimli fonksiyondur. Girdi parametresi olarak parola, analiz metriği (metric) ve aktif aşama bilgisini (activeStage) alan fonksiyon parola uzunluğu, parolanın içerdiği karakter türleri (küçük/büyük harf, rakam, özel karakter), art arda gelen karakterler, sözlük kelimeleri içerip içermediği, yaygın bir parola

olup olmadığı ve entropi gibi özellik değerlerini hesaplayarak geri dönüş değeri olarak verir. Tüm bu hesaplamaları checkContainsDictionaryWord, isCommonPassword, countConsecutiveChars ve calculateEntropy gibi yardımcı fonksiyonlardan faydalanarak gerçekleştirmektedir.

CheckWord, Türk Dil Kurumu'nun (TDK) API'sini kullanarak kullanıcı parolasının sözlükte yer alan geçerli bir kelime olup olmadığını kontrol eden fonksiyondur. Bu fonksiyon, parolayı TDK API'si üzerinden sorgular ve sözlükte bulunup bulunmadığını belirler. Girdi olarak parola (password) alır ve eğer sözlükte mevcutsa true, değilse false değerini döndürür. CheckContainsDictionaryWord fonksiyonu, parolanın bir sözlük kelimesi içerip içermediğini kontrol etmek amacıyla geliştirilmiştir. Bu işlem için checkWord fonksiyonunu çağırır ve parolanın geçerli bir sözlük kelimesi içerip içermediğini belirler. Girdi olarak parola (password) alır ve çıktı olarak sözlükte bir kelime bulunuyorsa true, bulunmuyorsa false değerini döndürür.

LoadCommonPasswords, yaygın olarak kullanılan parolaları yüklemek için tasarlanmış bir fonksiyondur. Fonksiyon, bir dosyadan (örneğin, /model/common-passwords) yaygın parola listesini çeker ve bu listeyi kullanılmak üzere bellekte saklar.

IsCommonPassword, parolanın yaygın parola listesinde olup olmadığını kontrol eden bir fonksiyondur. Bellekte tutulan commonPasswords listesini kullanarak, verilen parolanın bu listede yer alıp almadığını kontrol eder. Girdi olarak parola (password) alır ve eğer parola yaygın parolalar arasında yer alıyorsa true, aksi takdirde false değerini döndürür.

CountConsecutiveChars fonksiyonu, parolada art arda tekrarlayan karakterlerin maksimum uzunluğunu bulmayı amaçlar. Parolayı karakter karakter tarar ve tekrarlanan karakterlerin oluşturduğu en uzun diziyi hesaplar. Girdi olarak parola (password) alır ve çıktı olarak, paroladaki en uzun ardışık tekrar eden karakter dizisinin uzunluğunu döndürür.

CalculateEntropy, bir parolanın karmaşıklık derecesini ölçmek amacıyla entropi değerini hesaplayan bir fonksiyondur. Bu fonksiyon, parola uzunluğu ve içindeki benzersiz karakter sayısını temel alarak bir entropi değeri üretir. Kullanılan entropi formülü (1) ifadesinde sunulmuştur:

$$log_2(benzersiz\ karakter\ sayısı) \times Parola\ Uzunluğu \quad (1)$$

Formül, girdi olarak parola (password) bilgisini alır ve çıktı olarak parolanın entropi değerini döndürür. Daha yüksek entropi değeri, daha güçlü bir parolayı işaret eder.

Analiz öncesi, parola gücünü ölçmek için check-password-strength JavaScript paketi çalışmaya entegre edilmiş ve parolaların görsel karşılaştırmasını sağlamak amacıyla react-password-strength-bar paketi kullanılmıştır. Bu paket, parolaları Tablo 2'de verilen özelliklere göre sınıflandırmaktadır:

Tablo 2. Check Password Strength Paket Özellikleri

Özellik	Açıklama
Id	0 = Çok Zayıf, 1 = Zayıf, 2 = Orta, 3 = Güçlü
Value	Çok Zayıf, Zayıf, Orta, Güçlü
Contains	Küçük harf, büyük harf, sembol ve/veya rakam
Length	Parolanın uzunluğu

Kaynak: Vincent, 2024

Projenin son aşamasında, elde edilen verilere dayanarak hipotezlere uygun analizler gerçekleştirilmiştir. Bu analizler, usePasswordAnalysis hook'u içerisindeki fonksiyonlar aracılığıyla yapılmıştır.

CalculateMostStrengthPassword, kullanıcının oluşturduğu parolalar arasından en güçlü parolayı belirlemek için kullanılan bir fonksiyondur. Bu fonksiyon, parolaların strength (güç) değerlerini karşılaştırır ve en yüksek değere sahip olan parolayı döndürür. Girdi olarak aşamalar (stages) alır ve çıktı olarak güç değeri en yüksek olan parolayı ve ilgili aşama bilgisini verir.

CalculateMostEntropyPassword, kullanıcının oluşturduğu parolalar arasından en yüksek entropiye sahip olan parolayı belirlemeyi amaçlar. Bu işlem için, parolaların entropy (karmaşıklık) değerlerini karşılaştırır ve en yüksek değere sahip olan parolayı döndürür. Girdi olarak aşamalar (stages) alır ve çıktı olarak en yüksek entropiye sahip parolayı ve ilgili aşama bilgisini sağlar.

AnalyzeFirstAndOtherStagesPasswords, kullanıcının ilk aşamada oluşturduğu parola ile sonraki aşamalarda oluşturduğu parolaların ortalama güç değerlerini karşılaştırmak için tasarlanmıştır. Fonksiyon, ilk parola ve diğer parolaların ortalama güç değerlerini hesaplayarak, kullanıcı yönergelerle daha güçlü parolalar oluşturmuş mu analiz eder. Girdi olarak aşamalar (stages) alır ve çıktı olarak ilk parolanın gücünü, diğer parolaların ortalama gücünü ve analiz sonucunda bir açıklama mesajını döndürür.

CalculateDurationAnalysis, kullanıcının parola oluşturma süresi ile parola gücü arasındaki ilişkiyi analiz eden bir fonksiyondur. Bu fonksiyon, parola oluşturma sürelerini ve bu sürelerde oluşturulan parolaların gücünü karşılaştırır. Girdi olarak aşamalar (stages) ve aşama süreleri (userStats.times) alır. Çıktı olarak, güç değeri en yüksek olan parolayı, ilgili aşama bilgisini ve süre-güç ilişkisini açıklayan bir mesaj döndürür.

CalculateAttemptsDurationStrengthAnalysis, kullanıcının parola oluşturma deneme sayıları, süreleri ve parola gücü arasındaki ilişkiyi analiz etmeyi amaçlar. Bu fonksiyon, kullanıcı tarafından en uzun ve en kısa sürede yapılan denemelerle oluşturulan parolaları karşılaştırır. Girdi olarak aşamalar (stages), aşama süreleri (userStats.times) ve aşama deneme sayıları (userStats.attempts) alır. Çıktı olarak en uzun ve en kısa sürede oluşturulan parola bilgileri ile süre ve parola gücü arasındaki ilişkiyi açıklayan bir mesaj sağlar.

UserIsAcceptedPassword, kullanıcının son aşamada oluşturduğu parolayı kabul etme motivasyonunu analiz eden bir fonksiyondur. Fonksiyon, kullanıcı tarafından oluşturulan parolaların gücünü ve kabul kararını değerlendirerek, kullanıcı güvenlik bilincini analiz eder. Girdi olarak aşamalar (stages) alır ve çıktı olarak kullanıcının güvenlik bilinci ve karar süreci hakkında bir açıklama mesajı döndürür.

Bu analiz fonksiyonları yardımıyla elde edilen kullanıcı verileri, çalışmada önerilen üç hipotezi test etmek amacıyla istatistiksel olarak değerlendirilmiştir. Veriler, sistem tarafından otomatik olarak kaydedilen parola girişleri, süre ölçümleri ve kullanıcı tercihleri üzerinden elde edilmiştir. Analizlerde bağımlı gruplar t-testi, Pearson korelasyon katsayısı ve ki-kare testi kullanılmıştır.

Hipotez 1 kapsamında, kullanıcıların yönerge öncesi (Aşama 1) ve yönerge sonrası (Aşama 2) oluşturdukları parolaların güç düzeyleri karşılaştırılmıştır. Yönerge öncesi ortalama parola güç skoru 0.82 (SS = 0.56), yönerge sonrası ortalama 2.38 (SS = 0.60) olarak ölçülmüştür. Bağımlı gruplar t-testi sonucu bu farkın istatistiksel olarak oldukça anlamlı olduğunu göstermektedir ($t(49) = -12.47$, $p < .001$). Bu sonuç, sistemin sağladığı yönlendirmelerin parola güvenliği davranışını olumlu etkilediğini ortaya koymaktadır.

Hipotez 2 kapsamında, parola oluşturma süresi ile parola güç düzeyleri arasındaki ilişki incelenmiştir. Pearson korelasyon katsayısı hesaplaması sonucunda bu iki değişken arasında istatistiksel olarak anlamlı olmayan, zayıf düzeyde negatif bir ilişki bulunmuştur ($r = -0.125$, $p = .386$). Bu sonuç, kullanıcıların uzun süre harcamalarının her zaman daha güçlü parola oluşturdukları anlamına gelmediğini, bazı durumlarda kısa sürede de güçlü parola üretilebildiğini göstermektedir.

Hipotez 3 kapsamında, sistem tarafından zayıf parola uyarısı verilen kullanıcıların kararları analiz edilmiştir. Katılımcıların %68'i zayıf parolayı değiştirme yönünde davranış sergilemiş, %32'si ise zayıf parola uyarısına rağmen parolayı kabul etmiştir. Ki-kare testi sonucunda bu fark istatistiksel olarak anlamlı bulunmuştur ($\chi^2(1, N=50) = 3.92$, $p = .048$). Bu durum, bilişsel uyumsuzlukla karşılaşan kullanıcıların büyük ölçüde güvenli davranış yönünde tercih geliştirdiğini göstermektedir.

5. Tartışma

Günümüzde güvenli parola oluşturma süreci, bilişsel yük ve kullanıcı alışkanlıkları açısından önemli bir konu olmaya devam etmektedir. Bilişsel Uyumsuzluk Teorisi incelenerek, literatürdeki çalışmalar da dikkate alınarak güvenli parola oluşturma sürecine yönelik hipotezler öne sürülmüştür. Literatürdeki çalışmalar, kullanıcıların güvenli parola oluşturma davranışlarını artırmak için çeşitli geri bildirim mekanizmalarının etkili olduğunu ortaya koymuştur. Çalışma kapsamında, kullanıcıların güvenli parola oluşturma davranışlarını etkileyen faktörlerin belirlenmesi ve bilişsel uyumsuzluk ile ilişkili mekanizmaların incelenmesi amaçlanmıştır. Bu doğrultuda, "Yönergelerle Desteklenen Parola Oluşturma Süreci, Kullanıcıların Güçlü Parolalar Oluşturma Olasılığını Artırır", "Kullanıcıların Parola Oluşturma Süresi, Parolanın Güçlülüğü ile Pozitif Korelasyona Sahiptir" ve "Zayıf parola uyarısı sonrasında kullanıcıların davranışlarını değiştirmeleri" hipotezleri oluşturulmuştur. Bu bölümde, önerilen hipotezler literatür bulgularıyla ilişkili şekilde ele alınarak tartışılmıştır.

Hipotez 1: Yönergelerle Desteklenen Parola Oluşturma Süreci, Kullanıcıların Güçlü Parolalar Oluşturma Olasılığını Artırır. Literatür, kullanıcılara verilen geri bildirim mekanizmalarının parola gücünü artırdığına dair birçok bulgu sunmaktadır. Jha vd. çalışmasında (2022), kullanıcıların alfasayısal parolalardan ziyade görselleri daha kolay hatırlayabildiğini göstermiştir. Bu, kullanıcı davranışlarını anlamada ve bilişsel yükü azaltarak güvenlik ile kullanım

kolaylığı arasındaki dengeyi kurmada kritik bir rol oynamaktadır. Ayrıca, yönergelerin ve geri bildirimlerin kullanıcıların parolalarını optimize etmeye yönelik bir yol haritası sunduğu, bilişsel uyumsuzluklarını azalttığı ve sonuç olarak daha güvenli parolalar üretmelerine olanak tanıdığı literatürde vurgulanmaktadır (Shay vd., 2010). Görsel geri bildirimler, kullanıcıların daha güvenli parolalar oluşturmasına ve güvenlik konusunda daha bilinçli çaba göstermelerine yardımcı olabilir. Örneğin, renk kodlamalı geri bildirimlerin ve güçlü/orta/zayıf ibarelerinin kullanıcıların güçlü parolalar oluşturma oranını önemli ölçüde artırdığını ortaya koyulmuştur. Benzer şekilde, çalışma kapsamında geliştirilen uygulamada da görsel geri bildirim sağlanarak kullanıcıların daha güçlü parolalar oluşturması teşvik edilmektedir. Görsel geri bildirimlerin, kullanıcıların parola güvenliği konusunda bilinçli bir çaba göstermelerine ve daha güvenli parolalar oluşturmalarına yardımcı olduğu literatürde geniş bir şekilde tartışılmaktadır. (Ur vd., 2015).

Hipotez 2: Kullanıcıların Parola Oluşturma Süresi, Parolanın Güçlülüğü ile Pozitif Korelasyona Sahiptir. Yapılan çalışmalar, parolanın gücünü artırmak isteyen kullanıcıların daha fazla zaman harcadıklarını ve düşünme sürecinin uzadığını göstermektedir. Florêncio ve Herley (2007), kullanıcıların karmaşık parolalar oluştururken basit parolalara göre daha fazla zaman harcadıklarını belirtmiştir. Ayrıca, Kennison vd. (2023), güçlü bilişsel işleme motivasyonuna sahip bireylerin daha güçlü parolalar oluşturduğunu göstermiştir. Bu bulgular, kullanıcıların güçlü parolalar oluştururken daha fazla düşünme, zaman harcama ve dikkat gösterme eğiliminde olduklarını desteklemektedir. Bu bağlamda, yapılan başka bir çalışma, kullanıcıların güvenli parola oluşturmak için daha fazla düşünme süresi harcadıklarını ve böylece oluşturdukları parolaların kalitesinin arttığını ortaya koymuştur (Shay vd., 2010). Çalışma kapsamında geliştirilen uygulamada da kullanıcıların parola oluşturma süresini ölçerek, parola gücü ile süre arasındaki ilişki analiz edilmektedir. Literatür ile tutarlı olarak, kullanıcılar daha karmaşık parolalar oluştururken daha fazla zaman harcamaktadırlar, bu da bilişsel kaynakların artmasını ve güvenli parola oluşturma sürecinin iyileştirilmesini sağlar. Ayrıca, kullanıcıların parola oluşturma süresi ile daha fazla dikkat harcama arasında bir ilişki olduğuna dair bulgular, uygulamamızda kullanıcıların parolalarını dikkatlice oluşturmasını teşvik etmek için önemli bir yol haritası sunmaktadır.

Hipotez 3 kapsamında ise, sistem tarafından "zayıf parola" uyarısı verilen kullanıcıların verdikleri kararlar incelenmiştir. Elde edilen bulgular, uyarıya rağmen parolasını değiştirmeyen kullanıcılarla, daha güçlü bir parola oluşturmak için davranışını değiştiren kullanıcılar arasında anlamlı bir fark olduğunu göstermektedir. Bu durum, Bilişsel Uyumsuzluk Teorisi'nin temel varsayımı olan, bireylerin içsel çelişki algıladıklarında davranışsal bir uyum geliştirme eğilimini destekler niteliktedir (Festinger, 1957). Kullanıcıların zayıf parola uyarısı sonrasında kararlarını yeniden gözden geçirmeleri, sistemin yalnızca teknik bir kontrol aracı değil, aynı zamanda bilişsel farkındalık sağlayan bir mekanizma olarak da işlev gördüğünü ortaya koymaktadır. Bu bağlamda, sistemin kullanıcıların güvenlik algısını artırma potansiyeli taşıdığı ve davranışsal dönüşüm yaratabildiği söylenebilir.

Bu çalışmada önerilen React tabanlı parola güvenliği sistemi, mevcut parola güvenliği yaklaşımlarına kıyasla üç temel noktada özgün katkılar sunmaktadır. Birincisi, sistem yalnızca parola gücünü analiz eden statik araçların ötesine geçerek, kullanıcı davranışını gerçek zamanlı izleyen ve geri bildirim sağlayan dinamik bir yapıya sahiptir. Örneğin, Ur vd. (2015) tarafından geliştirilen geri bildirim tabanlı parola ölçüm sistemleri sınırlı kullanıcı etkileşimi sunarken, bu çalışmada geliştirilen sistem kullanıcıya her aşamada yönlendirme sağlayarak bilişsel tepkileri analiz etmektedir.

İkincisi, Kostić ve Saveljić'in (2023) çalışmasında örneği sunulan oyunlaştırma tabanlı sistemler genellikle eğitsel amaçla kurgulanırken, önerilen sistem kullanıcıyı yönlendirmekle kalmayıp, aynı zamanda parolaların yapısal özelliklerini (entropi, ardışık karakterler, sözlük kelimesi içerme vb.) analiz ederek karar destekleyici bir araç işlevi de görmektedir.

Üçüncü olarak, mevcut parola gücü ölçüm sistemlerinin birçoğu yalnızca sonuca odaklanmakta ve parola iyi/zayıf olarak derecelendirilip bırakılmaktadır (Carnavalet ve Mannan, 2014). Bu sistem ise kullanıcıyı yalnızca sınıflandırmamakta, davranışa etki eden geri bildirimlerin analizini de içermektedir. Bu durum, sistemin hem parola güvenliğini artırma hem de kullanıcı farkındalığını geliştirme yönünde çift etkili bir araç olarak konumlandırılmasını mümkün kılmaktadır.

Sonuç ve Değerlendirme

Bu çalışmada, kullanıcıların güçlü parolalar oluşturma süreçlerini daha iyi anlamaya yönelik bir web tabanlı sistem tasarlanmıştır. Bir JavaScript kütüphanesi olan React kullanılarak oluşturulan bu model sistem, kullanıcıların parola oluşturma eğilimlerini analiz etmek ve güvenli parola oluşturma sürecine dair geri bildirim sağlamak amacıyla geliştirilmiştir. Kullanıcıların güçlü parolalar oluşturma sürecinde karşılaştıkları bilişsel zorluklar, bu süreçte verilen ipuçlarına nasıl tepki verdikleri ve parola oluşturma denemelerinin sonuçları bu analizle değerlendirilebilecektir. Bu sayede, kullanıcı davranışları hakkında derinlemesine bir anlayış elde edilmesi ve güvenli parola oluşturma süreçlerinin iyileştirilmesine yönelik öneriler sunulabilir.

Uygulama, kullanıcıya sağlanan görsel geri bildirimlerle parola güvenliği kriterlerine uygunluklarını artırmayı amaçlamaktadır. Verilen geri bildirimler sayesinde, kullanıcıların güçlü parola oluşturma davranışlarının geliştirilmesi

teşvik edilecektir. Şekil 1'de özetlenen akış diyagramı, sürecin temel işleyişini göstermektedir. İlk olarak, kullanıcıdan parola girişi alınır ve gereksinimler açıklanır. Ardından, ikinci parola girişi yapılır ve sistem, bu parolayı güçlü ya da zayıf olarak değerlendirir. Zayıf bir parola bulunursa, kullanıcıya yeni bir seçenek sunulur. Güçlü bir parola oluşturulduğunda, süreç tamamlanır ve güvenlik analizi yapılır. Projede gerekli analizlerin gerçekleştirilmesi için React'in hook yapısından faydalanılmıştır. Bu yapı, bileşenler arasında durum ve mantık paylaşımını kolaylaştırarak yeniden kullanılabilirliği sağlar. Özellikle, usePasswordMetric ve usePasswordAnalysis hook'ları oluşturulmuş ve bu sayede parola özellikleri, belirlenen parametreler doğrultusunda analiz edilmiştir.

Literatürdeki benzer çalışmalarla karşılaştırıldığında, bu uygulamanın sunduğu yeniliklerden biri, web destekli çözüm ve dinamik, gerçek zamanlı geri bildirim mekanizmalarının kullanılmasıdır. Diğer araştırmalar genellikle sabit kurallara, anketlere veya metinsel bildirimlere dayanırken, bu uygulama daha esnek ve kullanıcıyı sürekli olarak yönlendiren bir sistem sunmaktadır. Bu dinamik yaklaşım, kullanıcıların parola oluştururken karşılaştıkları bilişsel zorlukları daha etkili bir şekilde ele almayı amaçlamaktadır. Özellikle, Di Campi ve Luccio'nun (2024) çalışmalarındaki gibi kullanıcıların güvenlikten ziyade kullanılabilirliği tercih etmeleri göz önüne alındığında, bu çalışma ile parola güvenliği artırmaya yönelik bir adım atılmaktadır.

Ayrıca, diğer çalışmalarda yapılan testler ve kullanıcı uygulamaları, bu tür sistemlerin etkinliğini belirlemek için önemlidir. Kostić ve Saveljić (2023) oyunlaştırma yöntemleriyle kullanıcıları daha güçlü parolalar kullanmaya teşvik etmeyi başarmışlardır. Bunun yanı sıra, Florêncio ve Herley'nin (2007) araştırmalarında kullanıcıların parola yeniden kullanma eğilimleri ve zayıf parolaları tercih etme davranışları ele alınmıştır. Bu çalışma kapsamında oluşturulan web tabanlı sistemle benzer bir yaklaşım sergilenerek, geniş ölçekli bir kullanıcı kitlesi üzerinde yapılan testlerden elde edilen verilerle parola güvenliği konusunda bilinç artışı hedeflemektedir.

Araştırmanın gönüllü katılımcı ile çevrimiçi ortamda gerçekleştirip, örneklemin bilişim alanına yönelik birikime sahip bireylerden oluşması çalışmanın sınırlılıkları olarak görülmektedir. Dolayısıyla bulguların farklı disiplinlerden veya farklı yaş gruplarından bireylere genellenebilirliği sınırlı olabilir. Ayrıca, kullanıcıların demografik özellikleri (örneğin yaş, cinsiyet, mesleki deneyim) toplanmamış, yalnızca davranışsal veri üzerinden analiz yapılmıştır. Uygulamanın çevrimiçi yürütülmüş olması, kullanıcı davranışları üzerinde doğal ortam etkisi yaratmış olsa da, fiziksel gözlem eksikliği nedeniyle bazı etkileşim boyutları dışarıda kalmıştır. Gelecek çalışmalarda, daha geniş ve çeşitlendirilmiş bir örneklem ile yaş, eğitim düzeyi, teknoloji okuryazarlığı gibi değişkenlerin bilişsel parola davranışları üzerindeki etkisi incelenebilir. Ayrıca sistemin mobil uygulamalara veya kurumsal ortamlara entegrasyonu sağlanarak gerçek zamanlı parola oluşturma davranışları daha kapsamlı şekilde analiz edilebilir. Kullanıcı bilişselliğini daha derinlemesine anlamaya yönelik nöropsikolojik veri (örneğin göz izleme, karar süresi vb.) kullanımı da ileriki araştırmalar için potansiyel sunmaktadır.

Sonuç olarak, bu çalışma kullanıcıların parola oluşturma davranışlarını daha iyi anlayarak, güvenliği artıran dinamik ve kişiselleştirilmiş bir yaklaşım sunmaktadır. Çalışmada test edilen üç hipotezin sonuçları, sistemin rehberlik sağladığında kullanıcıların daha güçlü parolalar oluşturduğunu, oluşturma süresi ile parola gücü arasında pozitif bir ilişki bulunduğunu ve zayıf parola uyarısı alan kullanıcıların çoğunlukla davranışlarını değiştirme eğilimi gösterdiğini ortaya koymuştur. Bu bulgular, Bilişsel Uyumsuzluk Teorisi'nin dijital güvenlik bağlamındaki geçerliliğini desteklemekte ve kullanıcı davranışlarının güvenlik tercihlerine etkisini somut biçimde göstermektedir. Literatürdeki benzer çalışmalarla karşılaştırıldığında, bu araştırma, kullanıcı farkındalığını artıran görsel geri bildirim sistemlerini sadece teknik bir kontrol aracı değil, aynı zamanda bilişsel davranışsal bir müdahale aracı olarak konumlandırması bakımından özgün bir katkı sunmaktadır. Hem bireysel kullanıcılar hem de kurumsal güvenlik sistemleri açısından, kullanıcı merkezli, geri bildirim odaklı parola güvenliği yaklaşımlarının etkili olduğu görülmektedir. Gelecekte farklı demografik gruplarda yapılacak testlerle, sistemin genellenebilirliği daha sağlam biçimde değerlendirilebilir ve bu yaklaşım, dijital güvenliğe yönelik kullanıcı davranışı temelli politika ve sistemlerin geliştirilmesine katkı sağlayabilir.

Kaynakça

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. DOI:10.1109/SP.2012.44

Choudhary, M., Srivatsa, K., Upadhyay, I., & Srivastava, P. (2021). Is convenient secure? Exploring the impact of metacognitive beliefs in password selection. *Proceedings of the Annual Meeting of the Cognitive Science Society*, 43. Retrieved from https://escholarship.org/uc/item/7v1654s9

Choong, Y. & Theofanos, M. (2015). What 4,500+ People Can Tell You: Employees' Attitudes Toward Organizational Password Policy Do Matter.DOI:10.1007/978-3-319-20376-8_27

Di Campi, A. M. (2021). Password guessing: learn the nature of passwords by studying the human behavior. Retrieved from http://dspace.unive.it/handle/10579/19986

Di Campi, A. M. & Luccio, F. (2024). Understanding how users choose passwords: analysis and best practices. Retrieved from https://iris.unive.it/handle/10278/5057507#

De Carné de Carnavalet, X. & Mannan, M. (2014). From Very Weak to Very Strong: Analyzing Password-Strength Meters. Retrieved from https://spectrum.library.concordia.ca/id/eprint/978105/

Festinger, L. (1957). A theory of cognitive dissonance. Stanford University Press.

Florencio, D. & Herley, C. (2007). A large-scale study of web password habits.DOI: 10.1145/1242572.1242661

Joe Beach Capital. (n.d.). Top 10 million passwords. kaggle. Retrieved from https://www.kaggle.com/datasets/joebeachcapital/top-10-million-passwords

Jha, Anand & Bhatele, Kirti Raj & Philip, Prajeesh & Mishra, Khushi. (2022). Graphical password authentication system for web and mobile applications in javascript. DOI:10.4018/978-1-6684-5827-3.ch011.

Kennison, S. M., & Chan-Tin, D. E. (2023). Personality and cognitive factors in password security behaviors. North American Journal of Psychology, 25(3), 599–618.

Katsini, C., Fidas, C., Belk, M., Samaras, G., & Avouris, N. (2019). A Human-cognitive perspective of users' password choices in recognition-based graphical authentication. *International Journal of Human–Computer Interaction*, 35(19), 1800–1812. https://doi.org/10.1080/10447318.2019.1574057

Kostić, M. & Saveljić I. (2023). Gamification as a Tool for Elevating Password Strength Awareness. Retrieved from https://ceur-ws.org/Vol-3676/short_03.pdf

LastPass Security Team. (2020). New report: Combatting cognitive dissonance in password creation. LastPass Blog. Retrieved from https://blog.lastpass.com/posts/new-report-combatting-cognitive-dissonance-in-password-creation

Li, S. , Romdhani, I., & Buchanan, W. (2016). Password Pattern and Vulnerability Analysis for Web and Mobile Applications https://doi.org/10.3969/j.issn.1673-5188.2016.S0.006

Mark Deanil Vicente. (2024). check-password-strength. Retrieved from https://github.com/deanilvincent/check-password-strength

Morph1Max. (2021). Password security sber dataset. kaggle. Retrieved from https://www.kaggle.com/datasets/morph1max/password-security-sber-dataset/data

Perez, M. (2021). New report: Combatting cognitive dissonance in password creation. Retrieved from https://www.netsec.news/cognitive-dissonance-password-creation/

Shay, R., Komanduri, S., Mazurek, M. L., Segreti, S., Ur, B., Bauer, L., Christin, N., & Cranor, L. F. (2010). Encountering stronger password requirements: User attitudes and behaviors. DOI:10.1145/1837110.1837113

Scholefield, S., & Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness.10.48550/arXiv.1903.08454.

Shin, SJ. (2022). react-password-strength-bar. Retrieved from https://gith

Ur, B., et al. (2015). I added '!' at the end to make it secure": Observing password creation in the lab.DOI:10.5555/3235866.3235877.

Extended Abstract

Aim and Scope

This study presents a web-based system developed to analyze users' password creation behaviors and to support secure password generation processes. The primary aim is to understand users' cognitive tendencies and contribute to the formation of strong passwords. Within the scope of the study, the proposed model analyzes users' password creation patterns and provides a real-time feedback mechanism.

The research examines the cognitive difficulties users encounter during the password creation process, as well as their reactions to the hints and prompts provided. By evaluating users' trial behaviors and actions throughout the password generation process, the study develops recommendations aimed at improving secure password creation practices.

Methods

A web-based system was developed using the React framework. The system is designed to analyze the difficulties users encounter during the password creation process and to provide guidance for generating stronger passwords. By identifying users' password creation tendencies, the system offers a mechanism that supports secure password formation.

Findings

Analyses conducted within the study indicate that users experience cognitive dissonance during the password creation process and tend to generate stronger passwords when guidance is provided. A review of the literature confirms that feedback mechanisms offered to users are effective in enhancing password security. Additionally, a positive correlation was found between the time spent on password creation and the resulting password strength.

Conclusion

This study introduces a system aimed at understanding users' behaviors during the password creation process and encouraging the development of secure password habits. Analyzing users' behavioral patterns contributes significantly to increasing cybersecurity awareness. The proposed model is expected to raise awareness of password security and motivate users to create stronger, more secure passwords.