Ad Soyad: _____ **Tarih:** _____ **Puan:** _____

Parola sızıntıları ve kimlik bilgisi güvenliği

Kimlik bilgisi doldurma, veri ihlalleri, karma algoritmaları, çok faktörlü kimlik doğrulama ve parola güvenliği.

PAROLA SIZINTILARINA GENEL BAKIŞ

GÜVENCEDE
VERİ ŞİFRELEME
256 bit AES Standardı

UYUMLU
KÜRESEL STANDARTLAR
GDPR ve CCPA çerçeveleri

SIFIR GÜVEN
ERİŞİM POLİTİKASI
Çok Faktörlü Kimlik Doğrulama

Hoş geldin! Bu etkinlik paketi sana parola sızıntıları ve kimlik bilgisi güvenliği konusunda rehberlik eder. Kimlik bilgisi doldurmayı (credential stuffing), veri ihlallerini, karma algoritmalarını, çok faktörlü kimlik doğrulamayı ve parola yöneticilerini keşfedeceksin.

ÇALIŞMA KÂĞIDI KONTROL NOKTALARI

- [ ] **Bölüm 1-4: Siber güvenlikte ve tehdit önlemede ustalaş.**
- [ ] **Bölüm 5-7: Çapraz bulmaca ve kelime avı bulmacalarını çöz.**
- [ ] **Bölüm 8-9: Vaka çalışmalarını ve şifre görevini çöz.**
- [ ] **Bölüm 10: Temel ve ileri düzey SSS sayfalarını gözden geçir.**
- [ ] **Bölüm 11: 10 ilginç gerçek dünya gerçeğini keşfet.**
- [ ] **Bonus: Hızlı Düşün görevi.**

VPN.com siber güvenlik rehberini aç

URL: https://www.vpn.com/tr/siber-guvenlik/sifre-sizintisi/

Parola Güvenliği Öğrenme Yol Haritan

- Karanlık web forumlarında kimlik bilgilerinin ifşa olma risklerini anla.
- Çok faktörlü kimlik doğrulama (MFA) ve ele geçirilmiş kimlik bilgisi izleme uygula.
- Hedefli sosyal mühendislik dolandırıcılıklarına karşı kurumsal güvenlik savunmaları tasarla.

PAROLA SIZINTILARI REHBERİ YÖNERGELERİ

Çoktan seçmeli ve doğru/yanlış sorularını cevapla, boşluk doldurma cümlelerini kelime bankasını kullanarak tamamla, tanımları eşleştir, çapraz bulmacayı ve kelime avı bulmacasını çöz. Bilgini şu konulara uygula: kimlik bilgilerinin korunması. Hızlı Düşün bonus etkinliğiyle bitir.

PAROLA SIZINTILARI VE KİMLİK BİLGİSİ GÜVENLİĞİ (GİRİŞ)

Parola sızıntıları, kullanıcı kimlik bilgilerini herkese açık sitelerde ve dark web'de ifşa eder. Parola yöneticisinden benzersiz parolalar, ihlal edilmiş parola taraması ve çok faktörlü kimlik doğrulama (MFA), kimlik bilgisi doldurma riskini azaltırken; tuzlanmış, yavaş parola özetleme (hashing) bir parola veritabanı çalınırsa zararı sınırlar.

HER KONTROL NOKTASINI DİKKATLE OKU VE DOĞRU CEVABI SEÇ YA DA YAZ.

Kontrol Noktası 1: Çoktan seçmeli görev

1. Kimlik bilgisi doldurma (credential stuffing) nedir?

- A. Sızdırılmış kullanıcı adı/parola kombinasyonlarını birden fazla sitede denemek için otomasyon kullanmak
- B. Yerel veritabanı depolama dosyalarını şifrelemek
- C. Web sunucularını ağ trafiği istekleriyle boğmak
- D. Klavye girdilerini gizlice izlemek

2. OWASP bugün parolaları saklamak için ilk tercih olarak hangi algoritmayı listeliyor?

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3. Çok faktörlü kimlik doğrulama (MFA), parola sızıntılarının riskini nasıl azaltır?

- A. Ek bir doğrulama faktörü gerektirir, bu yüzden çalınmış bir parola tek başına yeterli olmaz
- B. Parolayı her saat otomatik olarak değiştirir
- C. Kullanıcı adını iletim sırasında şifreler
- D. Sahte talepleri kredi bürosuna bildirir

4. Veri ihlali dökümü nedir?

- A. Çevrimiçi yayımlanan veya bilgisayar korsanı forumlarında satılan sızdırılmış kullanıcı kimlik bilgileri koleksiyonu
- B. Veritabanı dosyalarının site dışında saklanan yedek kopyası
- C. Web sunucusu kayıtlarının geçici önbelleği
- D. Kullanıcı parolalarını sıfırlamak için kullanılan bir yönetim aracı

5. Parola yöneticisinin rolü nedir?

- A. Her hesap için benzersiz, güçlü parolalar üretmek ve saklamak
- B. Parola sızıntıları için ağ trafiğini izlemek
- C. Otomatik kaba kuvvet saldırılarını ağ geçidinde engellemek
- D. Veritabanı depolama bloklarını şifrelenmemiş parolalar için taramak

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Parolaları birden fazla hesapta tekrar kullanmak, kimlik bilgisi doldurma riskini artırır.

Doğru Yanlış

7 Soru 7

7. SHA-1, modern parola depolama için önerilen bir karma işlevidir.

Doğru Yanlış

8 Soru 8

8. Yalnızca parola karmaşıklığını zorunlu kılmak (MFA olmadan) kimlik bilgisi doldurmayı tamamen durdurur.

Doğru Yanlış

9 Soru 9

9. Karanlık ağ izleme araçları, ele geçirilmiş kurumsal kimlik bilgileri için interneti tarar.

Doğru Yanlış

10 Soru 10

10. Tuzlu karmalar, gökkuşağı tablosu saldırılarını boşa çıkarmak için karmalamadan önce parolalara benzersiz rastgele veri ekler.

Doğru Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

Aşağıdaki her cümleyi oku ve boşluğu Kelime Bankası'ndaki doğru terimle doldur.

1. Sızdırılmış kimlik bilgilerini birçok web uygulamasında denemek, kimlik bilgisi _____ saldırısıdır.

2. OWASP tarafından hâlâ kabul gören yavaş, uyarlanabilir parola karma algoritması: _____ .

3. Gizli veritabanı dosyalarının internette açığa çıkmasına veri _____ denir.

4. Parolalara karma işleminden önce rastgele değerler eklemeye _____ denir.

5. Kullanıcı kimlik bilgileri için güvenli bir yerel veritabanı sunan araca _____ denir.

6. Girişe ikinci bir doğrulama adımı eklemeye _____ doğrulama denir.

KELİME BANKASI

BCRYPT · ÇOK FAKTÖRLÜ · DOLDURMA · GÖKKUŞAĞI · İHLAL · KİMLİK AVI · PAROLA KASASI · TUZLAMA

Cevaplarını buraya yaz:

1.
2.
3.
4.
5.
6.

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

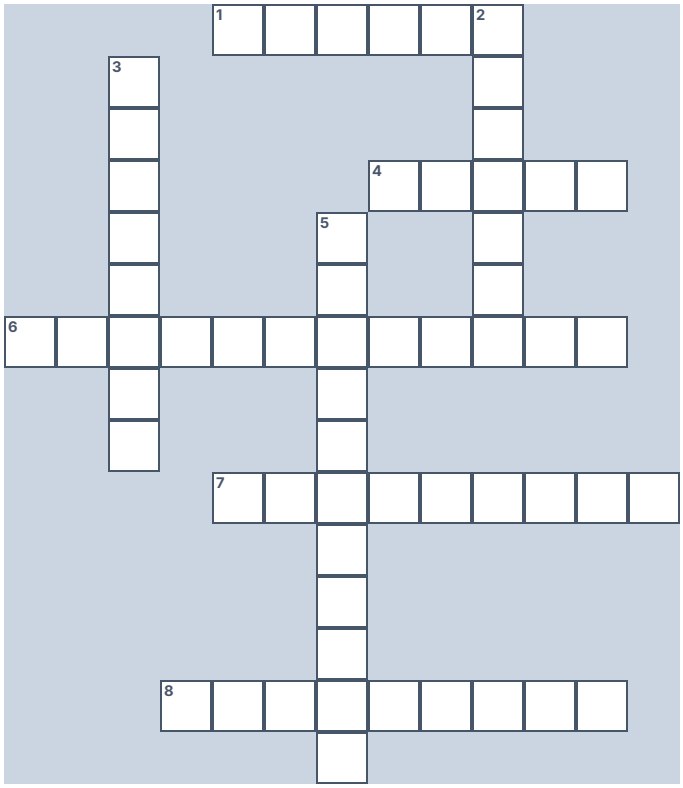
TANIM EŞLEŞTİRME

Soldaki her kelimeyi, doldurulabilir giriş kutusuna ilgili harfi (A-H) yazarak sağdaki doğru tanımıyla eşleştir.

☐	1. DOLDURMA	A	Önceden hesaplanmış parola özeti (hash) tablosu.
☐	2. BCRYPT	B	Çok faktörlü oturum açma kontrolü.
☐	3. İHLAL	C	Kimlik bilgisi depolama aracı.
☐	4. TUZLAMA	D	Yetkisiz veri tabanı ifşası.
☐	5. YÖNETİCİ	E	Girişleri çalmak için sosyal mühendislik.
☐	6. MFA	F	Sızdırılmış kimlik bilgilerini test etme.
☐	7. GÖKKUŞAĞI	G	Parola karmasına rastgele tuz eklemek.
☐	8. KİMLİK AVI	H	Yavaş parola karma algoritması.

Kontrol Noktası 5: Bulmaca

Bulmacayı, etkin beyaz kutulara harf yazarak çöz. Sayılar aşağıdaki ipuçlarına karşılık gelir.



SOLDAN SAĞA

1. Yavaş parola karma algoritması (6)

4. Yetkisiz veritabanı ifşası (5)

6. Kimlik bilgisi saklama aracı (12)

7. Parola karmalarının önceden hesaplanmış tablosu (9)

8. Oturum bilgilerini çalmak için sosyal mühendislik (9)

YUKARIDAN AŞAĞI

2. Parola karmasına rastgele tuz ekleme (7)

3. Sızdırılmış kimlik bilgilerini test etme (8)

5. Çok faktörlü giriş denetimi (11)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

Ekran okuyucu ve klavye kullanıcıları, bulmaca cevaplarını aşağıdaki metin alanlarına doğrudan yazabilir.

SOLDAN SAĞA

1 soldan sağa: Yavaş parola karma algoritması (6 harf):

4 soldan sağa: Yetkisiz veritabanı ifşası (5 harf):

6 soldan sağa: Kimlik bilgisi saklama aracı (12 harf):

7 soldan sağa: Parola karmalarının önceden hesaplanmış tablosu (9 harf):

8 soldan sağa: Oturum bilgilerini çalmak için sosyal mühendislik (9 harf):

YUKARIDAN AŞAĞI

2 yukarıdan aşağı: Parola karmasına rastgele tuz ekleme (7 harf):

3 yukarıdan aşağı: Sızdırılmış kimlik bilgilerini test etme (8 harf):

5 yukarıdan aşağı: Çok faktörlü giriş denetimi (11 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

Aşağıdaki ızgarada gizlenmiş 8 temel kelimeyi bul. Kelimeler yatay, dikey veya çapraz olabilir.

B C R Y P T H K L L İ Ö O G L
Ü L Ö P R Ş L İ S G D C R Ö N
L A Ğ R C A U M D S O Y T C Z
R M U F L İ Ğ L Z Ç L L D Ö Ü
Ö A O H C Ş B İ A Z D M D G J
T L İ A D N D K E G U H Ç Ö P
K Z Ö K E H R A Z R R F Ö K U
A U E A A Ö N V L O M Ş V K Ö
F T İ P Ş R Ç I L Y A B F U R
K Ü Ü I A P Z Y Y J G H L Ş P
O P A R O L A K A S A S I A İ
Ç K K S N Ğ Ö Ö G Z A N T Ğ F
T C Y P Y B Ğ K Z G I M O I M
Ü C K Z Y F V N U T J T O B M
U S K G T Ç Y T İ P B Ü Z V K

KELİME LİSTESİ

DOLDURMA BCRYPT İHLAL TUZLAMA PAROLAKASASI ÇOKFAKTÖRLÜ GÖKKUŞAĞI KİMLİKAVI

Kontrol Noktası 6, alternatif: Erişilebilir kelime eşleştirme

Kelime Bulmaca'daki 8 kelimenin her birini, boşluğa harfi (A-H) yazarak doğru tanımıyla eşleştir.

KELİME TERİMLERİ

- **A. DOLDURMA**
- **B. BCRYPT**
- **C. İHLAL**
- **D. TUZLAMA**
- **E. PAROLAKASASI**
- **F. ÇOKFAKTÖRLÜ**
- **G. GÖKKUŞAĞI**
- **H. KİMLİKAVI**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Oturum bilgilerini çalmak için sosyal mühendislik.
2. Yetkisiz veritabanı ifşası.
3. Yavaş parola karma algoritması.
4. Parola karmalarının önceden hesaplanmış tablosu.
5. Sızdırılmış kimlik bilgilerini test etme.
6. Parola karmasına rastgele tuz ekleme.
7. Kimlik bilgisi saklama aracı.
8. Çok faktörlü giriş denetimi.

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Temel siber güvenlik kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını verilen giriş kutularına yaz.

1. MDUDROAL
2. İLALH
3. PAAKSSRAILAO
4. UIĞKAŞGÖK
5. YRTBPC
6. MZATLAU
7. ÖAÇOTÜRLKKF
8. İİVKLİKAM

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Bugün başlayabileceğin güvenli alışkanlıklar			
2	Güçlü parola kuralları			
3	Bildiğin parola yöneticileri			
4	Bildiğin güvenlik araçları			
5	E-postadaki uyarı işaretleri			
6	Uzun bir parola cümlesi için eğlenceli sözcükler			
7	Parolasız oturum açma yolları			
8	Asla paylaşmaman gereken bilgiler			
9	Yazılımı güncelleme nedenleri			
10	Parola sızdığında yapılacaklar			
11	MFA gereken hesaplar			
12	Parolaların asla saklanmaması gereken yerler			
13	Bir bilgisayarın virüslü olduğunu gösteren işaretler			
14	İnsanların kullandığı kötü parolalar			
15	Yedeklediğin şeyler			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: KURUMSAL KİMLİK BİLGİSİ SIZINTISINI GİDERME



Senaryo: Bir karanlık ağ izleme hizmeti, kurumsal sistem yöneticilerinin parolalarını içeren bir veritabanı dökümünün çevrimiçi yayınlandığı konusunda bir kuruluşu uyarıyor.

Tartışma sorusu: Kimlik bilgisi sızıntısı risklerini analiz et ve bir yönetimsel sıfırlama stratejisi öner.

VAKA ÇALIŞMASI 2: PAROLA KARMALAMA STANDARTLARINI UYGULAMA



Senaryo: Bir kurumsal veritabanı şu anda kullanıcı parolalarını kriptografik tuz (salt) olmadan eskimiş MD5 özetleriyle (hash) saklıyor ve bu da parolaları hızlı çıkarılmaya karşı savunmasız kılıyor.

Tartışma sorusu: Veritabanı özetleme algoritmasını yükseltmek için bir geçiş stratejisi tasarla.

Kontrol Noktası 9: Şifreyi Çöz

Bir siber güvenlik uzmanı, ağ varlıklarını çevrimiçi tehdit aktörlerine karşı korur. Aşağıdaki Harf-Sayı anahtarını kullanarak, eşleşen harfleri boşluklara yazıp mesajın şifresini çöz.

HARFTEN SAYIYA ŞİFRELEME ANAHTARI

A=1 B=2 C=3 Ç=4 D=5 E=6 F=7 G=8 Ğ=9 H=10

I=11 İ=12 J=13 K=14 L=15 M=16 N=17 O=18 Ö=19 P=20

R=21 S=22 Ş=23 T=24 U=25 Ü=26 V=27 Y=28 Z=29

22	11	29	1	17		20	1	21	18	15	1	15	1	21	11		4	18	14

7	1	14	24	19	21	15	26		8	12	21	12	23	15	6		14	18	21	25

Çözülen mesaj:

İPUCU: HER SAYI, O HARFİN ALFABEDEKİ SIRASINI GÖSTERİR (ÖR. 1 = A, 2 = B, 29 = Z).

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm A)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q1: Parola sızıntısı nedir?

Parola sızıntısı, kullanıcı oturum açma bilgilerinin veri ihlalleri veya sunucu yanlış yapılandırmaları yoluyla açığa çıkmasıyla oluşur.

Q2: Bilgisayar korsanları sızdırılmış parolaları nasıl bulur?

Bilgisayar korsanları, ihlal verilerinin yayımlandığı dark web forumlarını, herkese açık veri tabanı dökümlerini ve paste sitelerini tarar [8].

Q3: Parola tekrar kullanımı tehlikeli midir?

Evet, çünkü bir site ele geçirilirse bilgisayar korsanları aynı kimlik bilgilerini binlerce başka platformda deneyebilir [3].

Q4: Kriptografik tuz (salt) nedir?

Tuz (salt), karma işleminden önce parolaya eklenen rastgele veridir ve önceden hesaplanmış arama saldırılarını etkisiz kılar [2].

Q5: MD5 neden eskimiştir?

MD5 hızlı ve eskimiş genel amaçlı bir özet (hash) işlevidir; bu yüzden saldırganlar, özellikle özetler tuzsuz olduğunda, parola tahminlerini son derece hızlı deneyebilir [2].

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm B)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Parola yöneticisi kullanıcıları nasıl korur?

Her site için karmaşık, benzersiz kimlik bilgilerini otomatik oluşturur; insanın bellek hatalarını ve yeniden kullanımı azaltır.

Q7: Kaba kuvvet saldırısı nedir?

Doğru parola bulunana kadar olası her karakter kombinasyonunu sistematik olarak deneyen saldırı [4].

Q8: Hesap kilitleme nasıl yardımcı olur?

Hesap kilitleme veya hız sınırlama, tekrarlanan çevrimiçi tahminleri yavaşlatır; izleme ve MFA ile birlikte kaba kuvvet saldırısı riskini azaltır [4].

Q9: Ana parolalar güvenli mi?

Başka web sistemlerinde asla yeniden kullanılmayan, yüksek entropili parola ibareleriyse güvenlidirler.

Q10: Parolalar düzenli olarak değiştirilmeli mi?

NIST, dönemsel değişikliğin zorlanmaması gerektiğini söyler; ele geçirilme kanıtı olduğunda değiştir ve uzunluğa, engelleme listelerine ve MFA'ya öncelik ver [1].

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm C)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q1: Argon2, bcrypt ile nasıl karşılaştırılır?

OWASP, ilk tercih olarak Argon2id'yi listeler; bellek yoğun ayarları, GPU ve ASIC ile kırmaya karşı bcrypt'ten daha iyi direnç gösterir [2].

Q2: Anahtar germe (key stretching) nedir?

Parola doğrulama sürecini yavaşlatmak için bir karma algoritmasını binlerce kez döngüye alan ve kırmayı pahalı hale getiren teknik [2].

Q3: Gökkuşağı tabloları nasıl çalışır?

Açık parolaları karma değerlerine bağlayan, tuzlanmamış karma değerlerini hızla tersine çevirmek için kullanılan önceden hesaplanmış arama tablolarıdır [2].

Q4: Kimlik bilgisi geri dönüşümü nedir?

Bir ihlalden çalınan kullanıcı adı/parola çiftlerini, özellikle insanların parolaları tekrar kullandığı yerlerde, diğer hizmetlere erişmek için yeniden kullanmak [3].

Q5: Parola yöneticileri hacklenebilir mi?

Evet. Çoğu sıfır bilgi şifrelemesi kullanır; bu yüzden sunucu ihlali yalnızca şifreli kasaları açığa çıkarır, ancak zayıf ana parolalar yine de çevrimdışı kırılabilir.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm D)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q6: Sözlük saldırısı nedir?

Rastgele harfler yerine yaygın sözcükleri, ifadeleri ve geçmişte sızdırılmış parolaları deneyen bir kaba kuvvet çeşidi.

Q7: Parola cümleleri neden tercih edilir?

Parola cümleleri birden çok rastgele sözcük kullanır; insanların hatırlaması kolay ama kırılması hesaplama açısından maliyetli yüksek entropi oluşturur [1].

Q8: Çoklu oturum açma (SSO) parola sızıntılarını nasıl etkiler?

SSO parola yayılımını azaltır, ancak kimlik sağlayıcısı güçlü, tercihen kimlik avına dayanıklı MFA gerektiren yüksek değerli bir hedef haline gelir [6].

Q9: Oturum kaçırma nedir?

Bir saldırganın geçerli bir oturum belirtecini ele geçirmesi veya kötüye kullanması ve parolaya yeniden ihtiyaç duymadan oturum açmış bir kullanıcının kimliğine bürünmesi [5].

Q10: Parola püskürtme (password spraying) nasıl tespit edilir?

Aynı birkaç parolanın birçok hesapta, çoğu zaman kilitlenme eşiklerinin altında kalmak için yavaşça denendiğini arayarak [7].

Bölüm 11: Siber güvenlikle ilgili 10 gerçek dünya gerçeği ve içgörüsü

Güvenlik ihlalleri, savunma mekanizmaları ve uyumluluk standartlarıyla ilgili gerçek dünya bilgilerini incele.

1. GÜVENLİK İPUCU

NIST SP 800-63B, yeni parolaların yaygın ve ele geçirilmiş parolalardan oluşan engelleme listelerine karşı kontrol edilmesini şart koşar [1].

2. GÜVENLİK İPUCU

2019 'Collection #1' dökümü, daha önceki birçok ihlalden gelen verileri, e-posta ve parola çiftlerinden oluşan tek bir dev dosyada birleştirdi [8].

3. GÜVENLİK İPUCU

NIST artık tek kimlik doğrulama faktörü olarak kullanılan parolaların en az 15 karakter uzunluğunda olmasını şart koşuyor [1].

4. GÜVENLİK İPUCU

ASIC donanımı saniyede milyarlarca SHA-256 karması hesaplayabilir; bu da ham SHA karmalamasını kullanıcı parolaları için güvensiz kılar [2].

5. GÜVENLİK İPUCU

Benzersiz tuzlar, tamamen aynı parolaya sahip iki kullanıcının veri tabanında farklı karma değerlere sahip olması anlamına gelir [2].

6. GÜVENLİK İPUCU

Birçok parola yöneticisi, kasa verilerini kullanıcının ana parolasından türetilen güçlü kriptografiyle yerel olarak şifreler.

7. GÜVENLİK İÇGÖRÜSÜ

Kimlik bilgisi doldurma işe yarar, çünkü birçok kişi aynı parolayı e-ticaret, bankacılık ve e-posta hesaplarında yeniden kullanır [3].

8. GÜVENLİK İÇGÖRÜSÜ

NIST SP 800-63B, doğrulayıcıların dönemsel parola değişikliği istememesi gerektiğini, yalnızca ele geçirilme kanıtı olduğunda değişiklik istenebileceğini söyler [1].

9. GÜVENLİK İÇGÖRÜSÜ

Kısa bir parolaya tek bir büyük harf ve sembol eklemek, modern otomatik GPU sözlük saldırılarını durdurmaz [1].

10. GÜVENLİK İPUCU

MFA, parola sızdıktan sonra bile birçok kimlik bilgisi doldurma girişimini engelleyebilir; kimlik avına dayanıklı MFA, SMS kodlarından daha güçlüdür [3].

Teknik Referanslar ve Kaynaklar

Çalışma kılavuzu ve etkileşimli bulmacalar, küresel NIST, OWASP ve veri gizliliği uyum standartlarından derlenmiştir.

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Soru 1** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Kimlik bilgisi doldurma (credential stuffing), sızdırılmış kullanıcı adı/parola çiftlerini diğer sitelerde denemek için otomasyon kullanır [3].

2 **Soru 2** — **Doğru cevap: A**

ÖĞRETMEN NOTU

OWASP önce Argon2id'i önerir; bcrypt ise esas olarak Argon2id veya scrypt'in bulunmadığı eski sistemler içindir [2].

3 **Soru 3** — **Doğru cevap: A**

ÖĞRETMEN NOTU

MFA ek bir faktör gerektirir, bu yüzden çalınmış bir parola tek başına hesabın kilidini açamaz [3].

4 **Soru 4** — **Doğru cevap: A**

ÖĞRETMEN NOTU

İhlal dökümleri, 2019'daki Collection #1 derlemesi gibi sızdırılmış kimlik bilgisi koleksiyonlarıdır [8].

5 **Soru 5** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Bir parola yöneticisi her hesap için benzersiz, güçlü bir parola üretir ve saklar, böylece yeniden kullanımı önler [3].

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Doğru: yeniden kullanılan parolalar, saldırganların bir siteden sızan kimlik bilgilerini diğer sitelerde denemesine olanak tanır [3].

7 **Soru 7** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: SHA-1 hızlı bir özet (hash) işlevidir; OWASP bunun yerine Argon2id, scrypt, bcrypt veya PBKDF2 önerir [2].

8 **Soru 8** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Yanlış: karmaşıklık kuralları tek başına yeniden kullanılan sızdırılmış parolalarla doldurma saldırısını durduramaz; MFA gerekir [3].

9 **Soru 9** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Doğru: izleme hizmetleri, açığa çıkmış kimlik bilgilerini ihlal dökümlerinde ve karanlık ağ kaynaklarında arar [8].

10 **Soru 10** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Doğru: her parola için benzersiz bir tuz (salt), önceden hesaplanmış gökkuşağı tablolarını etkisiz kılar [2].

Kelime anahtarları ve puanlama ölçeği

Öğretmen notlandırma ölçeği: 1 puan ver — doğru her eşleştirme için (toplam 8 puan) ve her bağlam terimi için (toplam 6 puan).

KONTROL NOKTASI 4: CEVAP ANAHTARI – KAVRAM EŞLEŞTİRME

F 1. DOLDURMA	H 2. BCRYPT	D 3. İHLAL	G 4. TUZLAMA
C 5. YÖNETİCİ	B 6. MFA	A 7. GÖKKUŞAĞI	E 8. KİMLİK AVI

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 DOLDURMA	2 BCRYPT	3 İHLAL	4 TUZLAMA
5 PAROLA KASASI	6 ÇOK FAKTÖRLÜ		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 H – KİMLİKAVI	2 C – İHLAL	3 B – BCRYPT	4 G – GÖKKUŞAĞI
5 A – DOLDURMA	6 D – TUZLAMA	7 E – PAROLAKASASI	8 F – ÇOKFAKTÖRLÜ

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin DOLDURMA, BCRYPT ve İHLAL terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

Vaka çalışmaları:
Öğrencilerden önerilerini varsayımlarla değil, çalışma kâğıdındaki bilgilerle desteklemelerini iste.

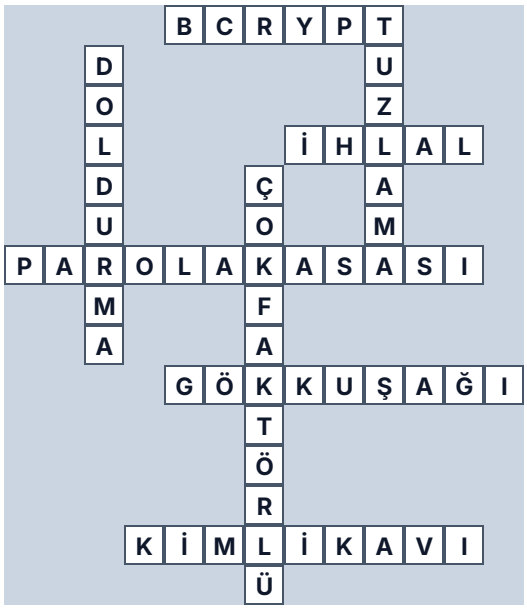
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ

B	C	R	Y	P	T	H	K	L	L	İ	Ö	O	G	L
Ü	L	Ö	P	R	Ş	L	İ	S	G	D	C	R	Ö	N
L	A	Ğ	R	C	A	U	M	D	S	O	Y	T	C	Z
R	M	U	F	L	İ	Ğ	L	Z	Ç	L	L	D	Ö	Ü
Ö	A	O	H	C	Ş	B	İ	A	Z	D	M	D	G	J
T	L	İ	A	D	N	D	K	E	G	U	H	Ç	Ö	P
K	Z	Ö	K	E	H	R	A	Z	R	R	F	Ö	K	U
A	U	E	A	A	Ö	N	V	L	O	M	Ş	V	K	Ö
F	T	İ	P	Ş	R	Ç	I	L	Y	A	B	F	U	R
K	Ü	Ü	I	A	P	Z	Y	Y	J	G	H	L	Ş	P
O	P	A	R	O	L	A	K	A	S	A	S	I	A	İ
Ç	K	K	S	N	Ğ	Ö	Ö	G	Z	A	N	T	Ğ	F
T	C	Y	P	Y	B	Ğ	K	Z	G	I	M	O	I	M
Ü	C	K	Z	Y	F	V	N	U	T	J	T	O	B	M
U	S	K	G	T	Ç	Y	T	İ	P	B	Ü	Z	V	K

BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

1 soldan sağa: BCRYPT Yavaş parola karma algoritması (6 harf)

4 soldan sağa: İHLAL Yetkisiz veritabanı ifşası (5 harf)

6 soldan sağa: PAROLAKASASI Kimlik bilgisi saklama aracı (12 harf)

7 soldan sağa: GÖKKUŞAĞI Parola karmalarının önceden hesaplanmış tablosu (9 harf)

8 soldan sağa: KİMLİKAVI Oturum bilgilerini çalmak için sosyal mühendislik (9 harf)

YUKARIDAN AŞAĞI

2 yukarıdan aşağı: TUZLAMA Parola karmasına rastgele tuz ekleme (7 harf)

3 yukarıdan aşağı: DOLDURMA Sızdırılmış kimlik bilgilerini test etme (8 harf)

5 yukarıdan aşağı: ÇOKFAKTÖRLÜ Çok faktörlü giriş denetimi (11 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	MDUDROAL	DOLDURMA	5.	YRTBPC	BCRYPT
2.	İLALH	İHLAL	6.	MZATLAU	TUZLAMA
3.	PAAKSSRAILAO	PAROLAKASASI	7.	ÖAÇOTÜRLKKF	ÇOKFAKTÖRLÜ
4.	UIĞKAŞGÖK	GÖKKUŞAĞI	8.	İİVKLİKAM	KİMLİKAVI

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"SIZAN PAROLALARI ÇOK FAKTÖRLÜ GİRİŞLE KORU"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Kurumsal Kimlik Bilgisi Sızıntısını Giderme

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir karanlık ağ izleme hizmeti, bir kuruluşu kurumsal sistem yöneticisi parolalarını içeren bir veritabanı dökümünün çevrimiçi yayımlandığı konusunda uyarır.
- Önerilen Strateji ve Çözüm: Tüm etkin yönetici oturumlarını iptal et ve kimlik bilgilerini yüksek entropili bir üreteçle sıfırla. Yönetici portallarında kimlik avına dayanıklı MFA uygula [6], etkilenen API anahtarlarını yenile, giriş günlüklerini incele, ilk açığa çıkma noktasını bul ve diğer yetkili hesapları kontrol et.

B Vaka Çalışması 2: Parola Karmalama Standartlarını Uygulama

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Kurumsal bir veritabanı, kullanıcı parolalarını şifreleme tuzu (salt) olmadan eski MD5 karma değerleriyle saklıyor; bu da parolaların hızla ele geçirilmesine açık hâle getiriyor.
- Önerilen strateji ve çözüm: Kullanıcı başına benzersiz bir tuzla (salt) Argon2id'yi (eski sistemlerde bcrypt) benimse [2]. Mevcut MD5 özetlerini şimdi yeni algoritmanın içine al, her kullanıcının bir sonraki girişinde doğrudan yeniden özetle ve uzun süredir etkin olmayan hesaplar için sıfırlamayı zorunlu kıl.