

Ara Sınav Haftası: Quiz-1

CEN429 Güvenli Programlama — Hafta 8

Dr. Öğr. Üyesi Uğur CORUH · 31.10–08.11.2026

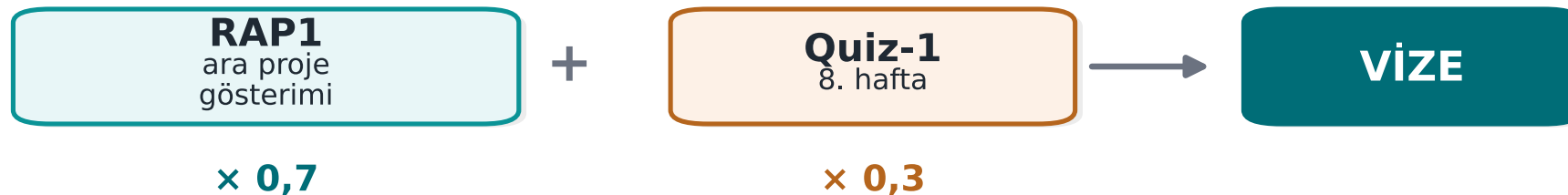
Quiz-1: ne, ne zaman?

- Kapsam: **1–6. haftalar** · vizenin **%40**'ı
- Tarih, saat, yer, süre, soru biçimi: **ders sınıfında** duyurulur
- Ölçülen: ezber değil, **neden** sorusu
- En iyi hazırlık: her haftanın **Kendini sinama** soruları + demoları yeniden çalıştırmak

Vize notu hesabı — şema

Vize notu nasıl hesaplanır?

iki bileşen, tek not



Başarı notu = $0,4 \cdot \text{Vize} + 0,6 \cdot \text{Final}$. Final de aynı biçimde RAP2 ve Quiz-2'den gelir.

Konu haritası (1)

Hafta	Ana kavramlar
1	CIA · varlık–tehdit–zafiyet–risk · beyaz kutu · Saltzer–Schroeder · 7 katman · koruma planı 7 adım · arayüz/varlık tablosu · STRIDE, VAD · saldırı ağacı · güvenli başlatma · bellek hataları · güvenli silme
2	Virüs/solucan/truva · salgın · kural tespiti · bütünlük izleme · BLP, Biba, Clark–Wilson · Unix/Windows ACL · RBAC · CWE, OWASP, CVE, CVSS · günlük enjeksiyonu
3	AEAD · özet/MAC/imza · CSPRNG · nonce/IV/tuz · ECB · Argon2id · HKDF · anahtar yaşam döngüsü · TLS 1.3 · sabitleme · fail-open · maskeleye · kabuklar

Quiz-1 kapsamı — şema

Quiz-1 kapsamı (1-6. haftalar)

ezber değil GEREKÇE sorulur: 'neden bu kip?', 'neyi korumaz?'

Hafta 1

CIA, saldırgan modeli, STRIDE, saldırı ağacı

Hafta 2

zararlı yazılım, BLP/Biba, CWE/CVE/CVSS

Hafta 3

verinin üç hâli, AEAD, nonce, KDF, TLS

Hafta 4

C/C++ hataları, sanitizer, derleyici korumaları

Hafta 5

enjeksiyon, deserialization, ProGuard, SBOM

Hafta 6

RASP: algıla / savun / caydır

Her haftanın 'Kendini sına' bölümünü cevaba bakmadan çözün.

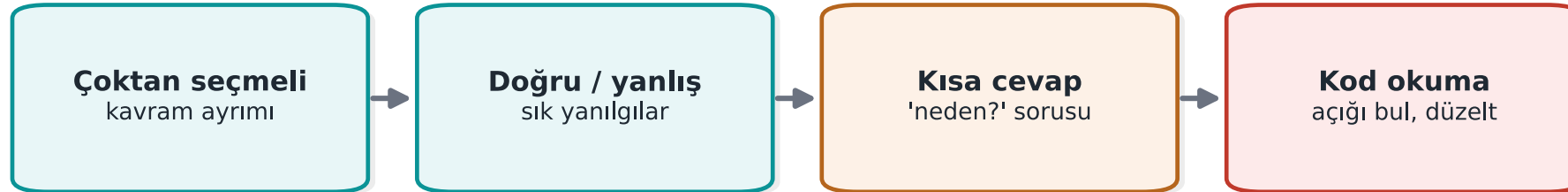
Konu haritası (2)

Hafta	Ana kavramlar
4	SEI CERT · girdi doğrulama · biçim dizisi · UAF · tamsayı/UB · hata işleme, sinyaller · statik analiz · sanitizer · fuzzing · kanarya/FORTIFY/ASLR/NX/RELRO/CFI · gizlemeye giriş
5	Yönetilen dil · CERT Java · enjeksiyon kökü · SQL/komut/yol · seri durumdan çıkarma · XXE/XSS · Python/JS, ReDoS · bayt kodu · ProGuard/R8 · SBOM, VEX
6	Algılama–savunma–caydırma · MATE · RASP mimarisi · bütünlük · hata ayıklayıcı/ortam/kanca · bellek koruması · root/imza · akış sayacı · tepki, decoy, cihaz bağlama

Soru tipleri — şema

Quiz-1 soru tipleri

dördü de 'anladın mı' diye sorar, 'ezberledin mi' diye değil



Kod okuma sorusunda önce açığın SINIFINI (CWE) söyleyin, sonra düzeltmeyi.

Sık karıştırılanlar (1)

A	B	Fark
Kodlama	Şifreleme	Kodlama anahtarsız, gizlilik yok
Özet	MAC	MAC gizli anahtar ister
MAC	İmza	İmza asimetrik → inkâr edilemezlik
Nonce	Tuz	Nonce asla tekrar etmez · tuz parola başına
PBKDF2/Argon2id	HKDF	Parola (yavaş) · yüksek entropili sır (hızlı)
Zincir doğrulama	Ad denetimi	"Güvenilir CA mı?" · "Bu sunucu için mi?"
Fail-open	Fail-closed	Hatada "geçti" · hatada "reddet"

Sık karıştırılanlar (2)

A	B	Fark
Kanarya	ASLR	Dönüşte taşma tespiti · adres rastgeleleştirme
ASan	UBSan	Bellek erişimi · tanımsız davranış
İşaretsiz sarma	İşaretli taşma	Tanımlı · tanımsız
Parametrelili sorgu	Kaçış	Asıl çözüm · ikinci hat
ProGuard	Dize gizleme	Adlar · dizgeler
Gizleme	Güvenli kodlama	Geciktirir · düzeltir
Maskeleye	Tokenizasyon	Gösterimde gizle · kasadaki değere bağlı belirteç
Takma ad	Anonim	Hâlâ kişisel veri · kişiye bağlanamaz

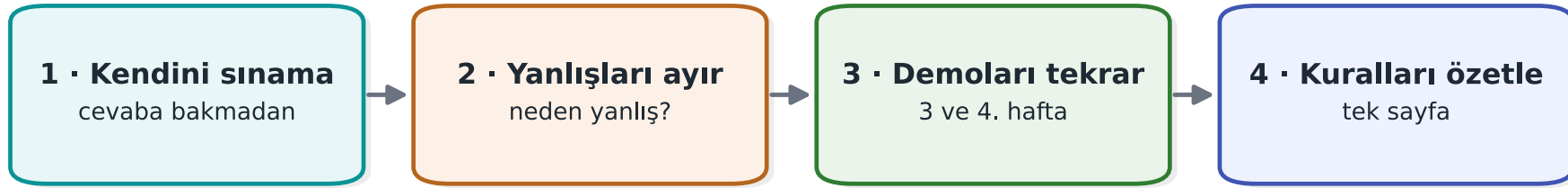
Bir haftalık plan

Gün	Ne yapılacak?
1	1. hafta: STRIDE, saldırı ağacı, koruma planı · Demo 1–4
2	2. hafta: BLP, Biba, Clark–Wilson · bir CVSS vektörünü kendin puanla
3	3. hafta (1): AEAD, nonce, KDF, rastgele sayı · Demo 1–5
4	3. hafta (2): anahtar yönetimi, TLS, sabitleme, kabuklar · Demo 6–9
5	4. hafta: CERT çiftleri, biçim dizisi, UAF, UB, korumalar
6	5–6. hafta: enjeksiyon, seri durumdan çıkarma, ProGuard, SBOM, RASP
7	Örnek soruları süre tutarak çöz, yanıřları oku

Çalışma planı — şema

Quiz öncesi çalışma planı

ezber değil, gerekçe ezberi



Bir kuralı 'kendi cümlelerinizle' anlatabiliyorsanız öğrenmişsinizdir.

Örnek: hatayı bulun (1)

```
void kaydet(const char *ad) {  
    char tampon[32];  
    sprintf(tampon, "kullanici=%s", ad);  
    syslog(LOG_INFO, tampon);  
}
```

```
char parola[64]; oku(parola, sizeof parola); dogrula(parola);  
memset(parola, 0, sizeof parola); return;
```

Örnek: hatayı bulun (2)

```
String sql = "SELECT * FROM notlar WHERE ogrenci = '" + no + "'";
```

```
EVP_DecryptUpdate(ctx, acik, &n, sifreli, sifreli_n);  
kullan(acik, n);  
EVP_DecryptFinal_ex(ctx, acik + n, &m);
```

```
try { pinDenetle(zincir); } catch (KeyStoreException e) { e.printStackTrace(); }
```

Örnek: senaryolar

1. Bütün kullanıcılarda **aynı gömülü AES anahtarı**: riskler ve öneri?
2. Dağıtılan paket **hata ayıklama derlemesi**: hangi bulgular?
3. "Bu işlemi ben yapmadım": hangi STRIDE harfi, hangi kanıt?
4. Arşiv açan fonksiyon: hangi hatalara karşı ne yaparsınız?
5. Log4Shell'de asıl sorun neydi, ne önlerdi?
6. RASP denetimleri neden tek bir **if** ile değerlendirilmemeli?

Gelecek hafta

Hafta 9 — Gelişmiş kod gizleme ve çeşitlendirme

- Gizleme taksonomisi, opak yüklemeler, veri kodlama
- Sanallaştırma ve derleyici tabanlı gizleme (kavram)
- Gizlemenin ölçülmesi: güç, dayanıklılık, maliyet

Ek · Hafta hafta konu haritası (1–6)

1. hafta · anahtar noktalar

- CIA üçlüsü; hata $\neq$ zafiyet.
- MATE (beyaz kutu) saldırgan.
- STRIDE, saldırı ağacı, DFD.
- Katmanlı savunma; tasarım ilkeleri.

2. hafta · anahtar noktalar

- Tehdit modelleme adımları.
- Güven sınırı; en az yetki.
- Varlık listesi ve C/I/I+ etiketi.

3. hafta · anahtar noktalar

- Verinin üç hâli.
- AEAD; nonce tekrarı felaketi.
- CSPRNG; KDF (parola → anahtar).
- Anahtar hiyerarşisi; ileri gizlilik.

4. hafta · anahtar noktalar

- Üç katman: kod → derleyici/OS → gizleme.
- CERT/CWE; UAF; tamsayı/UB.
- Sanitizer (ASan/UBSan), fuzzing.
- Derleyici korumaları (kanarya, ASLR, NX).

5. hafta · anahtar noktalar

- Yönetilen dil bellek hatasını çözer, enjeksiyonu çözmez.
- SQL/komut/yol enjeksiyonu → parametrelili/argüman dizisi.
- Deserialization; ProGuard/R8; SBOM.

6. hafta · anahtar noktalar

- RASP: algıla, savun, caydır.
- Bütünlük (self-hash), anti-debug, hook algılama.
- Çapraz denetim; tepki politikası; cihaz bağlama.

Sık karıştırılanlar

A	B	Fark
Hata	Zafiyet	Kötüye kullanılabilir hata
Kara kutu	Beyaz kutu (MATE)	Programa sahip
Simetrik	Asimetrik	Tek / çift anahtar
AEAD	Yalnız şifreleme	+ bütünlük
Gizleme	Güvenli kod	Hatayı düzeltmez

Ek · Çözümlü pratik sorular

Soru 1

MATE saldırgan neden kriptografiyi tek başına yetersiz bırakır?

Cevap: Anahtar bellekte; saldırgan programı çalıştırıp okur. Kripto gizliliği verir ama beyaz kutuda anahtar korunmaz; RASP/gizleme/whitebox gerekir.

Soru 2

AES-GCM'de aynı nonce iki kez kullanılırsa?

Cevap: Gizlilik ve bütünlük çöker; anahtar akışı ve veri sızabilir. Nonce her zaman benzersiz olmalı.

Soru 3

SQL enjeksiyonunu ne kesin önler?

Cevap: Parametrelili sorgu (prepared statement); veri asla komut olarak yorumlanmaz. String birleştirme yapılmaz.

Soru 4

ASan hangi taşmayı göremez?

Cevap: Aynı yapının içinde alandan alana taşmayı (arada zehirli bölge yoktur).

Soru 5

Kanarya neyi durdurur, neyi durdurmaz?

Cevap: Durdurur: dönüş adresine ulaşan yığın taşması. Durdurmaz: öbek taşması, önceki değişkenler, sızan kanarya.

Soru 6

RASP self-hashing tek başına neden yetmez?

Cevap: Saldırgan özet fonksiyonunu bulup atlatabilir. Gizleme + çapraz + örtüşen denetim gerekir.

Soru 7

Paroladan anahtar türetirken neden KDF ve tuz?

Cevap: Parola düşük entropili; KDF yavaşlatır, tuz aynı parolaların aynı anahtar üretmesini önler (gökkuşáğı tablosu).

Soru 8

En az yetki ilkesi bir örnekle?

Cevap: Uygulamanın DB kullanıcısı yalnız `SELECT` yapabilsin; `DROP` yetkisi olmasın. Fazla yetki = büyük hasar.

Soru 9

Tehdit modellemede STRIDE'in "E"si nedir, bir önlem?

Cevap: Elevation of privilege (yetki yükseltme). Önlem: en az yetki, yetki denetimi, güvenli varsayılan.

Soru 10

Deserialization neden tehlikeli, çözüm?

Cevap: Çıkarma sırasında kod çalışabilir (gadget). Çözüm: veri biçimi + şema; zorunda kalınırsa beyaz liste filtresi.

Örnek · çoktan seçmeli

Aşağıdakilerden hangisi bir AEAD kipidir?

A) ECB B) CBC C) **GCM** ✓ D) Ham RSA

Örnek · doğru/yanlış

- Gizleme hatayı düzeltir. (Y)
- Nonce gizli olmalı. (Y — benzersiz olmalı, gizli değil)
- Parametrelili sorgu SQL enjeksiyonunu önler. (D)

Çalışma planı

- Her haftanın "Kendini sınaama"sını cevaba bakmadan yap.
- Sık karıştırılanları ezberden değil **nedeniyle** öğren.
- iii. ve 4. haftanın demolarını bir kez daha gözden geçir.

Son söz (Quiz-1 hazırlık)

Ezber değil, **neden** ölçülür: "neden bu kip?", "neden bu denetim?", "neyi korumaz?"

İyi şanslar.