Hafta 16 — Final Dönemi: Quiz-2

Tarih	04–17.01.2027
Öğrenme çıktıları	ÖÇ.2–7
Süre	3 saat

Bu hafta ne oluyor?

Final döneminde **Quiz-2** yapılır. Kapsam **9–14. haftaların** konularıdır; Quiz-2 final notunun **%30'udur** (`Not_Final = 0,7·RAP2 + 0,3·QUIZ2`). Tarih, saat, yer, süre ve soru biçimi ders sınıfında duyurulur. Bu sayfa bir **çalışma rehberidir**.

En verimli çalışma yolu

Her haftanın "Kendini sınama" sorularını cevaplara bakmadan cevaplayın; 10. haftanın OpenSSL adımlarını ve 13. haftanın uyum matrisi etkinliğini bir kez daha kendiniz yapın. Ezber değil, **neden** sorusu ölçülür.

1. Konu haritası: 9–14. haftalar

Hafta	Konular (izlence)	Çalışırken odaklanın
9 Gelişmiş kod gizleme ve çeşitlendirme	Gizleme taksonomisi; opak yüklemler, sahte akış, ölü kod; veri kodlama; sanallaştırma tabanlı gizleme; gizlemenin ölçülmesi (güç, dayanıklılık, maliyet)	Gizlemenin amacı ve maliyeti; ölçme ölçütleri; 4. haftadaki temel teknikler
10 Sertifikalar ve kriptografik yöntemler	Algoritma ve anahtar uzunluğu seçimi; kipler ve dolgu; HMAC, şifrele-sonra-MAC, yeniden oynatma; RSA-OAEP/PSS, Ed25519/X25519; dijital imza; Diffie–Hellman ve araya girme; PKI, X.509, zincir; CRL/OCSP; PKCS#11/SoftHSM; kuantum sonrası	Güvenlik düzeyi tablosu; doğru kip ve dolgu; imza doğrulamasının tuzakları; zincir doğrulamanın dört sorusu
11 Whitebox kriptografi	Beyaz kutu ve kara kutu saldırgan modelleri; tablo tabanlı gerçekleştirim; anahtar koruması; bilinen saldırı aileleri ve karşı önlemler; yazılımsal güvenlik modülleri	Saldırgan modelleri; whitebox'ın katmanlı savunmadaki yeri ve sınırları
12 Sertifikasyon ve sızma testi planlaması	Bağımsız değerlendirmenin 13 adımı; standartların test beklentileri; zafiyet değerlendirmesi; sızma testi planı ve raporlama	Değerlendirme hedefi, gereksinim şablonu, bulgu–aksiyon, etki analizi, delta değerlendirme
13 Güvenlik gereksinimleri	İyi gereksinim; izlenebilirlik ve uyum matrisi; devredilen gereksinimler; Ortak Kriterler, EAL; FIPS 140-3; ETSI, GSMA, EMVCo, PCI, MASVS	Gereksinim → önlem → doğrulama → kanıt zinciri; CC ve FIPS kavramları
14 Tigress ve çeşitlendirme	Kaynaktan kaynağa gizleme; dönüşümleri birleştirme; tohumla çeşitlendirme; dayanıklılığın değerlendirilmesi	Çeşitlendirmenin amacı; maliyet ve etkinlik ölçümü

Quiz-2 kapsamı (9–14. haftalar)

ortak soru: 'bu koruma neyi korur, neyi korumaz, maliyeti ne?'

- **Hafta 9** — gizleme: beş aile, dört ölçüt, çeşitlendirme
- **Hafta 10** — kip, dolgu, imza, PKI, zincir, iptal
- **Hafta 11** — whitebox: üç model, kodlama, DCA, sınırlar
- **Hafta 12** — değerlendirme süreci, saldırı potansiyeli, CVSS
- **Hafta 13** — iyi gereksinim, izlenebilirlik, CC/FIPS/MASVS
- **Hafta 14** — Tigress, dönüşüm hattı, dayanıklılık ↔ maliyet

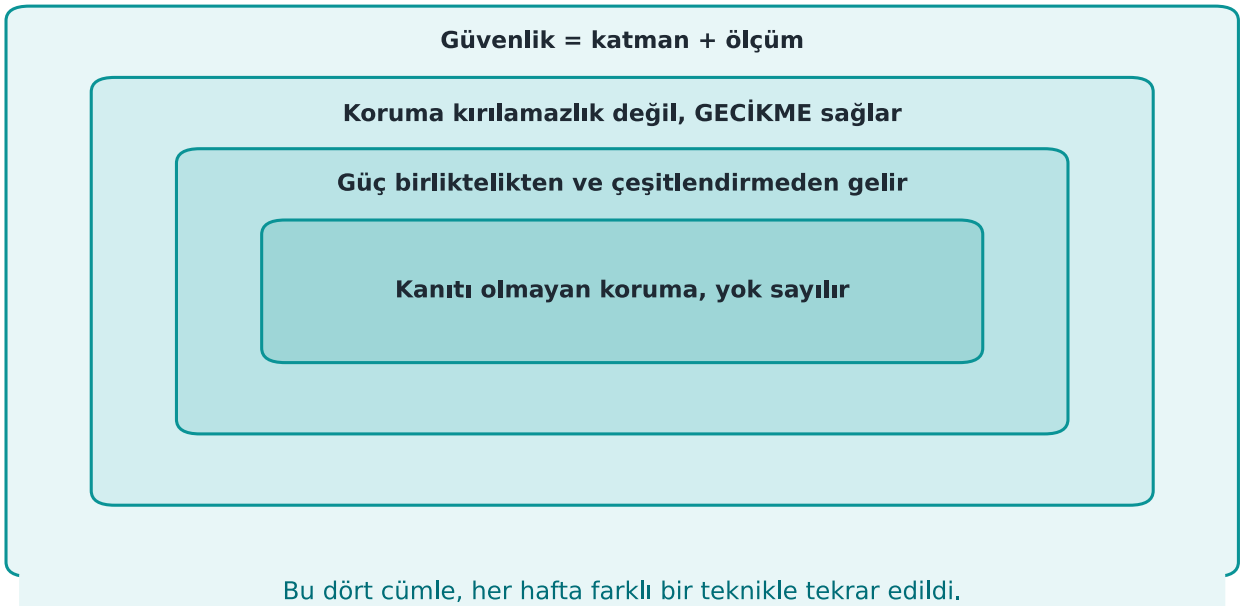
Koruma = gecikme; güç katmandan ve ÖLÇÜMDEN gelir.

2. Sık karıştırılan kavramlar

Kavram A	Kavram B	Fark
CBC	GCM	CBC yalnız gizlilik ve dolgu ister; GCM gizlilik + bütünlük (AEAD), dolgu yok
MAC	İmza	MAC simetrik; imza asimetrik ve inkâr edilemezlik sağlar
Şifrele-sonra-MAC	MAC-sonra-şifrele	İlki doğru sıra; ikincisi dolgu kâhinine açık
RSA-OAEP	RSA-PSS	OAEP şifreleme dolgusu, PSS imza dolgusu
Ed25519	X25519	Ed25519 imza, X25519 anahtar anlaşması
Kök CA	Ara CA	Kök çevrimdışı, kendini imzalar; ara CA günlük sertifikaları çıkarır
CN	SAN	Ad denetimi SAN'a yapılır
CRL	OCSP	Periyodik liste / anlık sorgu; zımbalama gizlilik ve hız sağlar
HSM	SoftHSM	Donanım koruması / yazılım benzetimi (aynı PKCS#11 arayüzü)
ST	PP	Ürüne özgü güvenlik hedefi / ürün sınıfı için ortak gereksinim seti
EAL	Saldırı potansiyeli	Değerlendirmenin derinliği / saldırganın gerektirdiği kaynak
FIPS 140-3 düzey 2	Düzey 3	Kurcalama izi / kurcalamaya direnç ve yanıt
Karşılandı	Devredildi	Ürün karşılar / başka bir taraf karşılar (kime, neden, nasıl yazılır)
ISO/IEC 27001	Ortak Kriterler	Kurumu sertifikalar / ürünü sertifikalar
Güvenlik etki analizi	Delta değerlendirme	Değişikliğin güvenlik etkisini belgeler / yalnız değişen kısmı yeniden değerlendirir

Dönemin tek cümlesi

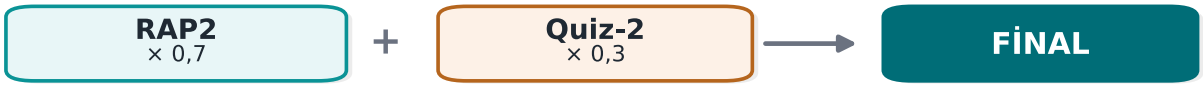
16 haftanın özeti



Bu dört cümle, her hafta farklı bir teknikle tekrar edildi.

Final ve başarı notu

iki aşamalı hesap



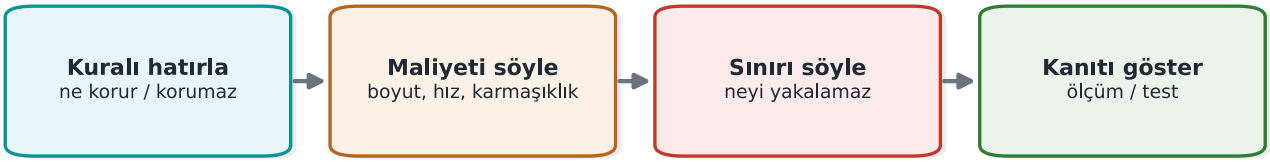
BAŞARI NOTU = 0,4 · Vize + 0,6 · Final — ağırlık finalde.

3. Örnek sorular

Kriptografi ve PKI (10. hafta)

Quiz-2'de beklenen cevap kalıbı

dört parçayı da söyleyen cevap tam puan alır



Bu kalıp aynı zamanda projenizin S9 ve S16 bölümlerinin yazım biçimidir.

1. Bir tasarımda RSA-2048 ile AES-256 birlikte kullanılıyor. Güvenlik düzeyi hakkında ne söylersiniz?

Sistem en zayıf halkası kadar güçlüdür: RSA-2048 yaklaşık 112 bit güvenlik verir; AES-256'nın 256 bitlik düzeyi boşa gider. 128 bit hedefleniyorsa RSA-3072 ya da X25519/Ed25519 kullanılmalıdır.

2. Bir sunucu çözme hatalarında 'dolgu geçersiz' ve 'MAC geçersiz' diye iki farklı ileti döndürüyor. Risk nedir?

Dolgu kâhini: saldırgan şifreli metni değiştirip iletilere bakarak mesajı çözebilir. Tek ve aynı hata döndürülmeli, tercihen AEAD kullanılmalıdır.

3. Bu imza doğrulama kodunda ne yanlış?

```
int r = EVP_DigestVerify(ctx, imza, imza_n, veri, n);
if (r) guncellemeyi_kur();
```

Negatif hata değerleri de doğru sayılır; denetim `r == 1` olmalıdır. Ayrıca imzalı içeriğin sürüm numarasını da kapsaması ve eski sürümlerin reddedilmesi gerekir.

4. `openssl verify -CAfile kok.crt sunucu.crt` hata verirken `-untrusted ara.crt` eklenince geçiyor. Neden? Sahada karşılığı nedir?

Zincir ara sertifika olmadan köke ulaşamaz. Sahada sunucunun ara sertifikayı göndermemesi yaygın bir yapılandırma hatasıdır.

5. OCSP yanıtlayıcısına ulaşılamadığında sertifikayı kabul etmek hangi örüntüdür? Nasıl azaltılır?

Fail-open (yumuşak başarısızlık). Zımbalama zorunluluğu (Must-Staple) ya da kısa ömürlü sertifikalar.

6. Kimliksiz Diffie–Hellman'a karşı araya girme nasıl engellenir?

DH değerleri kimliği bilinen bir anahtarla imzalanır (TLS 1.3'te `CertificateVerify`) ve karşı taraf bu kimliği doğrular.

Değerlendirme ve gereksinimler (12–13. haftalar)

7. Değerlendirme hedefinin (TOE) 'benzersiz' tanımlanması neden gerekir?

Rapor yalnız incelenen ikili dosya için geçerlidir; sürüm numarası tek başına aynı dosyayı garanti etmez. İkili + kaynak + özet değeri birlikte verilir.

8. Güvenlik etki analizi ile delta değerlendirme arasındaki ilişki nedir?

Etki analizi değişikliklerin güvenlik etkisini belgeler (değişiklik dizini, etkilenen dosyalar); delta değerlendirme bu belgeye dayanarak yalnız değişen kısmı yeniden değerlendirir.

9. 'Uygulama güvenli olmalıdır' neden kötü bir gereksinimdir? Nasıl düzeltilir?

Doğrulanamaz. Ölçülebilir ve tekil yazılır: ör. "sürüm derlemesi yığın koruyucu, PIE ve tam RELRO ile üretilmelidir".

10. Uyum matrisinde 'karşılandı' yazan ama kanıtı olmayan bir satır değerlendirici için ne anlama gelir?

Karşılanmamış sayılır; ilk bulgulardan biridir.

11. Bir kütüphane 'güvenli kurulum ve güncelleme' gereksinimini karşılayamıyorsa ne yapmalıdır?

Gereksinimi üst uygulamaya devretmeli ve kılavuzda kime, neden devredildiğini ve üst uygulamanın nasıl karşılayacağını yazmalıdır.

12. EAL4+ bir ürün hakkında 'EAL2 üründen daha güvenlidir' demek doğru mu?

Hayır. EAL değerlendirmenin derinliğidir; güvenlik, güvenlik hedefindeki tehdit ve amaçlara bağlıdır. "+" ek güvence bileşenlerini gösterir.

13. FIPS 140-3 doğrulanmış bir kütüphane kullanan bir uygulama FIPS uyumlu mudur?

Tek başına değil: doğrulama modülü kapsar. Uygulama modülü onaylı kipte ve doğru kullanmalı, anahtarları doğru yönetmelidir.

14. ETSI EN 303 645'in 'hassas güvenlik parametrelerini güvenle saklamak' başlığı projenizde hangi bölümlere karşılık gelir?

S5 varlık listesi, S7 veri güvenliği ve kabuk matrisi, S8 anahtar yaşam döngüsü.

9, 11 ve 14. haftalar

Bu haftaların örnek soruları, haftaların ders notları yayımlandığında bu bölüme eklenecektir. O zamana kadar ilgili konular için 4. haftanın "Kod gizlemeye giriş" ve "Kontrol akışı düzleştirme" bölümlerini ve 3. haftanın "Whitebox kriptografiye giriş" bölümünü tekrar edin.