

Hafta 15 – Final Proje Gösterimleri

Tarih	25.12.2026
Öğrenme çıktıları	ÖÇ.1-7
Süre	3 saat



Bu hafta ne oluyor?

Bu hafta ders anlatılmaz. Dönem projesinin **ikinci kontrolü (RAP2)** yapılır: her takım final raporunu (güvenlik kılavuzunun tamamı) teslim eder, korumalı uygulamasını ve test sonuçlarını gösterir. RAP2, final notunun **%70'idir**; kalan %30 final dönemindeki Quiz-2'dir ($Not_Final = 0,7 \cdot RAP2 + 0,3 \cdot QUIZ2$). Başarı notu $0,4 \cdot Not_Vize + 0,6 \cdot Not_Final$ ile hesaplanır. Ayrıntılı rubrik proje rehberindedir.



Teslim ve süre kuralları

Geç teslim kabul edilmez (izlence, bölüm G). Gösterim sırası, takım başına süre ve teslim saati ders sınıfında duyurulur. Vize kontrolünde aldığınız geri bildirimlerin nasıl kapatıldığını gösterecek bir bulgu-aksiyon listesi hazırlayın.

1. Final kontrolü neyi ölçer?

İzlencedeki final kontrolü rubriğinin kriterleri ve güvenlik kılavuzunuzda karşılık gelen bölümler:

RAP2 (final) teslimi: ne bekleniyor?

vizedeki yapının üzerine ölçüm ve kanıt eklenir

Tam ürün	C++ konsol + DLL/.so, CMake/CTest
S6-S15	kimlik, veri, kriptoloji, RASP, gizleme, hat
S16 · SONUÇLAR	plan değil, GÖZLENEN test sonuçları
S17 · Uyum matrisi	her satır kanıtlı
S14 · Devredilenler	gerekçeli, onaylı

RAP2 = 0,7 · final notu. En sık kayıp: S16'da sonuç yerine plan yazmak.

Kriter	Öğrenme çıktısı	Kılavuzda nerede?	Hangi haftalar?
Kriptografi uygulaması	ÖÇ.2	S8 algoritma envanteri, anahtar yaşam döngüsü ve hiyerarşisi, rastgele sayı	3, 10
Güvenli iletişim	ÖÇ.4	S6 kimlik doğrulama ve bağlama · S11 TLS, sabitleme, mesaj düzeyi koruma	3, 10
Varlık yönetimi	ÖÇ.5	S5 varlık listesi (tam) · S8 anahtarlar	1, 3, 13
İkili uygulama korumaları	ÖÇ.3	S9 kod sağlamlaştırma (ileri) · S15 derleme, imzalama ve dağıtım hattı	4, 5, 6, 9, 14
Güvenlik testi ve birim testleri	ÖÇ.6	S16 test ve doğrulama sonuçları	4, 12
Güvenlik standartları	ÖÇ.7	S1 kaynaklar · S14 varsayımlar ve devredilenler · S17 uyum matrisi	12, 13
Final rapor ve sunum	ÖÇ.7	Bütün bölümler; belge düzeni, tutarlılık, sunum	Tümü

Final raporunda bulunması gereken bölümler

Final kontrolünde bütün bölümler **tam** olarak beklenir:

No	Bölüm	Vizeden farkı
S0	Kapak, belge kontrolü, sürüm geçmişi	Sürüm geçmişi güncel; değişiklikler işaretli
S1	Kapsam, hedef kitle, kısaltmalar, kaynaklar	Tam
S2–S4	Ürün, mimari, tehdit modeli	Vize geri bildirimleriyle güncel
S5	Varlık listesi ve koruma şeması	Tam: her varlığın yaşam döngüsü ve C/I/I+
S6	Kimlik doğrulama, tanımlama, cihaz/sürüm bağlama	Yeni
S7	Veri güvenliği + güvenlik kabuğu matrisi	Güncel
S8	Kripto yöntemleri, anahtar yaşam döngüsü ve hiyerarşisi	Yeni
S9	Kod sağlamlaştırma	İleri (gizleme dahil)
S10	RASP + tepki politikası	Güncel
S11	Güvenli iletişim	Yeni
S12	Raporlama ve günlükleme politikası	Tam
S13	Geliştirme süreci, SBOM, değişiklik yönetimi	Güncel SBOM
S14	Varsayımlar ve devredilen gereksinimler	Yeni
S15	Derleme, imzalama ve dağıtım hattı	Yeni
S16	Güvenlik testi ve doğrulama	Sonuçlar (plan değil)
S17	Gereksinim uyum matrisi	Tam

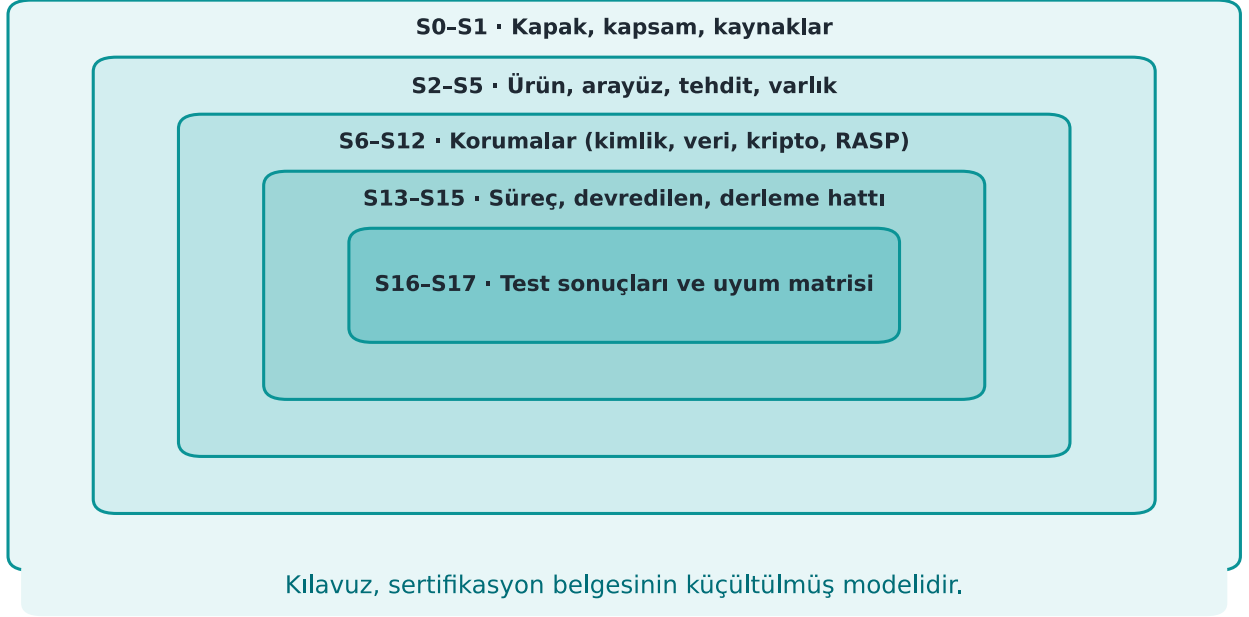
2. Hazırlık kontrol listesi (9–14. haftalar)

✓ 9. ve 14. haftalar — İleri kod sağlamlaştırma (S9, S15)

- ✓ Gizlemenin hangi fonksiyonlara, neden uygulandığı; maliyet ölçümü (süre, boyut) öncesi/sonrası tablosu.
- ✓ Derleme hattında gizleme ve imzalama adımları; sürüm kimliği ve özet değerleri.
- ✓ Gizleme öncesi ve sonrası için ölçütler (anlamli ad oranı, düz metin hassas dizge sayısı).

Güvenlik kılavuzu S0-S17

dıştan içe değil, alttan üste: her bölüm bir öncekine dayanır



✓ 10. hafta — Kriptoloji ve PKI (S8, S11)

- ✓ Algoritma envanteri: amaç, anahtar uzunluğu, kip, standart, kütüphane.
- ✓ Anahtar yaşam döngüsü tablosu: üretim, saklama, kriptoloji-periyot, yenileme, imha.
- ✓ TLS doğrulaması; varsa SPKI sabitleme ve yedek pin; güncelleme dosyasında imza doğrulaması.

✓ 11. hafta — Anahtar koruması (S8)

- ✓ En az bir hassas varlık için koruma yöntemi ve gerekçesi (ör. cihaza bağlama, katmanlı koruma); kullanılmıyorsa neden kullanılmadığının gerekçesi.

✓ 12. hafta — Test ve değerlendirme (S16)

- ✓ Test planı ve **sonuçları**: her test için amaç, yöntem, beklenen ve gözlenen sonuç.
- ✓ Birim testleri (kriptoloji ve koruma fonksiyonları için) ve sürekli entegrasyon kaydı.
- ✓ Vize geri bildirimlerinin bulgu-aksiyon listesi.

✓ 13. hafta — Gereksinimler (S14, S17)

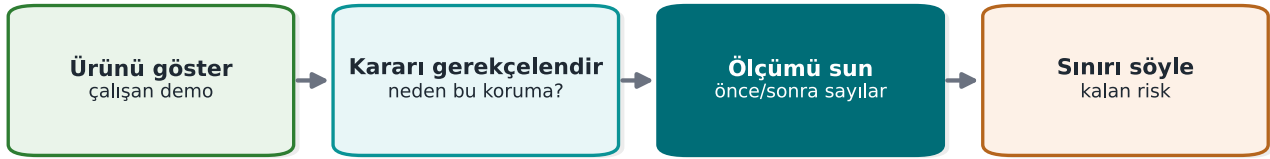
- ✓ Uyum matrisi: uygulanan her gereksinim için durum, bölüm, doğrulama, kanıt.
- ✓ Varsayımlar ve devredilen gereksinimler: kime, neden, nasıl.

3. Gösterim: önerilen akış

1. **Özet:** Ürün, mimari ve en kritik üç varlık (tek şema).
2. **Vizeden bu yana:** Geri bildirimler ve nasıl kapatıldıkları (bulgu–aksiyon listesi).
3. **Canlı gösterim:** Korumalı sürümü çalıştırın; krypto, güvenli iletişim ve en az bir koruma katmanını **çalışırken** gösterin (ör. kurcalanmış bir dosyanın ya da imzası bozuk bir güncellemenin reddedilmesi).
4. **Kanıt:** Testlerin, koruma tablosunun, SBOM'un ve uyum matrisinin kendisi; "şu komutla şu çıktı".
5. **Kalan risk:** Neyi bilerek kapsam dışı bıraktınız, neyi karşılayamadınız ve neden?

Final gösteriminin dört adımı

değerlendirici bu dördünü arar



Sınırını dürüstçe söyleyen takım, her şeyi 'güvenli' diyen takımdan yüksek alır.

Gösterimde sorulabilecek örnek sorular

- Bu anahtar hangi anahtardan türetiliyor, nerede duruyor, ne zaman siliniyor?
- Sertifika zincirinizi nasıl doğruluyorsunuz? Ad denetimi nerede yapılıyor?
- İmza doğrulamanız başarısız olursa ne oluyor? Eski ama geçerli imzalı bir sürüm yüklenebilir mi?
- Gizlemenin maliyetini ölçtünüz mü? Hangi fonksiyonları neden gizlediniz?
- Uyum matrisinizde "karşılandı" dediğiniz şu satırın kanıtı nerede?
- Hangi gereksinimi devrettiniz ve karşı taraf bunu nasıl karşılayacak?

Sık yapılan hatalar

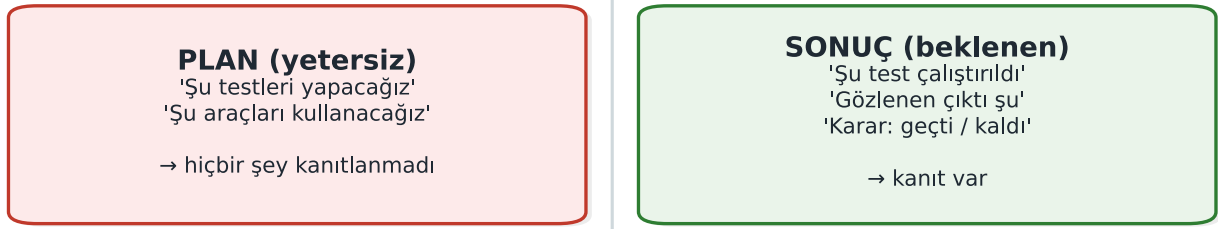
Hata	Neden sorun?
Test planı var ama sonuç yok	Final kontrolünde S16'nın sonuçları beklenir
Uyum matrisinde kanıtsız "karşılandı"	Değerlendirici gözünde karşılanmamış sayılır
Kılavuz ile kod arasında sürüm farkı	Değerlendirilen ürün belirsizleşir; sürüm kimliği ve özet değerleri tutarlı olmalı
Kalan risk bölümünün boş olması	Hiçbir ürünün kalan riski sıfır değildir; boş bölüm eksik analiz demektir
Vize geri bildirimlerinin yok sayılması	Bulgu–aksiyon döngüsü sürecin parçasıdır
Depoda gerçek sır ya da kişisel veri	Ciddi güvenlik hatası; bütün değerler sentetik olmalı

4. Akademik dürüstlük

İzlencenin "Akademik Dürüstlük" bölümü projede de geçerlidir. Teslim ettiğiniz her satırı açıklayabiliyor olmalısınız; gösterimde takımın her üyesine soru sorulabilir. Başkasının kodunu ya da metnini kullandıysanız kaynağını belirtin.

S16: plan mı, sonuç mu?

finalde S16'dan GÖZLENEN sonuç beklenir



Test kartı: amaç · ön koşul · adımlar · beklenen · GÖZLENEN · karar · kanıt.

5. Dönem sonunda

- Güvenlik kılavuzunuz, sertifikasyondan geçen ürünlerin belgelerinin küçültülmüş bir modelidir; iş başvurularında bir **portfolyo** ögesi olarak kullanabilirsiniz (gizli bilgi içermediğinden emin olun).
- Quiz-2 final döneminde yapılır; kapsam 9–14. haftalardır (16. hafta sayfası).