CyberTestify

Otomatik Güvenlik Tarama Raporu

ornek.com · Tam Kapsamlı Pentest Paketi

CyberTestify Güvenlik Taraması — Tamamlandı

Rapor No: **CT-ÖRNEK-332E**

Doğrulama Kodu: **EB4F-F4B1**

Bu rapor resmi sızma testi / sertifikasyon değildir.

İçindekiler

HEDEF
ornek.com

PAKET
Tam Kapsamlı Pentest Paketi

RAPOR NO
CT-ÖRNEK-332E

1. Yönetici Özeti

⚠ Bu örnek rapor, bilerek zafiyetli bırakılmış bir test uygulamasından alınmıştır. Gerçek sitelerde bulgu sayısı ve şiddeti hedefin mimarisine göre önemli ölçüde değişir.

⚡ Yönetim Kararı

Öncelikli ele alınması gereken **2** yüksek/kritik seviyeli gösterge tespit edildi; bunlar için acil bir düzeltme planı önerilir. Orta/düşük göstergeler planlı iyileştirmeyle giderilebilir.

- **Genel risk seviyesi: Yüksek** — en yüksek risk **Authenticated Enjeksiyon (SQLi/XSS)** alanında.
- **Kapsam:** Bu bölüm **kimlik-doğrulamalı (login'li)** bağlamda çalışır; çerez/oturum/yetki, authenticated enjeksiyon/IDOR ve **deterministik güvenlik kontrolleriyle** yetki yükseltme + çok-adımlı iş mantığı göstergelerini kapsar (backend güvenli uygular; ödeme/hesap-değişikliği tamamlama YOK). Cross-account (başka kullanıcının verisi) IDOR bu sürümün kapsamı dışındadır.
- **Önerilen ilk adım:** Çalıştırılan kontrollerdeki bulguları giderin; hazır adımlar "AI Çözüm Önerileri" bölümünde.

İyileştirme Öncelikleri

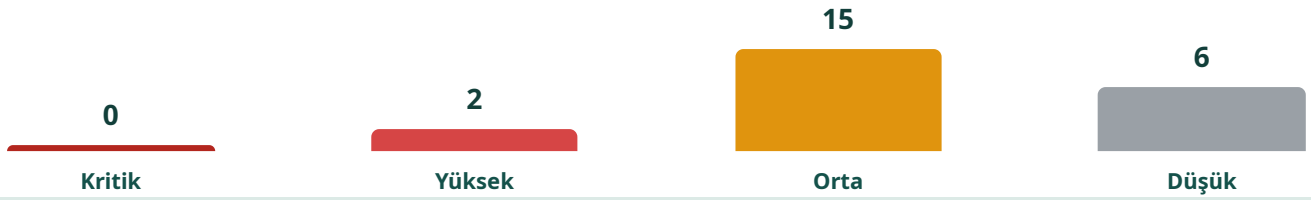
⚡ **En Acil / Öncelikli:** SQL Enjeksiyon göstergesi (GET /rest/products/search?q); Kimlik doğrulama baypas göstergesi — ' OR 1=1-- (POST /rest/user/login).

🛠 **Hızlı Kazanım (sunucu yapılandırması, ~1-2 gün):** DMARC politikası yetersiz (eksik veya zayıf) (ornek.com); HSTS (Strict-Transport-Security) eksik (ornek.com); Content-Security-Policy eksik (ornek.com); Referrer-Policy eksik (ornek.com).

🗓 **Orta Vadeli / Süreç (manuel doğrulama veya kod/mimari):** Oturum geçersizleştirme zayıflığı (/rest/user/whoami); Yetkisiz uç nokta erişimi (forced browsing) (/rest/admin/application-configuration); Yetkisiz uç nokta erişimi (forced browsing) (/api/Users); Yetkisiz uç nokta erişimi (forced browsing) (/metrics); Yetkisiz uç nokta erişimi (forced browsing) (/rest/admin/application-version); Yetkisiz nesne erişimi (IDOR) göstergesi (/api/products/1); Yetkisiz nesne erişimi (IDOR) göstergesi (/api/users/1); Güvensiz postMessage origin (main.js · message handler); Hassas veri istemci depolamasında (main.js · localStorage['token']); Hassas veri istemci depolamasında (main.js · localStorage['totp_tmp_token']); Hesap kilitleme / brute-force koruması yok (/rest/user/login); Aşırı veri ifşası (API/BOPLA) (/api/Products); API rate-limit yok (/api/BasketItems); Yansıyan XSS göstergesi (GET /redirect?to); Web cache / hassas önbellekleme göstergesi (/rest/user/whoami); CAA kaydı eksik (ornek.com); Permissions-Policy eksik (ornek.com).

2. Bulgular

2.1 Zafiyet Dağılımı



Bu taramada toplam **23** bulgu göstergesi tespit edildi; şiddet dağılımı aşağıdadır.

2.2 Master Bulgu Tablosu

ID	Başlık	Durum	Şiddet
CT-1	SQL Enjeksiyon göstergesi — GET /rest/products/search?q	Açık	Yüksek
CT-2	Kimlik doğrulama baypas göstergesi — ' OR 1=1-- — POST /rest/user/login	Açık	Yüksek
CT-3	Oturum geçersizleştirme zayıflığı — /rest/user/whoami	Açık	Orta
CT-4	Yetkisiz uç nokta erişimi (forced browsing) — /rest/admin/application-configuration	Açık	Orta
CT-5	Yetkisiz uç nokta erişimi (forced browsing) — /api/Users	Açık	Orta
CT-6	Yetkisiz uç nokta erişimi (forced browsing) — /metrics · güven: düşük (dolaylı gösterge)	Açık	Orta
CT-7	Yetkisiz uç nokta erişimi (forced browsing) — /rest/admin/application-version	Açık	Orta
CT-8	Yetkisiz nesne erişimi (IDOR) göstergesi — /api/products/1	Açık	Orta
CT-9	Yetkisiz nesne erişimi (IDOR) göstergesi — /api/users/1	Açık	Orta
CT-10	Güvensiz postMessage origin — main.js · message handler	Açık	Orta
CT-11	Hassas veri istemci depolamasında — main.js · localStorage['token']	Açık	Orta
CT-12	Hassas veri istemci depolamasında — main.js · localStorage['totp_tmp_token']	Açık	Orta
CT-13	Hesap kilitleme / brute-force koruması yok — /rest/user/login	Açık	Orta
CT-14	Aşırı veri ifşası (API/BOPLA) — /api/Products	Açık	Orta
CT-15	API rate-limit yok — /api/BasketItems	Açık	Orta
CT-16	DMARC politikası yetersiz (eksik veya zayıf) — ornek.com	Açık	Orta
CT-17	HSTS (Strict-Transport-Security) eksik — ornek.com	Açık	Orta
CT-18	Yansıyan XSS göstergesi — GET /redirect?to · güven: düşük (dolaylı gösterge)	Açık	Düşük
CT-19	Web cache / hassas önbellekleme göstergesi — /rest/user/whoami	Açık	Düşük
CT-20	CAA kaydı eksik — ornek.com	Açık	Düşük
CT-21	Content-Security-Policy eksik — ornek.com	Açık	Düşük
CT-22	Referrer-Policy eksik — ornek.com	Açık	Düşük
CT-23	Permissions-Policy eksik — ornek.com	Açık	Düşük

20 kontrol alanı çalıştırıldı — bulgular: 2 yüksek, 15 orta, 6 düşük

✓ ÇALIŞTIRILDI — ZAFİYET KANITI YOK

- **JWT / Token Güvenliği · Client-Side / JS Analizi · Girdi & Header Derinliği · Yapılandırma & İfşa Derinliği · Subdomain Takeover (Dangling DNS)**

⚠ BULGU VAR — AYRINTISI AŞAĞIDAKİ BÖLÜMLERDE

- **Logout / Oturum Geçersizleştirme · Forced Browsing / Fonksiyon-Seviye Yetki · Authenticated Enjeksiyon (SQLi/XSS) · Authenticated IDOR (kendi kaynakları) · Giriş Baypası (SQLi Göstergesi) · Client-Side Statik Analiz · Kimlik-Doğrulama Derinliği · API Güvenliği Derinliği (OWASP API Top 10) · E-posta & DNS Derinliği (Anti-Spoofing) · Taşıma Katmanı, CORS & Güvenlik Başlığı Derinliği**

⚠ UYGULANAMADI / KAPSAM DIŞI — "GÜVENLİ" ANLAMINA GELMEZ

- **Oturum Çerezi Bayrakları · Session Fixation · Yetki Yükseltme (Privilege Escalation) · Çok-Adımlı İş Mantığı · Oturum Güvenliği Derinliği**

2.3 Detaylı Bulgular

[YÜKSEK] CT-1 · SQL Enjeksiyon göstergesi

Durum: Açık

Etkilenen nokta: `GET /rest/products/search?q`

Açıklama: Bir giriş noktası, girdiyi veritabanı sorgusuna süzebiliyor (enjeksiyon göstergesi).

Nasıl Tespit Edildi: Yanıtta veritabanı hata imzası görüldü ("')" payload'ı ile): "SQLITE_ERROR"

İş Etkisi: Veritabanındaki müşteri/hesap kayıtlarına yetkisiz erişim veya değişiklik olabilir; veri sızıntısı, KVKK ihlali ve müşteri güveni kaybı riski.

ÖNERİLEN DÜZELTME

Tüm sorguları parametreli sorgu / hazırlanmış ifade ile yazın; veritabanı hata mesajlarını son kullanıcıya göstermeyin.

Referans: CWE-89 · OWASP A03:2021 Injection

[YÜKSEK] CT-2 · Kimlik doğrulama baypas göstergesi — ' OR 1=1--

Durum: Açık

Etkilenen nokta: `POST /rest/user/login`

Açıklama: Giriş formuna klasik SQLi payload'ı ile kimlik doğrulama atlatma göstergesi.

Nasıl Tespit Edildi: Kontrol (geçersiz kimlik) → HTTP 401 (başarısız). SQLi payload ' OR 1=1-- → HTTP 200 + AÇIK başarı sinyali: "{"authentication":{"token":"","bid":1,"umail":"admin@juice-sh.op"}}". Kimlik doğrulama SQL enjeksiyonuyla ATLATILIYOR (oturum/authorization token döndü — güçlü kanıt). Oturum ele geçirme/istismar YAPILMADI; token değeri raporda gösterilmez (redakte).

İş Etkisi: Kimlik doğrulama atlatılarak yetkisiz erişim mümkün olabilir; hesap ve veri güvenliği doğrudan tehlikede.

ÖNERİLEN DÜZELTME

Kimlik sorgularında parametreli sorgu kullanın; girdi doğrulama + hatalı girişte tek-tip hata mesajı.

Referans: CWE-287 · OWASP A07:2021 Identification & Authentication Failures

[ORTA] CT-3 · Oturum geçersizleştirme zayıflığı

Durum: Açık

Etkilenen nokta: `/rest/user/whoami`

Açıklama: Çıkıştan sonra oturum sunucu tarafında geçersizleştirilmiyor.

Nasıl Tespit Edildi: Logout çağrıldıktan SONRA da AYNI oturum token'ıyla korumalı uç (/rest/user/whoami) 200 döndürdü — oturum sunucu tarafında geçersizleştirilmiyor.

İş Etkisi: Çıkıştan sonra oturum geçerli kaldığından çalınan/paylaşılan bir oturum yeniden kullanılabilir; ortak cihazlarda hesap ele geçirme riski.

ÖNERİLEN DÜZELTME

Logout'ta oturumu sunucu tarafında iptal edin (revocation/expiry); istemci-tarafı silme yetmez.

Referans: CWE-613 · OWASP A07:2021 Identification & Authentication Failures

[ORTA] CT-4 · Yetkisiz uç nokta erişimi (forced browsing)

Durum: Açık

Etkilenen nokta: `/rest/admin/application-configuration`

Açıklama: Menüde olmayan bir yönetim/gizli uç noktaya, düşük yetkili oturumla erişilebiliyor.

Nasıl Tespit Edildi: /rest/admin/application-configuration uç noktası, düşük yetkili test hesabının oturumuyla 200 ve JSON veri döndürdü — eksik fonksiyon-seviye yetkilendirme (olası yetkisiz yönetim erişimi) göstergesi (dönen veri raporda gösterilmez).

İş Etkisi: Yetkisiz kullanıcı yönetim/gizli uç noktalara erişebilir; yetkisiz veri görüntüleme/değiştirme ve iç suistimal riski.

ÖNERİLEN DÜZELTME

Her hassas uç noktada sunucu-taraflı rol/yetki kontrolü uygulayın; UI'da gizlemek yetmez.

Referans: CWE-284 · OWASP A01:2021 Broken Access Control

[ORTA] CT-5 · Yetkisiz uç nokta erişimi (forced browsing)

Durum: Açık

Etkilenen nokta: `/api/Users`

Açıklama: Menüde olmayan bir yönetim/gizli uç noktaya, düşük yetkili oturumla erişilebiliyor.

Nasıl Tespit Edildi: /api/Users uç noktası, düşük yetkili test hesabının oturumuyla 200 ve JSON veri döndürdü — eksik fonksiyon-seviye yetkilendirme (olası yetkisiz yönetim erişimi) göstergesi (dönen veri raporda gösterilmez).

İş Etkisi: Yetkisiz kullanıcı yönetim/gizli uç noktalara erişebilir; yetkisiz veri görüntüleme/değiştirme ve iç suistimal riski.

ÖNERİLEN DÜZELTME

Her hassas uç noktada sunucu-taraflı rol/yetki kontrolü uygulayın; UI'da gizlemek yetmez.

Referans: CWE-284 · OWASP A01:2021 Broken Access Control

[ORTA] CT-6 · Yetkisiz uç nokta erişimi (forced browsing)

Durum: Açık

Etkilenen nokta: `/metrics`

Açıklama: Menüde olmayan bir yönetim/gizli uç noktaya, düşük yetkili oturumla erişilebiliyor.

Nasıl Tespit Edildi: /metrics uç noktası, düşük yetkili test hesabının oturumuyla 200 ve içerik döndürdü — eksik fonksiyon-seviye yetkilendirme (olası yetkisiz yönetim erişimi) göstergesi (dönen veri raporda gösterilmez).

İş Etkisi: Yetkisiz kullanıcı yönetim/gizli uç noktalara erişebilir; yetkisiz veri görüntüleme/değiştirme ve iç suistimal riski.

ÖNERİLEN DÜZELTME

Her hassas uç noktada sunucu-taraflı rol/yetki kontrolü uygulayın; UI'da gizlemek yetmez.

Referans: CWE-284 · OWASP A01:2021 Broken Access Control

[ORTA] CT-7 · Yetkisiz uç nokta erişimi (forced browsing)

Durum: Açık

Etkilenen nokta: `/rest/admin/application-version`

Açıklama: Menüde olmayan bir yönetim/gizli uç noktaya, düşük yetkili oturumla erişilebiliyor.

Nasıl Tespit Edildi: /rest/admin/application-version uç noktası, düşük yetkili test hesabının oturumuyla 200 ve JSON veri döndürdü — eksik fonksiyon-seviye yetkilendirme (olası yetkisiz yönetim erişimi) göstergesi (dönen veri raporda gösterilmez).

İş Etkisi: Yetkisiz kullanıcı yönetim/gizli uç noktalara erişebilir; yetkisiz veri görüntüleme/değiştirme ve iç suistimal riski.

ÖNERİLEN DÜZELTME

Her hassas uç noktada sunucu-taraflı rol/yetki kontrolü uygulayın; UI'da gizlemek yetmez.

Referans: CWE-284 · OWASP A01:2021 Broken Access Control

[ORTA] CT-8 · Yetkisiz nesne erişimi (IDOR) göstergesi

Durum: Açık

Etkilenen nokta: `/api/products/1`

Açıklama: Kimlik parametresi değiştirilerek başka bir kaydın erişilebildiğine dair sinyal.

Nasıl Tespit Edildi: ID değeri komşu bir değere değiştirilip istek gönderildi; farklı/geçerli kaynak dönüşü gözlendi (içerik saklanmadı).

İş Etkisi: Kimlik parametresi değiştirilerek başka kullanıcıların kayıtlarına erişilebilir; toplu veri sızıntısı ve KVKK ihlali riski.

ÖNERİLEN DÜZELTME

Her erişimde nesne-düzeyi yetki kontrolü uygulayın; tahmin edilebilir ID yerine UUID kullanın.

Referans: CWE-639 · OWASP A01:2021 Broken Access Control

[ORTA] CT-9 · Yetkisiz nesne erişimi (IDOR) göstergesi

Durum: Açık

Etkilenen nokta: `/api/users/1`

Açıklama: Kimlik parametresi değiştirilerek başka bir kaydın erişilebildiğine dair sinyal.

Nasıl Tespit Edildi: ID değeri komşu bir değere değiştirilip istek gönderildi; farklı/geçerli kaynak dönüşü gözlendi (içerik saklanmadı).

İş Etkisi: Kimlik parametresi değiştirilerek başka kullanıcıların kayıtlarına erişilebilir; toplu veri sızıntısı ve KVKK ihlali riski.

ÖNERİLEN DÜZELTME

Her erişimde nesne-düzeyi yetki kontrolü uygulayın; tahmin edilebilir ID yerine UUID kullanın.

Referans: CWE-639 · OWASP A01:2021 Broken Access Control

[ORTA] CT-10 · Güvensiz postMessage origin

Durum: Açık

Etkilenen nokta: `main.js · message handler`

Açıklama: postMessage mesaj işleyicisinde origin doğrulaması eksik göstergesi.

Nasıl Tespit Edildi: main.js içinde bir message olay dinleyicisi event.origin doğrulaması olmadan işlem yapıyor gibi görünüyor — güvensiz cross-origin mesaj işleme göstergesi. Gönderen origin'i allowlist ile doğrulanmalı.

İş Etkisi: postMessage origin doğrulaması eksik göstergesi; kötü-amaçlı sayfa mesaj enjekte edip veri sızdırabilir.

ÖNERİLEN DÜZELTME

`message` işleyicilerinde `event.origin`'i katı allowlist ile doğrulayın.

Referans: CWE-346 · OWASP A05:2021 Security Misconfiguration

[ORTA] CT-11 · Hassas veri istemci depolamasında

Durum: Açık

Etkilenen nokta: `main.js · localStorage['token']`

Açıklama: Hassas veri (token/oturum) localStorage/sessionStorage'a yazılıyor.

Nasıl Tespit Edildi: main.js içinde localStorage.setItem('token', ...) — hassas veri (oturum/kimlik göstergesi) istemci depolamasına yazılıyor (değer gösterilmez). localStorage/sessionStorage XSS ile okunabilir; oturum verisi için HttpOnly çerez tercih edilmelidir.

İş Etkisi: Hassas veri (token/oturum) localStorage/sessionStorage'a yazılıyor; XSS ile okunabilir — HttpOnly çerez tercih edilmeli.

ÖNERİLEN DÜZELTME

Oturum token'ını localStorage yerine `HttpOnly + Secure` çerezde tutun.

Referans: CWE-922 · OWASP A04:2021 Insecure Design

[ORTA] CT-12 · Hassas veri istemci depolamasında

Durum: Açık

Etkilenen nokta: `main.js · localStorage['totp_tmp_token']`

Açıklama: Hassas veri (token/oturum) localStorage/sessionStorage'a yazılıyor.

Nasıl Tespit Edildi: main.js içinde localStorage.setItem('totp_tmp_token', ...) — hassas veri (oturum/kimlik göstergesi) istemci depolamasına yazılıyor (değer gösterilmez). localStorage/sessionStorage XSS ile okunabilir; oturum verisi için HttpOnly çerez tercih edilmelidir.

İş Etkisi: Hassas veri (token/oturum) localStorage/sessionStorage'a yazılıyor; XSS ile okunabilir — HttpOnly çerez tercih edilmeli.

ÖNERİLEN DÜZELTME

Oturum token'ını localStorage yerine `HttpOnly + Secure` çerezde tutun.

Referans: CWE-922 · OWASP A04:2021 Insecure Design

[ORTA] CT-13 · Hesap kilitleme / brute-force koruması yok

Durum: Açık

Etkilenen nokta: `/rest/user/login`

Açıklama: Ardışık başarısız girişte kilitleme/kısıtlama gözlenmedi.

Nasıl Tespit Edildi: Art arda 5 başarısız giriş denemesinden sonra kilitleme, 429 veya belirgin gecikme gözlemlenmedi — zayıf/yok lockout & rate-limit göstergesi (brute-force'a açık olabilir). Gerçek hesap kilitlenmedi (throwaway kullanıcı kullanıldı).

İş Etkisi: Ardışık başarısız girişte kilitleme/kısıtlama gözlenmedi; kaba-kuvvet (brute-force) saldırısına açık.

ÖNERİLEN DÜZELTME

Hesap+IP bazlı kademeli gecikme/kilitleme ve CAPTCHA ekleyin.

Referans: CWE-307 · OWASP A07:2021 Identification & Authentication Failures

[ORTA] CT-14 · Aşırı veri ifşası (API/BOPLA)

Durum: Açık

Etkilenen nokta: `/api/Products`

Açıklama: API yanıtı gerekenden fazla/hassas alan (parola-hash/rol/iç-ID) döndürüyor.

Nasıl Tespit Edildi: API yanıtı (/api/Products) UI'nin ihtiyaç duymadığı iç/aşırı alan içeriyor (deletedAt) — iç ID/rol/durum alanları istemciye sızıyor (gösterge). Yanıtı yalnız gereken alanlarla sınırlayın (allowlist DTO).

İş Etkisi: API yanıtı gerekenden fazla/hassas alan (parola-hash/rol/iç-ID) döndürüyor; veri sızıntısı ve yetki haritalama.

ÖNERİLEN DÜZELTME

Yanıtları alan-allowlist (response DTO) ile sınırlayın; hassas alanları hiç göndermeyin.

Referans: CWE-213 · OWASP API3:2023 Broken Object Property Level Authorization

[ORTA] CT-15 · API rate-limit yok

Durum: Açık

Etkilenen nokta: `/api/BasketItems`

Açıklama: API ucunda rate-limit/kota gözlenmedi.

Nasıl Tespit Edildi: Bir API ucuna (/api/BasketItems) art arda 10 istek sonrası 429 veya rate-limit başlığı gözlenmedi — kısıtlanmamış kaynak tüketimi (API4) göstergesi (brute-force/scraping/DoS'a açık olabilir). Hedef yorulmadı (modest burst). Rate-limit + kota önerilir.

İş Etkisi: API ucunda rate-limit/kota gözlenmedi; brute-force, scraping ve kaynak tüketimi (DoS) riskine açık.

ÖNERİLEN DÜZELTME

Hesap+IP+endpoint bazlı rate-limit + kota; ağır uçlara maliyet-tabanlı sınır ekleyin.

Referans: CWE-770 · OWASP API4:2023 Unrestricted Resource Consumption

[ORTA] CT-16 · DMARC politikası yetersiz (eksik veya zayıf)

Durum: Açık

Etkilenen nokta: `ornek.com`

Açıklama: DMARC kaydı yok; SPF/DKIM uygulanmıyor.

Nasıl Tespit Edildi: DMARC p=none (org-alan (ornek.com)) — yalnız izleme; spoofing e-postaları alıcıda engellenmiyor (gösterge). p=quarantine→reject kademeli sıkılaştırma önerilir.

İş Etkisi: DMARC politikası olmadan sahte e-postalar engellenmez; phishing ve marka itibarı riski.

ÖNERİLEN DÜZELTME

`_dmarc` altına `v=DMARC1; p=quarantine` (izlemeyle başlayıp reject'e yükseltin).

Referans: CWE-290 · OWASP A07:2021 Identification & Authentication Failures

[ORTA] CT-17 · HSTS (Strict-Transport-Security) eksik

Durum: Açık

Etkilenen nokta: `ornek.com`

Açıklama: HSTS (Strict-Transport-Security) yok; tarayıcı HTTPS'e zorlanmıyor.

Nasıl Tespit Edildi: HTTPS yanıtında Strict-Transport-Security yok — ilk bağlantı HTTPS'e zorlanmıyor, MITM/downgrade riski. max-age≥15768000; includeSubDomains; preload önerilir.

İş Etkisi: İlk bağlantı HTTPS'e zorlanmadığından araya-girme (MITM) saldırısıyla trafik dinlenebilir/yönlendirilebilir.

ÖNERİLEN DÜZELTME

`Strict-Transport-Security: max-age=31536000; includeSubDomains` ekleyin (site tamamen HTTPS ise).

Referans: CWE-319 · OWASP A05:2021 Security Misconfiguration

[DÜŞÜK] CT-18 · Yansıyan XSS göstergesi

Durum: Açık

Etkilenen nokta: `GET /redirect?to`

Açıklama: Kullanıcı girdisi yanıt HTML'ine kodlanmadan yansıyor (yansıyan XSS göstergesi).

Nasıl Tespit Edildi: İşaret dizesi yansıdı ancak KISMİ/ENCODE EDİLMİŞ (özel karakterler < > " kaçırılmış) — bağlama bağlı düşük güvenli gösterge; manuel doğrulama önerilir.

İş Etkisi: Kullanıcının tarayıcısında betik çalıştırılarak oturum çalma/kimlik taklidi ve hesap ele geçirme mümkün olabilir.

ÖNERİLEN DÜZELTME

Çıktıyı bağlama uygun kodlayın (HTML entity encoding); CSP ile satır-içi script'i kısıtlayın.

Referans: CWE-79 · OWASP A03:2021 Injection

[DÜŞÜK] CT-19 · Web cache / hassas önbellekleme göstergesi

Durum: Açık

Etkilenen nokta: `/rest/user/whoami`

Açıklama: Hassas yanıt önbelleğe alınabiliyor veya unkeyed başlık yansıması var.

Nasıl Tespit Edildi: Kimlik-doğrulamalı yanıt (/rest/user/whoami) Cache-Control: no-store/no-cache/private içermiyor (gözlenen: yok) — tarayıcı/ara-proxy hassas içeriği önbelleğe alabilir.

İş Etkisi: Hassas yanıt önbelleğe alınabiliyor / unkeyed başlık yansıması göstergesi; cache poisoning veya hassas veri sızıntısı.

ÖNERİLEN DÜZELTME

Hassas yanıtlara `Cache-Control: no-store`; cache anahtarına ilgili başlıkları dahil edin.

Referans: CWE-525 · OWASP A05:2021 Security Misconfiguration

[DÜŞÜK] CT-20 · CAA kaydı eksik

Durum: Açık

Etkilenen nokta: `ornek.com`

Açıklama: CAA kaydı yok; herhangi bir CA sertifika verebilir.

Nasıl Tespit Edildi: CAA kaydı gözlenmedi — herhangi bir CA ornek.com için sertifika verebilir (yanlış-verilme riski göstergesi). CAA ile yetkili CA'lar kısıtlanabilir.

İş Etkisi: CAA kaydı yok; herhangi bir CA alan için sertifika verebilir — yanlış/kötü-amaçlı sertifika verme riski.

ÖNERİLEN DÜZELTME

Yetkili CA'ları `CAA` kaydıyla kısıtlayın (ör. `0 issue "letsencrypt.org"`).

Referans: CWE-295 · OWASP A05:2021 Security Misconfiguration

[DÜŞÜK] CT-21 · Content-Security-Policy eksik

Durum: Açık

Etkilenen nokta: `ornek.com`

Açıklama: Content-Security-Policy gönderilmiyor; tarayıcı-taraflı XSS azaltma katmanı yok.

Nasıl Tespit Edildi: Content-Security-Policy başlığı yok — enjekte edilen script'lere karşı tarayıcı-taraflı azaltma katmanı bulunmuyor (sertleştirme boşluğu, düşük).

İş Etkisi: İçerik enjeksiyonu ve XSS için tarayıcı-taraflı azaltma katmanı yok; enjekte edilen betikler çalışabilir.

ÖNERİLEN DÜZELTME

Sıkı bir CSP tanımlayın (`default-src 'self'`); üçüncü taraf kaynakları allowlist'leyin.

Referans: CWE-693 · OWASP A05:2021 Security Misconfiguration

[DÜŞÜK] CT-22 · Referrer-Policy eksik

Durum: Açık

Etkilenen nokta: `ornek.com`

Açıklama: Referrer-Policy yok; dış bağlantılara tam adres sızabilir.

Nasıl Tespit Edildi: Referrer-Policy başlığı yok — dış bağlantılara adres/oturum bilgisi sızabilir (bilgilendirici). Referrer-Policy: strict-origin-when-cross-origin önerilir.

İş Etkisi: Dış bağlantılara adres/oturum bilgisi sızabilir; düşük etkili bilgi ifşası riski.

ÖNERİLEN DÜZELTME

`Referrer-Policy: strict-origin-when-cross-origin` ekleyin.

Referans: CWE-200 · OWASP A05:2021 Security Misconfiguration

[DÜŞÜK] CT-23 · Permissions-Policy eksik

Durum: Açık

Etkilenen nokta: `ornek.com`

Açıklama: Permissions-Policy başlığı yok; tarayıcı özellik erişimi kısıtlanmıyor.

Nasıl Tespit Edildi: Permissions-Policy başlığı yok — tarayıcı özellik erişimi (kamera/mikrofon/konum) kısıtlanmıyor (bilgilendirici sertleştirme).

İş Etkisi: Permissions-Policy yok; tarayıcı özellik erişimi (kamera/mikrofon/konum vb.) kısıtlanmıyor (bilgilendirici sertleştirme).

ÖNERİLEN DÜZELTME

Kullanılmayan özellikleri kapatan bir `Permissions-Policy` ekleyin (ör. `geolocation=(), camera=(), microphone=()`).

Referans: CWE-693 · OWASP A05:2021 Security Misconfiguration

Pozitif Güvence

Şu kontroller çalıştırıldı ve belirgin bir zafiyet göstergesi bulunamadı: JWT / Token Güvenliği, Client-Side / JS Analizi, Girdi & Header Derinliği, Yapılandırma & İfşa Derinliği, Subdomain Takeover (Dangling DNS). Bu alanlar, tarama anındaki gözlemlerde temiz görünmektedir (kesin güvence için düzenli tekrar önerilir).

3. Kontrol Özeti ve Metodoloji

İnceleme Notu: Şu kontroller, hedefin mimarisine uygulanabilir bir giriş noktası bulunmadığından mimari gereği kapsam dışı bırakılmıştır (Kontrol Özeti tablosunda da işaretlidir): Oturum Çerezi Bayrakları, Session Fixation, Oturum Güvenliği Derinliği.

Değerlendirme Özeti (Authenticated)

Bu tarama, verilen TEST hesabının oturumuyla KİMLİK-DOĞRULAMALI (login'li) bağlamda yapılmıştır. 20 authenticated kontrol değerlendirildi; toplam **311** istek. En yüksek risk **Authenticated Enjeksiyon (SQLi/XSS)** alanında (aşağıda detaylı).

Şifre hiçbir aşamada dışarı/üçüncü bir servise gönderilmedi; backend deterministik login yapıp yalnız oturumu (cookie/token) kullandı.

KONTROL ÖZETİ

Kontrol	Sonuç	Güven
Oturum Çerezi Bayrakları	Uygulanabilir giriş noktası yok (Kapsam dışı)	Kapsam dışı
Session Fixation	Uygulanabilir giriş noktası yok (Kapsam dışı)	Kapsam dışı
Logout / Oturum Geçersizleştirme	⚠ Sınırlı gösterge	Orta
Forced Browsing / Fonksiyon-Seviye Yetki	⚠ Sınırlı gösterge	Orta
Authenticated Enjeksiyon (SQLi/XSS)	⚠ Zafiyet göstergesi	Yüksek
Authenticated IDOR (kendi kaynakları)	⚠ Sınırlı gösterge	Orta
Yetki Yükseltme (Privilege Escalation)	İncelenemedi — güvenli test edilebilir yüzey yok	Kapsam dışı
Çok-Adımlı İş Mantığı	İncelenemedi — güvenli test edilebilir yüzey yok	Kapsam dışı
JWT / Token Güvenliği	✓ Zafiyet kanıtı yok	Yüksek
Giriş Baypası (SQLi Göstergesi)	⚠ Zafiyet göstergesi	Yüksek
Client-Side / JS Analizi	✓ Zafiyet kanıtı yok	Yüksek
Client-Side Statik Analiz	⚠ Sınırlı gösterge	Orta
Kimlik-Doğrulama Derinliği	⚠ Sınırlı gösterge	Yüksek
Oturum Güvenliği Derinliği	Uygulanabilir giriş noktası yok (Kapsam dışı)	Kapsam dışı
Girdi & Header Derinliği	✓ Zafiyet kanıtı yok	Orta
Yapılandırma & İfşa Derinliği	✓ Zafiyet kanıtı yok	Yüksek
API Güvenliği Derinliği (OWASP API Top 10)	⚠ Sınırlı gösterge	Orta
E-posta & DNS Derinliği (Anti-Spoofing)	⚠ Sınırlı gösterge	Orta
Taşıma Katmanı, CORS & Güvenlik Başlığı Derinliği	⚠ Sınırlı gösterge	Orta
Subdomain Takeover (Dangling DNS)	✓ Zafiyet kanıtı yok	Orta

Güven yalnızca gerçekten uygulanabilen (giriş/çerez/uç bulunan) kontroller için gösterilir; uygulanamayan kontroller **Kapsam dışı**dır (ör. çerez yerine token kullanan oturumda çerez-bayrağı/fixation).

Logout / Oturum Geçersizleştirme

NE KONTROL EDİLDİ

- Oturumla 200 dönen korumalı bir uç (whoami/profil) tespit edildi.
- GET ile çağrılabilen bir logout uç noktası denendi (**POST yok** — state değişmez).
- Logout SONRASI AYNI token ile korumalı uca tekrar erişilebiliyor mu kontrol edildi.

BULGULAR

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
/rest/user/whoami	logout sonrası token yeniden kullanımı	Logout çağrıldıktan SONRA da AYNI oturum token'ıyla korumalı uç (/rest/user/whoami) 200 döndürdü — oturum sunucu tarafında geçersizleştirilmiyor.	Orta	yok	Orta

Kapsam ve yöntem: Bu paket, "kanıtla — istismar etme" ilkesiyle çalışır. Backend, hedefe sınırlı sayıda **zararsız** doğrulama probu göndermiştir; hiçbir veri çekilmemiş, değiştirilmemiş veya silinmemiştir. İstekler arası bekleme ve hedef-sağlığı devre kesici (art arda 5xx / aşırı yavaşlama / WAF) uygulanır. Bu bölüm, sağladığınız TEST hesabının oturumuyla kimlik-doğrulamalı (login'li) bağlamda çalıştırılmıştır; ödeme/hesap-durumu değişikliği tamamlama kod seviyesinde engellidir.

Forced Browsing / Fonksiyon-Seviye Yetki

NE KONTROL EDİLDİ

- Yaygın admin/yönetim uç noktalarına ELDEKİ (muhtemelen düşük yetkili) test hesabının oturumuyla **GET** isteği atıldı.
- Yanlış-pozitifi önlemek için yalnız ana-sayfa shell'inden **FARKLI** içerik/JSON dönen 200'ler bulgu sayıldı.
- Tek deneme, GET-only, devre kesiciye tabi.

BULGULAR

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
/rest/admin/application-configuration	düşük yetkili oturumla forced browsing (GET)	`/rest/admin/application-configuration` uç noktası, düşük yetkili test hesabının oturumuyla **200** ve JSON veri döndürdü — eksik fonksiyon-seviye yetkilendirme (olası yetkisiz yönetim erişimi) göstergesi (dönen veri raporda gösterilmez).	Orta	yok	Orta
/api/Users	düşük yetkili oturumla forced browsing (GET)	`/api/Users` uç noktası, düşük yetkili test hesabının oturumuyla **200** ve JSON veri döndürdü — eksik fonksiyon-seviye yetkilendirme (olası yetkisiz yönetim erişimi) göstergesi (dönen veri raporda gösterilmez).	Orta	yok	Orta
/metrics	düşük yetkili oturumla	`/metrics` uç noktası, düşük yetkili test hesabının oturumuyla **200** ve içerik döndürdü — eksik fonksiyon-seviye	Düşük	yok	Orta

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
	forced browsing (GET)	yetkilendirme (olası yetkisiz yönetim erişimi) göstergesi (dönen veri raporda gösterilmez).			
/rest/admin/application-version	düşük yetkili oturumla forced browsing (GET)	`/rest/admin/application-version` uç noktası, düşük yetkili test hesabının oturumuyla **200** ve JSON veri döndürdü — eksik fonksiyon-seviye yetkilendirme (olası yetkisiz yönetim erişimi) göstergesi (dönen veri raporda gösterilmez).	Orta	yok	Orta

Authenticated Enjeksiyon (SQLi/XSS)

NE KONTROL EDİLDİ

Taranan sayfalardan (ana sayfa + iç linkler + iyi-bilinen yollar) keşfedilen giriş noktaları (URL query parametreleri + form alanları) üzerinde, giriş noktası başına zararsız doğrulama probları:

- **SQLi (hata-tabanlı):** Tek tırnak (`'`) enjekte edilip yanıtta veritabanı hata imzası (MySQL/PostgreSQL/Oracle/MSSQL/SQLite) arandı.
- **SQLi (zaman-tabanlı):** Hata görülmeyen noktalarda tek bir zararsız gecikme probu (SLEEP) ile yanıt süresi baseline'a göre ölçüldü (blind SQLi göstergesi).
- **SQLi (boolean-tabanlı):** Sayısal/ID-benzeri noktalarda TRUE (`1=1`) ve FALSE (`1=2`) koşullu iki istek gönderilip yanıtları (status + içerik uzunluğu) karşılaştırıldı; TRUE tekrarında tutarlı ve FALSE'tan KALICI farklıysa boolean-based SQLi göstergesidir (yanlış-pozitife karşı stabilite doğrulaması yapılır).
- **XSS (yansıyan):** Benzersiz, zararsız bir işaret dizesi enjekte edilip yanıt HTML'inde **kaçırılmadan (unencoded)** yansıyıp yansımadığı kontrol edildi (JS çalıştırılmadı; stored XSS denenmedi).

BULGULAR

Giriş Noktası	Tür	Teknik	Kanıt	Güven (gerekçe)	Ciddiyet
GET /rest/products/search?q	SQLi	hata-tabanlı	Yanıtta veritabanı hata imzası görüldü ("')" payload'ı ile): "SQLITE_ERROR"	Yüksek — yanıtta veritabanı hata imzası (doğrudan kanıt)	Yüksek
GET /redirect?to	XSS	yansıma	İşaret dizesi yansıdı ancak KISMİ/ENCODE EDİLMİŞ (özel karakterler `< > "` kaçırılmış) — bağlama bağlı düşük güvenli gösterge; manuel doğrulama önerilir.	Düşük — yansıdı ancak kodlanmış/kaçırılmış; bağlama bağlı zayıf gösterge	Düşük

Authenticated IDOR (kendi kaynakları)

NE KONTROL EDİLDİ

Taranan sayfalardan keşfedilen, tahmin edilebilir/sayısal ID içeren uç noktalar (ör. `?id=123` , `/user/45`) üzerinde:

- ID değeri **komşu bir değere** (N-1 / N+1) değiştirilip, kimlik-doğrulamalı oturumla **GET** isteği gönderildi.
- Yalnızca yanıt **durumu ve boyutu** karşılaştırıldı; **dönen içerik saklanmadı/alıntılanmadı**.
- Farklı ve geçerli görünen bir kaynak dönmesi, numaralandırılabilir erişim göstergesi sayıldı.

BULGULAR

Uç Nokta	ID	Gözlem	Ciddiyet
/api/products/1	path-id	Kimlik doğrulaması olmadan komşu ID (2) için 200 yanıt ve aynı YAPIDA (JSON iskeleti) ancak FARKLI İÇERİKLİ yanıt döndü — büyük olasılıkla başka bir kaydın verisi (dönen veri raporda gösterilmez). Numaralandırılabilir kaynak erişimi (olası IDOR) göstergesi.	Orta
/api/users/1	path-id	Kimlik doğrulaması olmadan komşu ID (2) için 200 yanıt ve aynı YAPIDA (JSON iskeleti) ancak FARKLI İÇERİKLİ yanıt döndü — büyük olasılıkla başka bir kaydın verisi (dönen veri raporda gösterilmez). Numaralandırılabilir kaynak erişimi (olası IDOR) göstergesi.	Orta

KAPSAM SINIRI (ÖNEMLİ)

Bu bölüm, sağladığınız TEST hesabının **oturumuyla (login'li)** çalıştırılmıştır ve hesabın **kendi** numaralandırılabilir kaynaklarına yetkisiz erişimi test eder. **Cross-account** (başka bir kullanıcının verisine erişim) testi bu sürümün kapsamı dışındadır (iki ayrı hesap gerektirir). Bulgu olmaması, tüm kimlik-doğrulamalı akışlarda IDOR olmadığını kanıtlamaz.

> Ayrıca **1** koleksiyon-benzeri uçtan (ör. `/rest/products`) sıralı sayısal ID'ler (`/{1..3}`) türetilip GET ile içerik-farkı yöntemiyle test edildi.

Yetki Yükseltme (Privilege Escalation)

NE KONTROL EDİLDİ

- Keşfedilen authenticated yüzeyde **deterministik olarak** yetki-alanı içeren form/API (kayıt/profil/ayar tipi) arandı.
- Güvenli test edilebilir bir yüzey bulunduysa **güvenli, authenticated-light** fonksiyonla TEK gözlemsel mass-assignment probu (`role/isAdmin` ek alan) uygulandı.

⚠ Gerçek yükseltme TAMAMLANMADI; yükseltilmiş yetkiyle tekrar giriş yapılmadı; oturum dışına çıkılmadı; hesap-değiştiren/checkout hedeflerine **yazılmadı** (kod-seviyesi blocklist).

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

> Mass-assignment göstergesi yalnızca ilk yanıttan çıkarılmıştır (düşük güven); kesin doğrulama manuel test gerektirir.

> Yetki-yükseltme için GÜVENLE test edilebilir (YASAK olmayan; kayıt/profil/ayar tipi) bir form/uç bu hedefte bulunamadı — bu kontrol **İncelenemedi** (deterministik prob için uygun authenticated yüzey yok). Not: bazı açıklar (API'de gizli `role` kabulü vb.) UI/DOM'da görünmez; kesin sonuç manuel test gerektirir.

Çok-Adımlı İş Mantığı

NE KONTROL EDİLDİ

- **Deterministik olarak** çok-adımlı akış/fiyat-kupon alanı arandı; backend YALNIZ **GET-gözlem** yaptı.
- İstemci-değiştirilebilir gizli fiyat/miktar/kupon alanı + ön koşulsuz erişilebilen "onay" adımı gözlemlendi.

⚠ Yalnız sepete/forma kadar; **ödeme/checkout TAMAMLANMADI** (kod-seviyesi blocklist); hiçbir kaynak tüketilmedi.

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

İş mantığı zafiyetleri bağlama özeldir; bu kontrol yüzey/gösterge seviyesindedir.

Bu kontrol **deterministik olarak** çalıştırıldı (gözlemsel adım-atlama + istemci-değiştirilebilir fiyat/miktar/kupon alanı). AI otonom analiz katmanı **varsayılan olarak devre dışıdır** (deneyde ek doğrulanmış kanıt üretmediği için).

JWT / Token Güvenliği

NE KONTROL EDİLDİ

- Oturum bir **JWT bearer** taşıyorsa token OFFLINE çözülüp analiz edildi: imza algoritması (**alg=none / imzasız**), imza sırrının **zayıf/yaygın** olup olmadığı (yaygın sırlarla OFFLINE doğrulama), ve token gövdesindeki **hassas/aşırı claim** (parola/sır, rol/yetki).
- Ek olarak TEK, zararsız gözlem: imzasız (alg=none) forge edilmiş bir token korumalı bir uçta KABUL ediliyor mu (yalnız gözlem; erişim kullanılmadı).

⚠ Gerçek istismar YOK — token ele geçirme/yetki yükseltme yapılmadı; yalnız güvenlik göstergesi raporlandı.

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

Zayıf-sır ve alg=none KABUL göstergeleri kesindir (yüksek güven); claim gözlemleri bilgilendirmedir.

Token'da son kullanma (exp) claim'i yok — süresiz token, çalınması durumunda kalıcı erişim riski taşır. alg=none kabul gözlemi için doğrulanabilir bir korumalı okuma ucu (whoami/profil) bulunamadı — bu gözlem atlandı. JWT/token güvenlik göstergesi bulunamadı (alg=none değil, zayıf sır doğrulanmadı, hassas claim yok).

Giriş Baypası (SQLi Göstergesi)

NE KONTROL EDİLDİ

- Giriş (login) ucuna önce **geçersiz kimlik** (kontrol) gönderildi; ardından klasik SQLi payload'ları (`' OR '1'='1` vb.) denenip, kontrolün AKSİNE oturum/başarı (token/2xx) dönüp dönmediği gözlemlendi.
- Login POST'u zaten izinli akıştır; TEK, zararsız gözlemdir.

⚠ Oturum ele geçirme/istismar YOK — yalnız "kimlik doğrulama atlatma göstergesi var mı" gözlemi.

BULGULAR

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
POST /rest/user/login	giriş baypası (SQLi: `' OR 1=1--`)	Kontrol (geçersiz kimlik) → HTTP 401 (başarısız). SQLi payload `' OR 1=1--` → HTTP 200 + AÇIK başarı sinyali: "{"authentication": {"token":"***","bid":1,"umail":"admin@juice-sh.op"}}". Kimlik doğrulama SQL enjeksiyonuyla ATLATILIYOR (oturum/authorization token döndü — güçlü kanıt). Oturum ele geçirme/istismar YAPILMADI; token değeri raporda gösterilmez (redakte).	Yüksek	yok	Yüksek

> Gösterge, kontrol denemesiyle karşılaştırmaya dayanır; kesin doğrulama manuel test gerektirir.

Client-Side / JS Analizi

NE KONTROL EDİLDİ

- Sayfanın yüklediği JS bundle'ları (script src'leri + inline) çekilip **statik** analiz edildi — aktif istismar YOK, yalnız indir + oku.
- **A) Sır taraması:** özel anahtar, AWS/GCP kimliği, Stripe **sk_live_**, GitHub/GitLab/Slack token, DB bağlantı dizesi gibi GERÇEK sırlar arandı (değerler REDAKTE).
- **Public-by-design ayrımı:** Firebase apiKey, GTM/GA ölçüm ID, Google Maps browser key, Stripe **pk_**, reCAPTCHA site key tasarım gereği herkese açıktır → "ifşa/sır" SAYILMAZ, yalnız bilgilendirici listelenir.
- **B) Source-map ifşası:** `//# sourceMappingURL` yorumları + `.js.map` adayları denendi; erişilebilir `.map` → orijinal kaynak kod/ağaç sızıntısı.
- **C) Bilinen-zafiyetli kütüphane:** yüklenen kütüphaneler + SÜRÜMLERİ tespit edilip bilinen CVE'lerle MUHAFAZAKÂR eşlendi; sürüm güvenle okunamazsa CVE eşleme YAPILMADI ("yama teyidi gerekir" dili; "istismar edilebilir" denmez).

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

> Tümü pasif/statiktir; kütüphane bulguları sürüm-tabanlı göstergedir (dağıtımınız yamalı/backport'lu olabilir — teyit önerilir).

> Tarandı: **3** same-origin JS dosyası + **1** inline script; **0** kütüphane tespit edildi; **3** source-map adayı denendi. (0 harici/CDN script sürüm için incelendi.)

Client-Side Statik Analiz

NE KONTROL EDİLDİ

- Aynı JS/HTML corpus'u üzerinde **statik** olarak (aktif istismar YOK) 6 istemci-tarafı kontrol yapıldı.
- **1) DOM-based XSS (gösterge):** tehlikeli sink (innerHTML/document.write/eval/.html()/location=) ile kullanıcı-kontrollü kaynak (location.hash/search, referrer, window.name) AYNI ifadede mi — **kanıtlanmış XSS DEĞİL**, düşük güvenli gösterge (dinamik doğrulama gerekir).
- **2) postMessage:** `message` olay dinleyicilerinde **event.origin doğrulaması** var mı.
- **3) Browser storage:** localStorage/sessionStorage'a **hassas veri** (token/JWT/oturum) yazımı (statik; değer REDAKTE).
- **4) Eksik SRI:** harici script/style'larda `integrity` attribute'u var mı (tedarik-zinciri).
- **5) Reverse tabnabbing:** `target="_blank"` linklerinde `rel="noopener/noreferrer"` var mı.
- **6) Open redirect:** HTML'de GÖZLENEN yönlendirme parametrelerine **tek güvenli prob** — zararsız harici URL gönderilip Location gözlendi; **redirect TAKİP EDİLMEDİ**.

BULGULAR

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
main.js · message handler	web messaging (postMessage) origin	`main.js` içinde bir `message` olay dinleyicisi **event.origin doğrulaması olmadan** işlem yapıyor gibi görünüyor — güvensiz cross-origin mesaj işleme göstergesi. Gönderen origin'i allowlist ile doğrulanmalı.	Orta	yok	Orta

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
	doğrulaması analizi				
main.js · localStorage['token']	browser storage statik hassas-veri analizi	`main.js` içinde `localStorage.setItem('token', …)` — hassas veri (oturum/kimlik göstergesi) istemci depolamasına yazılıyor (değer gösterilmez). localStorage/sessionStorage XSS ile okunabilir; oturum verisi için HttpOnly çerez tercih edilmelidir.	Orta	yok	Orta
main.js · localStorage['totp_tmp_token']	browser storage statik hassas-veri analizi	`main.js` içinde `localStorage.setItem('totp_tmp_token', …)` — hassas veri (oturum/kimlik göstergesi) istemci depolamasına yazılıyor (değer gösterilmez). localStorage/sessionStorage XSS ile okunabilir; oturum verisi için HttpOnly çerez tercih edilmelidir.	Orta	yok	Orta

DOM-XSS bulguları STATİK göstergedir (yanlış-pozitif potansiyeli yüksek; dinamik doğrulama gerekir). Diğerleri deterministik gözlemdir.

Statik ayrıştırıldı: **3** same-origin JS + **1** inline script; **0** harici kaynak SRI için, **0** `target=_blank` link tabnabbing için kontrol edildi; **0** redirect-parametresi güvenli probla denendi (redirect TAKİP EDİLMEDİ). DOM-XSS eşleşmeleri STATİK **göstergedir** (kanıtlanmış XSS değil); yüksek yanlış-pozitif potansiyeli taşır ve dinamik doğrulama gerektirir. HTML'de gözlemlenen bir yönlendirme (redirect) parametresi bulunamadı — open redirect probu **kapsam dışı**.

Kimlik-Doğrulama Derinliği

NE KONTROL EDİLDİ

- 9 kimlik-doğrulama derinlik kontrolü (WSTG-ATHN/IDNT) — **güvenli, düşük hacim**; brute-force/DoS YOK.
- **1) Hesap enumerasyonu:** geçerli (test hesabı) vs geçersiz (rastgele) kullanıcıda yanıt farkı — birer BAŞARISIZ deneme; hesap oluşturmaz.
- **2) Varsayılan kimlik:** küçük sabit liste (admin/admin vb.) — yalnız başarısız login; kabul edilirse oturum KULLANILMAZ.
- **3) Zayıf lockout/rate-limit:** THROWAWAY (rastgele) kullanıcıyla birkaç hatalı deneme — **gerçek hesap ASLA kilitlenmez**.
- **4) Parola sıfırlama:** mekanizma gözlemi (güvenlik sorusu/token) — **GERÇEK sıfırlama e-postası TETİKLENMEZ** (var-olmayan e-posta).
- **5) Parola/kayıt politikası:** yalnız client-side gözlem — **GERÇEK kayıt YAPILMAZ**.
- **6) "Beni hatırla" çerezi · 7) Authenticated sayfa cache (Cache-Control) · 8) MFA varlığı (bilgilendirici) · 9) Kimlik şifresiz kanalda (HTTP).**

BULGULAR

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
/rest/user/login	hesap kilitleme / login hız-sınırı gözlemi (throwaway kullanıcıyla)	Art arda 5 başarısız giriş denemesinden sonra kilitleme, 429 veya belirgin gecikme gözlemlenmedi — **zayıf/yok lockout & rate-limit göstergesi** (brute-force'a açık olabilir). Gerçek hesap kilitlenmedi (throwaway kullanıcı kullanıldı).	Orta	yok	Orta

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
/rest/user/whoami	authenticated yanıt cache başlığı gözlemi	Kimlik-doğrulamalı yanıt (`/rest/user/whoami`) `Cache-Control: no-store/no-cache/private` içermiyor (gözlenen: `yok`) — tarayıcı/ara-proxy hassas içeriği önbelleğe alabilir.	Orta	yok	Düşük

> Enumerasyon/lockout/reset bulguları "gösterge"dir (doğrulama gerekir). Güvenlik: gerçek hesap kilitlenmedi, reset e-postası gitmedi, kayıt yapılmadı, başarılı giriş bulunsa bile oturum kullanılmadı.

> Parola sıfırlama ucu gözlemlendi; token/mekanizma statik olarak doğrulanamadı (gerçek e-posta tetiklenmedi) — bu bölüm için sınırlı. Ana sayfada client-side parola alanı gözlemlenmedi (SPA/ayrı sayfa olabilir) — parola politikası statik olarak sınırlı incelendi. Oturum bearer/token tabanlı (çerez-tabanlı "beni hatırla" kalıcı çerezi kapsam dışı). Login akışında MFA/2FA göstergesi gözlemlenmedi (bilgilendirici; ikinci faktör önerilir). Denenen: **16** güvenli auth-probu (varsayılan-kimlik yalnız başarısız login; lockout THROWAWAY kullanıcıyla; reset var-olmayan e-posta ile; kayıt YAPILMADI; gerçek hesap kilitlenmedi).

Girdi & Header Derinliği

NE KONTROL EDİLDİ

- Güvenli/read-only girdi & header kontrolleri (yalnız GET/OPTIONS/TRACE — durum-değiştiren/yıkıcı istek YOK).
- **D1 Host header injection:** sahte `X-Forwarded-Host` gönderilip yanıtta yansıma gözlendi (gösterge).
- **D2 HTTP parameter pollution:** aynı parametre tekrarlanıp işleniş farkı gözlendi (gözlemsel).
- **D3 HTTP methods / TRACE:** OPTIONS ile izinli method keşfi + TRACE gözlemi — **PUT/DELETE GÖNDERİLMEDİ**.
- **D4 Mixed content:** HTTPS sayfada HTTP kaynak (script/img/iframe) statik tespit.
- **D5 Stored-XSS giriş noktası:** kalıcı bağlama yansıyabilecek ADAY alanlar işaretlendi — **hiçbir veri GÖNDERİLMEDİ/kaydedilmedi** (düşük güven, dinamik doğrulama gerekir).

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

> Host-injection/HPP/D5 "gösterge/aday"dır (gerçek saldırı/gönderim yapılmadı). TRACE/mixed-content deterministik gözlemdir.

> Parametreli same-origin uç gözlemlenmedi — HPP için test edilebilir yüzey yok. Denenen: **4** güvenli girdi/header probu (yalnız GET/OPTIONS/TRACE — PUT/DELETE GÖNDERİLMEDİ; stored-XSS yalnız aday, veri OLUŞTURULMADI). Mixed content: 0 HTTP kaynak.

Yapılandırma & İfşa Derinliği

NE KONTROL EDİLDİ

- Güvenli GET + statik yapılandırma/ifşa kontrolleri. **SPA catch-all 200 (ana sayfa shell)** dönen tahmin edilen yollar GERÇEK sayılmaz — yalnız gerçekten erişilebilen, AYIRT EDİCİ yanıt bulgu üretir (Sütun 0 provenance).
- **E1 Yedek/eski dosya:** `.env/.bak/.sql/.git/config` vb. güvenli GET (shell 200 elendi).

- **E2 Admin arayüz:** yaygın yönetim yolları dışarıdan erişilebilir mi (aynı provenance).
- **E3 Cloud storage:** HTML/JS'te public S3/GCS/Azure bucket referansı + **listelenebilir** mi.
- **E4 Cache / poisoning göstergesi:** Cache-Control/Vary + unkeyed-header yansıması (zehirleme YAPILMADI).
- **E5 Yorum & metadata sızıntısı:** dev yorumu / iç IP-hostname / sunucu dosya yolu (statik).

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

> Yedek/admin bulguları yalnız GERÇEKTEN erişilebilen, SPA-shell OLMAYAN yanıtlar için üretilir. Cache/host göstergeleri "gösterge"dir; içerik/hassas veri REDAKTE.

> Denenen: **14** yedek/eski dosya + **11** admin yolu (SPA catch-all shell 200'ler ELENDİ — gerçek/ayırt-edici olmayan yanıt bulgu sayılmadı); **0** bulut-depo referansı; yorum/metadata statik tarandı.

API Güvenliği Derinliği (OWASP API Top 10)

NE KONTROL EDİLDİ

- Aynı-origin JS/HTML'den keşfedilen, JSON dönen (SPA catch-all shell OLMAYAN) GERÇEK API uçlarında 5 kontrol — hepsi read-only. Gerçek API yoksa (Firebase/istemci-SDK/SPA) bu bölüm **kapsam dışıdır**.
- **F1 BOLA/BFLA (API1/API5):** nesne/fonksiyon-seviyesi yetki — **Authenticated IDOR** + **Forced Browsing** bölümlerinde değerlendirildi (çift bulgu önlemek için burada tekrar probe edilmedi).
- **F2 Aşırı veri ifşası / BOPLA (API3):** API yanıtında hassas/aşırı alan (parola-hash/rol/iç-ID) — değer REDAKTE.
- **F3 Rate-limit (API4):** MODEST burst (DoS DEĞİL) sonrası 429/rate-limit başlığı çıkıyor mu — hedef yorulmadı.
- **F4 Shadow/deprecated sürüm (API9):** /v1,/v2,/api/v1 gibi sürüm uçları erişilebilir mi (SPA-shell elendi).
- **F5 GraphQL introspection (APIT-99):** GraphQL ucu varsa introspection açık mı — **read-only sorgu; mutasyon YOK**.

BULGULAR

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
/api/Products	aşırı veri ifşası / BOPLA (API3) — yanıt alan gözlemi	API yanıtı (`/api/Products`) UI'nin ihtiyaç duymadığı iç/aşırı alan içeriyor (`deletedAt`) — iç ID/rol/durum alanları istemciye sızıyor (gösterge). Yanıtı yalnız gereken alanlarla sınırlayın (allowlist DTO).	Orta	yok	Orta
/api/BasketItems	API rate-limit / kısıtlanmamış tüketim gözlemi (modest burst — DoS değil)	Bir API ucuna (`/api/BasketItems`) art arda 10 istek sonrası **429 veya rate-limit başlığı gözlenmedi** — kısıtlanmamış kaynak tüketimi (API4) göstergesi (brute-force/scraping/DoS'a açık olabilir). Hedef yorulmadı (modest burst). Rate-limit + kota önerilir.	Orta	yok	Orta

> Bulgular "gösterge"dir; yalnız GERÇEKTEN gözlemlenen (JSON, SPA-shell olmayan) uçlarda. Hassas veri REDAKTE; mutasyon/veri-değiştirme/DoS yapılmadı.

> BOLA/BFLA (OWASP API1/API5 — nesne/fonksiyon-seviyesi yetki) **Authenticated IDOR** ve **Forced Browsing** bölümlerinde değerlendirilmiştir (çift bulgu önlemek için burada tekrar probe edilmedi). Keşfedilen gerçek API ucu: **8** (aynı-origin, JSON,

SPA-shell olmayan). Denenen: **38** güvenli prob (yalnız GET + read-only introspection; mutasyon/veri-değiştirme/DoS YOK).

E-posta & DNS Derinliği (Anti-Spoofing)

NE KONTROL EDİLDİ

- Yalnız GERÇEK org-alandan okunan DNS kayıtları; hepsi PASİF DNS/TXT + tek güvenli MTA-STS GET (saldırı/state-değişimi yok). Alt-alan için DMARC **organizasyonel alan** seviyesinde değerlendirilir.
- **G1 DMARC** politika gücü (p=none/quarantine/reject, pct, sp alt-alan, adkim/aspf, rua).
- **G2 SPF** derinliği (-all/~all/?all/+all + üst-seviye DNS-arama sayısı, RFC 7208).
- **G3 DKIM** yaygın seçici keşfi (default/google/selector1…) + anahtar uzunluğu (~1024/2048) + iptal (p= boş).
- **G4 MTA-STS** (_mta-sts TXT + politika: enforce/testing/none) · **G5 TLS-RPT** raporlama.
- **G6 DNSSEC** (imza/doğrulama — AD bayrağı, yalnız gözlem) · **G7 CAA** (sertifika-verme kısıtı) + **BIMI** (bilgilendirici).

BULGULAR

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
ornek.com	pasif DNS/TXT gözlemi	DMARC **p=none** (org-alan (ornek.com)) — yalnız izleme; spoofing e-postaları alıcıda engellenmiyor (gösterge). `p=quarantine` → `reject` kademeli sıkılaştırma önerilir.	Yüksek	yok	Orta
ornek.com	pasif DNS/TXT gözlemi	CAA kaydı **gözlenmedi** — herhangi bir CA `ornek.com` için sertifika verebilir (yanlış-verilme riski göstergesi). CAA ile yetkili CA'lar kısıtlanabilir.	Yüksek	yok	Düşük

Kanıt = DNS'in gerçekten döndürdüğü public kayıt (redaksiyon gereksiz). "gösterge" dili; e-posta göndermeyen alanda (MX yok) eksik DMARC/SPF şiddeti düşürülür. Uydurma/tahmin kayıt yok.

DMARC org-alan (ornek.com): `v=DMARC1; p=none; rua=mailto:rua@dmarc.brevo.com` SPF: `v=spf1 include:spf.improvmx.com ~all` SPF **~all** (softfail) — kabul edilebilir; kesin koruma için `-all` düşünülebilir. DKIM: yaygın seçicilerde (default/google/selector1…) kayıt **gözlenmedi** — kesin yokluk DEĞİL; özel seçici kullanılıyor olabilir (dürüst). MTA-STS: `_mta-sts` TXT gözlenmedi — SMTP MITM/downgrade koruması yok (düşük/olgunluk göstergesi). TLS-RPT (`_smtp._tls` TXT) gözlenmedi — SMTP TLS teslim sorunları raporlanmıyor (bilgilendirici). DNSSEC: alan **imzalı ve doğrulandı** (AD bayrağı) — DNS bütünlüğü korumalı (olumlu). BIMI (`default._bimi` TXT) gözlenmedi — bilgilendirici, güvenlik etkisi yok. Sorgulanan org-alan: **ornek.com** (hedef alt-alan: ornek.com). Toplam **20** pasif DNS sorgusu + en fazla 1 güvenli MTA-STS GET. Saldırı/state-değişimi/çözümleyici-saldırısı YOK.

Taşıma Katmanı, CORS & Güvenlik Başlığı Derinliği

NE KONTROL EDİLDİ

- Hepsi read-only/pasif gözlem — veri değiştirme, DoS, cipher istismarı YOK.
- **H1 CORS:** keşfedilen GERÇEK uçlara kurgu `Origin` ile tek istek — ACAO yansıması + ACAC=true (kimlik-bilgili sızıntı → Yüksek), yalnız yansıma (Orta, "tasarım olabilir"), `*` (bilgilendirici), `null` kabul (gösterge).
- **H3 TLS protokol/cipher:** protokol başına 1 güvenli handshake — TLS 1.0/1.1 (eski, gösterge), zayıf cipher (RC4/3DES/NULL/EXPORT). Sertifika süre/hostname/zincir yalnız GERÇEK sorunda bulgu (çift-CT yok).
- **H4 güvenlik başlığı derinliği:** HSTS (varlık + max-age yeterlilik + preload), clickjacking (X-Frame-Options **veya** CSP frame-ancestors çift-mekanizma), CSP zayıflık (unsafe-inline/eval/*), Referrer-Policy / Permissions-Policy / X-Content-Type-Options.

- Temel başlık VARLIK kontrolü diğer paketlerde kalır; bu bölüm DERİNLİK katar (kopyalanmadı).

BULGULAR

Giriş/Uç Nokta	Teknik	Kanıt	Güven	Yan-etki riski	Ciddiyet
ornek.com	HSTS (Strict-Transport-Security) başlık gözlemi	HTTPS yanıtında **Strict-Transport-Security yok** — ilk bağlantı HTTPS'e zorlanmıyor, MITM/downgrade riski. `max-age≥15768000; includeSubDomains; preload` önerilir.	Yüksek	yok	Orta
ornek.com	CSP varlık gözlemi	Content-Security-Policy başlığı **yok** — enjekte edilen script'lere karşı tarayıcı-taraflı azaltma katmanı bulunmuyor (sertleştirme boşluğu, düşük).	Yüksek	yok	Düşük
ornek.com	Referrer-Policy başlık gözlemi	Referrer-Policy başlığı yok — dış bağlantılara adres/oturum bilgisi sızabilir (bilgilendirici). `Referrer-Policy: strict-origin-when-cross-origin` önerilir.	Yüksek	yok	Düşük
ornek.com	Permissions-Policy başlık gözlemi	Permissions-Policy başlığı yok — tarayıcı özellik erişimi (kamera/mikrofon/konum) kısıtlanmıyor (bilgilendirici sertleştirme).	Yüksek	yok	Düşük

> Bulgular gerçek gözleme dayanır ("gösterge, doğrulama gerekir"); reflected-CORS + credentials NET kötüdür (Yüksek), credentials'sız yansıma tasarım olabilir (Orta). Deterministik (aynı host → aynı protokol/başlık).

> CORS: `/` `Access-Control-Allow-Origin: *` (credentials yok) — public kaynak için yaygın/kabul edilebilir (bilgilendirici). TLS: desteklenen protokoller — **TLS 1.2, TLS 1.3** (TLS 1.2/1.3 mevcut — olumlu). TLS sertifikası (süre/hostname/zincir) handshake sırasında geçerli görünüyor — belirgin sertifika sorunu gözlenmedi (olumlu). Denenen: **11** güvenli gözlem (CORS origin probu + TLS handshake + başlık okuması). Veri değiştirme / DoS / cipher istismarı / takeover-claim YOK. Sertifika geçerliliği yalnız GERÇEK sorunda bulgu (çift-CT yok).

Subdomain Takeover (Dangling DNS)

NE KONTROL EDİLDİ

- Certificate Transparency (crt.sh/certSpotter) ile keşfedilen GERÇEK alt-alanlarda CNAME çözümü.
- CNAME bilinen 3P servise (S3/GitHub Pages/Heroku/Azure/Netlify/Fastly/Shopify/... kapsamlı liste) işaret ediyor **VE** "sahiplenilmemiş" parmak-izi (NoSuchBucket / "There isn't a GitHub Pages site here" / NXDOMAIN vb.) dönüyorsa → OLASI takeover.
- Yalnız DNS çözümü + tek güvenli GET (parmak-izi gözlemi) — HİÇBİR kayıt/registrasyon/claim YAPILMAZ. Uydurma alt-alan yok.

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

> Yalnız dangling + parmak-izi eşleşince bulgu; canlı/sahiplenilmiş CNAME bilgilendirici. CT kaynağı erişilemezse "incelenemedi" (temiz değil).

> Keşfedilen alt-alan: **7** (CT logu), CNAME çözülen: **7**, dangling takeover göstergesi: **0**. Uydurma alt-alan yok — yalnız CT'de gözlenenler. Hiçbir kayıt/registrasyon/claim yapılmadı.

Metodoloji

Aşama	Açıklama
Keşif	Hedefin dış yüzeyi, sayfaları ve (SPA ise) JS bundle'ından gerçek uç/parametreler çıkarılır.
Otomatik tespit	Keşfedilen yüzeyde deterministik, güvenli (read-only) göstergeler aranır.
Manuel-deterministik doğrulama	Bulgular kod-tabanlı kurallarla doğrulanır; “kanıtla, istismar etme”.
Yetki & oturum	Kimlik-doğrulamalı pakette çerez/oturum/yetki ve login-sonrası yüzey incelenir.
Yapılandırma	Başlık, TLS, e-posta/DNS ve ifşa yapılandırmaları gözlemlenir.

Risk Derecelendirme Kriterleri

Şiddet	Tanım
Kritik	Doğrudan/kolay istismar edilebilen, ciddi veri/erişim etkisi olan gösterge.
Yüksek	Öne çıkan, öncelikli giderilmesi gereken güçlü gösterge.
Orta	Dikkat gerektiren, bağlama göre doğrulanması önerilen gösterge.
Düşük	Sertleştirme/olgunluk fırsatı; düşük öncelikli.

Şiddet yalnız bant etiketidir (sayısal CVSS skoru kullanılmaz); tüm bulgular “gösterge, doğrulama gerekir” çerçevesindedir.

---

4. AI Çözüm Önerileri

Bu bölüm, çalıştırılan authenticated kontrollerde tespit edilen bulgular için düzeltme önerileri içerir.

Oturum Çerezi Bayrakları

Çerez Güvenliği — proaktif sertleştirme

- Oturum çerezlerinde Secure/HttpOnly/SameSite bayraklarını proaktif olarak zorunlu kılın.

Session Fixation

Session Fixation — proaktif sertleştirme

- Girişte oturum id yenilemeyi (session regeneration) standart hale getirin.

Logout / Oturum Geçersizleştirme

Oturum Geçersizleştirme — düzeltme

- Logout’ta oturum token’ını **sunucu tarafında geçersiz kılın** (revocation/expiry); istemci-tarafı token silme tek başına yeterli değildir.

Forced Browsing / Fonksiyon-Seviye Yetki

Fonksiyon-Seviye Yetkilendirme — düzeltme

- Her yönetim/hassas uç noktasında **sunucu-taraflı rol/yetki kontrolü** uygulayın; yalnız UI’da gizlemek yeterli değildir.

Authenticated Enjeksiyon (SQLi/XSS)

Enjeksiyon (SQLi/XSS) — düzeltme

- **SQLi:** Tüm veritabanı sorgularını **parametreli sorgu / hazırlanmış ifade (prepared statement)** ile yazın; kullanıcı girdisini asla string olarak sorguya eklemeyin. ORM kullanıyorsanız ham SQL birleştirmeden kaçının. Veritabanı hata mesajlarını son kullanıcıya göstermeyin.
- **XSS:** Kullanıcı girdisini HTML'e basarken **bağlama uygun çıktı kodlaması** (HTML entity encoding) uygulayın; mümkünse otomatik kaçış yapan şablon motoru kullanın. `Content-Security-Policy` başlığı ile satır-içi script'leri kısıtlayın.
- Giderdikten sonra aynı giriş noktalarını yeniden test edin.

Authenticated IDOR (kendi kaynakları)

Yetkisiz Erişim (IDOR) — düzeltme

- **Nesne-düzeyi yetkilendirme:** Her kaynak erişiminde, isteyen kullanıcının o nesneye erişim hakkı olup olmadığını sunucu tarafında doğrulayın (sadece ID'nin geçerli olması yeterli değildir).
- **Tahmin edilemez tanımlayıcılar:** Sıralı sayısal ID yerine UUID/rastgele tanımlayıcı kullanın; numaralandırmayı zorlaştırın.
- Herkese açık olmaması gereken kaynakları kimlik doğrulama arkasına alın.

Yetki Yükseltme (Privilege Escalation)

Yetki Yükseltme / Mass-Assignment — proaktif sertleştirme

- Mass-assignment koruması (alan allowlist) uygulayın; rol/yetki alanlarını istemciden kabul etmeyin (proaktif).

Çok-Adımlı İş Mantığı

Çok-Adımlı İş Mantığı — proaktif sertleştirme

- Kritik değerleri sunucuda doğrulayın; adım sırası + kupon tekrar-kullanım kontrolü uygulayın (proaktif).

JWT / Token Güvenliği

JWT / Token Güvenliği — proaktif sertleştirme

- İmza algoritmasını sabitleyin, güçlü sır kullanın, `exp` ekleyin ve hassas claim taşımayın (proaktif).

Giriş Baypası (SQLi Göstergesi)

Giriş Baypası / SQL Enjeksiyonu — düzeltme

- Kimlik doğrulama sorgularında **parametreli sorgu / hazırlanmış ifade (prepared statement)** kullanın; kullanıcı girdisini asla SQL'e doğrudan koymayın.
- Girdi doğrulama + ORM güvenli API'leri; hatalı girişte tek-tip hata mesajı döndürün.

Client-Side / JS Analizi

Client-Side / JS Güvenliği — proaktif sertleştirme

- İstemci JS'inde sır bulundurmayın; source-map'leri üretimde yayımlamayın; kütüphaneleri güncel tutup bağımlılık taraması uygulayın (proaktif).

Client-Side Statik Analiz

Client-Side Statik Güvenlik — düzeltme

- DOM-XSS: kullanıcı-kontrollü veriyi innerHTML/eval/document.write yerine textContent + güvenli API ile işleyin; gerekiyorsa DOMPurify ile sanitize edin.
- postMessage: her `message` handler'ında `event.origin`'i allowlist ile doğrulayın.
- Storage: oturum token'ını localStorage yerine **HttpOnly + Secure çerezde** tutun.

- SRI: harici script/style'lara `integrity` + `crossorigin` ekleyin. Tabnabbing: `target="_blank"` linklere `rel="noopener noreferrer"`.
- Open redirect: yönlendirme hedeflerini sunucuda **allowlist** ile sınırlayın; harici mutlak URL'lere yönlendirmeyin.

Kimlik-Doğrulama Derinliği

Kimlik-Doğrulama Sertleştirme — düzeltme

- Enumerasyon: login/reset/register'da **tek-tip** yanıt/mesaj/süre döndürün (kullanıcı var/yok sızdırmayın).
- Varsayılan kimlik: tüm varsayılan hesapları kaldırın/parolalarını zorunlu değiştirin.
- Lockout: art arda hatalı denemede **hesap+IP bazlı hız-sınırı / geçici kilit** uygulayın; CAPTCHA ekleyin.
- Parola sıfırlama: **token-tabanlı** (tek-kullanımlık, kısa ömür), güvenlik-sorusundan kaçının; Host header'ı reset linkinde kullanmayın.
- Parola politikası: sunucuda **min 8+ / karmaşıklık**; şifresiz kanal: login'i **yalnız HTTPS**'te yapın; hassas sayfalara `Cache-Control: no-store`; **MFA** sunun.

Oturum Güvenliği Derinliği

Oturum Güvenliği Sertleştirme — proaktif sertleştirme

- Oturum çerezine SameSite + __Host- prefix, 128-bit rastgele session-id, URL'de oturum taşımama, anti-CSRF token, makul timeout (proaktif).

Girdi & Header Derinliği

Girdi & Header Sertleştirme — proaktif sertleştirme

- Host allowlist, TRACE kapalı, tüm kaynaklar HTTPS, kalıcı girdilerde çıktı-kodlama/sanitizasyon, parametre tekilleştirme (proaktif).

Yapılandırma & İfşa Derinliği

Yapılandırma & İfşa Sertleştirme — proaktif sertleştirme

- Yedek/.git/.env dizin dışında, admin arayüzü kimlik/ağ arkasında, bucket private/list-kapalı, cache Vary doğru, üretimde yorum/metadata temiz (proaktif).

API Güvenliği Derinliği (OWASP API Top 10)

API Güvenliği Sertleştirme — düzeltme

- BOLA/BFLA: her API isteğinde nesne-sahipliği + fonksiyon-rol kontrolünü sunucuda zorunlu kılın (ID geçerliliği yetmez).
- Aşırı veri: yanıtları **alan-allowlist (DTO)** ile sınırlayın; parola-hash/sır/iç-ID/rol'ü istemciye göndermeyin.
- Rate-limit: hesap+IP+endpoint bazlı **rate-limit + kota**; ağır uçlara maliyet-tabanlı sınır.
- Sürüm: kullanılmayan/eski API sürümlerini kapatın. GraphQL: üretimde **introspection'ı kapatın**; sorgu derinliği/karmaşıklık limiti ekleyin.

E-posta & DNS Derinliği (Anti-Spoofing)

E-posta & DNS Sertleştirme — düzeltme

- DMARC: `p=none` → `quarantine` → `reject` (pct=100) kademeli sıkılaştırın; `rua=` ile raporlamayı açın; alt-alanlar için `sp=reject`.
- SPF: `-all` (hardfail) kullanın; `+all` / `?all`'dan kaçının; DNS-arama sayısını ≤10 tutun (PermError).
- DKIM: 2048-bit anahtar, iptal edilen seçicileri kaldırın. MTA-STS: `mode=enforce`. TLS-RPT ekleyin.
- DNSSEC'i etkinleştirin (DS+RRSIG). CAA ile yetkili CA'ları kısıtlayın.

Taşıma Katmanı, CORS & Güvenlik Başlığı Derinliği

Taşıma Katmanı & Başlık Sertleştirme — düzeltme

- CORS: origin'i allowlist'leyin; `credentials` ile wildcard/yansıtma kullanmayın; `null` origin kabul etmeyin.
- TLS: yalnız TLS 1.2/1.3 bırakın; RC4/3DES/NULL/EXPORT cipher'ları kapatın; modern AEAD (ECDHE+AES-GCM/CHACHA20).
- HSTS `max-age≥15768000; includeSubDomains; preload`; clickjacking için X-Frame-Options **ve/veya** CSP frame-ancestors.
- CSP'den unsafe-inline/unsafe-eval kaldırın (nonce/hash); Referrer-Policy/Permissions-Policy/X-Content-Type-Options ekleyin.

Subdomain Takeover (Dangling DNS)

Subdomain Takeover — proaktif sertleştirme

- Alt-alan CNAME envanteri temiz; boşta/dangling kayıt yok (proaktif).

5. Ek — Sözlük

SQL Injection	Kullanıcı girdisinin veritabanı sorgusuna karışabildiği bir enjeksiyon zafiyeti.
XSS	Cross-Site Scripting — sayfaya kötü amaçlı betik enjekte edilebilmesi.
IDOR	Yetkisiz Nesne Erişimi — kimlik parametresiyle başka kaydın erişilebilmesi.
CSRF	Cross-Site Request Forgery — kullanıcının istemsiz işlem yapmasını sağlama.
OWASP	Açık web uygulama güvenliği topluluğu; Top 10 ve test kılavuzlarıyla bilinir.
TLS	Taşıma katmanı şifrelemesi (HTTPS'in temeli).
HSTS	Tarayıcıyı yalnız HTTPS kullanmaya zorlayan güvenlik başlığı.
CSP	İçerik Güvenlik Politikası — XSS/enjeksiyon azaltma başlığı.
CORS	Kaynaklar-arası paylaşım politikası; gevşek yapılandırma risklidir.
JWT	JSON Web Token — oturum/yetki taşıyan imzalı belirteç.
Clickjacking	Sayfanın görünmez iframe içine alınıp kullanıcı tıklamalarının kandırılması.
Forced Browsing	Menüde olmayan (ör. yönetici) uç noktalara URL bilerek erişme.