CyberTestify

Otomatik Güvenlik Tarama Raporu

ornek.com · Aktif Doğrulama Paketi

CyberTestify Güvenlik Taraması — Tamamlandı

Rapor No: **CT-ÖRNEK-715E**

Doğrulama Kodu: **4B2E-B284**

Bu rapor resmi sızma testi / sertifikasyon değildir.

İçindekiler

HEDEF
ornek.com

PAKET
Aktif Doğrulama Paketi

RAPOR NO
CT-ÖRNEK-715E

1. Yönetici Özeti

GENEL DEĞERLENDİRME

Yüksek Risk

Çalıştırılan kontrollerde en yüksek risk Enjeksiyon (SQLi/XSS) Doğrulama alanında (aktif doğrulama ile enjeksiyon zafiyeti KANITLANDI.) tespit edildi; öncelikli olarak giderilmesi/doğrulanması önerilir. 8 benzersiz sayfa/uç nokta tarandı, 19 giriş noktasında toplam 149 istek gönderildi. SSRF/RCE zaman-tabanlı/dolaylıdır. Aşağıda her kontrol ayrı ayrı raporlanmıştır.

⚡ 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 **Enjeksiyon (SQLi/XSS) Doğrulama** alanında (aktif doğrulama ile enjeksiyon zafiyeti KANITLANDI.).
- **Kapsam dürüstlüğü:** Bu paket, kimlik doğrulaması **gerektirmeyen dış yüzeye** odaklanır — herkese açık uç noktalar (açık formlar/API'lar, arama, login/kayıt akışının kendisi). IDOR / İş Mantığı / Race-Mass-Assignment kontrolleri **yalnızca login-öncesi erişilebilir yüzeyde** (ör. genel API'lar, herkese açık id-tabanlı uç noktalar) çalışır; bu nedenle bu kategorilerde bazı hedeflerde **sınırlı veya "İncelenemedi"** sonuç normal ve beklenendir (siteye özgü yüzey azlığından; motor eksikliğinden değil). Login-**sonrası** oturum içi derin yetkilendirme/iş mantığı zafiyetleri kapsam dışıdır, **Tam Kapsamlı Pentest**'te ele alınır. Bu taramada en güçlü sonuç **Enjeksiyon (SQLi/XSS) Doğrulama** alanında tespit edilmiştir.
- **API saldırı yüzeyi: 1** API uç noktası keşfedildi ancak **kimlik doğrulama gerektiriyor** (401/403) — kimlik-doğrulamalı derin test bu paketin kapsamı dışında olduğundan probe edilmedi (Tam Kapsamlı Pentest önerilir).
- **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).

🗓 **Orta Vadeli / Süreç (manuel doğrulama veya kod/mimari):** Yetkisiz nesne erişimi (IDOR) göstergesi (/api/products/1); Yansıyan XSS göstergesi (GET /redirect?to).

2. Bulgular

2.1 Zafiyet Dağılımı

Kritik	Yüksek	Orta	Düşük

Bu taramada toplam **4** 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	Yetkisiz nesne erişimi (IDOR) göstergesi — /api/products/1	Açık	Orta
CT-4	Yansıyan XSS göstergesi — GET /redirect?to · güven: düşük (dolaylı gösterge)	Açık	Düşük

8 doğrulama kategorisi çalıştırıldı — 2 temiz, 3 kategoride bulgu var, 3 incelenemedi

✓ DENENDİ — ZAFİYET KANITI BULUNAMADI

- **SSRF Doğrulama** Temiz (2 giriş noktası denendi, kanıt bulunamadı)
- **RCE / Komut Enjeksiyonu Doğrulama** Temiz (4 giriş noktası denendi, kanıt bulunamadı)

⚠ BULGU VAR — AYRINTISI AŞAĞIDAKİ BÖLÜMLERDE

- **Enjeksiyon (SQLi/XSS) Doğrulama** Bulgu var (2 — zafiyet göstergesi; yukarıda)
- **Yetkisiz Erişim (IDOR) Doğrulama** Bulgu var (1 — sınırlı/dolaylı gösterge; yukarıda)
- **Giriş Baypası (SQLi Göstergesi)** Bulgu var (1 — zafiyet göstergesi; yukarıda)

⚠ İNCELENEMEDİ — "GÜVENLİ" ANLAMINA GELMEZ

- **Dosya Yükleme Doğrulama** İncelenemedi (test edilebilir giriş noktası bulunamadı — "temiz" DEĞİL)
- **İş Mantığı Doğrulama** İncelenemedi (test edilebilir giriş noktası bulunamadı — "temiz" DEĞİL)
- **Race / Mass-Assignment Doğrulama** İncelenemedi (test edilebilir giriş noktası bulunamadı — "temiz" DEĞİL)

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 · 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

[DÜŞÜK] CT-4 · 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

Pozitif Güvence

Şu kontroller çalıştırıldı ve belirgin bir zafiyet göstergesi bulunamadı: SSRF Doğrulama, RCE / Komut Enjeksiyonu Doğrulama, Dosya Yükleme Doğrulama, İş Mantığı Doğrulama, Race / Mass-Assignment Doğrulama. 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): Dosya Yükleme Doğrulama, İş Mantığı Doğrulama, Race / Mass-Assignment Doğrulama.

Değerlendirme Özeti

7 aktif güvenlik kontrol kategorisinin tamamı değerlendirildi. 8 benzersiz sayfa/uç nokta tarandı, **19** giriş noktası test edildi, toplam **149** istek gönderildi. **2** kontrolde yüksek/kritik seviyeli zafiyet göstergesi bulundu (aşağıda detaylı).

*Keşif yöntemi: Bu tarama, JavaScript ile render edilen (SPA) hedef tespit edildiği için sayfalar **headless tarayıcı ile render edilerek** gerçekleştirilmiştir.*

KONTROL ÖZETİ

Kontrol	Sonuç	Güven
Enjeksiyon (SQLi/XSS) Doğrulama	⚠ Zafiyet göstergesi	Yüksek
Yetkisiz Erişim (IDOR) Doğrulama	⚠ Sınırlı gösterge	Orta
SSRF Doğrulama	✓ Zafiyet kanıtı yok	Orta
Dosya Yükleme Doğrulama	Giriş noktası yok (Kapsam dışı)	Kapsam dışı
İş Mantığı Doğrulama	Giriş noktası yok (Kapsam dışı)	Kapsam dışı
Race / Mass-Assignment Doğrulama	Giriş noktası yok (Kapsam dışı)	Kapsam dışı
RCE / Komut Enjeksiyonu Doğrulama	✓ Zafiyet kanıtı yok	Orta
Giriş Baypası (SQLi Göstergesi)	⚠ Zafiyet göstergesi	Yüksek

Güven yalnızca gerçekten test çalıştırılan (giriş noktası bulunan) kontroller için gösterilir; giriş noktası bulunamayan kontroller **Kapsam dışı**dır. Test edilenlerde: SSRF/RCE dolaylı (zaman-tabanlı, OOB yok) → Orta; gözlemsel (Dosya Yükleme/İş Mantığı/Race) → Düşük; Enjeksiyon hata/yansıma-tabanlı → Yüksek.

POZİTİF GÜVENCE — DENENEN AKTİF DOĞRULAMA YÖNTEMLERİ

Bulgu çıkmayan kontroller de dâhil, 8 aktif kontrol kategorisinin her biri keşfedilen yüzeyde gerçekten çalıştırıldı (toplam **149** istek, **8** benzersiz sayfa). Aşağıdaki tablo, "bulgu yok" sonuçlarını da — kaç giriş noktası denendi, kaçında kanıt bulunamadı — şeffaf gösterir:

Kontrol	Denenen giriş noktası	Gönderilen istek	Sonuç
Enjeksiyon (SQLi/XSS) Doğrulama	10	121	**⚠ Bulgu var (2 — zafiyet göstergesi; yukarıda)**
Yetkisiz Erişim (IDOR) Doğrulama	2	6	**⚠ Bulgu var (1 — sınırlı/dolaylı gösterge; yukarıda)**
SSRF Doğrulama	2	3	**✓ Temiz (2 giriş noktası denendi, kanıt bulunamadı)**

Kontrol	Denenen giriş noktası	Gönderilen istek	Sonuç
Dosya Yükleme Doğrulama	0	1	⚠ **İncelenemedi (test edilebilir giriş noktası bulunamadı — "temiz" DEĞİL)**
İş Mantığı Doğrulama	0	1	⚠ **İncelenemedi (test edilebilir giriş noktası bulunamadı — "temiz" DEĞİL)**
Race / Mass-Assignment Doğrulama	0	1	⚠ **İncelenemedi (test edilebilir giriş noktası bulunamadı — "temiz" DEĞİL)**
RCE / Komut Enjeksiyonu Doğrulama	4	13	✅ **Temiz (4 giriş noktası denendi, kanıt bulunamadı)**
Giriş Baypası (SQLi Göstergesi)	1	3	⚠ **Bulgu var (1 — zafiyet göstergesi; yukarıda)**

> **Üç-durum ayrımı (dürüstlük):** ✅ *Temiz* = kontrol çalıştı, kanıt bulunamadı · ⚠ *Bulgu var* = yukarıda detaylı · ⚠ *İncelenemedi* = test edilebilir giriş noktası bulunamadı (güvenli anlamına GELMEZ).

Bu paket NE değerlendirir, NE değerlendirmez

> **EDER ("kanıtla — istismar etme" ilkesiyle; zararsız, veri-değiştirmeyen problar):** SQLi/XSS enjeksiyonu, yetkisiz erişim (IDOR), SSRF, dosya yükleme, iş mantığı, race/mass-assignment ve RCE/komut enjeksiyonu göstergeleri — kimlik doğrulaması **gerektirmeyen** yüzeyde, keşfedilen 8 sayfada.

> **ETMEZ:** Veri değiştiren/silen istismar, ödeme tamamlama veya gerçek RCE çalıştırma **yapılmaz** (yalnızca gösterge/kanıt toplanır). IDOR / İş Mantığı / Race-Mass-Assignment kontrolleri **yalnızca login-öncesi erişilebilir yüzeyde** çalışır; **login-SONRASI** oturum içi derin yetkilendirme/yetki-yükseltme/iş-mantığı zafiyetleri bu paketin **dışındadır** — bunlar **Tam Kapsamlı Pentest** (kimlik-doğrulamalı, kapsam sözleşmeli) kapsamındadır. Bu nedenle bu üç kategoride bazı hedeflerde **sınırlı veya "İncelenemedi"** sonuç normal ve beklenendir (siteye özgü yüzey azlığından; motor eksikliğinden değil). Bir kontrolde "bulgu yok", aktif istismar bilinçli olarak sınırlı/pasif-güvenli tutulduğu için **güvenli olduğunu KANITLAMAZ**.

Enjeksiyon (SQLi/XSS) Doğrulama

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

> **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. Kimlik doğrulama gerektiren alanlar ve iç mantık bu paketin kapsamı dışındadır.

Yetkisiz Erişim (IDOR) Doğrulama

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 doğrulaması olmadan **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

KAPSAM SINIRI (ÖNEMLİ)

Bu paket **kimlik doğrulaması olmadan** çalışır. Bu nedenle yalnızca **herkese açık, numaralandırılabilir kaynaklara** yetkisiz erişimi tespit edebilir. Klasik IDOR (bir kullanıcının, oturum açmış başka bir kullanıcının verisine erişmesi) **iki farklı hesap/oturum** gerektirir ve bu paketin kapsamı dışındadır. Bu bölümde bulgu olmaması, kimlik doğrulamalı akışlarda IDOR olmadığını **kanıtlamaz** — bu, ayrı bir kimlik-doğrulamalı test gerektirir (**İnceleme gerekli / Kapsam Dışı**).

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

SSRF Doğrulama

NE KONTROL EDİLDİ

- Sunucu-taraflı fetch tetikleyebilecek parametreler (url/webhook/image/redirect vb.) tespit edildi.
- Bu parametrelere, **kontrolümüzdeki** gecikmeli bir echo URL'i verildi; hedefin yanıt süresi baseline ile karşılaştırıldı (sunucu bu URL'i çekerse yanıt gecikir).
- İç ağ / bulut-metadata / localhost (169.254.169.254, RFC1918, 127.0.0.1 vb.) **asla** hedeflenmedi (koda gömülü hard-guard).

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

> OOB doğrulama altyapısı kullanılmadığı için bu tespit **zaman-tabanlı, dolaylı ve orta güvenilirliktedir**; kesin doğrulama için ek/manuel test önerilir.

RCE / Komut Enjeksiyonu Doğrulama

NE KONTROL EDİLDİ

- Komuta ulaşabilecek giriş parametreleri tespit edildi.
- Yalnızca **zararsız, zaman-tabanlı** gecikme payload'ları (sleep) gönderildi; yanıt süresi baseline ile karşılaştırıldı (blind kanıt).
- Gerçek komut çalıştırma (dosya okuma/yazma, ağ bağlantısı, reverse shell) **asla** denenmedi (koda gömülü hard-guard: yalnız sabit sleep payload listesi).

BULGULAR

Gönderilen zararsız problara karşı belirgin bir zafiyet göstergesi bulunamadı.

> OOB/canary altyapısı kullanılmadığı için bu tespit **zaman-tabanlı, dolaylı ve orta güvenilirliktedir** (ağ gecikmesi yanıltabilir); kesin doğrulama için manuel test önerilir.

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 bir akıştır; bu, TEK ve zararsız bir 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.

Metodoloji

Aşama	Açıklama
Keşif	Hedefin dış yüzeyi, sayfaları ve (SPA ise) JS bundle'ından gerçek uç/parametreler çıkarılır.

Aşama	Açıklama
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 aktif doğrulama kontrollerinde tespit edilen bulgular için düzeltme önerileri içerir.

Enjeksiyon (SQLi/XSS) Doğrulama

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.

Yetkisiz Erişim (IDOR) Doğrulama

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.

SSRF Doğrulama

SSRF — proaktif sertleştirme

- Kullanıcıdan URL alan tüm alanlarda sunucu-taraflı **allowlist** + iç ağ engellemesi uygulayın (proaktif).
- Dış fetch gerektiğinde şema/host doğrulaması + zaman aşımı + boyut limiti koyun.

Dosya Yükleme Doğrulama

Dosya Yükleme — proaktif sertleştirme

- Yükleme uç noktalarında sunucu-taraflı tip/MIME doğrulaması + allowlist + web-kökü dışı depolama uygulayın (proaktif).

İş Mantığı Doğrulama

İş Mantığı — proaktif sertleştirme

- Kritik değerleri (fiyat/miktar) sunucu tarafında doğrulayın; çok adımlı akışlarda adım sırası kontrolü uygulayın (proaktif).

Race / Mass-Assignment Doğrulama

Race / Mass-Assignment — proaktif sertleştirme

- Model bağlamada alan allowlist'i (mass-assignment koruması) uygulayın; kritik işlemlerde atomik/idempotent tasarım kullanın (proaktif).

RCE / Komut Enjeksiyonu Doğrulama

RCE / Komut Enjeksiyonu — proaktif sertleştirme

- Sistem komutu çağıran kod yollarını gözden geçirin; girdiyi allowlist ile doğrulayın, shell string birleştirmeden kaçının (proaktif).
- En düşük yetki + giden ağ kısıtı uygulayın.

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.

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.
SSRF	Server-Side Request Forgery — sunucuyu istenmeyen isteklere zorlama.