CyberTestify

Otomatik Güvenlik Tarama Raporu

rest.vulnweb.com · Dış Yüzey & Yapılandırma Paketi

CyberTestify Güvenlik Taraması — Tamamlandı

Rapor No: **CT-ÖRNEK-7CE5**

Doğrulama Kodu: **73DD-A368**

Bu rapor resmi sızma testi / sertifikasyon değildir.

İçindekiler

1. Yönetici Özeti

2. Bulgular

- 2.1 Zafiyet Dağılımı
- 2.2 Master Bulgu Tablosu
- 2.3 Detaylı Bulgular

3. Kontrol Özeti ve Metodoloji

4. AI Çözüm Önerileri

5. Ek — Sözlük

HEDEF
rest.vulnweb.com

PAKET
Dış Yüzey & Yapılandırma Paketi

RAPOR NO
CT-ÖRNEK-7CE5

1. Yönetici Özeti

GENEL DEĞERLENDİRME

Yüksek Risk

Bu hedef HTTPS üzerinden yanıt vermiyor; iletişim şifresiz (düz metin) taşınıyor — öncelikli olarak geçerli bir TLS sertifikasıyla HTTPS'e geçilmelidir. Diğer alanlar http:// üzerinden incelenmiştir. En yüksek risk SSL/TLS Yapılandırma Denetimi alanında (sertifika ve/veya protokol düzeyinde acil ele alınması gereken bir sorun tespit edildi.) tespit edildi; öncelikli olarak giderilmesi önerilir. Aşağıda her alan ayrı ayrı raporlanmıştır.

⚡ Yönetim Kararı

Öncelikli ele alınması gereken **3** yüksek/kritik seviyeli gösterge tespit edildi; bunlar için acil bir düzeltme planı önerilir. Orta/düşük göstergeler planlı iyileştirmeyle giderilebilir.

- **Genel risk seviyesi: Yüksek** — 5 alan incelendi; en yüksek risk **SSL/TLS Yapılandırma Denetimi** alanında (sertifika ve/veya protokol düzeyinde acil ele alınması gereken bir sorun tespit edildi.).
- ⚠ **HTTPS desteklenmiyor:** Hedef HTTPS (443) üzerinden yanıt vermedi; iletişim şifresiz (düz metin) taşınıyor. Tarama http:// üzerinden yürütüldü. Bu başlı başına ciddi bir bulgudur (aşağıda).
- **Önerilen ilk adım:** En yüksek riskli alandan başlayın; her bulgu için adım adım hazır komutlar "AI Çözüm Önerileri" bölümünde sunulur.

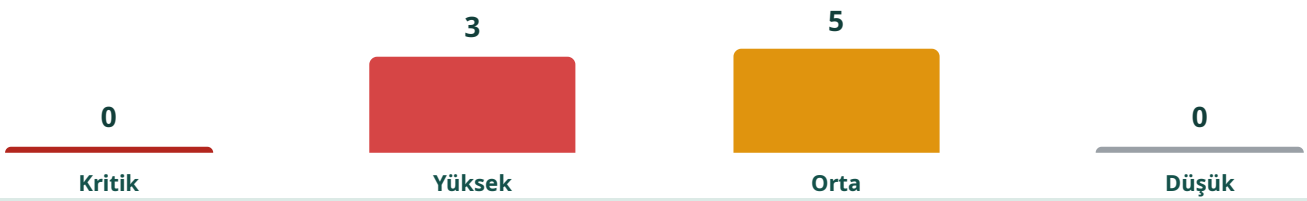
İyileştirme Öncelikleri

⚡ **En Acil / Öncelikli:** HTTPS desteklenmiyor (şifresiz iletişim); Güncel olmayan bileşen (CVE).

🛠 **Hızlı Kazanım (sunucu yapılandırması, ~1-2 gün):** Açıkta hassas dosya — /db.sql; HSTS (Strict-Transport-Security) eksik; Content-Security-Policy eksik; X-Frame-Options eksik (clickjacking); X-Content-Type-Options eksik (MIME-sniffing); DMARC politikası yetersiz (eksik veya zayıf).

2. Bulgular

2.1 Zafiyet Dağılımı



Bu taramada toplam **8** bulgu göstergesi tespit edildi; şiddet dağılımı aşağıdadır.

2.2 Master Bulgu Tablosu

ID	Başlık	Durum	Şiddet
CT-1	HTTPS desteklenmiyor (şifresiz iletişim)	Açık	Yüksek
CT-2	Açıkta hassas dosya — /db.sql	Açık	Yüksek
CT-3	Güncel olmayan bileşen (CVE)	Açık	Yüksek
CT-4	HSTS (Strict-Transport-Security) eksik	Açık	Orta
CT-5	Content-Security-Policy eksik	Açık	Orta
CT-6	X-Frame-Options eksik (clickjacking)	Açık	Orta
CT-7	X-Content-Type-Options eksik (MIME-sniffing)	Açık	Orta
CT-8	DMARC politikası yetersiz (eksik veya zayıf)	Açık	Orta

8 kontrol alanı çalıştırıldı — 4 alanda sorun bulunmadı, 4 alanda bulgu var

✓ KONTROL EDİLDİ — SORUN BULUNMADI

- **CORS & Çerez Güvenliği** Sorun bulunmadı
- **Dizin listeleme (autoindex / "Index of /") · CWE-548** 6 dizin denendi, listeleme yok
- **Ayrıntılı hata / sunucu-yol ifşası · CWE-209** Gösterge bulunamadı
- **Parola alanı autocomplete politikası · CWE-522** Uygun / parola alanı gözlenmedi

⚠ BULGU VAR — AYRINTISI AŞAĞIDAKİ BÖLÜMLERDE

- **SSL/TLS Yapılandırma Denetimi** Bulgu var (Yüksek — yukarıda ayrıntılı)
- **Güvenlik Başlıkları & Bilgi Sızıntısı** Bulgu var (Yüksek — yukarıda ayrıntılı)
- **DNS & E-posta Güvenliği** Bulgu var (Orta — yukarıda ayrıntılı)
- **CSP (İçerik Güvenlik Politikası) Analizi** Bulgu var (Orta — yukarıda ayrıntılı)

2.3 Detaylı Bulgular

[YÜKSEK] CT-1 · HTTPS desteklenmiyor (şifresiz iletişim)

Durum: Açık

Açıklama: Site HTTPS üzerinden yanıt vermiyor; iletişim şifresiz (düz metin) HTTP ile yürüyor.

Nasıl Tespit Edildi: Site HTTPS'e yanıt vermiyor; tüm trafik şifresiz (düz metin) taşınıyor — dinlenebilir/değiştirilebilir, oturum/şifre çalınabilir. Çözüm: geçerli TLS sertifikası + HTTP→HTTPS yönlendirme + HSTS.

İş Etkisi: Site HTTPS üzerinden yanıt vermiyor; sayfaya gelen/giden tüm trafik ŞİFRESİZ (düz metin) taşınıyor. Aynı ağdaki bir saldırgan trafiği dinleyebilir, oturum/şifre çalabilir veya içeriği değiştirebilir; modern tarayıcılar sayfayı "Güvenli değil" olarak işaretler.

ÖNERİLEN DÜZELTME

Geçerli bir TLS sertifikası kurun (ücretsiz: Let's Encrypt), tüm HTTP isteklerini kalıcı olarak (301) HTTPS'e yönlendirin ve HSTS başlığını ekleyin.

Referans: CWE-319 · OWASP A02:2021 Cryptographic Failures

[YÜKSEK] CT-2 · Açıkta hassas dosya — /db.sql

Durum: Açık

Açıklama: Hassas dosya (.git/.env/yedek) dışarıya açık.

Nasıl Tespit Edildi: İçerik doğrulandı; yapılandırma/kaynak sızıntısı riski. Erişim derhal engellenmeli.

İş Etkisi: Kaynak kodu, yedek veya gizli anahtar gibi hassas dosyalar dışa açık; kimlik bilgisi/sistem sırrı sızıntısı riski.

ÖNERİLEN DÜZELTME

Bu yolları engelleyin; kaynak/yedek/sır dosyalarını web-kökünden çıkarın.

Referans: CWE-538 · OWASP A05:2021 Security Misconfiguration

[YÜKSEK] CT-3 · Güncel olmayan bileşen (CVE)

Durum: Açık

Açıklama: Güncel olmayan bir bileşen/CMS parmak izi ve olası bilinen CVE.

Nasıl Tespit Edildi: PHP 7.x serisi resmen desteklenmiyor (7.x güvenlik güncellemeleri 2022 sonunda bitti). Bilinen çok sayıda güvenlik açığı yamasız kalır. CWE-1104 · OWASP A06:2021 (Güncel Olmayan/Savunmasız Bileşenler). Çözüm: güncel ve desteklenen bir PHP sürümüne (8.2+) yükseltin; sürüm imzasını gizleyin (expose_php=Off).

İş Etkisi: Güncel olmayan bileşen bilinen CVE'lerle istismara açıktır; hedefli saldırı riski.

ÖNERİLEN DÜZELTME

Bileşen/eklenti/tema sürümlerini güncel tutun; otomatik güncelleme + bağımlılık taraması kurun.

Referans: CWE-1104 · OWASP A06:2021 Vulnerable & Outdated Components

[ORTA] CT-4 · HSTS (Strict-Transport-Security) eksik

Durum: Açık

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

Nasıl Tespit Edildi: HTTPS zorunluluğu tarayıcıya bildirilmiyor; downgrade saldırılarına açık.

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

[ORTA] CT-5 · Content-Security-Policy eksik

Durum: Açık

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

Nasıl Tespit Edildi: Tarayıcı hangi kaynakların yükleneceğini kısıtlayamıyor; XSS ve içerik enjeksiyonuna karşı temel savunma yok. Taranan 2 benzersiz sayfanın TAMAMINDA eksik.

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

[ORTA] CT-6 · X-Frame-Options eksik (clickjacking)

Durum: Açık

Açıklama: Sayfa, X-Frame-Options / CSP frame-ancestors olmadığından başka bir sitenin iframe'ine gömülebilir.

Nasıl Tespit Edildi: Sayfa başka bir sitenin iframe'ine gömülebilir; clickjacking ile kullanıcı kandırılabilir. Taranan 2 benzersiz sayfanın TAMAMINDA eksik.

İş Etkisi: Sayfa görünmez bir çerçeveye alınıp kullanıcılar istemeden işlem yapmaya kandırılabilir (clickjacking); hesap ve işlem güvenliğini zayıflatır.

ÖNERİLEN DÜZELTME

`X-Frame-Options: SAMEORIGIN` ekleyin veya CSP'ye `frame-ancestors 'self'` koyun.

Referans: CWE-1021 · OWASP A05:2021 Security Misconfiguration

[ORTA] CT-7 · X-Content-Type-Options eksik (MIME-sniffing)

Durum: Açık

Açıklama: X-Content-Type-Options yok; tarayıcı içerik türünü tahmin edebilir (MIME-sniffing).

Nasıl Tespit Edildi: Savunma derinliği zayıf. (2/2 sayfada eksik)

İş Etkisi: Tarayıcı içerik türünü tahmin edip zararlı içeriği çalıştırabilir; XSS/enjeksiyon saldırı yüzeyini genişletir.

ÖNERİLEN DÜZELTME

`X-Content-Type-Options: nosniff` başlığını ekleyin.

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

[ORTA] CT-8 · DMARC politikası yetersiz (eksik veya zayıf)

Durum: Açık

Açıklama: DMARC kaydı yok; SPF/DKIM uygulanmıyor.

Nasıl Tespit Edildi: SPF/DKIM sonuçları uygulanmıyor.

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

3. Kontrol Özeti ve Metodoloji

TESPİT EDİLEN RİSKLER

Bulgu	Şiddet	Açıklama
HTTPS desteklenmiyor (şifresiz iletişim)	Yüksek	Site HTTPS'e yanıt vermiyor; tüm trafik şifresiz (düz metin) taşınıyor — dinlenebilir/değiştirilebilir, oturum/şifre çalınabilir. Çözüm: geçerli TLS sertifikası + HTTP→HTTPS yönlendirme + HSTS.

SSL/TLS Yapılandırma Denetimi

TLS SERTİFİKA DURUMU

⚠ Bu hedef **HTTPS (443) üzerinden yanıt vermedi**; geçerli bir TLS sertifikası bulunamadı. Site yalnızca **şifresiz HTTP** üzerinden yayında.

TLS PROTOKOL & CIPHER

- **Aktif protokol:** tespit edilemedi
- **Cipher:** tespit edilemedi
- **Eski/zayıf sürüm desteği:** Gözlemlenmedi (yalnızca TLS 1.2+ görüldü)

HSTS (HTTP Strict Transport Security)

- **Durum:** Yok — Tarayıcıya HTTPS zorunluluğu bildirilmiyor; ilk isteklerde SSL-stripping/downgrade saldırısı riski var.

TESPİT EDİLEN RİSKLER

Bulgu	Şiddet	Açıklama
HTTPS desteklenmiyor (şifresiz iletişim)	Yüksek	Site HTTPS'e yanıt vermiyor; tüm trafik şifresiz (düz metin) taşınıyor. Aynı ağdaki bir saldırgan dinleyebilir, oturum/şifre çalabilir veya içeriği değiştirebilir. Çözüm: geçerli TLS sertifikası + HTTP→HTTPS yönlendirme + HSTS.
HSTS eksik	Orta	HTTPS zorunluluğu tarayıcıya bildirilmiyor; downgrade saldırılarına açık.

Güvenlik Başlıkları & Bilgi Sızıntısı

HTTP GÜVENLİK BAŞLIKLARI

Başlık	Durum	Açıklama
Strict-Transport-Security	Yok	HTTPS zorunluluğu bildirilmiyor; SSL-stripping riski.
Content-Security-Policy	Yok	XSS/enjeksiyona karşı tarayıcı savunması yok.
X-Frame-Options	Yok	Clickjacking'e açık; iframe'e gömülebilir.
X-Content-Type-Options	Yok	MIME-sniffing mümkün.
Referrer-Policy	Yok	Referrer bilgisi dış kaynaklara sızabilir.
Permissions-Policy	Yok	Hassas tarayıcı API'leri kısıtlanmamış.
X-XSS-Protection	Yok	Eski tarayıcı XSS filtresi ayarlı değil (modernlerde kritik değil).

BİLGİ SIZINTISI / AÇIKTA DOSYALAR

Yaygın hassas yollar tek GET ile kontrol edildi (içerik doğrulandı — yalnız HTTP 200 kanıt sayılmaz):

Yol	Durum	Not
`/.git/config`	Kapalı	HTTP 400 / boş gövde — erişilebilir değil
`/.env`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/.git/HEAD`	Kapalı	HTTP 400 / boş gövde — erişilebilir değil
`/backup.zip`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil

Yol	Durum	Not
`/.DS_Store`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/wp-config.php.bak`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/ftp`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/backup`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/backups`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/uploads`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/files`	Kapalı	HTTP 400 / boş gövde — erişilebilir değil
`/admin`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/.svn/entries`	Kapalı	HTTP 400 / boş gövde — erişilebilir değil
`/.htaccess`	Kapalı	HTTP 403 / boş gövde — erişilebilir değil
`/config.php.bak`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/db.sql`	⚠ AÇIK	beklenen dosya formatı doğrulandı (catch-all değil)
`/dump.sql`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/backup.tar.gz`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/backup.tar`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/www.zip`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/site.zip`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/backup.old`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/backup.backup`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/index.php.bak`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/index.php~`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/.env.bak`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/.env.old`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil
`/database.sql`	Kapalı	HTTP 404 / boş gövde — erişilebilir değil

EK BİLGİ-SIZINTISI GÖZLEMLERİ

Kontrol	Sonuç
Dizin listeleme (autoindex / “Index of /”) · CWE-548	✓ 6 dizin denendi, listeleme yok
Ayrıntılı hata / sunucu-yol ifşası · CWE-209	✓ Gösterge bulunamadı
Parola alanı autocomplete politikası · CWE-522	✓ Uygun / parola alanı gözlenmedi

> Hepsi GET-only/pasif gözlemdir — içerik ÇEKİLMEZ/gösterilmez; sızan yol REDAKTE edilir. “Gösterge bulunamadı” güvenli olduğunu KANITLAMAZ; yalnız denenen pasif yöntemlerle gösterge çıkmadığını gösterir.

TESPİT EDİLEN RİSKLER

Bulgu	Şiddet	Açıklama
Hassas dosya erişilebilir (`/db.sql`)	Yüksek	İçerik doğrulandı; yapılandırma/kaynak sızıntısı riski. Erişim derhal engellenmeli.
Eski/desteksiz yazılım sürümü ifşa ediliyor (PHP/7.1.26 — EOL)	Yüksek	PHP 7.x serisi resmen desteklenmiyor (7.x güvenlik güncellemeleri 2022 sonunda bitti). Bilinen çok sayıda güvenlik açığı yamasız kalır. CWE-1104 · OWASP A06:2021 (Güncel Olmayan/Savunmasız Bileşenler). Çözüm: güncel ve desteklenen bir PHP sürümüne (8.2+) yükseltin; sürüm imzasını gizleyin (expose_php=Off).
Güncel olmayan yazılım sürümü ifşa ediliyor (Apache/2.4.25 — çok eski yama)	Orta	Apache 2.4 serisi desteklenmekle birlikte Apache/2.4.25 çok eski bir yama düzeyidir; aradaki güvenlik yamaları uygulanmamış görünüyor. CWE-1104 · OWASP A06:2021 (Güncel Olmayan/Savunmasız Bileşenler). Çözüm: 2.4 serisinin güncel yamasına yükseltin; sürüm imzasını gizleyin (ServerTokens Prod).
Kritik güvenlik başlığı eksik: Content-Security-Policy	Orta	Tarayıcı hangi kaynakların yükleneceğini kısıtlayamıyor; XSS ve içerik enjeksiyonuna karşı temel savunma yok. Taranan 2 benzersiz sayfanın TAMAMINDA eksik.
Kritik güvenlik başlığı eksik: X-Frame-Options	Orta	Sayfa başka bir sitenin iframe’ine gömülebilir; clickjacking ile kullanıcı kandırılabilir. Taranan 2 benzersiz sayfanın TAMAMINDA eksik.
Ek başlıklar eksik (Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, X-XSS-Protection)	Orta	Savunma derinliği zayıf. (2/2 sayfada eksik)

DNS & E-posta Güvenliği

SPF (Gönderen Politikası) — kontrol edilen alan: `vulnweb.com`

- **Durum:** Var — `v=spf1 ~all`
- **Sertlik:** `~all` — yumuşak (softfail; kabul edilebilir, ideal değil).

DMARC (Kimlik Doğrulama Politikası) — kontrol edilen alan: `vulnweb.com`

- **Durum:** Yok — DMARC kaydı bulunamadı. SPF/DKIM sonuçlarına göre uygulama yapılmıyor; spoofing’e karşı koruma zayıf.

DKIM (İmza)

- **Durum:** Tespit edilemedi — Yaygın seçicilerde (default/google/selector1…) DKIM kaydı bulunamadı. Farklı bir seçici kullanıyor olabilirsiniz; bu kesin “yok” anlamına gelmez.

DNSSEC

- **Durum:** Pasif/yok — DNS yanıtları imzalı değil; DNS spoofing/cache-poisoning riskine daha açık.

TESPİT EDİLEN RİSKLER

Bulgu	Şiddet	Açıklama
DMARC eksik	Orta	SPF/DKIM sonuçları uygulanmıyor.
DKIM tespit edilemedi	Bilgilendirme	Yaygın seçicilerde bulunamadı (farklı seçici olabilir).
DNSSEC pasif	Bilgilendirme	DNS yanıtları imzalı değil.

CORS & Çerez Güvenliği

CORS YAPILANDIRMASI (2/2 sayfada test edildi)

- **Test Origin:** `https://cybertestify-cors-probe.example` — her sayfaya zararsız bir Origin başlığı gönderilip yanıt değerlendirildi.
- **En açık gözlemlenen politika** (`/`): Access-Control-Allow-Origin: gönderilmiyor (kapalı — güvenli varsayılan); Allow-Credentials: gönderilmiyor.

ÇEREZ BAYRAKLARI (2 sayfada gözlemlenen tüm çerezler)

- Taranan 2 sayfanın hiçbirinde Set-Cookie gözlemlenmedi.

TESPİT EDİLEN RİSKLER

- CORS ve çerez yapılandırmasında belirgin bir risk öne çıkmadı.

CSP (İçerik Güvenlik Politikası) Analizi

CSP DURUMU

- **Durum:** Yok — Content-Security-Policy başlığı hiç gönderilmiyor.

CSP DİREKTİF ANALİZİ

- Uygulanan bir CSP olmadığından direktif analizi yapılamadı.

TESPİT EDİLEN RİSKLER

Bulgu	Şiddet	Açıklama
CSP tamamen eksik	Orta	XSS ve içerik enjeksiyonuna karşı tarayıcı seviyesinde savunma yok. Taranan 2 sayfanın TAMAMINDA CSP başlığı yok.

POZİTİF GÜVENCE — KONTROL EDİLEN ALANLAR

Bulgu çıkmayan alanlar da dâhil, dış-yüzey kontrolleri ana sayfa dâhil **2 benzersiz sayfada** gerçekten çalıştırıldı. Aşağıdaki tablo, "sorun bulunamadı" sonuçlarını da şeffaf biçimde gösterir:

Kontrol Alanı	Sonuç
SSL/TLS Yapılandırma Denetimi	⚠ **Bulgu var (Yüksek — yukarıda ayrıntılı)**
Güvenlik Başlıkları & Bilgi Sızıntısı	⚠ **Bulgu var (Yüksek — yukarıda ayrıntılı)**
DNS & E-posta Güvenliği	⚠ **Bulgu var (Orta — yukarıda ayrıntılı)**
CORS & Çerez Güvenliği	✓ **Sorun bulunmadı**

Kontrol Alanı	Sonuç
CSP (İçerik Güvenlik Politikası) Analizi	⚠ **Bulgu var (Orta — yukarıda ayrıntılı)**
Dizin listeleme (autoindex / "Index of /") · CWE-548	✓ **6 dizin denendi, listeleme yok**
Ayrıntılı hata / sunucu-yol ifşası · CWE-209	✓ **Gösterge bulunamadı**
Parola alanı autocomplete politikası · CWE-522	✓ **Uygun / parola alanı gözlenmedi**

Üç-durum ayrımı (dürüstlük): ✓ *Sorun bulunmadı* = kontrol çalıştı, temiz çıktı · ⚠ *Bulgu var* = yukarıda detaylı · ⚠ *İncelenemedi* = veri toplanamadı (güvenli anlamına GELMEZ).

Bu paket NE kontrol EDER, NE ETMEZ

EDER (pasif — yalnız GET ile sayfa çekme + zararsız Origin/DNS sorgusu): TLS/sertifika, HTTP güvenlik başlıkları, CORS politikası, çerez bayrakları (Secure/HttpOnly/SameSite), Content-Security-Policy, DNS/e-posta kayıtları (SPF/DKIM/DMARC/DNSSEC), açıkta hassas dosya (yaygın yedek kalıpları dâhil), dizin listeleme (autoindex), ayrıntılı-hata/sunucu-yol ifşası (redakte), parola alanı autocomplete politikası, eski/desteksiz yazılım sürümü — keşfedilen 2 sayfada.

ETMEZ: Aktif zafiyet doğrulaması (SQLi/XSS/IDOR gibi payload/prob denemesi), kimlik-doğrulamalı akış testi, iş-mantığı istismarı. Bunlar **Aktif Doğrulama** ve **Tam Kapsamlı Pentest** paketlerinin kapsamındadır. Bu rapor pasif gözleme dayanır; bir alanda "bulgu yok" ifadesi, aktif istismar denenmediği için **güvenli olduğunu KANITLAMAZ** — yalnız dışarıdan gözlemlenen yapılandırmanın temiz olduğunu gösterir.

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, dış yüzey taramanızda tespit edilen tüm eksiklikler için alan alan düzeltme önerileri içerir. Sunucunuza uygun örnekleri (Nginx/Firebase/Apache/DNS) kopyalayın.

SSL/TLS Yapılandırma Denetimi

Aşağıdaki öneriler rest.vulnweb.com için TLS/şifreleme yapılandırmasını güçlendirir.

1. HSTS başlığını ekleyin

Tarayıcıya siteye yalnızca HTTPS ile bağlanmasını söyler (yalnızca siteniz tamamen HTTPS ise uygulayın):

Nginx:

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
```

Firebase Hosting — `firebase.json`:

```
{
  "hosting": {
    "headers": [
      {
        "source": "**",
        "headers": [
          { "key": "Strict-Transport-Security", "value": "max-age=31536000; includeSubDomains" }
        ]
      }
    ]
  }
}
```

Apache — `.htaccess`:

```
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

Güvenlik Başlıkları & Bilgi Sızıntısı

Aşağıdaki öneriler, rest.vulnweb.com ana sayfasında tespit edilen eksik güvenlik başlıklarını gidermeye yöneliktir. Her başlık için önce kısa açıklama, ardından Nginx örneği verilmiştir; en sonda Nginx dışı platformlar (Firebase, Vercel, Next.js, Apache) için hazır bloklar bulabilirsiniz. Kendi sunucunuza uygun olanı kopyalayın.

1. Content-Security-Policy (CSP) ekleyin

XSS ve içerik enjeksiyonuna karşı en etkili tarayıcı savunmasıdır. Sitenize uygun temel bir politikayla başlayıp zamanla sıkılaştırın:

```
add_header Content-Security-Policy "default-src 'self'; img-src 'self' data:; script-src 'self'; style-src '
```

Üçüncü taraf script kullanıyorsanız (GTM, Analytics, Pixel) ilgili alan adlarını `script-src` / `connect-src` e ekleyin.

2. X-Frame-Options ekleyin

Sayfanızın başka bir sitenin iframe'ine gömülüp clickjacking'e maruz kalmasını engeller:

```
add_header X-Frame-Options "SAMEORIGIN" always;
```

Modern alternatif olarak CSP `frame-ancestors 'self'` de aynı korumayı sağlar.

3. X-Content-Type-Options ekleyin

Tarayıcının MIME-type sniffing yapıp içeriği yanlış yorumlamasını (ve bunun açtığı XSS riskini) engeller:

```
add_header X-Content-Type-Options "nosniff" always;
```

4. Strict-Transport-Security (HSTS) ekleyin

HTTPS'i zorunlu kılar ve SSL-stripping/MITM saldırılarını zorlaştırır. (Yalnızca siteniz tamamen HTTPS ise uygulayın.)

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
```

5. Referrer-Policy ekleyin

Dış bağlantılara giden `Referer` başlığındaki bilgi sızıntısını azaltır:

```
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
```

6. Permissions-Policy ekleyin

Tarayıcı API'lerini (kamera, mikrofon, konum vb.) kısıtlar; üçüncü taraf iframe'lerin istenmeyen erişimini engeller:

```
add_header Permissions-Policy "geolocation=(), microphone=(), camera=()" always;
```

7. X-XSS-Protection (savunma derinliği)

Eski tarayıcılar için tarihi bir başlıktır; asıl koruma CSP'dedir. İsteğe bağlı olarak ekleyebilirsiniz:

```
add_header X-XSS-Protection "1; mode=block" always;
```

Tümünü birleştiren yapılandırma — Nginx

Sunucu bloğunuza (server { ... }) ekleyip `nginx -t` ile doğrulayın, ardından `systemctl reload nginx` ile yeniden yükleyin:

```
add_header Content-Security-Policy "default-src 'self'; frame-ancestors 'self'" always;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-Content-Type-Options "nosniff" always;
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
add_header Permissions-Policy "geolocation=(), microphone=(), camera=()" always;
```

Diğer platformlar için hazır yapılandırma

Aynı başlıkları, sunucunuz Nginx değilse aşağıdaki hazır bloklardan uygun olanıyla ekleyebilirsiniz.

Firebase Hosting — `firebase.json` :

```
{
  "hosting": {
    "headers": [
      {
        "source": "**",
        "headers": [
          { "key": "Content-Security-Policy", "value": "default-src 'self'; frame-ancestors 'self'" },
          { "key": "X-Frame-Options", "value": "SAMEORIGIN" },
          { "key": "X-Content-Type-Options", "value": "nosniff" },
          { "key": "Strict-Transport-Security", "value": "max-age=31536000; includeSubDomains" },
          { "key": "Referrer-Policy", "value": "strict-origin-when-cross-origin" },
```

```
          { "key": "Permissions-Policy", "value": "geolocation=(), microphone=(), camera=()" }
        ]
      }
    ]
  }
}
```

Vercel — `vercel.json`:

```
{
  "headers": [
    {
      "source": "/(.*)",
      "headers": [
          { "key": "Content-Security-Policy", "value": "default-src 'self'; frame-ancestors 'self'" },
          { "key": "X-Frame-Options", "value": "SAMEORIGIN" },
          { "key": "X-Content-Type-Options", "value": "nosniff" },
          { "key": "Strict-Transport-Security", "value": "max-age=31536000; includeSubDomains" },
          { "key": "Referrer-Policy", "value": "strict-origin-when-cross-origin" },
          { "key": "Permissions-Policy", "value": "geolocation=(), microphone=(), camera=()" }
      ]
    }
  ]
}
```

Next.js — `next.config.js`:

```
module.exports = {
  async headers() {
    return [
      {
        source: '/(.*)',
        headers: [
          { key: 'Content-Security-Policy', value: 'default-src 'self'; frame-ancestors 'self'' },
          { key: 'X-Frame-Options', value: 'SAMEORIGIN' },
          { key: 'X-Content-Type-Options', value: 'nosniff' },
          { key: 'Strict-Transport-Security', value: 'max-age=31536000; includeSubDomains' },
          { key: 'Referrer-Policy', value: 'strict-origin-when-cross-origin' },
          { key: 'Permissions-Policy', value: 'geolocation=(), microphone=(), camera=()' }
        ],
      },
    ];
  },
};
```

Apache — `.htaccess` (mod_headers):

```
Header always set Content-Security-Policy "default-src 'self'; frame-ancestors 'self'"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), microphone=(), camera=()"
```

IIS / ASP.NET — `web.config`:

```
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
      <add name="Content-Security-Policy" value="default-src 'self'; frame-ancestors 'self'" />
      <add name="X-Frame-Options" value="SAMEORIGIN" />
      <add name="X-Content-Type-Options" value="nosniff" />
      <add name="Strict-Transport-Security" value="max-age=31536000; includeSubDomains" />
      <add name="Referrer-Policy" value="strict-origin-when-cross-origin" />
      <add name="Permissions-Policy" value="geolocation=(), microphone=(), camera=()" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

Değişikliklerden sonra tarayıcı geliştirici araçları (Network sekmesi) veya `curl -I https://rest.vulnweb.com` ile başlıkların yanıta eklendiğini doğrulayın.

Açıkta kalan dosyalara erişimi engelleyin

Tespit edilen yollar: `/db.sql`. Sunucu seviyesinde erişimi kapatın:

Nginx:

```
location ~ /\.(git|env|ht) { deny all; return 404; }
location ~* \.(bak|old|zip|sql)$ { deny all; return 404; }
```

Apache — `.htaccess`:

```
RedirectMatch 404 /\.git
RedirectMatch 404 /\.env
<FilesMatch "\.(bak|old|zip|sql)$">
  Require all denied
</FilesMatch>
```

Ayrıca bu dosyaların web köküne (public) hiç konmaması en sağlıklısıdır.

DNS & E-posta Güvenliği

Aşağıdaki öneriler vulnweb.com alan adının e-posta kimlik doğrulamasını güçlendirir. Kayıtları DNS sağlayıcınızın (Cloudflare/GoDaddy/...) TXT arayüzünden ekleyin.

DMARC kaydı ekleyin/sıkılaştırın

Önce `p=none` ile izleyin, raporları inceleyip yanlış-pozitif olmadığından emin olunca `quarantine` → `reject` yapın:

```
_dmarc.vulnweb.com.  TXT  "v=DMARC1; p=quarantine; rua=mailto:dmarc@vulnweb.com; fo=1"
```

DKIM imzalamayı etkinleştirin

E-posta sağlayıcınızın (Google Workspace/Microsoft 365/gönderim servisi) panelinden DKIM üretin ve verdiği TXT kaydını `seçici._domainkey` altına ekleyin:

```
google._domainkey.vulnweb.com.  TXT  "v=DKIM1; k=rsa; p=<sağlayıcının-verdiği-anahtar>"
```

DNSSEC'i etkinleştirin

DNS sağlayıcınızın panelinden **DNSSEC**'i açın; sağlayıcı DS kaydını üretir, bunu alan adı kayıt operatörünüze (registrar) girin. DNS yanıtlarını imzalayarak cache-poisoning'i zorlaştırır.

CORS & Çerez Güvenliği

Aşağıdaki öneriler rest.vulnweb.com için CORS ve çerez güvenliğini güçlendirir.

CORS ve çerez yapılandırmanız güvenli varsayılanlara yakın. Yeni uç noktalar eklerken origin allowlist ve çerez bayrakları (Secure/HttpOnly/SameSite) prensibini koruyun.

CSP (İçerik Güvenlik Politikası) Analizi

Aşağıdaki öneriler rest.vulnweb.com için Content-Security-Policy'yi güçlendirir. CSP'yi önce `Content-Security-Policy-Report-Only` başlığıyla test edip, siteyi bozmadığından emin olduktan sonra uygulanan (enforce) başlığa geçin.

Temel (başlangıç) CSP

Kendi üçüncü taraf alan adlarınızı (analytics, CDN, font) `script-src` / `connect-src` / `img-src` 'ye ekleyerek genişletin:

Nginx:

```
add_header Content-Security-Policy "default-src 'self'; img-src 'self' data:; script-src 'self'; style-src '
```

Firebase Hosting — `firebase.json`:

```
{
  "hosting": {
    "headers": [
      {
        "source": "**",
        "headers": [
          { "key": "Content-Security-Policy", "value": "default-src 'self'; img-src 'self' data:; script-src
        ]
      }
    ]
  }
}
```

Apache — `.htaccess`:

```
Header always set Content-Security-Policy "default-src 'self'; img-src 'self' data:; script-src 'self'; styl
```

Report-Only ile test

```
Content-Security-Policy-Report-Only: default-src 'self'; report-uri /csp-report
```

Raporları izleyip yanlış-pozitifleri giderdikten sonra başlığı `Content-Security-Policy` olarak yayınlayın.

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.
CWE	Common Weakness Enumeration — zafiyet türleri sınıflandırması.

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.
Clickjacking	Sayfanın görünmez iframe içine alınıp kullanıcı tıklamalarının kandırılması.