CyberTestify

Otomatik Güvenlik Tarama Raporu

testasp.vulnweb.com · Basit Tarama

CyberTestify Güvenlik Taraması — Tamamlandı

Rapor No: **CT-ÖRNEK-0D8B**

Doğrulama Kodu: **F1DE-4625**

Bu rapor resmi sızma testi / sertifikasyon değildir.

İçindekiler

HEDEF
testasp.vulnweb.com

PAKET
Basit Tarama

RAPOR NO
CT-ÖRNEK-0D8B

1. Yönetici Özeti

GENEL DEĞERLENDİRME

Yüksek Risk

Ziyaretçilere doğrudan güvenlik uyarısı gösterebilecek acil bir sorun (ör. sertifika süresi/hostname) tespit edildi; öncelikli olarak giderilmesi önerilir.

⚡ Yönetim Kararı

Öncelikli ele alınması gereken **1** yüksek/kritik seviyeli gösterge tespit edildi; bunlar için acil bir düzeltme planı önerilir. Orta/düşük göstergeler planlı iyileştirmeyle giderilebilir.

- **Genel risk seviyesi: Yüksek** — site HTTPS desteklemiyor; iletişim şifresiz (düz metin) taşınıyor — dinlenebilir/değiştirilebilir. Öncelikli olarak HTTPS'e geçilmelidir.
- ⚠ Bu hedef HTTPS (443) üzerinden yanıt vermedi; tarama **http:// üzerinden** yürütüldü. HTTPS eksikliği başlı başına bir bulgudur (aşağıda).
- 6/6 önemli güvenlik başlığı eksik: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Referrer-Policy, Permissions-Policy.
- **Kapsam:** Güvenlik başlığı ve sürüm imzası kontrolleri, ana sayfa dâhil **8 benzersiz sayfada** yürütüldü (tek sayfa değil).
- **Önerilen ilk adım:** Geçerli bir TLS sertifikası kurup tüm trafiği HTTPS'e taşıyın; adım adım hazır komutlar "AI Çözüm Önerileri" eklentisinde sunulur.

Kapsam ve sınır: Bu paket **pasif, GET-tabanlı** bir dış gözlemdir; hiçbir aktif istismar veya prob denenmemiştir. Bir alanda "bulgu yok" ifadesi, aktif test yapılmadığı için **güvenli olduğunu KANITLAMAZ** — yalnızca dışarıdan gözlemlenen yapılandırmanın temiz olduğunu gösterir.

İyileştirme Öncelikleri

⚡ **En Acil / Öncelikli:** HTTPS desteklenmiyor (şifresiz iletişim).

🛠 **Hızlı Kazanım (sunucu yapılandırması, ~1-2 gün):** Content-Security-Policy eksik; X-Frame-Options eksik (clickjacking); X-Content-Type-Options eksik (MIME-sniffing); HSTS (Strict-Transport-Security) eksik; Referrer-Policy eksik.

🗓 **Orta Vadeli / Süreç (manuel doğrulama veya kod/mimari):** Permissions-Policy eksik.

2. Bulgular

2.1 Zafiyet Dağılımı

6

Bu taramada toplam **7** 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	Content-Security-Policy eksik	Açık	Orta
CT-3	X-Frame-Options eksik (clickjacking)	Açık	Orta
CT-4	X-Content-Type-Options eksik (MIME-sniffing)	Açık	Orta
CT-5	HSTS (Strict-Transport-Security) eksik	Açık	Orta
CT-6	Referrer-Policy eksik	Açık	Orta
CT-7	Permissions-Policy eksik	Açık	Orta

3 kontrol alanı çalıştırıldı — 1 alanda sorun bulunmadı, 2 alanda bulgu var

✓ KONTROL EDİLDİ — SORUN BULUNMADI

- **Sunucu/yazılım sürüm imzası (8 sayfada)** Sorun bulunmadı (bilinen eski/EOL sürüm imzası saptanmadı)

⚠ BULGU VAR — AYRINTISI AŞAĞIDAKİ BÖLÜMLERDE

- **HTTP güvenlik başlıkları (8 sayfada)** Bulgu var (6/6 önerilen başlık eksik — yukarıda detaylı)
- **TLS / sertifika** Bulgu var (HTTPS yanıt vermedi — şifresiz iletişim)

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; sayfaya gelen/giden tüm trafik şifresiz (düz metin) taşınıyor — aynı ağdaki bir saldırgan trafiği dinleyebilir, oturum/şifre çalabilir veya içeriği değiştirebilir. Tarama http:// üzerinden yürütüldü.

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

[ORTA] CT-2 · 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 8 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-3 · 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 8 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-4 · 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: Tarayıcı içerik türünü tahmin edebilir (MIME-sniffing); yüklenen dosyalar script gibi çalıştırılabilir. Taranan 8 benzersiz sayfanın TAMAMINDA 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-5 · HSTS (Strict-Transport-Security) eksik

Durum: Açık

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

Nasıl Tespit Edildi: HTTPS zorunluluğu tarayıcıya bildirilmiyor; ilk isteklerde SSL-stripping/MITM riski var. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.

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-6 · Referrer-Policy eksik

Durum: Açık

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

Nasıl Tespit Edildi: Dış bağlantılara tam URL (Referer) gönderilir; oturum/gizlilik bilgisi sızabilir. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.

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

[ORTA] CT-7 · Permissions-Policy eksik

Durum: Açık

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

Nasıl Tespit Edildi: Kamera/mikrofon/konum gibi hassas API'ler kısıtlanmamış; üçüncü taraf içerik kötüye kullanabilir. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.

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

3. Kontrol Özeti ve Metodoloji

HTTP GÜVENLİK BAŞLIKLARI

Başlık	Durum	Açıklama
Strict-Transport-Security	Yok	HTTPS zorunluluğu tarayıcıya bildirilmiyor; ilk isteklerde SSL-stripping/MITM riski var.
Content-Security-Policy	Yok	Tarayıcı hangi kaynakların yükleneceğini kısıtlayamıyor; XSS ve içerik enjeksiyonuna karşı temel savunma yok.
X-Frame-Options	Yok	Sayfa başka bir sitenin iframe'ine gömülebilir; clickjacking ile kullanıcı kandırılabilir.
X-Content-Type-Options	Yok	Tarayıcı içerik türünü tahmin edebilir (MIME-sniffing); yüklenen dosyalar script gibi çalıştırılabilir.
Referrer-Policy	Yok	Dış bağlantılara tam URL (Referer) gönderilir; oturum/gizlilik bilgisi sızabilir.
Permissions-Policy	Yok	Kamera/mikrofon/konum gibi hassas API'ler kısıtlanmamış; üçüncü taraf içerik kötüye kullanabilir.
X-XSS-Protection	Yok	Eski tarayıcı XSS filtresi ayarlı değil (modern tarayıcılarda kritik değildir; asıl koruma CSP'dir).
Content-Type	Var	text/html

TLS SERTİFİKA DURUMU

⚠ Bu hedef **HTTPS (443) üzerinden yanıt vermedi**; geçerli bir TLS sertifikası bulunamadı. Site yalnızca **şifresiz HTTP** üzerinden yayında (bkz. Tespit Edilen Riskler → "HTTPS desteklenmiyor"). Aşağıdaki başlık kontrolleri http:// üzerinden yürütülmüştür.

SUNUCU / TEKNOLOJİ İMZASI

- Sunucu: Microsoft-IIS/8.5
- X-Powered-By: ASP.NET

TESPİT EDİLEN RİSKLER

Bulgu	Şiddet	Açıklama
HTTPS desteklenmiyor (şifresiz iletişim)	Yüksek	Site HTTPS'e yanıt vermiyor; sayfaya gelen/giden tüm trafik şifresiz (düz metin) taşınıyor — aynı ağdaki bir saldırgan trafiği dinleyebilir, oturum/şifre çalabilir veya içeriği değiştirebilir. Tarama http:// üzerinden yürütüldü.
Kritik güvenlik başlığı eksik: Content-Security-Policy	Orta	Tarayıcı hangi kaynakların yükleneceğini kısıtlayamıyor; XSS ve içerik enjeksiyonuna karşı temel savunma yok. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.
Kritik güvenlik başlığı eksik: X-Frame-Options	Orta	Sayfa başka bir sitenin iframe'ine gömülebilir; clickjacking ile kullanıcı kandırılabilir. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.
Güvenlik başlığı eksik: X-Content-Type-Options	Orta	Tarayıcı içerik türünü tahmin edebilir (MIME-sniffing); yüklenen dosyalar script gibi çalıştırılabilir. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.
Güvenlik başlığı eksik: Strict-Transport-Security	Orta	HTTPS zorunluluğu tarayıcıya bildirilmiyor; ilk isteklerde SSL-stripping/MITM riski var. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.
Güvenlik başlığı eksik: Referrer-Policy	Orta	Dış bağlantılara tam URL (Referer) gönderilir; oturum/gizlilik bilgisi sızabilir. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.
Güvenlik başlığı eksik: Permissions-Policy	Orta	Kamera/mikrofon/konum gibi hassas API'ler kısıtlanmamış; üçüncü taraf içerik kötüye kullanabilir. Taranan 8 benzersiz sayfanın TAMAMINDA eksik.

POZİTİF GÜVENCE — KONTROL EDİLEN ALANLAR

Bulgu çıkmayan alanlar da dâhil, Basit Tarama kontrolleri ana sayfa dâhil **8 benzersiz sayfada** gerçekten çalıştırıldı. Aşağıdaki tablo, "sorun bulunamadı" sonuçlarını da şeffaf biçimde gösterir:

Kontrol Alanı	Sonuç
HTTP güvenlik başlıkları (8 sayfada)	⚠ **Bulgu var (6/6 önerilen başlık eksik — yukarıda detaylı)**
TLS / sertifika	⚠ **Bulgu var (HTTPS yanıt vermedi — şifresiz iletişim)**
Sunucu/yazılım sürüm imzası (8 sayfada)	✓ **Sorun bulunmadı (bilinen eski/EOL sürüm imzası saptanmadı)**

> **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, hiçbir prob/payload gönderilmez):** HTTP güvenlik başlıkları, TLS/sertifika durumu (geçerlilik · hostname · TLS sürümü), sunucu-yazılım sürüm imzası ve bilinen eski/EOL sürüm tespiti — keşfedilen 8 sayfada.

> **ETMEZ:** CORS politikası, çerez bayrağı detayı, Content-Security-Policy analizi, DNS/e-posta kayıtları (SPF/DKIM/DMARC) ve açıkta hassas dosya taraması **Dış Yüzey** paketindedir; KVKK/PCI/ISO çerçeve-eşlemesi **Uyum** paketinde; subdomain/API/CVE keşfi **Keşif** paketinde; aktif zafiyet doğrulaması (SQLi/XSS/IDOR prob'u) **Aktif Doğrulama** ve **Tam Kapsamlı Pentest** paketlerinde ele alınır. Bu rapor pasif gözleme dayanır; "bulgu yok", aktif istismar denenmediği için **güvenli olduğunu KANITLAMAZ**.

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

Aşağıdaki öneriler, testasp.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://testasp.vulnweb.com` ile başlıkların yanıta eklendiğini doğrulayın.

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.
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.
KVKK	Kişisel Verilerin Korunması Kanunu (Türkiye).
Clickjacking	Sayfanın görünmez iframe içine alınıp kullanıcı tıklamalarının kandırılması.