

PARS

// PENTEST AUTONOMOUS RECON SYSTEM //
POWERED BY MESTEG TEKNOLOJİ

TARGET ACQUISITION <http://google-gruyere.appspot.com>

SCAN DATE 11.12.2025 05:07:05

DURATION 0:02:06

TOTAL REQUESTS 716



/// GÜVENLİK DURUŞU ANALİZİ

Bu rapor, **Mesteg Teknoloji** tarafından geliştirilen ve **Synara AI** bilinci ile güçlendirilmiş **PARS** (Pentest Autonomous Recon System) motoru tarafından oluşturulmuştur. Skor, tespit edilen zafiyetlerin CVSS v3.1 standartlarına göre ağırlıklandırılmasıyla hesaplanmıştır.

TOPLAM CVSS ETKİSİ

20.5

TESPİT EDİLEN BULGULAR

32

SUCCESS

PRE_SCAN 05:05:02

SRP Düşüş: 0.0 | 2 parametre bulundu. Örn: 0_hackers(LOW), 1_gruyere(LOW)

WARNING

WAF_DETECT 05:05:02

GÜVENLİK DUVARI TESPİT EDİLDİ: Generic WAF (Tepki: 200) | Yöntem: Aktif Provokasyon (' OR 1=1 --)

SUCCESS

OSINT 05:05:08

DNS ve IP adresi çözüldü: 142.250.184.148

INFO

SUBDOMAIN 05:05:35

Başarılı: 19 adet alt alan adı tespit edildi. Örn: dev.google-gruyere.appspot.com, beta.google-gruyere.appspot.com, webmail.google-gruyere.appspot.com, mail.google-gruyere.appspot.com, test.google-gruyere.appspot.com

INFO

INTERNAL_SCAN 05:05:35

Tüm kritik çekirdek dosyaları yerinde.

INFO

INTERNAL_SCAN 05:05:35

Açık kod dosyalarında hardcoded secret bulunamadı.

INFO

INTERNAL_SCAN 05:05:35

Manifesto'da kritik bölümler eksik: ## 1. MİMARİ, ## 2. GÜVENLİK KURALLARI, ## 3. VERİ YAPILARI

SUCCESS

INTERNAL_SCAN 05:05:35

Harici bağımlılık (Nuclei) PATH'te bulundu. Kullanıma hazır.

CRITICAL

JSON_API CVSS: 3.0 05:05:36

Kritik Hata: TypeError ('dict' object cannot be interpreted as an integer) [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

XSS CVSS: 10.0 05:05:36

Kritik Hata: TypeError ('dict' object cannot be interpreted as an integer) [Exploit Önerisi: Kullanıcı girdisine enjekte et.]

INFO

IDOR 05:05:36

INFO: Orijinal yanıt alınamadığı için IDOR taraması atlandı.

CRITICAL

SQLi 05:05:36

Kritik Hata: TypeError ('dict' object cannot be interpreted as an integer) [Exploit Önerisi: Manuel doğrulama önerilir.]

SUCCESS

BUSINESS_LOGIC 05:05:36

Stateful İş Mantığı Fuzzing'i tamamlandı.

INFO

HEURISTIC 05:05:36

Sunucu yazılımı: Standart HTML/Backend Framework.

INFO

HEURISTIC 05:05:36

Sunucu: Google Frontend

SUCCESS

HEADERS 05:05:36

GÜVENLİ: Teknoloji bilgisi (X-Powered-By) gizlenmiş.

INFO

HEADERS 05:05:36

[BBH Filtresi] UYARI: Content-Security-Policy (CSP) bulunamadı (Kapsam Dışı/INFO).

INFO

HEADERS 05:05:36

[BBH Filtresi] UYARI: HSTS (HTTPS Zorlama) başlığı eksik (Kapsam Dışı/INFO).

INFO

HEADERS 05:05:36

[BBH Filtresi] UYARI: X-Frame-Options başlığı eksik (Kapsam Dışı/INFO).

INFO

HEADERS 05:05:36

BİLGİ: Yanitta Set-Cookie başlığı bulunamadı (Oturum cerezleri ayarlanmıyor olabilir).

INFO

HEADERS 05:05:36

[BBH Filtresi] BİLGİ: 'X-Content-Type-Options: nosniff' eksik (Kapsam Dışı/INFO).

INFO

HEADERS 05:05:36

BİLGİ: 'Referrer-Policy' başlığı eksik. Kullanıcı gizliliği için ayarlanmalı.

INFO

HEADERS 05:05:36

BİLGİ: 'Permissions-Policy' başlığı eksik. Kamera/Mikrofon gibi özellikler kısıtlanmamış.

SUCCESS

HEURISTIC 05:05:36

GÜVENLİ: Heuristic yansımıma kontrolü temiz.

WARNING

SYSTEM CVSS: 1.5 05:05:37

AÇIK PORT: 80 (HTTP) | Banner: HTTP/1.0 404 Not Found Content-Length: 272 Content

WARNING

SYSTEM CVSS: 1.5 05:05:37

AÇIK PORT: 443 (HTTPS)

INFO

GRAPHQL 05:05:37

Yaygın GraphQL endpoint'leri bulunamadı.

INFO

FILES 05:05:38

BİLGİ: robots.txt mevcut. İçeriği kontrol edilmeli.

SUCCESS

FILES 05:05:38

Kritik hassas dosya ifşası tespit edilmedi.

INFO

CLOUD_EXPLOIT 05:05:39

S3 Bucket Mevcut (Erişim Engelli): <https://appspot.s3.amazonaws.com>

INFO

CLOUD_EXPLOIT 05:05:39

S3 Bucket Mevcut (Erişim Engelli): <https://appspot-logs.s3.amazonaws.com>

WARNING

CHAINING CVSS: 4.5 05:07:05

RİSK ZİNCİRLEME: API endpoint'lerinde XSS/SQLi potansiyeli ve JSON API Fuzzing hataları tespit edildi. Bağlam zafiyeti riski.

GENERATED BY PARS (SYNARA AI CORE) v17.1 ULTIMATE
MESTEG TEKNOLOJİ LTD. ŞTİ. - CONFIDENTIAL REPORT