

PARS

// PENTEST AUTONOMOUS RECON SYSTEM //

POWERED BY MESTEG TEKNOLOJİ

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

SCAN DATE 11.12.2025 02:28:53

DURATION 0:01:46

TOTAL REQUESTS 715



/// 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

33

SUCCESS

CLIENT_LOGIC 02:27:10

Client-side Logic taraması tamamlandı.

SUCCESS

PRE_SCAN 02:27:10

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

WARNING

WAF_DETECT 02:27:10

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

SUCCESS

OSINT 02:27:16

DNS ve IP adresi çözüldü: 142.251.38.244

INFO

SUBDOMAIN 02:27:22

Başarılı: 19 adet alt alan adı tespit edildi. Örn: server.google-gruyere.appspot.com, vpn.google-gruyere.appspot.com, shop.google-gruyere.appspot.com, api.google-gruyere.appspot.com, remote.google-gruyere.appspot.com

INFO

INTERNAL_SCAN 02:27:23

Tüm kritik çekirdek dosyaları yerinde.

INFO

INTERNAL_SCAN 02:27:23

Açık kod dosyalarında hardcoded secret bulunamadı.

INFO

INTERNAL_SCAN 02:27:23

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

SUCCESS

INTERNAL_SCAN 02:27:23

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

CRITICAL
JSON_API CVSS: 3.0 02:27:23

Kritik Hata: TypeError (unsupported operand type(s) for +: 'coroutine' and 'coroutine') [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL
XSS CVSS: 10.0 02:27:23

Kritik Hata: TypeError ('coroutine' object is not iterable) [Exploit Önerisi: Kullanıcı girdisine `␣` enjekte et.]

INFO
IDOR 02:27:23

INFO: Orijinal yanıt alınamadığı için IDOR taraması atlandı.

CRITICAL
SQLi 02:27:23

Kritik Hata: TypeError (unsupported operand type(s) for +: 'coroutine' and 'list') [Exploit Önerisi: Manuel doğrulama önerilir.]

SUCCESS
BUSINESS_LOGIC 02:27:23

Stateful İş Mantığı Fuzzing'i tamamlandı.

INFO
HEURISTIC 02:27:24

Sunucu yazılımı: Standart HTML/Backend Framework.

INFO
HEURISTIC 02:27:24

Sunucu: Google Frontend

SUCCESS

HEADERS 02:27:24

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

INFO

HEADERS 02:27:24

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

INFO

HEADERS 02:27:24

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

INFO

HEADERS 02:27:24

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

INFO

HEADERS 02:27:24

BİLGİ: Yanıtta Set-Cookie başlığı bulunamadı (Oturum çerezleri ayarlanmıyor olabilir).

INFO

HEADERS 02:27:24

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

INFO

HEADERS 02:27:24

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

INFO

HEADERS 02:27:24

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

SUCCESS

HEURISTIC 02:27:24

GÜVENLİ: Heuristic yansımaya kontrolü temiz.

WARNING

SYSTEM CVSS: 1.5 02:27:24

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

WARNING

SYSTEM CVSS: 1.5 02:27:24

AÇIK PORT: 443 (HTTPS)

INFO

GRAPHQL 02:27:24

Yaygın GraphQL endpoint'leri bulunamadı.

INFO

FILES 02:27:25

BİLGİ: robots.txt mevcut. İçeriği kontrol edilmeli.

SUCCESS

FILES 02:27:25

Kritik hassas dosya ifşası tespit edilmedi.

INFO

CLOUD_EXPLOIT 02:27:26

S3 Bucket Mevcut (Eriřim Engelli): https://appspot.s3.amazonaws.com

INFO

CLOUD_EXPLOIT 02:27:26

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

WARNING

CHAINING CVSS: 4.5 02:28:53

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