

PARS

// PENTEST AUTONOMOUS RECON SYSTEM //

POWERED BY MESTEG TEKNOLOJİ

TARGET ACQUISITION <http://testphp.vulnweb.com>

SCAN DATE 10.12.2025 23:36:27

DURATION 0:02:04

TOTAL REQUESTS 2629



/// 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

13.5

TESPİT EDİLEN BULGULAR

43

SUCCESS

PRE_SCAN 23:34:28

SRP Düşüş: 0.0 | 21 parametre bulundu. Örn: background-color(LOW), siteName(LOW), content(LOW), mailto(LOW), goButton(LOW), text-align(LOW)

SUCCESS

CLIENT_LOGIC 23:34:28

Client-side Logic taraması tamamlandı.

INFO

WAF_DETECT 23:34:29

Herhangi bir WAF koruması tespit edilemedi.

INFO

SUBDOMAIN 23:34:57

Başarılı: 0 adet alt alan adı tespit edildi. Örn:

INFO

IDOR 23:34:57

INFO: Orijinal yanıt alınamadığı için IDOR taraması atlandı.

SUCCESS

BUSINESS_LOGIC 23:34:57

Stateful İş Mantığı Fuzzing'i tamamlandı.

INFO

HEADERS 23:34:57

[BBH Filtresi] RİSK: 'X-Powered-By' ifşası tespit edildi! (PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1) (Kapsam Dışı/INFO)

INFO

HEADERS 23:34:57

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

INFO

HEADERS 23:34:57

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

INFO

HEADERS 23:34:57

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

INFO

HEADERS 23:34:57

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

INFO

HEADERS 23:34:57

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

INFO

HEADERS 23:34:57

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

INFO

HEADERS 23:34:57

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

INFO

HEURISTIC 23:34:57

Teknoloji İpucu: Jinja2 (SSTI) parmak izi bulundu.

INFO

HEURISTIC 23:34:57

Sunucu: nginx/1.19.0

SUCCESS

Kritik hassas dosya ifşası tespit edilmedi.

CRITICAL

AUTH_BYPASS CVSS: 12.0 23:34:57

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/admin// [İçerik Tamamen Farklı (0.07 Sim)]
[Exploit Önerisi: Manuel doğrulama önerilir.]

SUCCESS

HEURISTIC 23:34:57

GÜVENLİ: Heuristic yansımaya kontrolü temiz.

WARNING

SYSTEM CVSS: 1.5 23:34:57

AÇIK PORT: 80 (HTTP)

CRITICAL

AUTH_BYPASS 23:34:57

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/admin/%2e/ [İçerik Tamamen Farklı (0.07 Sim)]
[Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:34:58

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/admin/%2e%2e/ [İçerik Tamamen Farklı (0.04 Sim)]
[Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:34:58

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/dashboard/%2e%2e/ [İçerik Tamamen Farklı (0.04 Sim)]
[Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:34:58

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/administrator/%2e%2e/ [İçerik Tamamen Farklı (0.04 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:34:58

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/admin/. [İçerik Tamamen Farklı (0.07 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:34:58

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/admin/. [İçerik Tamamen Farklı (0.07 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

HIGH

AUTH_BYPASS 23:34:59

BYPASS ŞÜPHESİ (HIGH): http://testphp.vulnweb.com/admin? [Status: 301, Size: 169, Sim: 0.26] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:00

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/admin/static/..%2f [İçerik Tamamen Farklı (0.07 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:00

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/login/%2e%2e/ [İçerik Tamamen Farklı (0.04 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:00

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/wp-admin/%2e%2e/ [İçerik Tamamen Farklı

(0.04 Sim)) [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:01

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/cpanel/%2e%2e/ [İçerik Tamamen Farklı (0.04 Sim)) [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:01

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/config/%2e%2e/ [İçerik Tamamen Farklı (0.04 Sim)) [Exploit Önerisi: Manuel doğrulama önerilir.]

WARNING

SQLi 23:35:02

RİSK: Boolean-based SQLi şüphesi. Parametre: 'document_title_rgn'. True/False yükleri farklı yanıt üretti (Δ≈4788 byte, oran=0.97). Payload(OR): ' OR '1'='1'-- - [AUTO-POC OLUŞTURULDU]

WARNING

SQLi 23:35:02

RİSK: Boolean-based SQLi şüphesi. Parametre: 'sectionLinks'. True/False yükleri farklı yanıt üretti (Δ≈4788 byte, oran=0.97). Payload(OR): ' OR '1'='1'-- - [AUTO-POC OLUŞTURULDU]

WARNING

SQLi 23:35:03

RİSK: Boolean-based SQLi şüphesi. Parametre: 'searchFor'. True/False yükleri farklı yanıt üretti (Δ≈4788 byte, oran=0.97). Payload(OR): ' OR '1'='1'-- - [AUTO-POC OLUŞTURULDU]

WARNING

SQLi 23:35:03

RİSK: Boolean-based SQLi şüphesi. Parametre: 'text-align'. True/False yükleri farklı yanıt üretti (Δ≈4788 byte, oran=0.97). Payload(OR): ' OR '1'='1'-- - [AUTO-POC OLUŞTURULDU]

WARNING

SQLi 23:35:04

RİSK: Boolean-based SQLi şüphesi. Parametre: 'clsid'. True/False yükleri farklı yanıt üretti ($\Delta \approx 4788$ byte, oran=0.97). Payload(OR): ' OR '1'='1'-- - [AUTO-POC OLUŞTURULDU]

CRITICAL

AUTH_BYPASS 23:35:04

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/root/%2e%2e/ [İçerik Tamamen Farklı (0.01 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:05

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/system/%2e%2e/ [İçerik Tamamen Farklı (0.01 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:05

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/auth/%2e%2e/ [İçerik Tamamen Farklı (0.01 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:05

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/panel/%2e%2e/ [İçerik Tamamen Farklı (0.01 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:08

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/controlpanel/%2e%2e/ [İçerik Tamamen Farklı (0.01 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

CRITICAL

AUTH_BYPASS 23:35:08

KRİTİK YETKİ ATLAMA: http://testphp.vulnweb.com/secure/%2e%2e/ [İçerik Tamamen Farklı (0.01 Sim)] [Exploit Önerisi: Manuel doğrulama önerilir.]

