

Sızma Testi Raporu

WHOIS (BILGI)

Domain kayıt ve DNS sunucu bilgileri elde edildi. Domainin park edilmiş olduğu görülüyor.

- Registrar: HOSTINGER operations, UAB

- Name

SUBFINDER (BILGI)

Hedef domaine ait bir adet subdomain tespit edildi.

- www.mgorkemkilic.com

AMASS (BILGI)

Subdomain taraması Subfinder sonuçlarını teyit etti.

- www.mgorkemkilic.com

DIG (BILGI)

DNS sorgusu, standart kayıtlar yerine RFC8482'ye uygun genel bir yanıt döndürdü.

- DNS sorgusuna verilen yanıt: HINFO "RFC8482" "". Bu durum, sunucunun belirli DNS sorgu tiplerine karşı bilgi vermemeye ayarlandığını gösterir.

NMAP (DÜŞÜK)

Hedef sistemde standart web portları (80, 443) açık ve OpenResty web sunucusu çalışıyor.

- IP Adresi: 34.120.137.41 (googleusercontent.com)

- Açık Po

GOBUSTER (DÜŞÜK)

Dizin taramasında hassas bir dosya bulunamadı ancak bazı yolların (400, 404) 200 (OK) durum kodu döndürdüğü görüldü.

- '/400' ve '/404' yolları 200 HTTP durum kodu ile yanıt veriyor. Bu durum otomatik tarayıcıları yanıltabilir.

- Yaygın
döndürü

NIKTO (BILGI)

Araç çalıştırılmadı/Sonuç yok

NUCLEI (BILGI)

Araç çalıştırılmadı/Sonuç yok

SQLMAP (BILGI)

SQL enjeksiyonu zafiyeti bulunamadı. Araç, hedefte bir WAF/IPS koruması olduğunu tespit etti.

- Heuristics detected that the target is protected by some kind of WAF/IPS.

- Temel

DALFOX (BILGI)

XSS zafiyeti tespit edilmedi ancak HSTS ve CSP gibi önemli güvenlik başlıklarının varlığı doğrulandı.

- Strict-Transport-Security (HSTS) başlığı mevcut ve güçlü bir yapılandırmaya sahip: max-age=63072000; includeSubDomains; preload

- Conten

COMMIX (ARAÇ HATASI)

Araç teknik hata verdi.

WAPITI (ORTA)

Web uygulamasında kritik güvenlik başlıklarının (CSP, X-Frame-Options) eksik veya yanlış yapılandırıldığı tespit edildi.

- Content-Security-Policy (CSP) başlığında 'default-src', 'script-src', 'object-src', 'base-uri'

direktifleri eksik.

- X-Fram

HYDRA (BILGI)

Araç çalıştırılmadı/Sonuç yok

APKLEAKS (ARAÇ HATASI)

Araç teknik hata verdi. Ancak, hatalı çalışmasına rağmen potansiyel bir Google API anahtarı sızıntısı raporladı.

- Potansiyel Google API Anahtarı sızıntısı: AlzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE

APKTOOL (BILGI)

Araç çalıştırılmadı/Sonuç yok