

Sızma Testi Raporu

WHOIS (BILGI)

'www' alt alan adı için WHOIS kaydı bulunamadı, bu normal bir durumdur. Ana alan adı için sorgulama yapılmalıdır.

- 'www.mgorkemkilic.com' için doğrudan bir WHOIS kaydı bulunamadı.

Subfinder (BILGI)

Araç, 'www.mgorkemkilic.com' hedefi için herhangi bir ek alt alan adı bulamadı.

- Hedef alan adı için ek alt alan adı tespit edilmedi.

Amass (BILGI)

Hedef alan adı ve muhtemelen hatalı bir kayıt olan 'www.www.mgorkemkilic.com' bulundu.

- 'www.www.mgorkemkilic.com' ve 'www.mgorkemkilic.com' alt alan adları tespit edildi.

Dig (BILGI)

DNS sorgusu, 'www.mgorkemkilic.com' alan adının Hostinger'a yönlendirilen bir CNAME kaydı olduğunu gösterdi.

- www.mgorkemkilic.com. IN CNAME connect.hostinger.com.

Nmap (BILGI)

Hedef IP adresinde (34.120.137.41) port 80 (HTTP) ve 443 (HTTPS) açık olarak bulundu. Web sunucusu olarak OpenResty tespit edildi.

- Port 80/tcp (http) açık.

- Port 443/tcp (https) açık.

Gobuster (ARAÇ HATASI)

Araç teknik hata verdi.

- Araç 'flag provided but not defined: -wildcard' hatası ile sonlandı. Yanlış parametre kullanılmış.

Nikto (BILGI)

Araç çalıştırılmadı/Sonuç yok.

Nuclei (BILGI)

Araç, hedefe (port 80) erişemediği için taramayı atladi.

- Nuclei, hedefin 30 denemede yanıt vermediğini belirterek HTTP üzerinden tarama yapamadı.

Sqlmap (BILGI)

Sqlmap, yaptığı temel testlerde herhangi bir SQL Injection zafiyeti tespit edemedi.

- Test edilen parametrelerde SQL Injection zafiyeti bulunamadı.

Dalfox (BILGI)

Dalfox, yaptığı testlerde herhangi bir XSS (Cross-Site Scripting) zafiyeti bulamadı.

- Ana sayfa üzerinde yapılan XSS taramasında zafiyet tespit edilmedi.

Commix (ARAÇ HATASI)

Araç teknik hata verdi.

- Araç, muhtemelen eksik veya yanlış parametreler nedeniyle hata verdi.

Wapiti (DÜŞÜK)

Güvenlik başlıklarında (Security Headers) eksiklikler tespit edildi. Özellikle Content-Security-Policy (CSP) ve X-Frame-Options başlıkları eksik.

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

- X-Fram

Hydra (BILGI)

SSH servisine (port 22) yapılan kaba kuvvet saldırısı denemesi, port kapalı olduğu için başarısız oldu.

- Hedef IP adresinde (34.120.137.41) SSH portu (22) kapalı veya erişilemez durumda.

Apkleaks (YÜKSEK)

Hedefle ilişkili olduğu varsayılan bir APK dosyasının analizinde, koda gömülü (hard-coded) bir Google API anahtarı ve çok sayıda dahili yol (endpoint) bilgisi sızdırıldığı tespit edildi.

- Google API Anahtarı sızıntısı: 'AlzaSyDRKQ9d6kfsoZT2IUnZcZnBYvH69HEXNPE'

- Uygula
/canOpe

Apktool (BILGI)

Araç çalıştırılmadı/Sonuç yok.