Project Subject

“{oak.gs} - PENTEST PROJESI ve BULGULARI”

Full Name

Hacktivity Group

H. Can KOTANOĞLU

Hasan BAŞPINAR

Yusuf ORAL

Hanımzer TEKİN

Fatemah ALİZADEH

Necdet KABACA

Ömer AKSOY

Ercan YILMAZ

Nuerbiya Saimi

Project Duration

27 - 30.05.2025

1. Projenin Tanımı, Amacı ve Kapsamı

1.1. Giriş ve Görev Tanımı

- Bu belgede, arkadaşlarımızla birlikte oak.gs alan adı ve ilişkili sistemleri üzerinde gerçekleştirdiğimiz sızma testi projemizin sonuçları sunulmaktadır.

Eğitmenimizin verdiği görev tanımındaki adımlar takip edilmiştir. Tam olarak istenilen görevler aşağıda listenildiği gibidir:

“ Bu projenin amacı, bir şirketin internete açık hizmetlerindeki güvenlik açıklarını tespit etmektir. Bunun için, ilgili şirketin ana alan adı adresinden başlayarak ilişkili alan adlarını (domain) belirlemeniz gerekmektedir. Ayrıca, belirlediğiniz bu alan adlarında çalışan hizmetleri de tespit etmelisiniz.

*İlk hedef olarak **oak.gs** alan adıyla başlayabilirsiniz. Daha sonra şu adımları izleyin:*

- *Verilen alan adının **IP adresini ve geçmişteki değişimlerini gösterin**. (DNS istihbarat servislerini kullanabilirsiniz.)*
- ***Geçmişte aynı IP adresinde barındırılmış diğer alan adlarını listeleyin**.*
- ***Topladığınız alan adlarının alt alan adlarını (subdomain) bulun**.*
- ***Bulduğunuz her alan adı için, hizmetlerini** (port numarası vb.) **ve alt alan adlarını listeleyin**.*
- ***Tüm alan adları ve alt alan adları üzerindeki hizmetleri ve güvenlik açıklarını tespit edin**.*
- ***Projede kullandığınız her aracın ismini ve sürüm (versiyon) numaralarını belirtin**.*
- ***Yaptığınız tüm çalışmaları detaylı şekilde belgeleyin**.”*

1.2. Projenin Temel Amacı

- Verilen oak.gs alan adından başlayarak şirketin internete açık servislerini ve ilişkili alan adlarını tespit etmek.
- Bu alan adları ve servisler üzerindeki potansiyel güvenlik zafiyetlerini belirlemek.

1.3. Kapsam

- **Ana Hedef:** oak.gs
- **İlişkili Sistemler:** Keşfedilen tüm alt alan adları, IP adresleri ve bu adreslerde çalışan servisler.
- **Özel Odak:** sign.oak.gs alt alan adı üzerinde OWASP ZAP ve Nessus Essentials ile detaylı zafiyet taramaları gerçekleştirilmiştir.

2. Kullanılan Metodoloji ve Araçlar

2.1. Metodoloji Aşamaları

- **Pasif Bilgi Toplama:** Sistemle doğrudan etkileşime girmeden, halka açık kaynaklardan bilgi toplama.
- **Aktif Bilgi Toplama ve Tarama:** Sistemle kontrollü etkileşime girerek daha detaylı bilgi edinme ve zafiyet arama.
- **Zafiyet Değerlendirme:** Tespit edilen potansiyel zafiyetlerin etki ve olasılıklarını analiz ederek risklerini belirleme.

2.2. Kullanılan Başlıca Araçlar

- **DNS ve Genel Bilgi Toplama:** whois, nslookup, dig, SecurityTrails, VirusTotal
- **Alt Alan Adı Keşfi:** subfinder, gobuster
- **Port Tarama ve Servis Tespiti:** nmap
- **SSL/TLS Yapılandırma Analizi:** sslscan, nmap (ilgili scriptler)
- **Web Application Firewall (WAF) Tespiti:** wafw00f
- **Web Uygulama Zafiyet Taraması (Otomatik):** OWASP ZAP (sign.oak.gs üzerinde)
- **Ağ ve Sistem Zafiyet Taraması (Otomatik):** Nessus Essentials (sign.oak.gs üzerinde)
- **Exploit Veritabanı Sorgulama:** searchsploit
- **SQL Injection Test Aracı:** sqlmap (Belirli bir URL üzerinde kontrollü test)

3. oak.gs Ana Alan Adı: Genel İnceleme ve IP Adres Tarihçesi

3.1. Whois Kayıt Analizi

- **Kayıtçı Firma:** GoDaddy
- **E-posta Altyapı Sağlayıcısı:** Yandex

3.2. IP Adres Tarihçesi (SecurityTrails Verileri)

- **Mevcut Barındırma:** Ağırlıklı olarak AWS (Amazon Web Services) altyapısı (S3, CloudFront, Global Accelerator).
- **Geçmiş Barındırma Kayıtları:** Contabo GmbH gibi farklı sağlayıcılarda da barındırıldığı tespit edilmiştir.

3.3. DNS Kayıt Analizi (SecurityTrails, nslookup, dig)

- **Temel DNS Kayıtları:** A, MX (Yandex), NS (GoDaddy), TXT (SPF kaydı mevcut).
- **Tespit Edilen Eksiklik:** AAAA (IPv6) kaydı bulunmamaktadır.
- **DNSSEC Durumu:** İMZALANMAMIŞ (Unsigned).
    - **İlişkili Risk:** Düşük. DNS sahteciliği (spoofing) ve önbellek zehirlenmesi (cache poisoning) saldırılarına karşı bir zafiyet teşkil edebilir.

Öneri: DNSSEC'in etkinleştirilmesi değerlendirilmelidir.

4. Alt Alan Adı Keşfi ve Saldırı Yüzeyi Analizi

4.1. Kullanılan Araçlar ve Yöntemler

- SecurityTrails, subfinder, gobuster.

4.2. Tespit Edilen Önemli Alt Alan Adları (Örnekler)

- sign.oak.gs (Bu alan adı detaylı incelemeye tabi tutulmuştur)
- xmpp.*, storage.*, api.*, test.*
- sentry.*, sonarqube.*, graylog.* *(Bu isimlerin genellikle geliştirme, test veya izleme araçlarına işaret ettikleri değerlendirilmektedir)*

4.3. Risk Değerlendirmesi

Orta. Çok sayıda alt alan adının varlığı, potansiyel giriş noktalarını ve yönetilmesi gereken saldırı yüzeyini doğal olarak artırmaktadır.

5. Odak Noktası: sign.oak.gs Alt Alan Adı Detaylı Analizi

5.1. İnceleme Gerekçesi

- Bu alt alan adı, potansiyel olarak kritik bir işlev barındırabileceği veya temsili bir web uygulaması olabileceği düşüncesiyle daha ayrıntılı bir incelemeye alınmıştır.

5.2. DNS Çözümlemesi

- Alan adı, d38159j2yt9llc.cloudfront.net adresine yönlenen bir CNAME kaydına sahiptir. Bu, servisin Amazon CloudFront CDN (Content Delivery Network) arkasında çalıştığını göstermektedir.

5.3. WAF Tespiti (wafw00f aracı ile)

- Amazon CloudFront WAF kullanıldığı tespit edilmiştir.

5.4. SSL/TLS Yapılandırma Analizi

- **Desteklenen Güçlü Protokoller:** TLSv1.2, TLSv1.3.
- **Eski ve Zayıf Protokoller (SSLv2, SSLv3, TLSv1.0, TLSv1.1):** Devre Dışı (Güvenli bir yapılandırma).
- **Heartbleed Zafiyeti (CVE-2014-0160):** Tespit Edilmedi (Güvenli).
- **Kullanılan Şifreleme Takımları (Cipher Suites):** Güçlü ve modern algoritmalar tercih edilmiş.

Genel Değerlendirme: sign.oak.gs'in SSL/TLS yapılandırması genel olarak iyi ve güncel güvenlik standartlarına uygun bulunmuştur.

6. Nessus ve OWASP ZAP Tarama Sonuçları (sign.oak.gs)

6.1. Nessus Taraması

- **Genel Sonuç:** 0 Kritik, 0 Yüksek, 1 Orta, 0 Düşük ve 24 Bilgilendirme seviyesinde bulgu tespit edilmiştir.
- **Orta Seviye Zafiyet: HSTS Başlığı Eksik (Plugin ID: 142960)**
    - **Açıklama:** Sunucu, HTTPS üzerinden hizmet verirken HSTS başlığını göndermemektedir. Bu başlık, tarayıcılara gelecekteki tüm iletişimlerin yalnızca HTTPS üzerinden yapılması gerektiğini bildirir.
    - **Risk (CVSSv3.0 Skor: 6.5):** Bu eksiklik, kullanıcıları SSL Stripping gibi ortadaki adam (Man-in-the-Middle) saldırılarına karşı savunmasız bırakabilir.
    - **Öneri:** Strict-Transport-Security HTTP yanıt başlığının uygulanması şiddetle tavsiye edilir.
- **Bilgilendirme Seviyesindeki Bulgular: Eksik Güvenlik Başlıkları (Clickjacking Koruması)**
    - X-Frame-Options veya Content-Security-Policy: frame-ancestors başlıkları eksik veya yetersiz yapılandırılmıştır.
    - **Risk:** Düşük-Orta. Web sitesinin, kötü niyetli başka siteler içerisinde bir <iframe> ile çağrılarak kullanıcı arayüzünü taklit eden clickjacking saldırılarına maruz kalma potansiyelini artırır.
    - **Öneri:** Bu başlıkların X-Frame-Options: DENY ve/veya Content-Security-Policy: frame-ancestors 'self' gibi kısıtlayıcı değerlerle eklenmesi önerilir.

6.2. OWASP ZAP Taraması

- **Hassas Dosya ve Dizin Erişimi:** WEB-INF/web.xml, .env, phpinfo.php gibi yaygın olarak bilinen hassas dosya ve dizinlere erişim denemelerinin büyük çoğunluğu 404 Not Found yanıtı ile sonuçlanmıştır. Bu, olumlu bir güvenlik göstergesidir.
- **Bulut Platformu Metadata Servisi Erişimi:** /latest/meta-data/ (AWS) gibi bulut sağlayıcı metadata servislerine erişim denemelerinin tamamı 403 Forbidden yanıtı ile sonuçlanmıştır. Bu, SSRF (Server-Side Request Forgery) zafiyetlerine karşı iyi bir güvenlik önlemidir.

Genel Değerlendirme: İncelenen ZAP çıktılarına göre, sign.oak.gs üzerinde bariz, doğrudan sömürülebilir bir web uygulaması zafiyeti tespit edilmemiştir.

sign.oak.gs Ana Bilgisayarı İçin Güvenlik Açığı Özeti

Bu rapor, sign.oak.gs ana bilgisayarında tespit edilen güvenlik açıklarını ve bilgilendirme amaçlı bulguları özetlemektedir.

Genel Bakış

Kritik: 0 **Yüksek:** 0 **Orta:** 1 **Düşük:** 0 **Bilgi:** 24 **Toplam Tespit:** 25

Önem Derecesi	CVSS v3.0	Plugin ID	Açıklama
ORTA	6.5	142960	HSTS HTTPS Sunucusunda Eksik (RFC 6797)
BİLGİ	N/A	45590	Ortak Platform Numaralandırması (CPE)
BİLGİ	N/A	54615	Cihaz Türü
BİLGİ	N/A	84502	HSTS HTTPS Sunucusunda Eksik
BİLGİ	N/A	10107	HTTP Sunucu Türü ve Sürümü
BİLGİ	N/A	12053	Ana Bilgisayar Tam Nitelikli Alan Adı (FQDN) Çözümlemesi
BİLGİ	N/A	24260	HyperText Transfer Protocol (HTTP) Bilgileri
BİLGİ	N/A	50344	Eksik veya İzin Veren Content-Security-Policy frame-ancestors HTTP Yanıt Başlığı
BİLGİ	N/A	50345	Eksik veya İzin Veren X-Frame-Options HTTP Yanıt Başlığı
BİLGİ	N/A	11219	Nessus SYN tarayıcı
BİLGİ	N/A	19506	Nessus Tarama Bilgileri
BİLGİ	N/A	209654	İşletim Sistemi Parmak İzleri Tespit Edildi
BİLGİ	N/A	11936	İşletim Sistemi Tanımlaması
BİLGİ	N/A	206982	QUIC Hizmet Tespiti
BİLGİ	N/A	56984	Desteklenen SSL/TLS Sürümleri
BİLGİ	N/A	10863	SSL Sertifika Bilgileri
BİLGİ	N/A	21643	Desteklenen SSL Şifre Paketleri
BİLGİ	N/A	57041	Desteklenen SSL Perfect Forward Secrecy Şifre Paketleri
BİLGİ	N/A	94761	SSL Kök Sertifika Yetkilisi Sertifika Bilgileri
BİLGİ	N/A	22964	Hizmet Tespiti
BİLGİ	N/A	84821	TLS ALPN Desteklenen Protokol Numaralandırması
BİLGİ	N/A	136318	TLS Sürüm 1.2 Protokol Tespiti
BİLGİ	N/A	138330	TLS Sürüm 1.3 Protokol Tespiti
BİLGİ	N/A	10287	Traceroute Bilgileri
BİLGİ	N/A	91815	Web Uygulama Site Haritası

7. Kapsamlı Güvenlik Değerlendirmesi ve Öneriler

7.1. Mevcut Güvenlik Yapısındaki Güçlü Yönler

- **Modern Bulut Teknolojilerinin Etkin Kullanımı:** Sistemin altyapısının büyük ölçüde Amazon Web Services (AWS) üzerinde yapılandırıldığı gözlemlenmiştir. Bu, gelişmiş güvenlik özellikleri, esneklik ve dayanıklılık sunar.
- **Temel Ağ Güvenliği Önlemlerinin Varlığı:** Content Delivery Network (CDN) ve Web Application Firewall (WAF) gibi temel ağ güvenliği mekanizmalarının devrede olduğu tespit edilmiştir.
- **Etkin Port Filtreleme:** Kritik olmayan birçok portun filtrelendiği ("filtered") görülmüştür. Bu, "en az ayrıcalık" prensibine uygun olarak saldırı yüzeyinin daraltıldığını göstermektedir.

7.2. İyileştirme Gerektiren Alanlar ve Ana Risk Faktörleri

- **Geniş ve Yönetimi Zor Alt Alan Adı Yüzeyi (Risk: Orta):** xmpp.*, storage.*, api.*, test.* gibi çok sayıda alt alan adının keşfedilmesi, yönetilmesi gereken toplam saldırı yüzeyinin oldukça geniş olduğunu göstermektedir. Unutulmuş, güncellenmemiş veya zayıf yapılandırılmış bir alt alan adı, tüm organizasyon için bir giriş noktası haline gelebilir.
- **HTTP Strict Transport Security (HSTS) Başlığının Eksikliği (Risk: Orta):** sign.oak.gs alan adında HSTS başlığının gönderilmemesi, kullanıcıları SSL Stripping saldırılarına karşı savunmasız bırakır.
- **DNSSEC İmzasının Aktif Olmaması (Risk: Düşük):** oak.gs için DNSSEC imzalamasının aktif olmadığı görülmüştür. Bu durum, alan adını DNS sahteciliği ve önbellek zehirlenmesi saldırılarına karşı savunmasız hale getirir.
- **E-posta Güvenlik Yapılandırmasında Geliştirme Alanları (Risk: Düşük-Orta):** Temel bir SPF kaydı mevcut olsa da, e-posta sahteciliğine (spoofing) ve kimlik avı (phishing) saldırılarına karşı daha kapsamlı koruma için DKIM ve DMARC kayıtlarının eksik veya sıkı olmayan politikalarla yapılandırılması gerekmektedir.

7.3. Genel Güvenlik Önerileri

- **Kapsamlı Alt Alan Adı Yönetimi:** Tüm aktif alt alan adlarının düzenli olarak güncellenen bir envanterini oluşturun. Artık kullanılmayan veya gereksiz hale gelmiş alt alan adlarını ve DNS kayıtlarını kaldırın.
- **DNS Güvenliğini Artırın:** oak.gs ve önemli alt alan adları için DNSSEC'i etkinleştirin. Mevcut SPF kaydına ek olarak DKIM ve DMARC kayıtlarını doğru ve sıkı politikalarla yapılandırın.
- **Uygulama Güvenliği Testlerini Yaygınlaştırın:** www.oak.gs ve diğer tüm alt alan adları üzerinde düzenli olarak kapsamlı web uygulama sızma testleri gerçekleştirin.
- **Etkin İzleme ve Yama Yönetimi:** Tüm kritik sistemler için merkezi loglama (günlük kaydı) ve güvenlik izleme (SIEM vb.) mekanizmaları kurun. Kullanılan tüm yazılımlar, kütüphaneler ve işletim sistemleri için düzenli bir yama yönetimi süreci işletin.

Disclosures

Orta Seviye Riskler

- **Geniş Saldırı Yüzeyi:** Çok sayıda alt alan adının (xmpp.*, sentry.* vb.) keşfedilmesi, yönetilmesi gereken saldırı yüzeyini genişletmekte ve unutulmuş, güncellenmemiş veya zayıf yapılandırılmış sistemler aracılığıyla risk oluşturmaktadır.
- **HSTS Başlığı Eksikliği:** sign.oak.gs alt alan adı, HTTPS üzerinden hizmet vermesine rağmen Strict-Transport-Security (HSTS) başlığını göndermemektedir. Bu durum, kullanıcıları SSL Stripping gibi ortadaki adam (Man-in-the-Middle) saldırılarına karşı savunmasız bırakabilir.

Düşük-Orta Seviye Riskler

- **Eksik Güvenlik Başlıkları (Clickjacking Riski):** sign.oak.gs üzerinde, sitenin başka bir web sitesi içinden <iframe> ile çağrılmasını engelleyen X-Frame-Options veya Content-Security-Policy başlıkları eksiktir. Bu, kullanıcıların farkında olmadan istemedikleri eylemleri gerçekleştirmesine neden olabilecek clickjacking saldırılarına zemin hazırlayabilir.
- **Yetersiz E-posta Güvenlik Yapılandırması:** Temel bir SPF kaydı mevcut olsa da , e-posta sahteciliğine (spoofing) ve kimlik avı (phishing) saldırılarına karşı daha güçlü koruma sağlayan DKIM ve DMARC kayıtları eksiktir veya sıkı yapılandırılmamıştır.

Düşük Seviye Riskler

- **DNSSEC Eksikliği:** Ana alan adı olan oak.gs için DNS Güvenlik Eklentileri (DNSSEC) imzalaması aktif değildir. Bu durum, sistemi DNS sahteciliği (spoofing) ve önbellek zehirlenmesi (cache poisoning) saldırılarına karşı teorik olarak savunmasız bırakır.

Olumlu Bulgular (Zafiyet Tespit Edilmeyen Alanlar)

- Yapılan testlerde sign.oak.gs üzerinde kritik SSL/TLS zafiyetleri (Heartbleed gibi) , SQL Injection ve hassas dosyalara (WEB-INF, .env vb.) veya bulut metadata servislerine yetkisiz erişim gibi önemli zaafiyetler **tespit edilmemiştir**. Bu, sistemin bu saldırı vektörlerine karşı güvenli olduğunu gösteren olumlu bir bulgudur.

Participant	Training Institution
Haydar Can Kotanoglu	Oak Academy