Sunum Adı:
Çevrimiçi Web Zayıflık Tarama Platformu

<-- Hazırlayan: Ali Ekber KARA-->

Sunum Akışı

1. **Problem**
2. **Öz**
3. **Giriş**
4. **Literatür Taraması**
5. **Sonuç**
6. **Önerilen Çalışmalar**

Problem

- **Gün geçtikçe gelişen teknolojiyle birlikte siber saldırıların artması**
- **Web zafiyeti tarama araçlarının kullanımının kolaylaştırılması**
- **Web zafiyeti tarama araçlarının tarama kapsamının genişletilmesi**

Çevrimiçi Web Zayıflık Tarama Platformu Nedir?

Çevrimiçi web zayıflık tarama platformu, bir web sitesini veya uygulamayı güvenlik açıkları için taramak için kullanılan bir yazılımdır. Bu platformlar, farklı tarama araçlarını tek bir platformda birleştirerek, web sitesini kapsamlı bir şekilde taramayı ve güvenlik açıklarını tespit etmeyi kolaylaştırır.

Çevrimiçi web zayıflık tarama platformları, web siteleri ve uygulamalar için önemli bir güvenlik önlemidir. Bu platformlar, web sitelerini ve uygulamaları olası saldırılara karşı korumaya yardımcı olur.

Önemi ve Özgün Değeri

Çevrimiçi web zayıflık tarama platformları, web siteleri ve uygulamaların güvenlik açıklarını tespit etmek için kullanılan yazılımlardır. Bu platformlar, farklı tarama araçlarını tek bir platformda birleştirerek, web sitelerini ve uygulamaları kapsamlı bir şekilde taramayı ve güvenlik açıklarını tespit etmeyi kolaylaştırır.

Yapılan literatür taramalarında incelenen Pentest Tools, Zenmap vb. modellere bakıldığında, pasif veya aktif tarama için kullanılan NMAP Scanner, Google Hacking, Domain Finder, Subdomain Finder, TCP Port Taraması, XSS Scanner, SQLi Scanner, Website Vulnerability Scanner, Network Vulnerability Scanner vb. bazı tarama modüllerini içerisinde bulundurduğu gözlemlenmiştir. Ancak Acunetix, Tenable veya OpenVAS gibi sistemlerin kurumlara yönelik olduğu, son kullanıcıya yönelik olsa bile çok pahalı ücretlerle piyasaya sunulduğu görülmektedir. Ücretsiz olan versiyonlarının ise çok daha az modüle sahip olduğu veya modüllerin az sayıda parametrelerle taramalar yaptığı anlaşılmıştır. Ayrıca tarama bulgularının son kullanıcıya gösterilmesinde hem düzensiz bir rapor oluşturması hem de sunulan önerilerin yetersiz olduğu görülmektedir.

İçerisinde bulunduracağı daha fazla tarama aracı veya modül ile bulgu sonuçlarına göre ihtimal zafiyetlere göre CVE numarası göstermesi, zafiyetlerin önlenmesi ile alakalı olarak çeşitli çözüm önerileri sunması ve literatürde bulunan modellere göre open source bir kaynak olması projeyi özgün bir değer olarak bir adım öne taşımaktadır.

Amaç ve Hedef

Araştırma kapsamında literatürde bulunan port tarama, web tarama, dizin tarama, SQL Injection taraması ve XSS taraması gibi farklı tarama araçları bir araya getirilerek bir platform oluşturulacaktır. Geliştirilecek olan platformun literatürde önerilen Web Zafiyet Tarama Platformu modellerine göre daha detaylı, güçlü ve çevrimiçi olarak çalışabilen olması hedeflenmektedir. Ayrıca içerisinde Türkçe dil desteğinin de bulunması ülke bazında ürünü bir adım öne taşımaktadır. Araştırma sonrasında Türkiye'ye dönülmesine mutabık geliştirilen Web Zafiyet Tarama Platformunun milli teknolojimize önemli bir katkı sağlayacak olan milli bir ürün haline dönüştürülmesi ve ülkemize uluslararası pazarda önemli bir nitelik kazandırması için gerekli proje başvurularının yapılması amaçlanmaktadır.

Kullanılan Yazılımlar


Flask


Bootstrap 5


Jinja


ubuntu

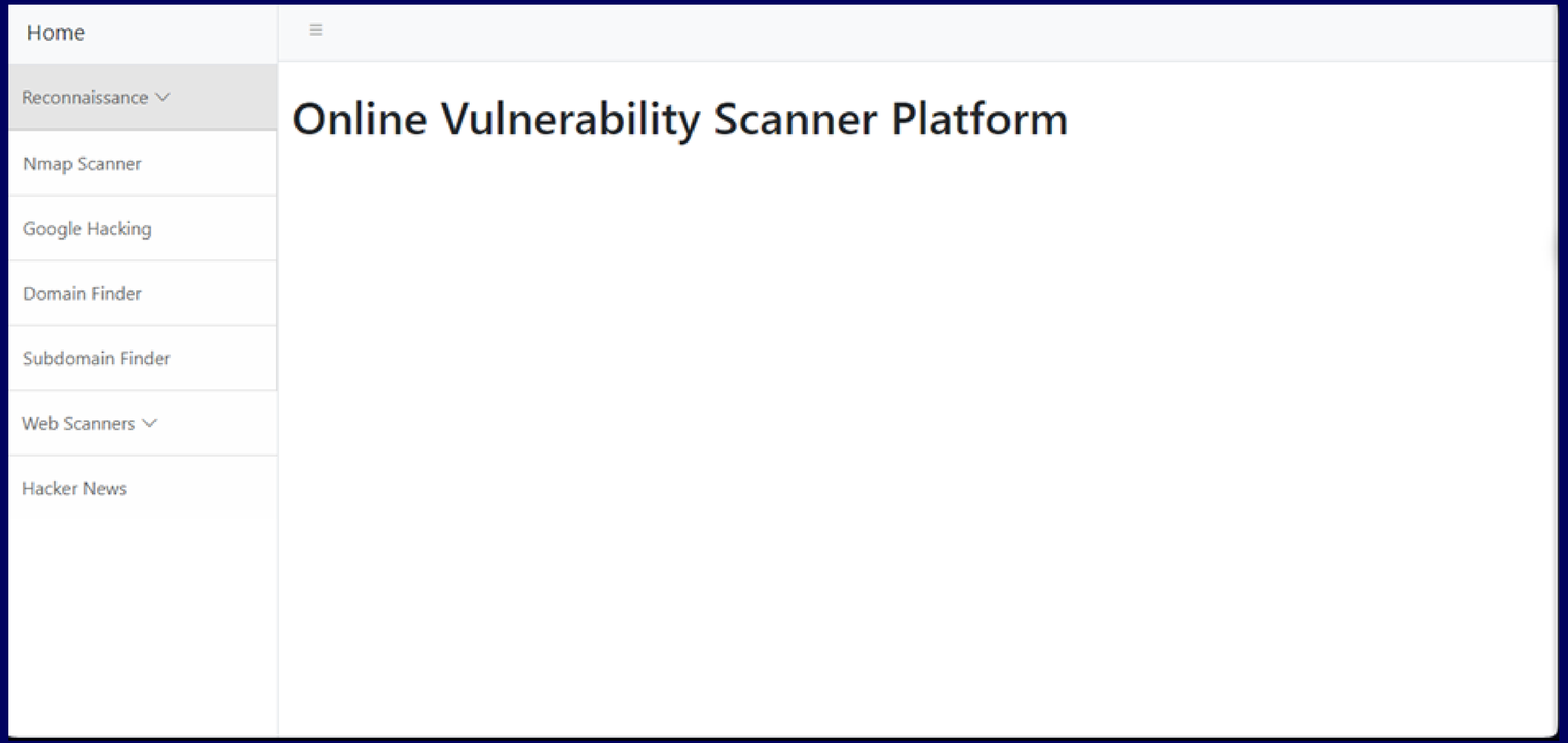

NMAP


Subfinder

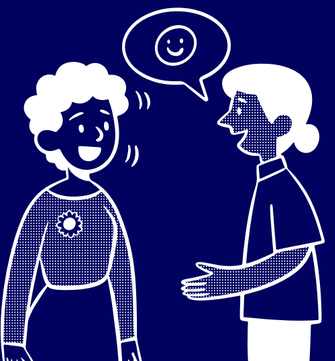
Uygulama

Projenin genel tasarımı yapılıp taslak bir proje oluşturulmuştur. Proje tasarımında HTML, CSS, Bootstrap 5 ve Javascript kullanılmıştır. Projenin arka planında ise Flask kullanılmıştır.

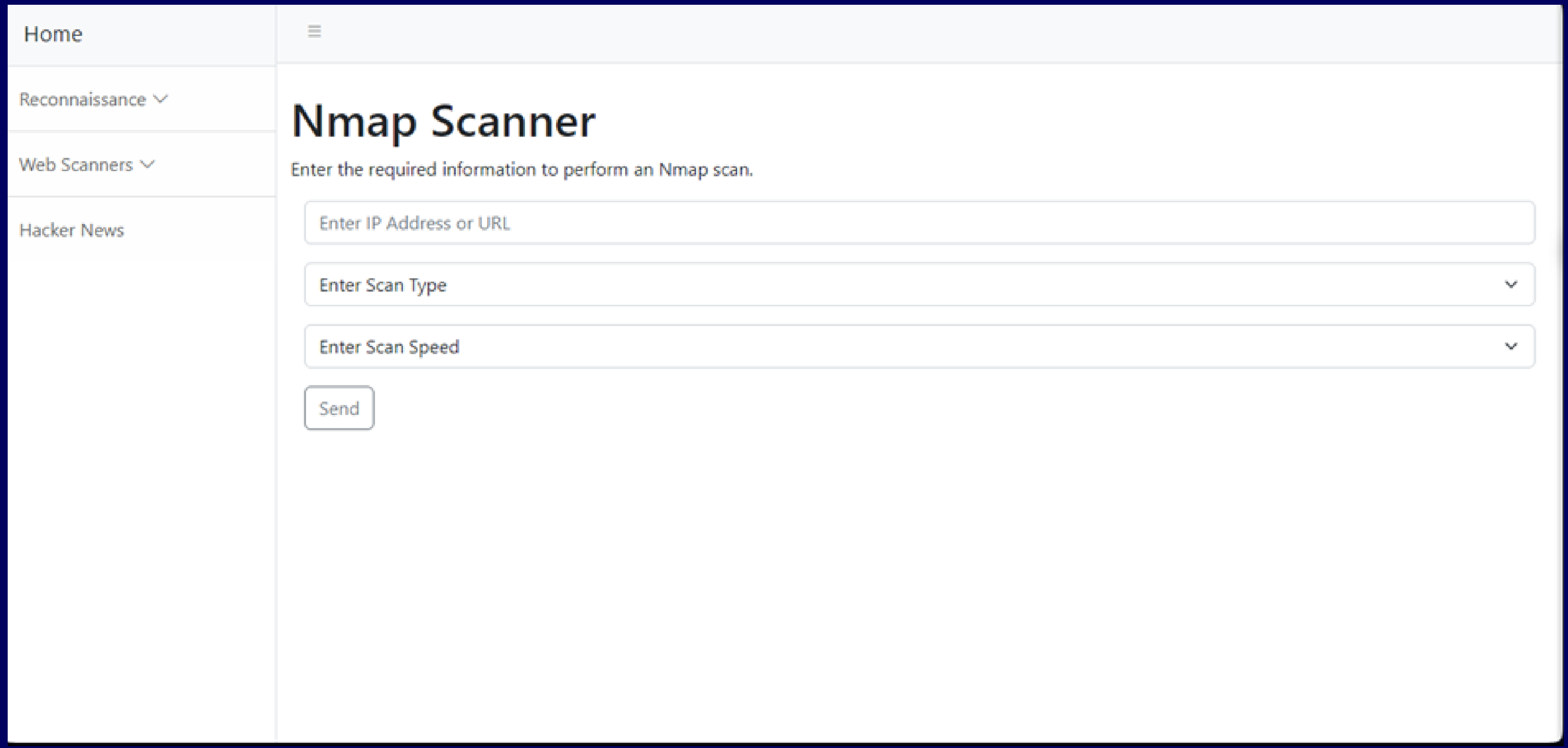
Kullanılacak olan modüllerin yerleştirilmesinde Bootstrap 5’ de bulunan Collapse yapısı kullanılarak menü kısmının daha az alan kaplaması planlanmıştır.


Home
Reconnaissance
Nmap Scanner
Google Hacking
Domain Finder
Subdomain Finder
Web Scanners
Hacker News
Online Vulnerability Scanner Platform

Proje planına uygun olarak Pasif Tarama olarak adlandırılan Keşif (Reconnaissance) kategorisi oluşturulmuş bu kategori içerisinde Nmap Scanner, Google Hacking, Domain Finder ve Subdomain Finder modülleri eklenmiş olup gerekli yazılımları yapılmıştır. Ayrıca web üzerinde yapılacak SQL Injection Detection ve XSS Detection modülleri için de Web Scanner kategorisi oluşturulmuştur. Bu kategorilerin dışında site içerisinde Siber Güvenlik ile alakalı güncel haberlere ulaşabileceğimiz bir bölümde oluşturulmuştur. Aşağıda yapılan modüllerin açıklamaları, yapılış şekilleri ve kullanılan araçlar yer almaktadır.



Nmap Scanner


Home
Reconnaissance
Web Scanners
Hacker News
Nmap Scanner
Enter the required information to perform an Nmap scan.
Enter IP Address or URL
Enter Scan Type
Enter Scan Speed
Send

Bu modül Linux sistemlerinde Siber Güvenlik Uzmanlarının sıklıkla kullandığı Nmap aracının online versiyonu olarak düşünülmüş ve bu kullanıcıya yönelik bir hale getirilmiştir. Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. İsmini Network Mapper'in kısaltmasından almaktadır. Ağ yöneticileri Nmap'i sistemlerinde hangi cihazların çalıştığını belirlemek, mevcut ana makineleri ve sundukları hizmetleri keşfetmek, açık bağlantı noktaları bulmak ve güvenlik risklerini taramak için kullanırlar. Nmap, yüz binlerce cihazı ve alt ağı kapsayan geniş ağların yanı sıra tek ana bilgisayarı izlemek için kullanılabilir.

Projede yer alan modül, Ubuntu Server üzerinde Nmap aracına 10 farklı tarama türü ve 5 farklı tarama hızı parametreleri ile birleştirerek Python’ da bulunan “sh” modülü kullanılarak çalıştırılmasını ve bulguları web sitesi üzerinde düzenli bir şekilde gösterilmesini sağlamaktadır.

PORT	STATE	SERVICE	VERSION	SCRIPT
21/tcp	open	ftp		
25/tcp	open	smtp		
80/tcp	open	http		
110/tcp	open	pop3		
143/tcp	open	imap		
443/tcp	open	https		
8008/tcp	open	http		
8010/tcp	open	xmpp		

OS Guesses

iPXE 1.0.0+ (100%)

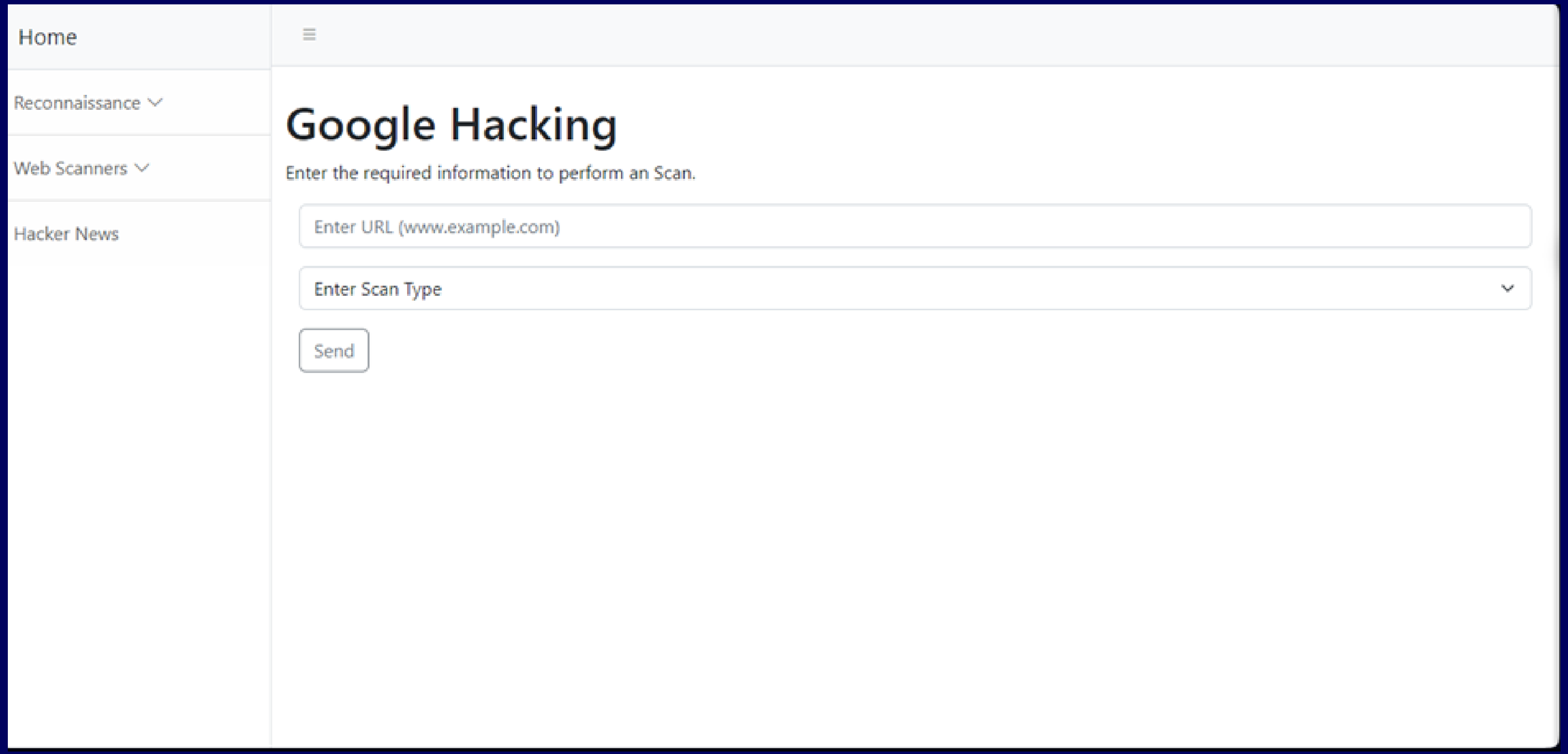
Tomato 1.28 (Linux 2.4.20) (100%)

Tomato firmware (Linux 2.6.22) (100%)

Sony Ericsson U8i Vivaz mobile phone (100%)

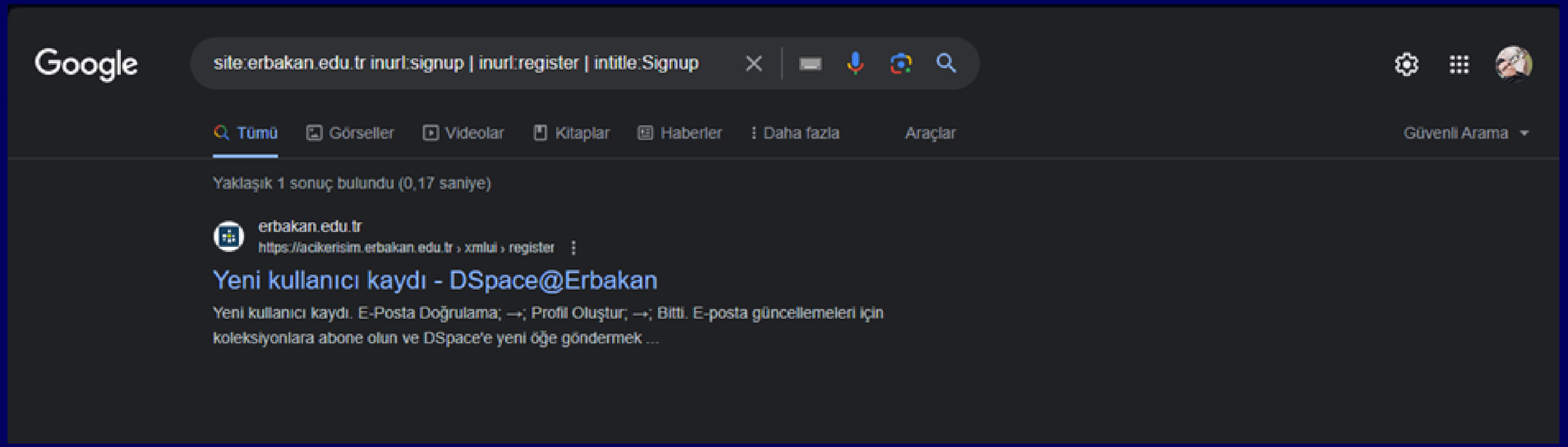
Nmap taraması sonucunda 6 farklı bilgi verilmektedir. Taranan portlar, portların açık, kapalı veya filtreli olması durumları, service bilgisi, version taraması yapılmışsa version bilgileri, NSE Taraması yapılmışsa script bilgileri ve İşletim Sistemi taraması sonunda işletim sistemi bilgileri yer almaktadır.

Google Hacking


Home
Reconnaissance
Web Scanners
Hacker News
Google Hacking
Enter the required information to perform an Scan.
Enter URL (www.example.com)
Enter Scan Type
Send

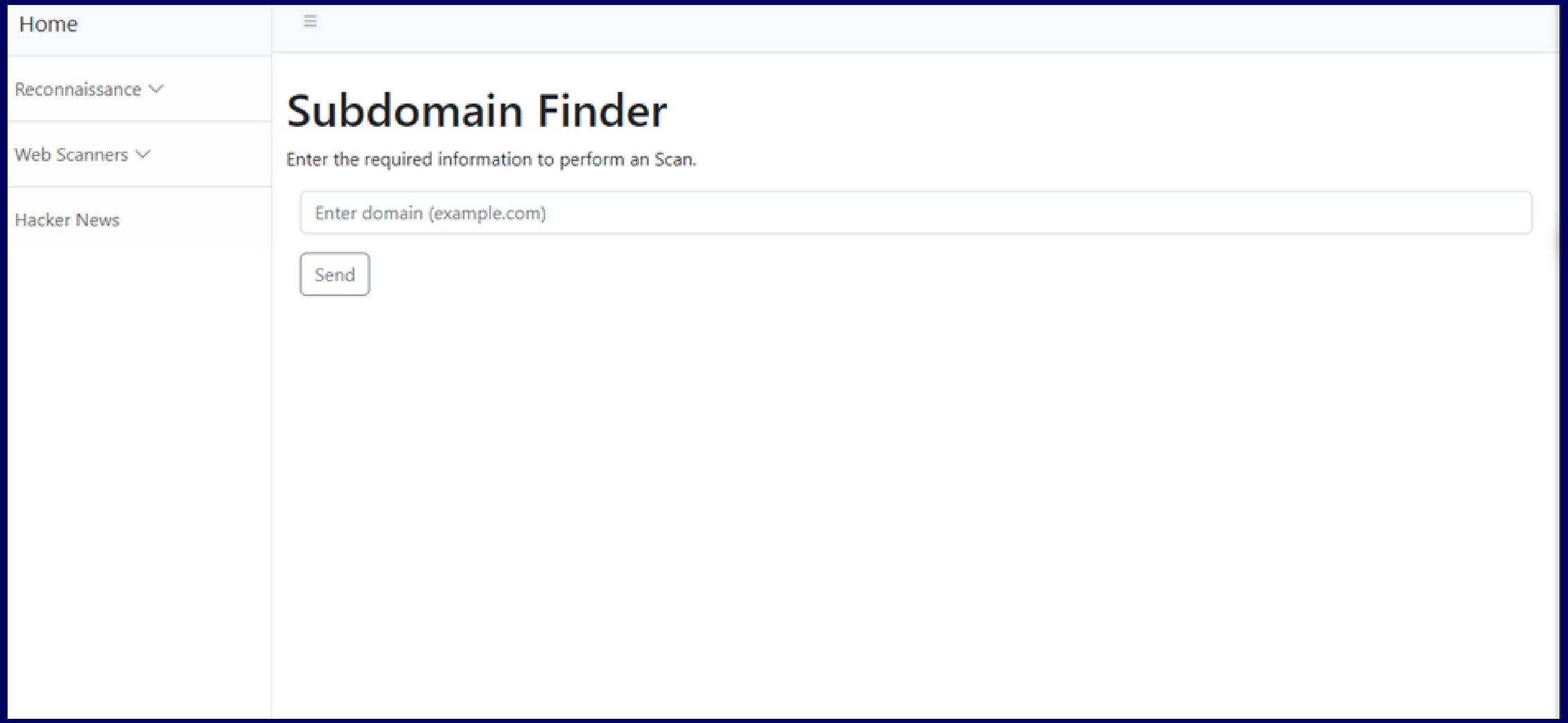
Bu modül, 18 farklı parametre ile Google arama motorunda bir site veya kişi hakkında Google arama sorguları ile verilere hızlı bir şekilde ulaşmamızı sağlayabilen ve sonuçları Google üzerinde karşımıza çıkaran bir modüldür.

Google Hacking kullanılarak web sunucularının içine girmeyi kolaylaştıracak tutunma noktaları, kullanıcı isimlerinin bulunduğu dosyaları, oldukça hassas ve gizli dosyaların bulunduğu web dizinlerini, web sunucu yapılarını, zafiyetli sunucular ile dosyaları, hata mesajlarını (sistem ya da uygulama kurulum hatalarından sızan hassas veriler), şifre ya da kullanıcı adı dışında başka ilginç ve hassas verileri içeren dosyaları, birçok parolayı barındıran dosyaları, hassas online alışveriş bilgilerini, internete bağlı yazıcı, kamera ve diğer cihazları, başka sitelerde yayınlanmış zaafiyet ihbarları ve güvenlik açıklıkları, yedekleme (backup) dosyaları ve veritabanı yedekleri, hata çıktıları ve kurulum açıklıkları gibi oldukça ilginç sonuçlar bulunabilmektedir.



Google Hacking ile bir arama yapıldığında çeşitli dorklar kullanılarak Google'ın indekslediği sonuçlar ekrana gelmektedir.

Subdomain Finder


Home
Reconnaissance
Web Scanners
Hacker News
Subdomain Finder
Enter the required information to perform an Scan.
Enter domain (example.com)
Send

Bu modül, Linux sistemlerinde sıklıkla kullanılan “Sublist3r” aracı kullanılarak elde edilen bulguların web sitesine düzenli bir şekilde aktarılması sağlanmaktadır.

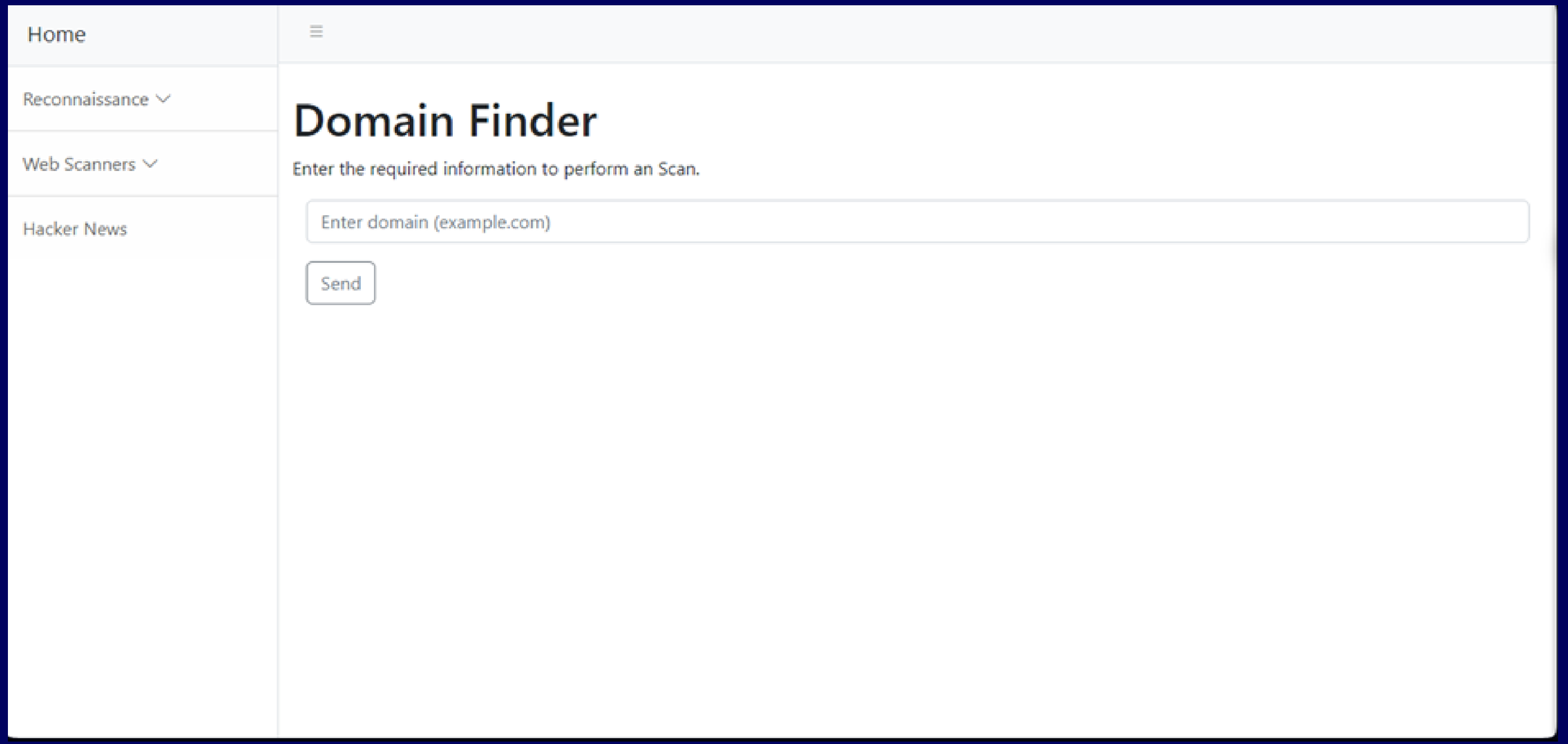
Sublist3r, Python'da tasarlanmış bir araçtır ve web sitelerinin alt alanlarını numaralandırmak için OSINT kullanır. Test edenlerin, hedefleri olan bir alan için alt alan adlarını toplamasına ve toplamasına yardımcı olur. Doğru sonuçları almak için Subliste3r, Google, Yahoo vb. gibi birçok arama motorunu ve hatta Netcraft, Virustotal vb. araçları kullanır.

→ Output

SUBDOMAIN
www.macvendors.com
api.macvendors.com
www.api.macvendors.com
staging.api.macvendors.com
app.macvendors.com
octane.macvendors.com
staging.macvendors.com
api.staging.macvendors.com
app.staging.macvendors.com
status.macvendors.com
www2.macvendors.com

Subdomain Finder taraması sonucunda elde edilen örnek subdomainler gösterilmektedir.

Domain Finder


Home
Reconnaissance
Web Scanners
Hacker News
Domain Finder
Enter the required information to perform an Scan.
Enter domain (example.com)
Send

Bu modül, crt.sh sitesinden herkese açık olan sertifika kayıtlarının çekilmesi ve içerisinden subdomainlerin taranıp sonuçların rapor şeklinde sunulmasıyla hazırlanmış bir modüldür.

Alan adları dünya çapında çeşitli şirketlere tahsis edilen İnternet kaynaklarıdır. Bir şirket, işin çeşitli amaçları için (örneğin ana web sitesi, müşteri portalı, tedarikçi uygulamaları vb.) kullanılabilecek birden fazla alan adına sahip olabilir.

Bir şirketin sahip olduğu tüm alan adlarını bulmak, sızma testinin bilgi toplama aşamasında veya hata tespit faaliyetleri sırasında önemli bir adımdır. Bunun nedeni, bu ilişkili alan adlarının, ana alanda bulunanlardan daha az güvenli olan şirket kaynaklarını açığa çıkarabilmesidir.

Sonuç olarak, saldırı yüzeyini ek alanlardan keşfetmek, sızma testi veya hata ödülü sırasında verimli bir yol olabilir.

→ Output

DOMAIN
facebook.com
thefacebook.com
china--facebook.com
tihonoff@facebook.com
news--facebook.com
the--facebook.com
f--facebook.com

Domain Finder taraması sonucunda o alan adına ait sertifikalardan elde edilen başka alan adları gösterilmektedir.

WAF Detection

WAF (Web Application Firewall) Detection

Enter the required information to perform an Scan. Make sure the domain is https.

Enter a url (https://example.com)

Send

Bu modül, Linux sistemlerinde sıklıkla kullanılan “wafw00f” aracı kullanılarak elde edilen bulguların web sitesine düzenli bir şekilde aktarılması sağlanmaktadır.

WAF (Web Application Firewall), basit olarak, bir web uygulaması ile internet arasındaki http trafiğini filtreleyerek ve izleyerek web uygulamasının korunmasına yardımcı olur.

Wafw00f aracı da işte web uygulamalarınızı koruyan çözümlerin olup olmadığını ve varsa WAF adını ve üreticisini bulmaya yaramaktadır. Aşağıda çalışma mantığı gösterilmektedir.

- **Normal bir http isteği gönderir ve yanıtı analiz eder.**
- **Başarılı olamazsa bir dizi (potansiyel kötü amaçlı) http isteği gönderir ve hangi WAF uygulaması olduğunu bulmak için basit bir mantık kullanır.**
- **Bu adımda başarılı olmazsa, daha önce döndürülen yanıtları analiz eder ve bir WAF veya güvenlik çözümünün saldırılarımıza aktif olarak yanıt verip vermediğini tahmin etmek için başka bir basit algoritma kullanır.**

→ Output

URL	FIREWALL	COMPANY
https://siberkuvvet.com	Cloudflare	Cloudflare Inc.

WAF Detection taraması sonucundan elde edilen WAF adı ve üretici bilgileri gözükmektedir.

Hacker News

Hacker News

Cryptominers Targeting Misconfigured Apache Hadoop and Flink with Rootkit in New Attacks

Fri, 12 Jan 2024 13:26:00 +0530

Cybersecurity researchers have identified a new attack that exploits misconfigurations in Apache Hadoop and Flink to deploy cryptocurrency miners within targeted environments. "This attack is particularly intriguing due to the attacker's use of packers and rootkits to conceal the malware," Aqua security researchers Nitzan Yaakov and Assaf Moragsaidin an analysis published earlier...

Act Now: CISA Flags Active Exploitation of Microsoft SharePoint Vulnerability

Fri, 12 Jan 2024 12:05:00 +0530

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) hasaddeda critical security vulnerability impacting Microsoft SharePoint Server to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation. The issue, tracked asCVE-2023-29357(CVSS score: 9.8), is a privilege escalation flaw that could be exploited by an attacker to gain...

Bu modül siber güvenlik dünyasından güncel haberleri almak adına “thehackernews.com” gibi sitelerin RSS yapılarından çekilen veriler kullanılarak tasarlanmıştır. RSS, web sitesine her yeni eklenen içeriğin kolaylıkla takip edilmesini sağlayan bir web sayfası bildirimcisidir. İnternette bir konuda her güncellemeyi almak zordur. Her gün aynı web sitelerini ziyaret etmek yerine, bu sitelerdeki başlıkları toplamak ve bunları doğrudan bilgisayarınıza veya uygulamaya otomatik olarak yüklemek ya da web sitesinde görüntülenmesini sağlamak için RSS’den (Really Simple Syndication) faydalanılabilir.

Sonuç

Çevrimiçi Web Zafiyeti Tarama Platformu projesinde, Nmap Scanner, Domain Finder, Google Hacking, Subdomain Finder, WAF Detection ve Hacker News adlı modüller geliştirilmiştir. Bu modüller, web uygulamalarında bulunan güvenlik açıklarını tespit etmek için kullanılmaktadır.

Proje sonucunda, aşağıdaki sonuçlar elde edilmiştir:

- **Geliştirilen modüller, web uygulamalarında bulunan yaygın güvenlik açıklarını tespit edebilmektedir.**
- **Modüller, otomatik olarak çalışabilmektedir. Bu sayede, web uygulamalarında bulunan güvenlik açıklarının tespiti hızlı ve kolay bir şekilde yapılabilmektedir.**
- **Modüller, kullanıcı dostu bir arayüze sahiptir. Bu sayede, modülleri kullanması kolaydır.**

Proje, web uygulamalarının güvenliğini sağlamak için önemli bir adımdır. Geliştirilen modüller, web uygulamalarının güvenlik açıklarını tespit ederek, bu açıkların saldırganlar tarafından kullanılmasının önüne geçilmesine yardımcı olacaktır.

Gelecek Çalışmalar

Proje kapsamında geliştirilen modüller, gelecekte aşağıdaki geliştirmeler ile daha da güçlendirilecektir:

- **Modüllerin kapsamı genişletilerek, daha fazla güvenlik açığının tespit edilebilmesi sağlanacaktır.**
- **Modüllerin hassasiyeti artırılarak, daha az sayıda yanlış alarm verilmesi sağlanacaktır.**
- **Modüllerin performansı artırılarak, daha hızlı tarama yapılabilmesi sağlanacaktır.**
-

Bu geliştirmeler ile birlikte, web uygulamalarının güvenliğinin sağlanmasına yönelik önemli bir katkı sağlanacaktır.

Sonuç olarak, web zafiyeti tarama platformu geliştirme projesi, web uygulamalarının güvenliğini sağlamak için önemli bir adımdır. Geliştirilen modüller, web uygulamalarının güvenlik açıklarını tespit ederek, bu açıkların saldırganlar tarafından kullanılmasının önüne geçilmesine yardımcı olacaktır.

Kaynaklar

- **https://pentest-tools.com/alltools**
- **https://www.beyaz.net/tr/guvenlik/makaleler/nmap_nedir_ve_nasil_kullanilir.html**
- **https://coderspace.io/sozluk/flask-nedir#:~:text=En%20çok%20kullanılan%2020%20web,çalışır%20ve%20kaynak%20tüketimi%20azdır.**

Teşekkürler

Ali Ekber KARA - Necmettin Erbakan Üniversitesi
Bilgisayar Mühendisliği 4.sınıf