|  |
| --- |
| ***Web Güvenliği Zafiyet Testi Toolları*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Web uygulama güvenliği için Bilgi toplama ve güvenlik açık tespiti için kulanılan; OwaspZAP,Rapidscan,Skipfish,Vooki,Waes,Wapiti,Xsspwn araçlarının kurulumu ve kullanımı hakkında bilgi vereceğim. |

**28.07.2021**

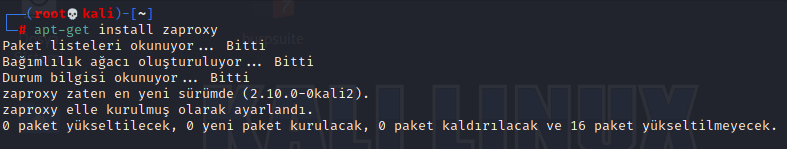
***OWASPZAP(ZAPROXY)***

-Zaafiyet testleri arasında ücretsiz en popüler araçlardandır.Paralı uygulamalar ile performansını karşılaştırdığımızda başa baş gitmektedir.Zaproxy Kali linux sürümlerinde normalde kurulu olarak gelmektedir fakat Kali Linux’un yeni sürümlerinde artık kurulu olarak gelmiyor.

Kurulumu ile başlayalım;

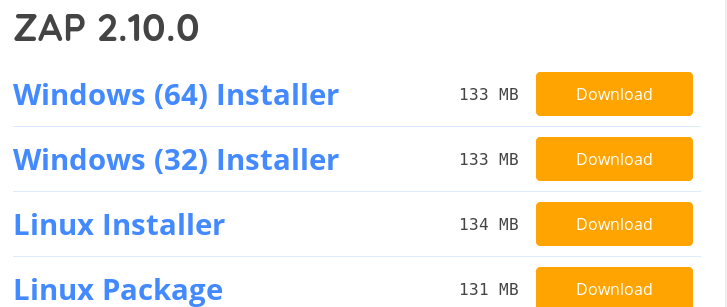
-Kurulu olarak gelmeyen bir sanal makine kullanmaktaysanız.

-Apt-get install zaproxy komutu ile indirme işlemi başlatabilirsiniz.

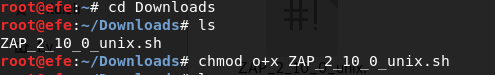


-Benim kullanmış olduğum Linux sürümünde bu kodu çalıştırdığımda hata mesajı ile karşılaştım bu yüzden manuel olarak kurulum işleminide gerçekleştireceğim.

-İlk olarak “zaproxy.org” bağlantısına geçiş yapıyorum ve Download bölümüne geçiyorum.



-Download bölümünden ise “Linux installer” seçeneğinden indirme işlemini başlatıyorum.



-Ardından indirdiğim dosya dizinine geçiş yapıyorum ve “chmod o+x” komutu ile kullanıcılara çalıştırma iznini veriyorum.

C:\Users\ogutk\AppData\Local\Microsoft\Windows\INetCache\Content.Word\3.png

-İşlem sonrasında “ls” komutu ile görüntüleme yaptığım zaman renginin bu şekilde değişmiş olması gerekmektedir.



-Ardından “./” komutu ile yükleme işlemini başlatıyorum.

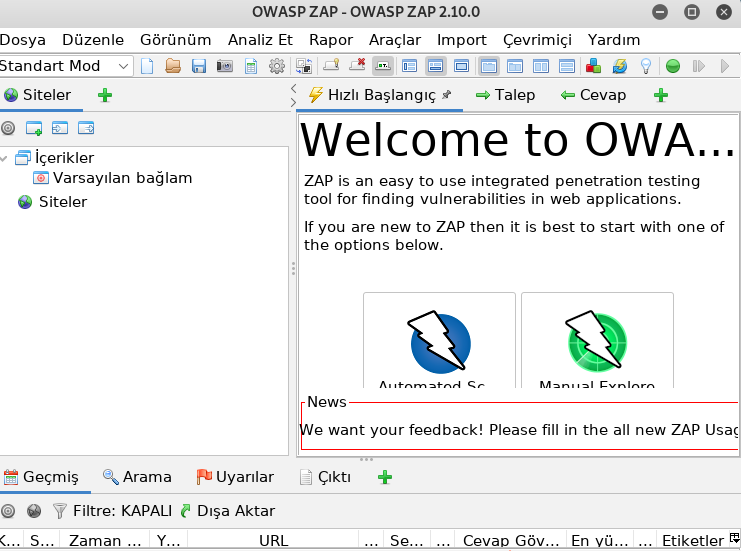


-Komut istemci üzerinden çalıştırma işleminden sonra,Kurulum sihirbazı ekrana gelecektir.Basit bir şekilde kurulum yapıyoruz.

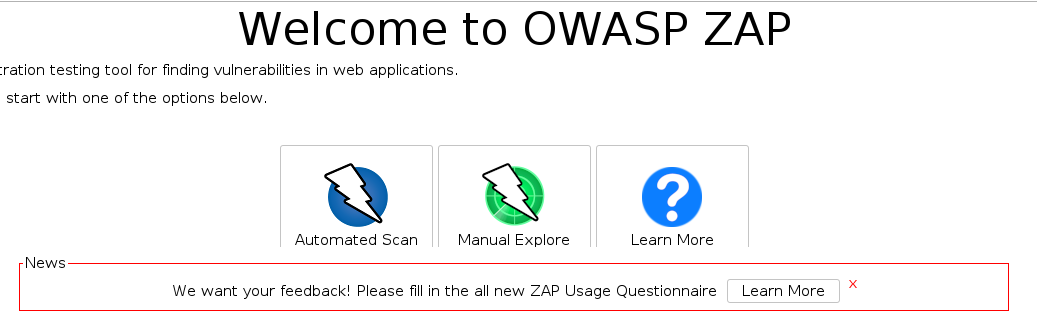


-Linux makinamıza geçiş yaptıktan sonra uygulamalar içerisinde arama yapıyoruz ve başarılı bir şekilde yüklendiğini görüntülüyoruz.

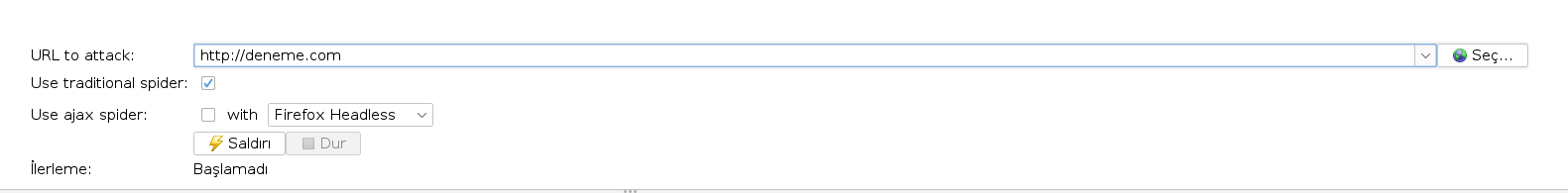
-



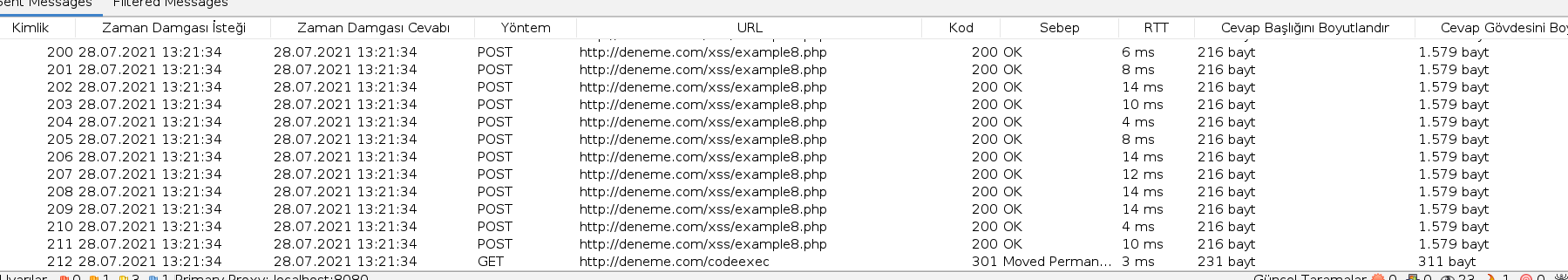
-Uygulama açıldığında bizi böyle bir ekran karşılıyor.Tarama işlemi için manuel ayarlama ve otomatik ayarlama yapabileceğimiz iki adet ayarı vardır.



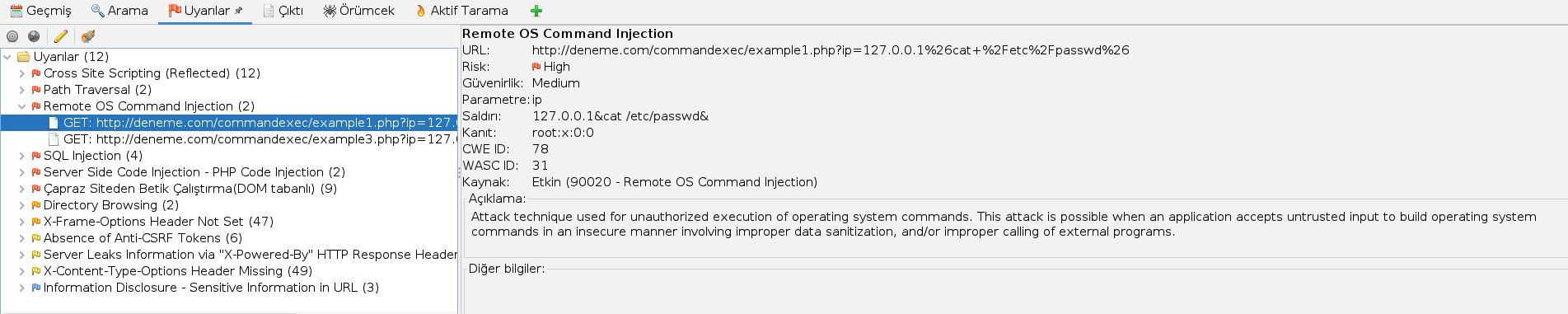
-Otomatik arama butonuna basıyorum.



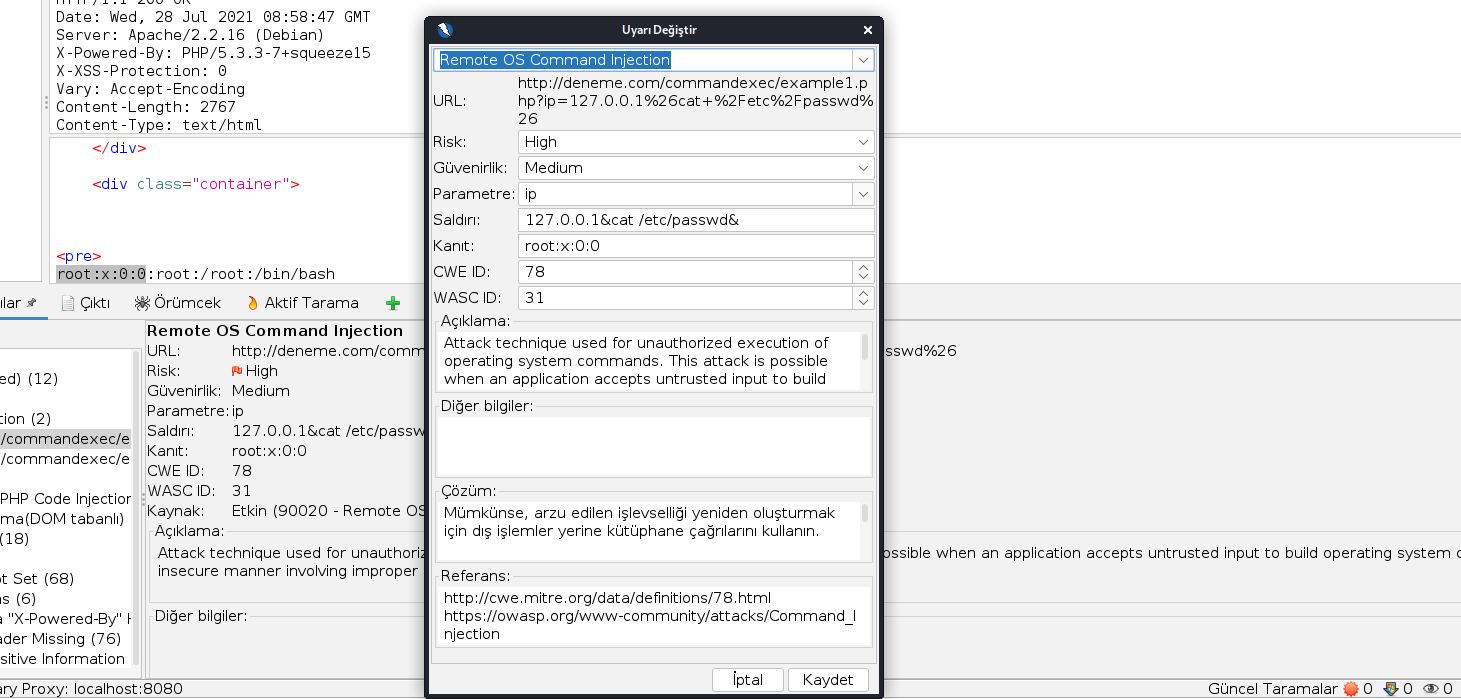
-Ardından açılan sekme üzerinde hangi URL üzerinde işlem yapacaksam buraya ekliyorum ve Saldırı butonu ile işlemi başlatıyorum.



-Tarama işlemini başlattığımda böyle bir ekranla karşılaşıyorum.Burada yapılan tarama işlemlerini görüntüleyebiliyorum.



-İşlem sona erdiğinde tarafıma bu şekilde bir rapor gelecektir.Burada bulmuş olduğu zafiyetleri ve detaylarını görüntüleyebiliyorum.



-Bulduğu zafiyet üzerinde çift tıklama işlemi yaptığımda zafiyet hakkında kullanılan payload,çözüm,açıklama gibi bilgilere erişim sağlayabiliyorum.

***RAPIDSCAN***

-Çok amaçlı bir güvenlik açığı aracıdır.

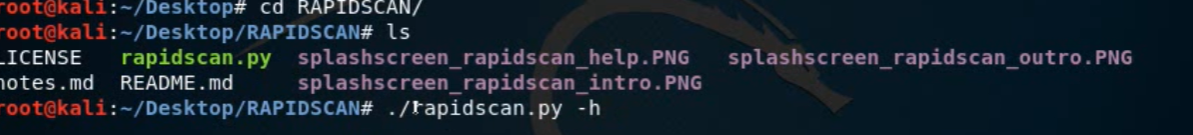
-İçerisinde 10’dan farklı araç bulunmaktadır ve yaklaşık 80 adet arama işlemi gerçekleştirir

-Yapmış olduğum işlemler yaklaşık 2 saat sürmektedir.

Kurulumuna geçersek;



-Git clone üzerinden “<https://github.com/pcdunyasitv/RAPIDSCAN>” bağlantısını kullanarak indirme işlemini başlatabiliriz.



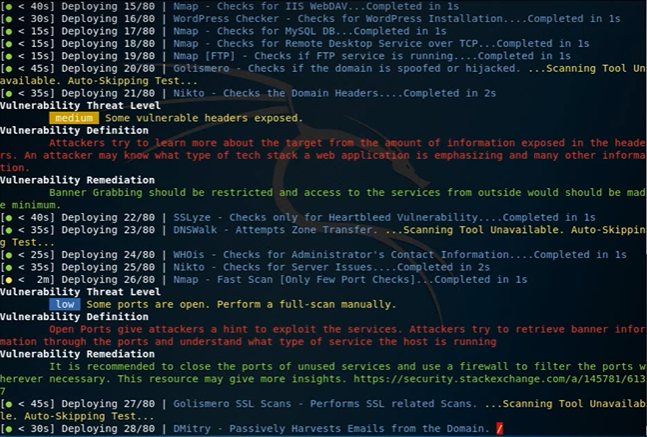
-İndirme işleminin ardından dosya üzerine geçiş yapıyorum ve “./” komutu ile .py uzantılı dosyayı çalıştırıyorum.



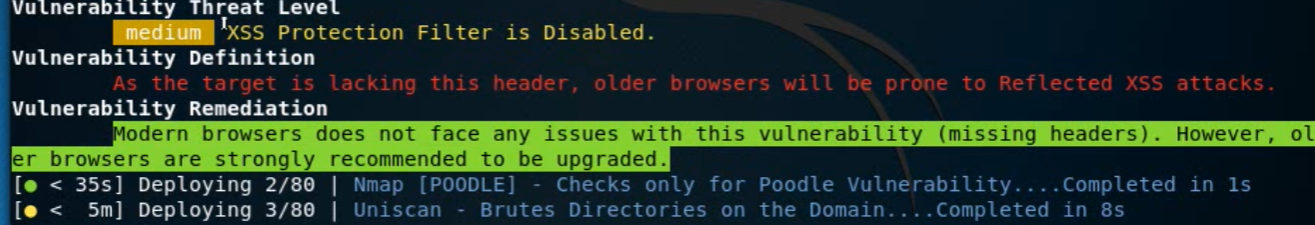
-Program çalıştıktan sonra “-h” parametresi ile program üzerinde kullanabileceğim komutları ve yazım biçimlerini görüntüleyebiliyorum.



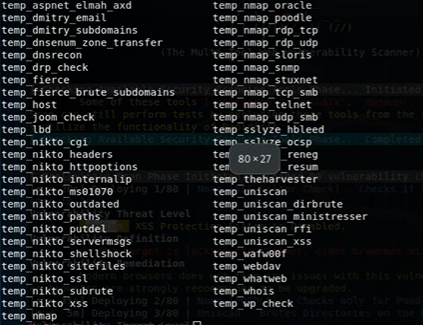
“rapidscantest.com” bağlantısına bir zafiyet testi başlatıyorum.



-İşlem başladıktan sonra takip edebilmemiz için bu şekilde bir tarama ekranı gelir.DDOS saldırısı gibi kapsamlı saldırılarda yaptığı için işlem diğerlerine kıyasla uzun sürer.



-Çok fazla sonuç olduğu için hepsini göstermem mümkün değil fakat uygulama fakat uygulama esnasında birlikte bakacağız.Formatının bu şekilde olduğunu bilmemiz şuan için yeterlidir.

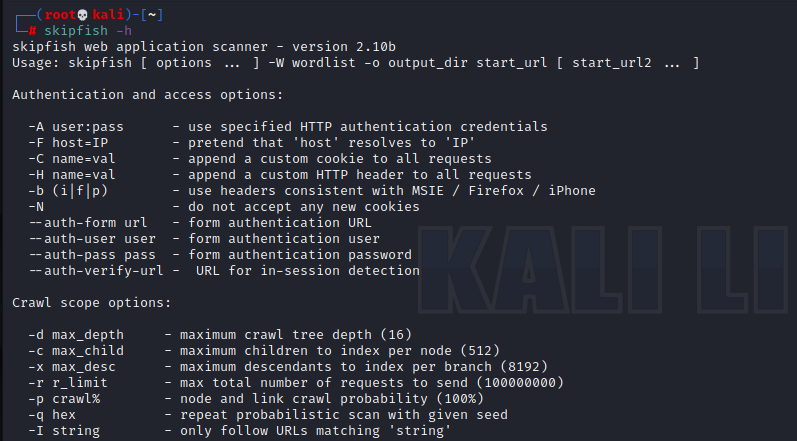


-Ayrıca RAPIDSCAN'in kurulu olduğu dosyanın içerisinde “ls” komutunu çalıştırırsak çıkan sonuçları dosya formatında da görebiliriz.

***SKİPFİSH***

C:\Users\ogutk\AppData\Local\Microsoft\Windows\INetCache\Content.Word\1.png

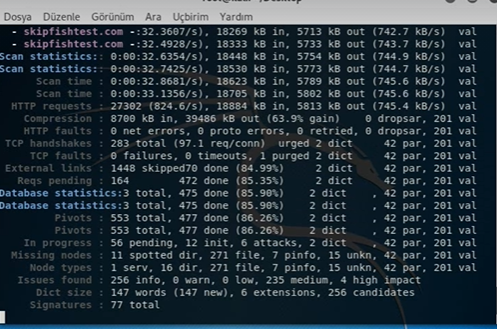
-Çoğu Linux sürümlerinde kurulu olarak gelmektedir.Fakat kurulu olarak gelmediyse “apt-get install skipfish” komutu ile kurulum yapabilirsiniz.



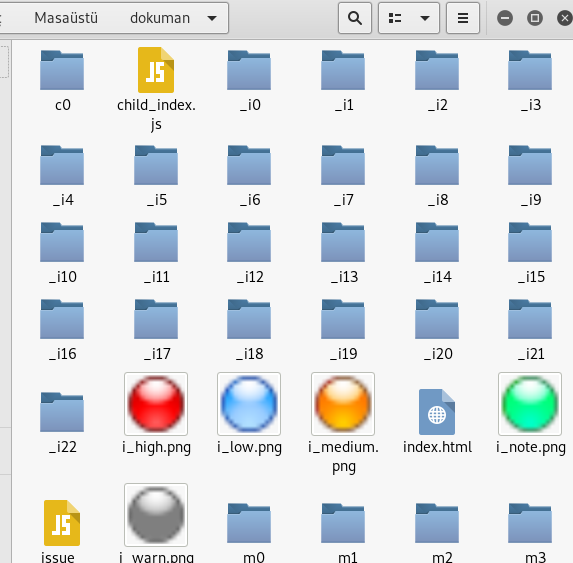
“skipfish –h” komutu ile skipfish aracı ile kullanabileceğimiz komutları ve kullanım formatlarını görüntüleyebiliyoruz.

C:\Users\ogutk\AppData\Local\Microsoft\Windows\INetCache\Content.Word\2.png

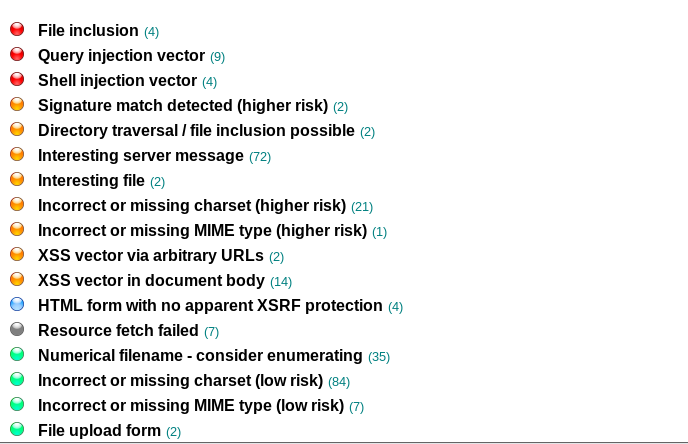
-Kullanım formatı doğrultusunda bir URL’ye zafiyet testi işlemi başlatıyorum. “-o” parametresi ile raporun kaydedileceği dizinin ismini belirtiyorum ve raporu işlemi başlattığım dizine kayıt edecektir.



-Tarama işlemi sırasında bu şekilde bir ekran bizi karşılar ve buradan işlemin akışını kontrol edebiliriz.



-Tarama işlemi bittiğinde dizin olarak kaydedilmiş “sonuç” klasörüne geçiş yapıyorum.Çok fazla klasör olduğunu görüntülüyorum fakat zafiyetleri çok basit bir şekilde “index.html” dosyasını görüntüleyerek elde edebiliyorum.



-“Index.html” dosyasını görüntülediğimde böyle bir tarayıcı sayfası ile karşılaşıyorum ve burada bulmuş olduğu zafiyetleri listeliyor.



-“Shell injection vector” zafiyetini görüntülediğimde bana bulduğu zafiyetleri kullanmış olduğu payload’ı ekleyip URL şeklinde döndürüyor.



-Zafiyet URL’sinin yanında bulunan “Show Trace” butonuna tıkladığımda;Request,Response kullanılan payload gibi bilgilere erişim sağlayabiliyorum.

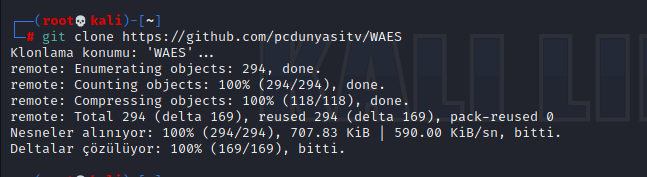
***WAES***

-Linux platformu için tasarlanmış bir web güvenlik zafiyeti aracıdır.

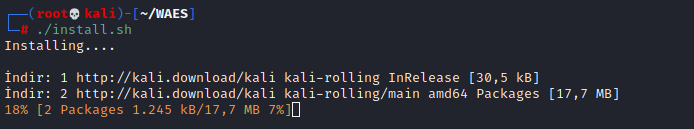
-İçerisinde yaklaşık 10 adet araç vardır.Sırasıyla bu araçları çalıştırıp bize bir rapor hazırlar.

-Yapmış olduğu işlem yaklaşık 15-20 dakika sürmektedir.

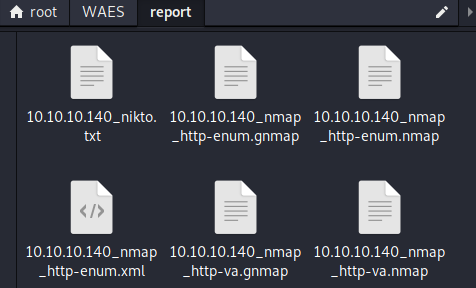
Kurulumuyla başlayalım.



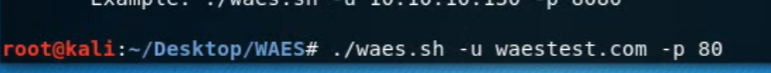
-Git clone üzerinden “https://github.com/pcdunyasitv/WAES” bağlantısını kullanarak indirme işlemini başlatabiliriz.



-İndirme işleminin ardından indirdiğim dosya dizinine geçiş yapıyorum ve “./” komutu ile install.sh uzantılı dosyayı çalıştırıp kurulumu gerçekleştiriyorum.

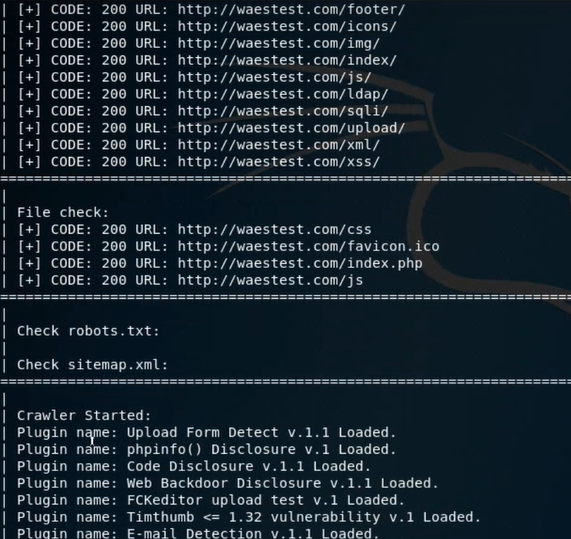


-Waes kurulumundan sonra report dosyaları içerisinde ki dosyalar basic olarak oluşturulmuştur.Karışıklık olmaması için bu dosyaları silmenizi tavsiye ederim.



-Kurulum işlemi tamamlandıktan sonra “./waes.sh – u zafiyettest.com –p 80” komutu ile zafiyet tarama işlemini başlatıyorum.Portun 80 olmasının sebebi HTTP bağlantısının 80.port üzerinden bağlantı sağlamasıdır.

-Sırasıyla 10 araç kullanıp 15-20 dakikalık bir tarama yapıyor.Wafw00f,Nmap gibi scriptler kullanarak port taraması yapıyor.



-Sonuç olarak bize bu şekilde bir rapor döndürür.Oluşturduğu rapor diğer zafiyet testlerinde oluşan raporlara benzemektedir.

***WAPITI***

-Açık kaynak kodlu bir araçtır.

-Kara kutu yöntemi ile sızma testi yapmaktadır.

-Hedef sitenin kaynak kodlarına ulaşmadan sadece link üzerinden tarama yapan bir araçtır.

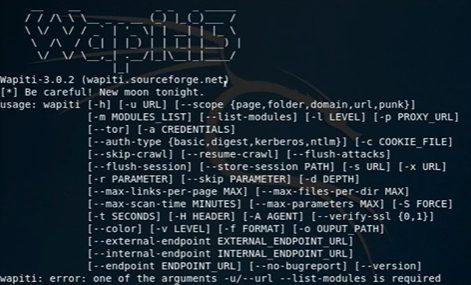
Kuruluma geçelim;



-Git clone üzerinden “https://github.com/pcdunyasitv/WAPITI” bağlantısını kullanarak indirme işlemini başlatabiliriz.



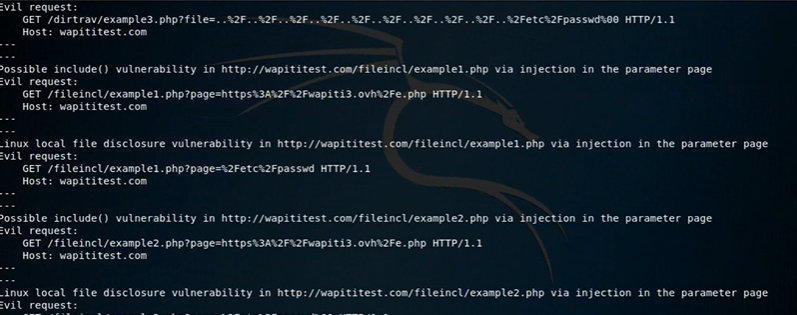
-İndirme işleminin ardından python komutundan yararlanarak kurulumunu gerçekleştiriyoruz.



-Kurulumun ardından uçbirime “Wapiti” yazarak kullanımıyla ilgili bilgi alabiliriz.



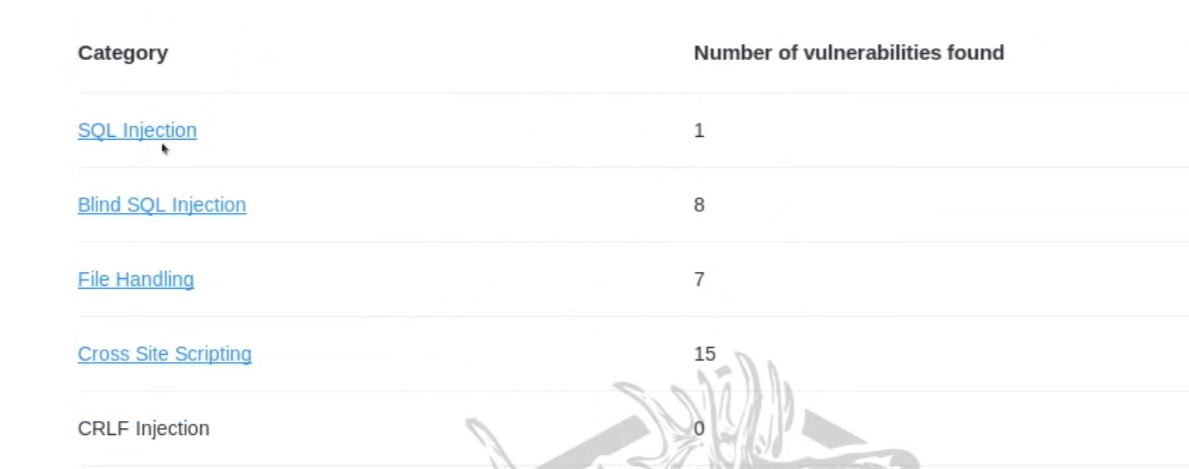
-Uç birim üzerinde “wapiti -u http://site.com/” formatıyla çalışır sonuna mutlaka “ /” koyulmalıdır yoksa işlem başlamaz.



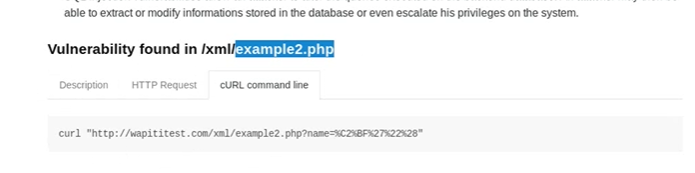
-Yapılan işlemleri bu ekran üzerinden takip edebiliriz.



-Zaafiyet testi bittikten sonra Yapılan işlemlerle ilgili raporu html formatıyla kaydeder ve bu linki raporu incelemek için kopyalıyorum.



-Tarayıcı üzerinde kopyalamış olduğum linki çalıştırıyorum.Bulduğu zafiyetler ve sayılarını tarafıma rapor olarak aktarmaktadır.



-Bulduğu zafiyetlere tıklayıp genişletirsem kullanmış olduğu payload ve Request bilgilerine erişim sağlayabiliyorum.

***VOOKİ***

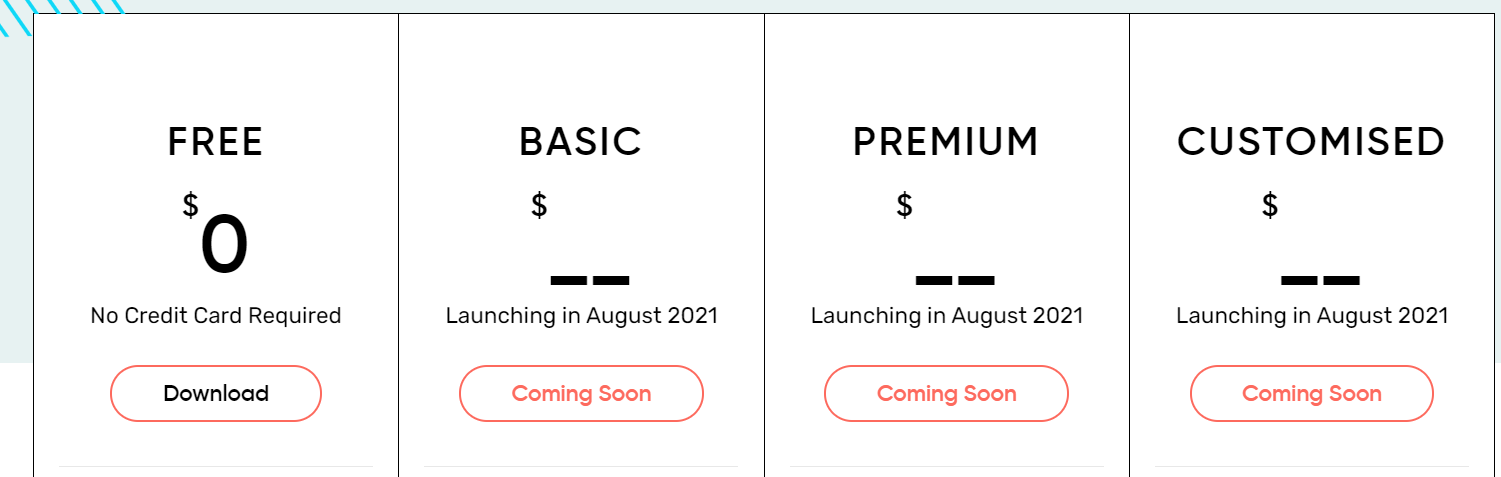
-Hem Windows hem de linux sistemlerinde kullanım sağlanabilir.

-Tamamen ücretsiz bir araçtır.

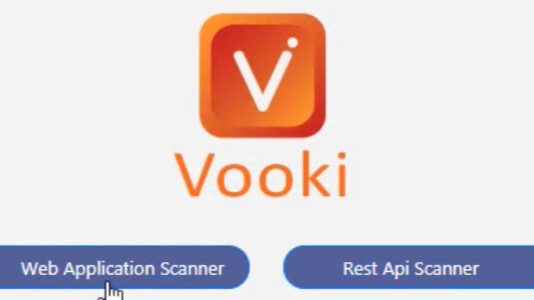
-Bilgi toplama,link tespiti ve zafiyet bulma işlemlerini gerçekleştirir.

-Diğer araçlardan farklı olarak farklı bir IP adresi üzerinden tarama işlemi gerçekleştirilebilir.

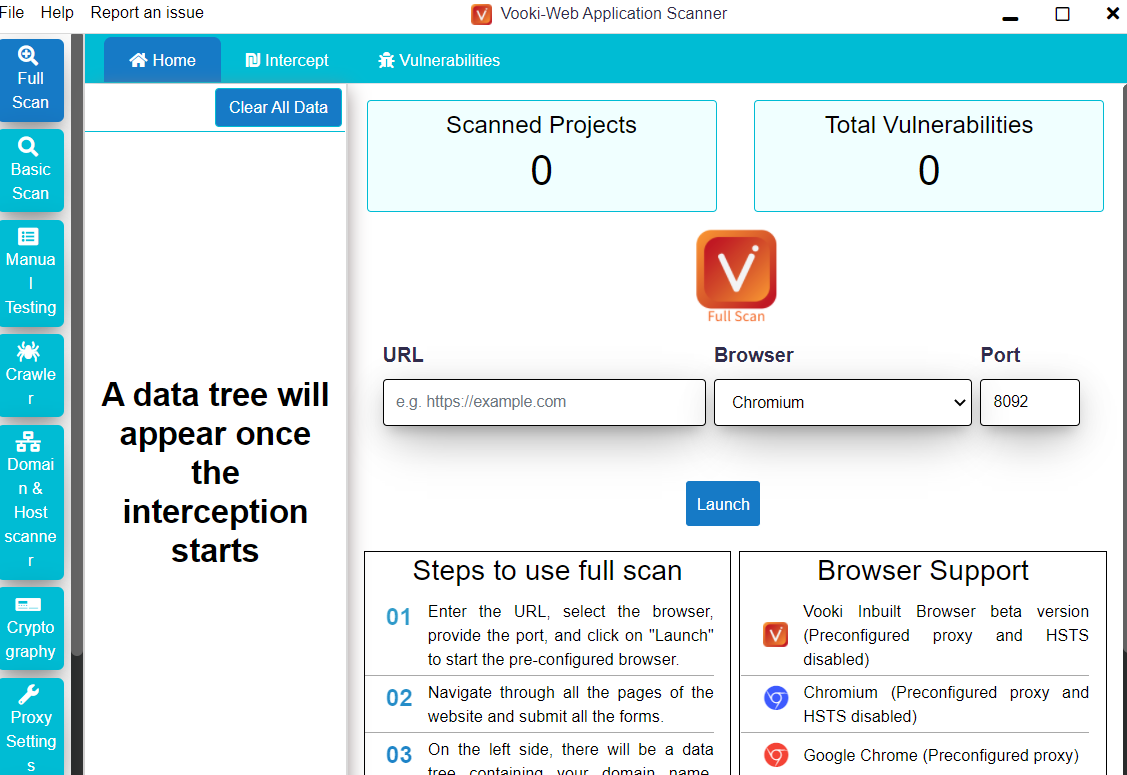
Gelelim kurulumuna;



-"https://www.vegabird.com/vooki/" bağlantısından ücretsiz bir şekilde indirilebilir.



-Kurulumu basit bir şekilde yaptıktan sonra programı açıyorum ve WebApplicationScanner sekmesi ile devam ediyorum.



Uygulama açıldığında bizi böyle bir ekran karşılıyor.Sol tarafta bulunan bar üzerinde ki işlemleri inceleyelim.

-Full-Basic Scan olmak üzere 2 adet tarama şekli vardır.Full olan diğerine kıyasla çok daha uzun sürse de daha kapsamlı bir işlem gerçekleştirmektedir.

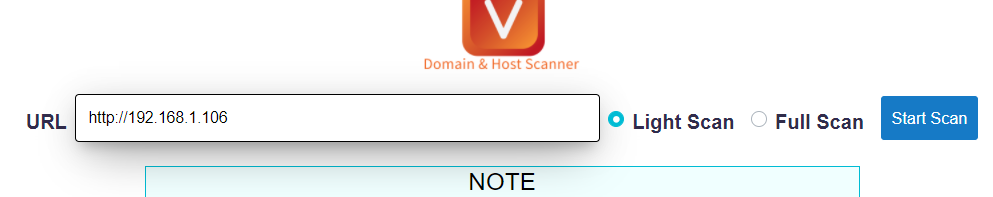
-“Spidering” kısmında link taraması işlemini gerçekleştirir.

-“Domain & Host Scanner” kısmında Link tespiti ve bilgi toplama işlemleri gerçekleştiriliyor.

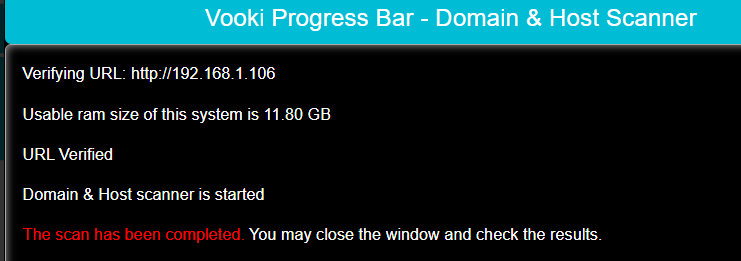


-Proxy Settings kısmına geçiş yaptığımızda burada proxy ayarlarını yapabileceğimiz bir sayfa bizi karşılıyor.

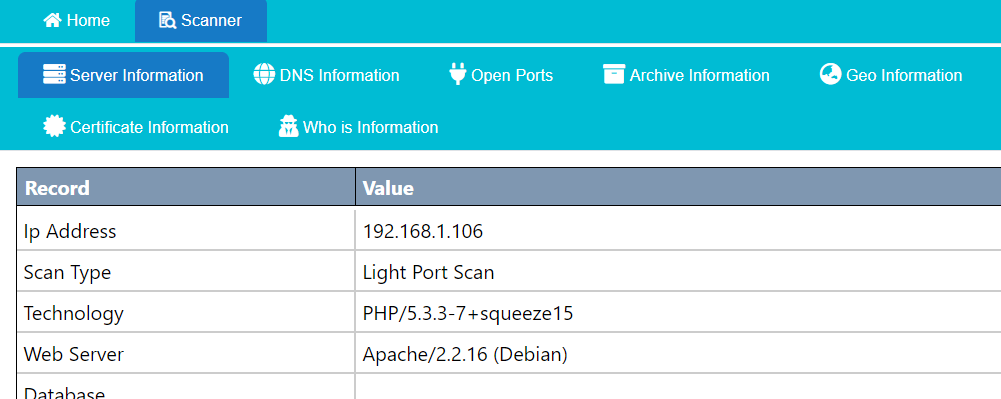
***Domain Host Scanner***



-Tarama işlemi yapacağım URL’i yazıyorum ve ardından “Start scan” ile işlemi başlatıyorum.



-Tarama işleminin süreci bu ekran üzerinde görüntülenmektedir.Bittiğinde ise görselde gözüktüğü gibi “The scan has been completed” yazısı gelmektedir.

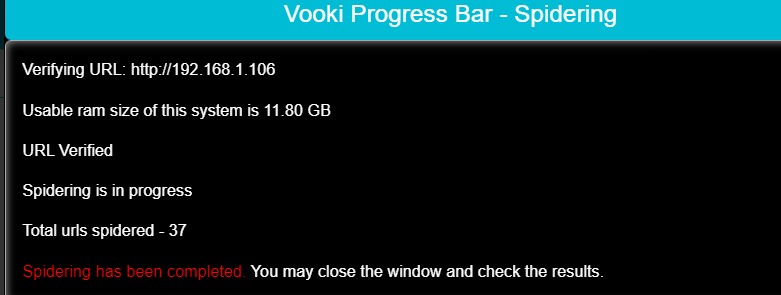


-Sonuç ekranında görüntüleyebildiğimiz bilgiler bu şekildedir.

***Spidering***



-“Spidering” kısmına geçiş yaptığımızda yine “Scan” sekmesinde olduğu gibi bir arama ekranı bizi karşılıyor buraya işlem yapacağımız URL’i yapıştırıyorum ve tarama işlemini başlatıyorum.



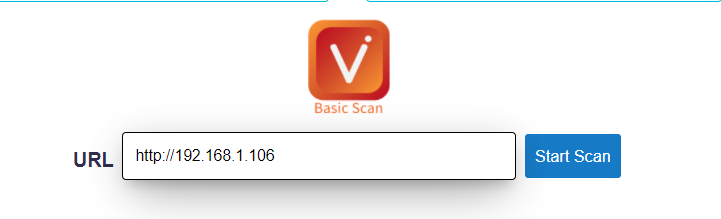
-Tarama işleminin süreci bu ekran üzerinde görüntülenmektedir.Bittiğinde ise görselde gözüktüğü gibi “Spidering has been completed” yazısı gelmektedir.



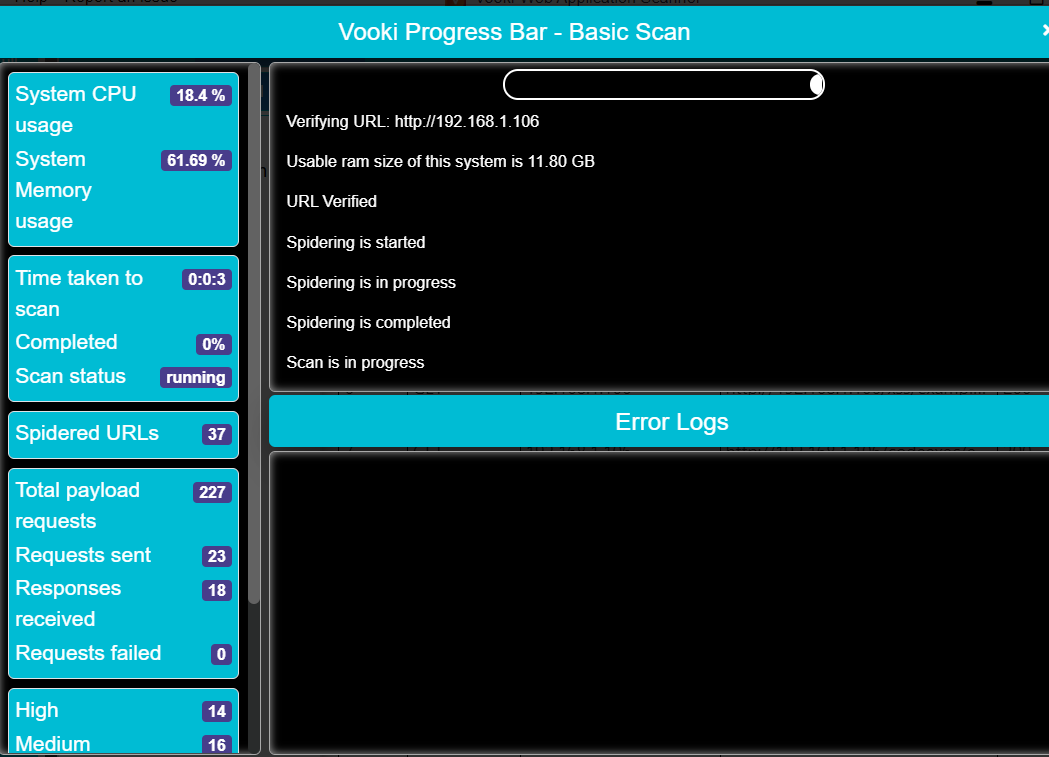
-İşlem sona erdiğinde spidering sonucunda bulduğu zafiyetleri görüntüleyebiliyoruz.

***Full/Basic Scan***

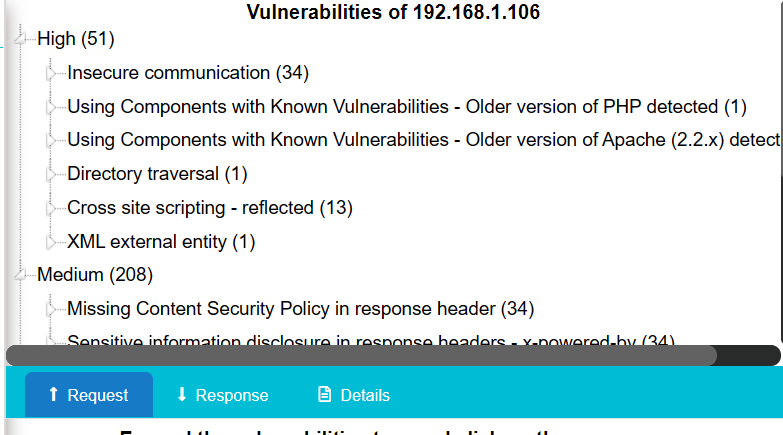
-Son olarak full scan uzun sürdüğü için basic scan ile bitiriyorum.Linkimi yazıp tarama işlemini başlatıyorum.



-“Full/Basic Scan” kısmına geçiş yaptığımızda yine önceki işlemlerde olduğu gibi bir arama ekranı bizi karşılıyor buraya işlem yapacağımız URL’i yapıştırıyorum ve tarama işlemini başlatıyorum.



-Tarama işlemi sırasında bu ekran üzerinden işlem takibi yapabilmekteyiz.



-Bulduğu zaafiyetleri bu şekilde raporlamaktadır.Request,Response ve Detail sekmeleri ile daha detaylı bilgi alabiliriz.

***XSSPWN***

-Diğerlerinden farklı olarak; XSS güvenlik açığı bulunan veya xss için ilgilenilmesi gereken linklerden dilediğimiz parametrelerin incelenmesini sağlar ve bizlere payloadlar döndürür.

-XSSPWN’in kullanmış olduğu kütüphaneler yeni Linux sürümlerinde kullanılmamaktadır.Bu sebeple program çalışmamaktadır.Linux’un eski sürümlerinde kullanım sağlanmalıdır.

Kurulumuyla başlayalım;



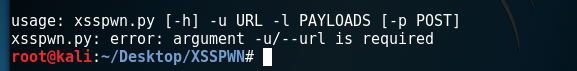
-Git clone üzerinden “https://github.com/pcdunyasitv/XSSPWN” bağlantısını kullanarak indirme işlemini başlatabiliriz.



-İndirme işleminin ardından python komutu ile install.py uzantısını çalıştırıp kuruluma başlıyorum.



-Kurulum işleminin ardından Python komutu ile xsspwn’i çalıştırıyorum.

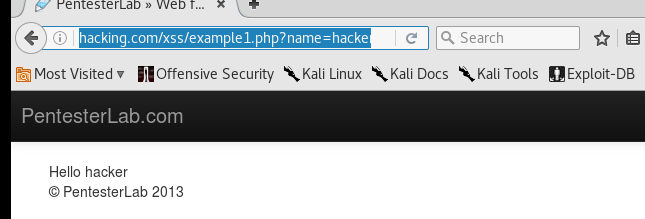


-Xsspwn’i çalıştırdıktan sonra bana kullanımıyla ilgil bir bilgi vermektedir.

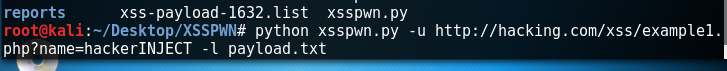


-“ls” komutuyla dosyanın içeriğine baktığımda uygulamanın kendi üzerinde bir payload’ı bulunduğunu görebiliyorum.

-Kullanımını da teorik olarak görüntüledik artık tarama işlemine geçiş yapabiliriz.



-Zaafiyet bulunan sitemin URL’sini kopyalıyorum.

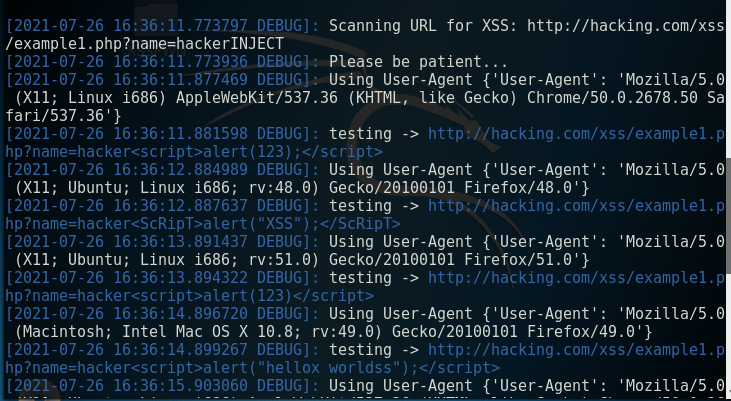


-Yazmış olduğum komutu incelediğimizde python komutu ile xsspwn.py uzantısını çalıştırıyorum.

-“-u” parametresi ile URL’imi ekliyorum ve sonuna eklediğim INJECT ile payloadın hangi konum üzerinde işlem yapacağını belirtiyorum.

-“-l “ parametresi ile kullanacağım payloadı belirtiyorum.

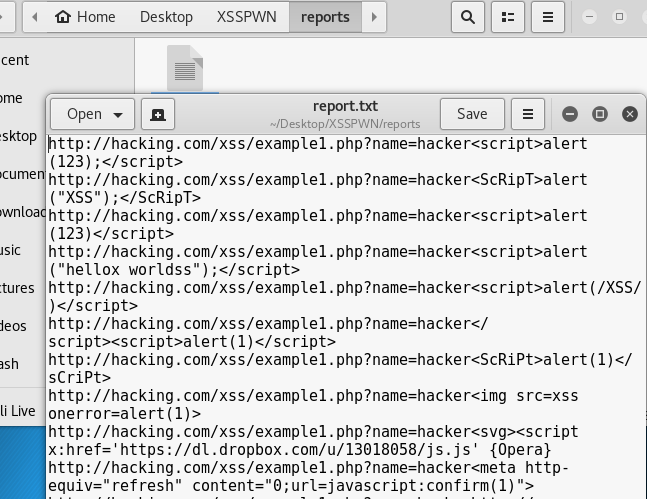
Gerekli bilgilendirmeyi yaptıktan sonra kodumu çalıştırıyorum.



-İşlemim başladı yaklaşık olarak 400 kadar payload denemesi yapılacak.

-Denenecek Payload sayısı .txt uzantılı dosyamın içerisinde ki payload sayısına göre değişmektedir.

-Payload sayısı arttıkça yapılan işlemin uzunluğu artmaktadır.Bu sebeple yapılan işlemin ne kadar süreceği hakkında bilgi veremiyorum.



-İşlem tamamlandıktan sonra XSSPWN>Reports dosyası içerisinde bulunan .txt dosyasında tarama yaptığım URL üzerinde bulduğu zaafiyetler için kullanabileceğim payloadları veriyor.