|  |
| --- |
| ***WEB UYGULAMA*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ*  -Web sunucu bilgisi öğrenme  -Web Uygulamasına ait Dizin ve Dosya Keşfi  -HTML Koruma Site Üzerinde Brute Force  -XSS üzerinden Browser Erişimi  -XSS üzerinden Yerel Ağ Taraması  -HTTP Metodu ile Güvenlik Zafiyeti |
|  |

**05.08.2021**

***Web sunucu bilgisi***

-Hedef sisteme ait şuan ve geçmiş yönelik kullandığı işletim sistemi ve kullanılan uygulamaları tespit etmeye çalışalım.

-Netcraft.com ve Nmap uygulamasından yararlanacağız.

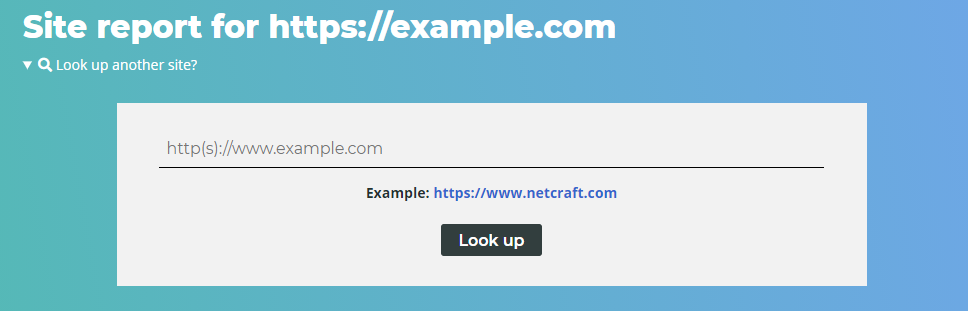
--------

**Netcraft**

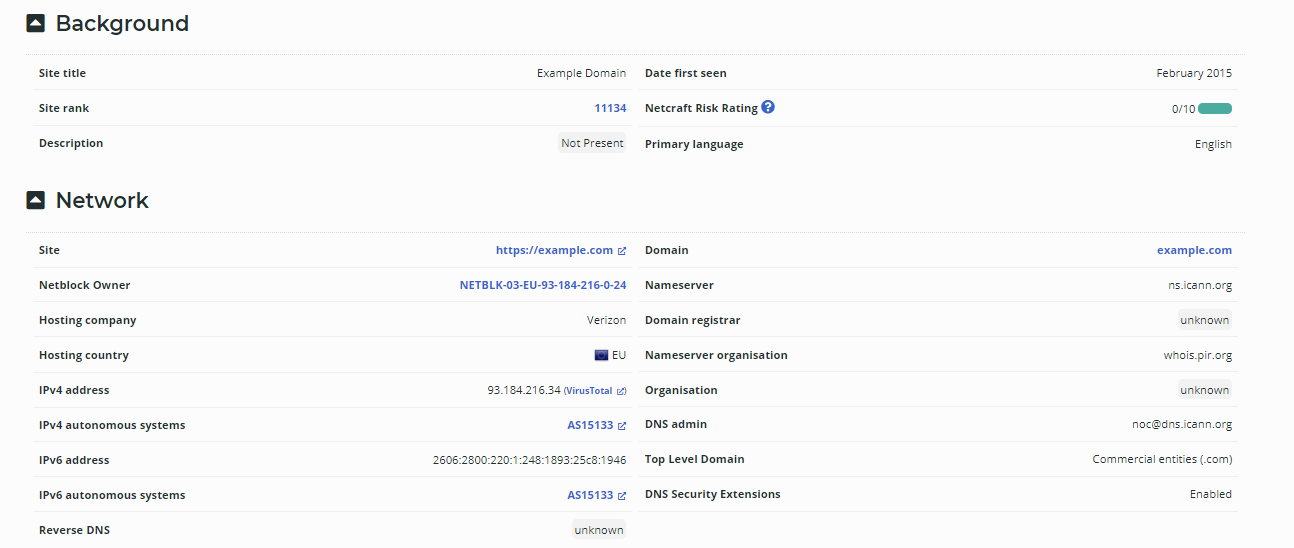
-Öncelikle işletim sistemimiz açıp tarayıcıyı çalıştırıyoruz.



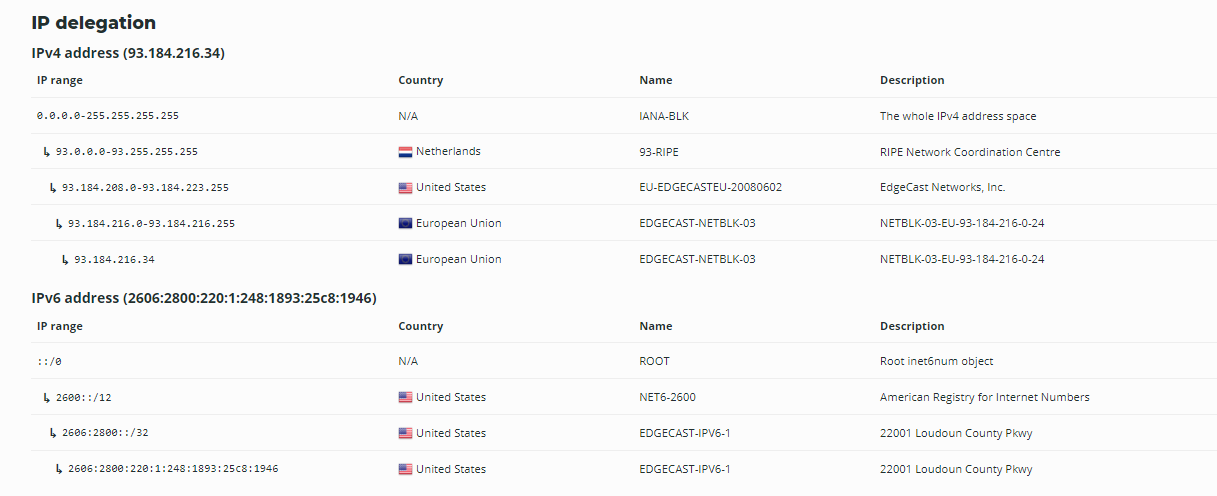
-“Netcraft” Sitesine geçiyorum.



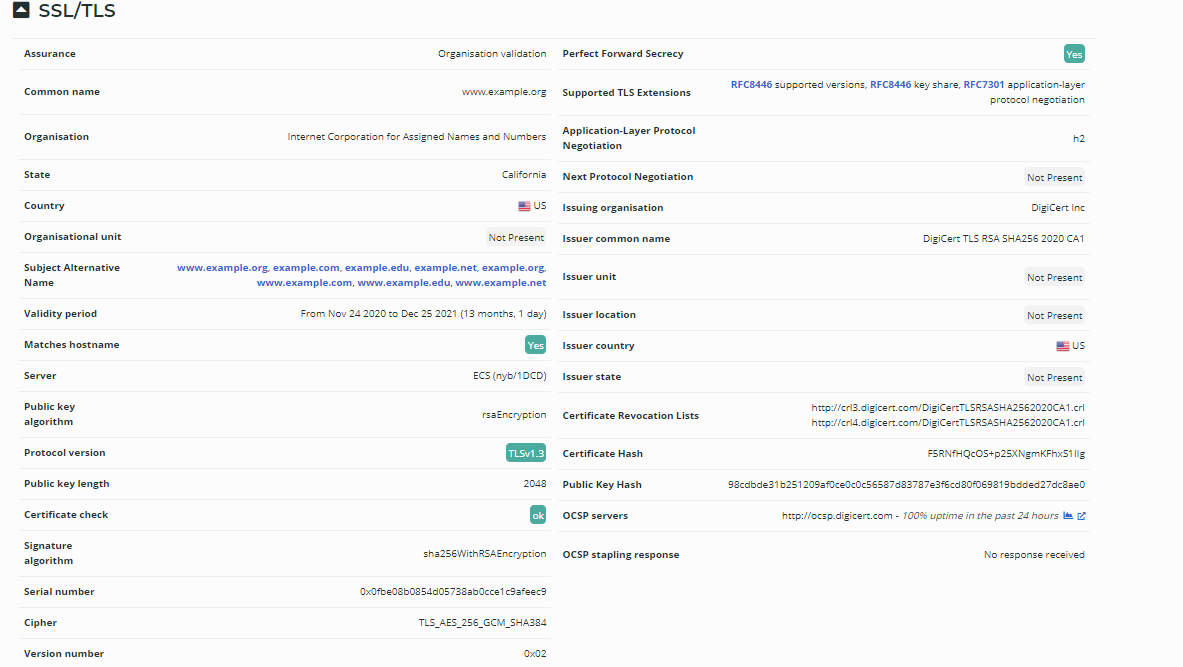
-Site üzerinde bilgi almak(taramak) istediğim sunucunun adresini giriyorum.



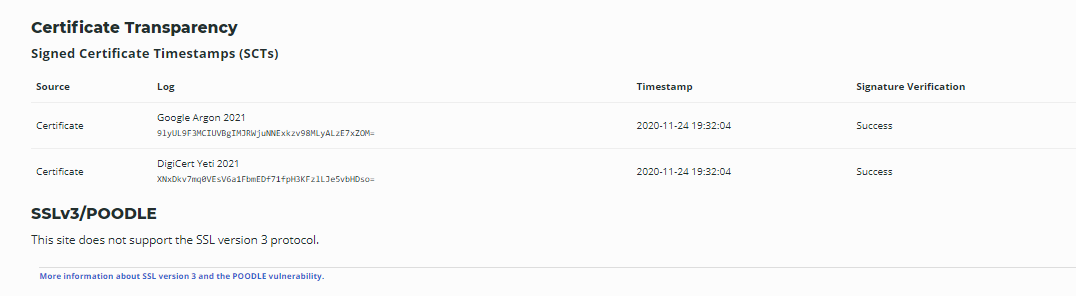
-Network ve Background ayarlarını görüntülüyoruz.



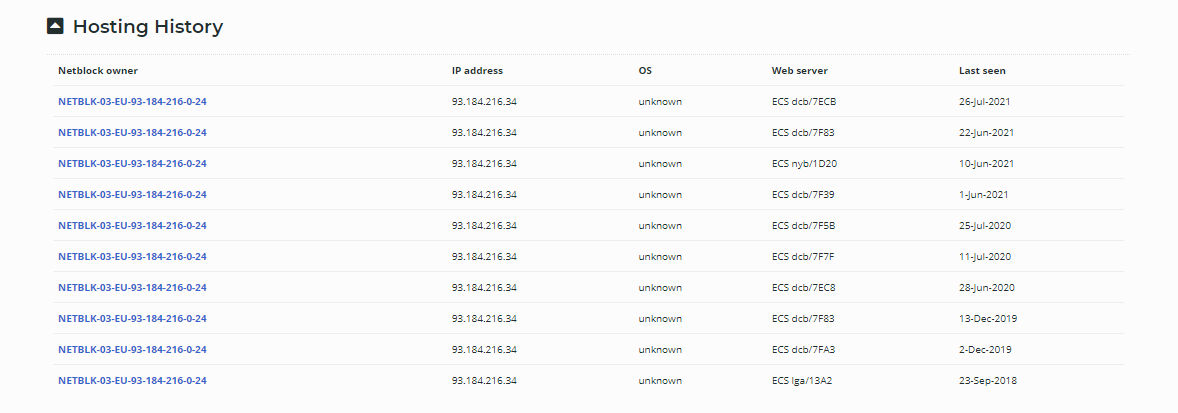
-Şuan ve geçmişte kullandığı IP adreslerini görüntüleyebiliyorum.



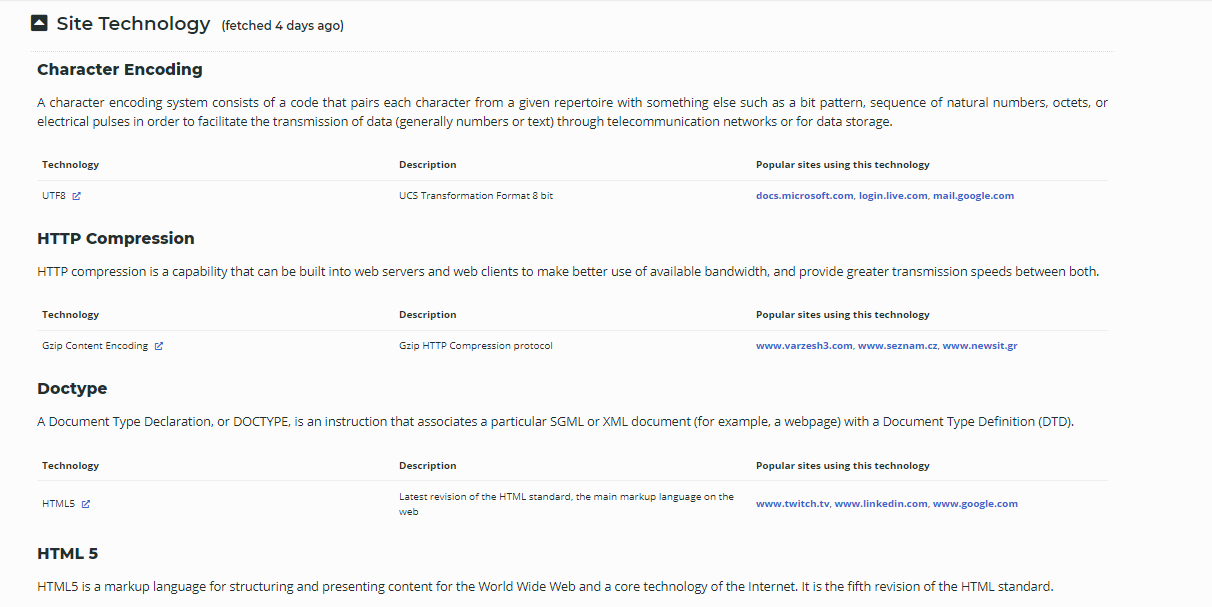
-SSL ve TLS ayarlarıyla ilgili bilgilere buradan erişebiliyorum.



-Kullandığı sertifika ve protokol bilgilerine erişiyorum.



-Kullanmış olduğu host adreslerini burada görüntüleyebiliyorum.



-Kullandığı HTML dili,Klavye karakter tipi gibi ayrıntıları görebiliyorum.

-Netcraft’ın verdiği bilgileri yüzeysel olarak bu şekilde görüntüleyebiliriz.

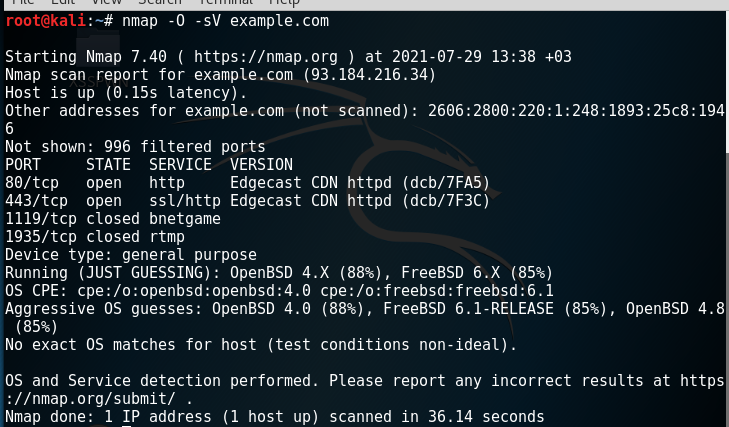
**Nmap**

-İlk önce linux sanal makinemi çalıştırıyorum ve Uç birimi açıyorum.



- O parametresi İşletim sistemini bilgilerine erişim sağlamamızı sağlayacak.

- sV parametresi ise kullanılan uygulamaların versiyon bilgilerini döndürücek.



-Kullanmış olduğu port bilgisi,IP adresi,işletim sistemi gibi bilgilere erişim sağladık.

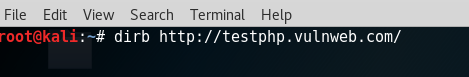
-NMAP üzerinde ki işlemlerimiz bu kadardır.

**Dizin ve Dosya Keşifi**

-Web uygulamasında gizlenmeye çalışan veya gizlenmeyen dizinlere ve dosyalara erişim sağlamaya çalışacağız.

-Bu uygulama için dirb ve dirbuster araçlarından yararlanacağız.Bu araçlar aynı işi yapsalar da bir tanesi görsel iken diğeri komut satırı üzerinden işlem gerçekleştirecektir.

Dirb : Linux makinelerinde kurulu olarak gelmektedir.Kullanımı çok basit bir uygulamadır.



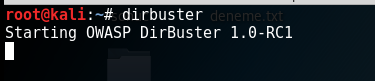
-Linux makinem üzerinden Uçbirimi açıyorum ve “dirb <http://siteadresi.com>” düzeninde işlemi başlatıyorum.



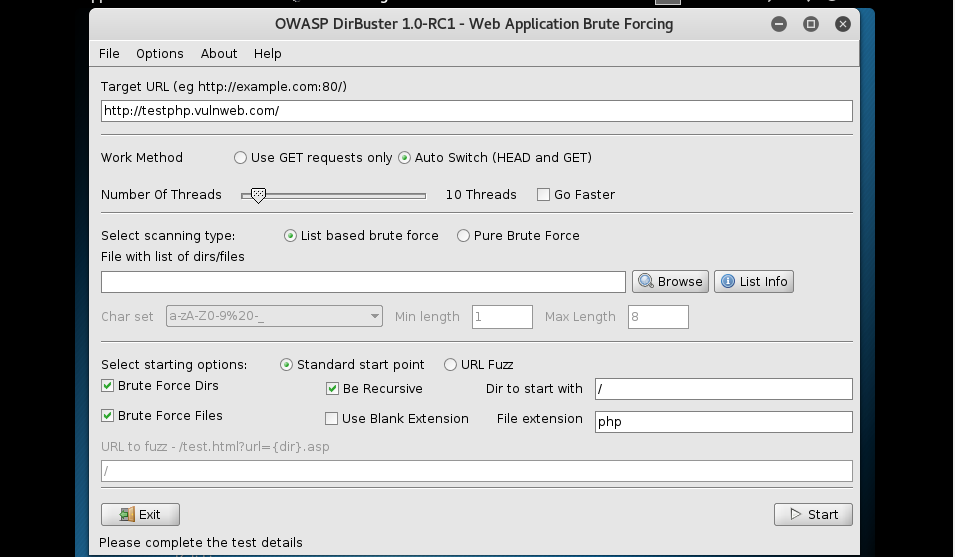
-Program içerisinde “4612” adet payload bulunmaktadır.Bu payloadlar ile port taraması gerçekleştirip bize bilgi aktarımı yapmaktadır.

-Bu işlem arka planda devam ederken Dirbuster aracını çalıştıralım.Tarama işlemi yaklaşık 15-20 dakika sürecektir.

-Dirbuster aracı da dirb gibi Linux makinelerinde kurulu olarak gelmektedir.

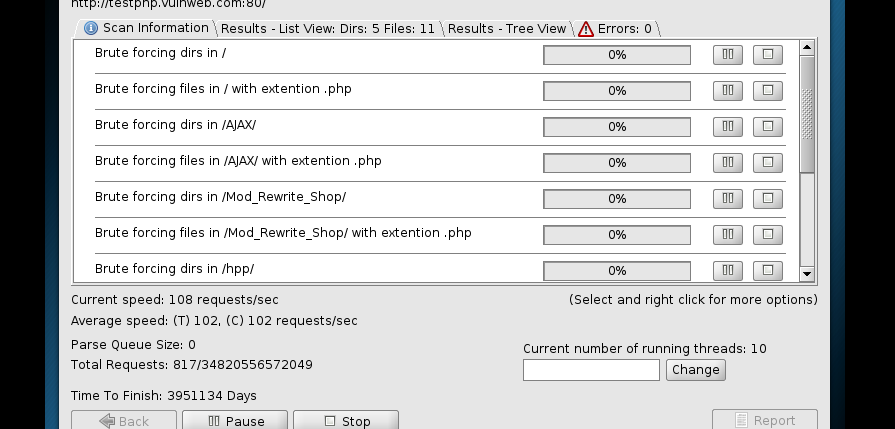


-“dirbuster” komutu ile aracı çalıştırıyorum.

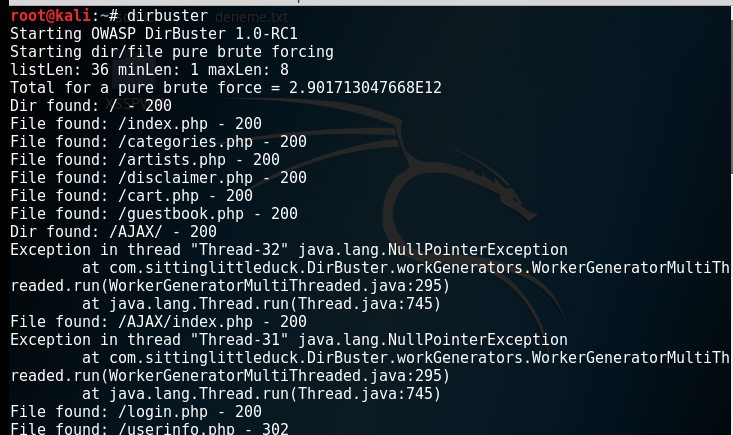


- Program açıldığında beni bu şekilde bir ekran karşılayacak ve BruteForce işlemi ile dosya keşfi gerçekleştiricek.

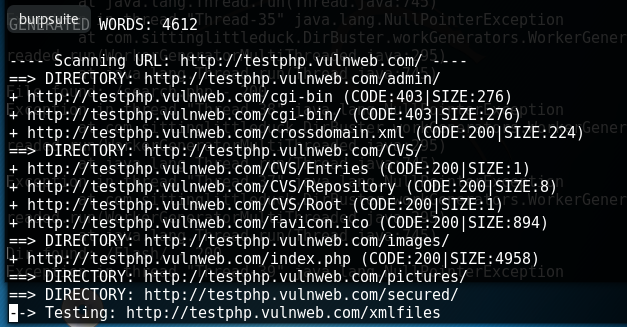
-Yazma dili veya denenecek karakterler isteğe bağlı olarak seçilebilir.Start butonu ile işlemi başlatıyorum.



-Tüm dosya ve dizinleri bulmak için işlem takibini buradan yapabiliriz.

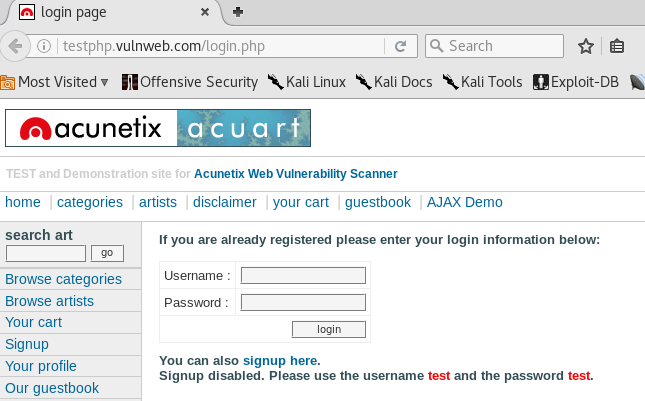


-Dirbuster aracının sonuçlarının bir kısmını görüntülediğimizde .php uzantılı dosyalar hakkında da bilgi verdiğini görüntülüyoruz.



-Dirb aracının da sonuçları daha tam olarak bitmese de bir kısmını buradan görüntülediğimiz de bu aracında .php uzantılı dosyalar ve xml dosyalarının yerini gösterdiğini görüntülüyoruz.

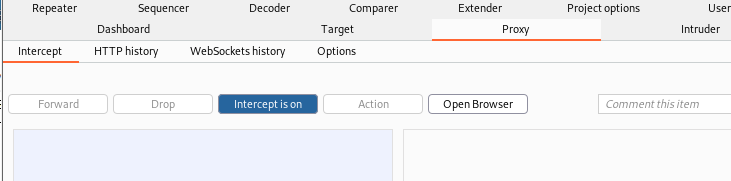
**HTML Form Koruma Site Üzerinde Brute Force İşlemi**



-Vulnweb web sitesi zafiyetlere oldukça açık bizim bu zafiyetler üzerinde işlem yapmamıza olanak sağlayan bir test sitesidir.Bu siteyi kendimizi geliştirmek için kullanabiliriz.

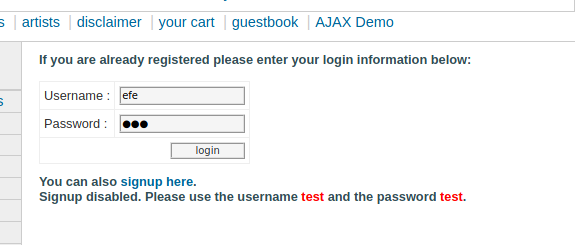
-Siteyi incelediğimde bir adet giriş text ekranı bizi karşılıyor.

-Bu işlemlerde yine her zaman olduğu gibi Burpsuite aracından yararlanacağız.

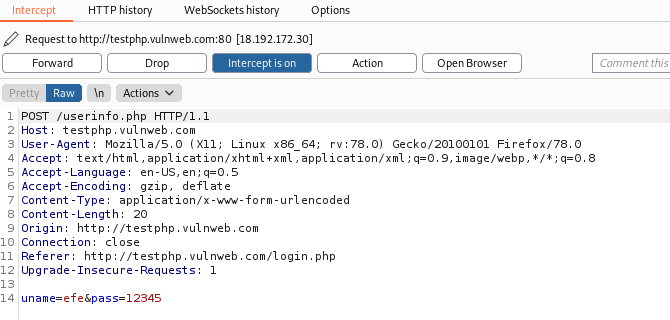


-Burpsuite aracını çalıştırıyorum.Https protokolü içeren bir web sitesine yönelik işlem yapmak için PRO versiyonuna erişim sağlamamız gerekmektedir.

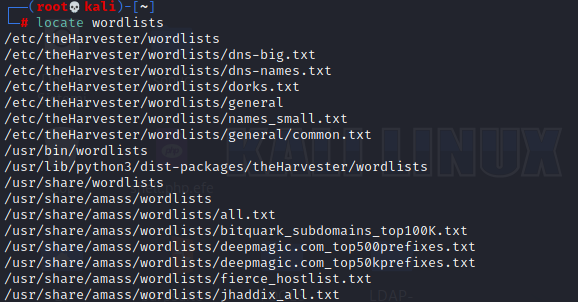
-Burpsuite'in bu site ile iletişim kurabilmesi için proxy ayarlarını gerçekleştiriyorum.



-Giriş bilgilerini random olarak giriyorum ve ardından login işlemini gerçekleştirdiğimde bütün bilgiler burpsuite üzerine çekilecek.



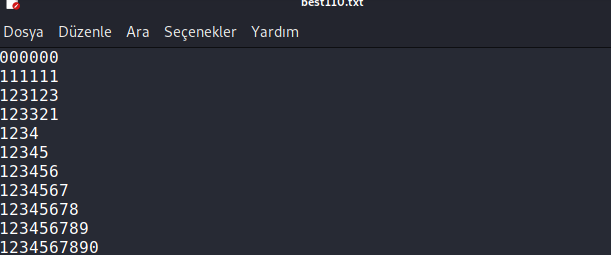
-Site üzerinden işlem yapabilmem için gerekli tüm bilgiler Burpsuite üzerine çekildi.



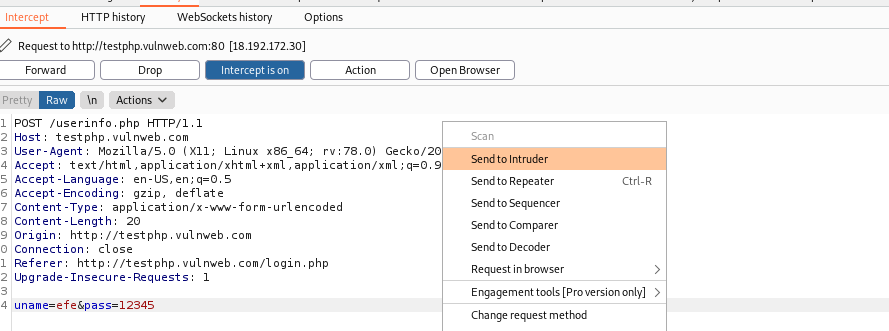
-Şimdi ise bir wordlist üzerinden Burpsuite aracı sayesinde Brute-Force saldırısı gerçekleştireceğim.İlk önce linux üzerinde bulunan wordlistlere göz atıyorum.

-İçlerinden bir tanesini seçiyorum ve Bruteforce saldırı gerçekleştireceğim.

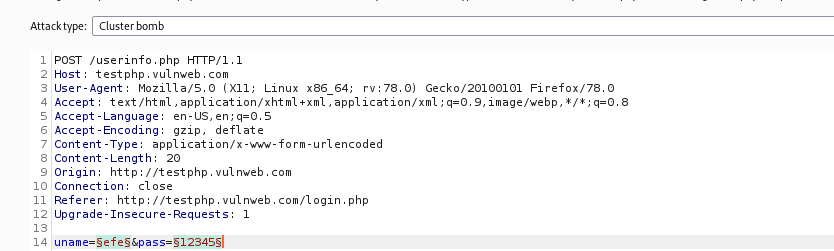
-Daha kapsamlı bir tarama yapmak için WEB üzerinde bulunan daha yüksek payload içeren wordlistler kullanılabilir.



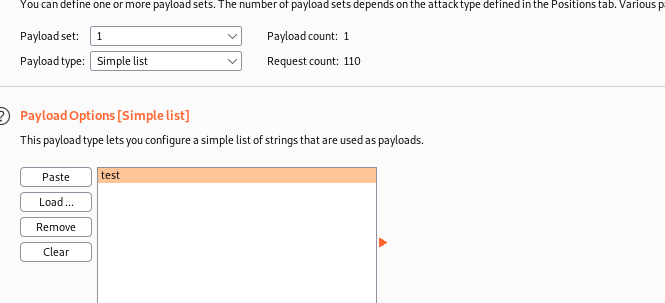
-Best110.txt dosyasını açtım ve içerisinde ki paylaodları kopyaladım.Ardından burpsuite üzerine geçiş yapıyorum.



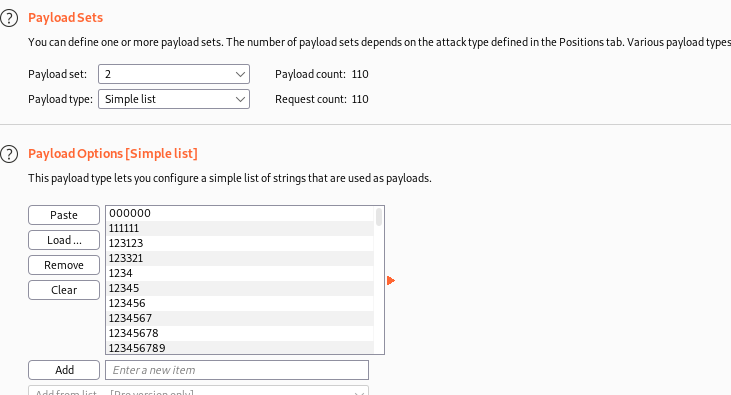
-Send to Intruder seçeneği ile bilgileri Intruder sekmesine gönderdim.



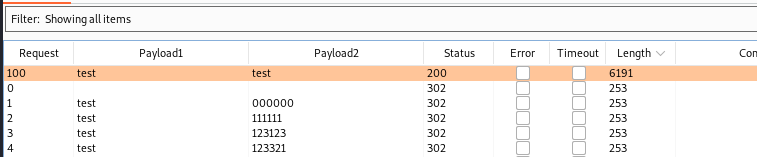
-Seçili bölümler üzerinde işlem gerçekleştireceğim için ayarları ellemiyorum ve “Cluster bomb” seçeneği ile devam ediyorum.



-Ardından payloads kısmına geçiş yapıyorum burada bu kullanıcı adı ile işlem yapacağım için sadece “test” ekliyorum.



- Şifre kısmı için ise paylaod’ı ekleyip işlemi başlatıyorum.



- İşlemi başlatıyorum burada ise doğru sonucu “length” sekmesi üzerinden bulacağım.Length değeri farklı olan değer doğru değerim olacaktır.

-Doğru kullanıcı adı ve şifre başarılı bir şekilde bulundu.

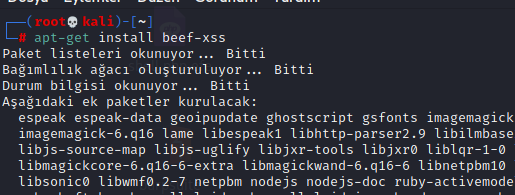
***XSS ile Browser Erişimi;***

-XSS zafiyeti bulunan bir web sitesi sayesinde,Beef aracı kullanarak hedef kişinin Browserini yönetmek.

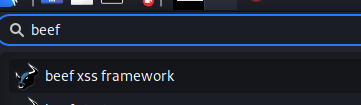
-Bu işlem için bize bir adet XSS açıklı site ve Beef aracı gerekmektedir.

- İşlemimizi dış ağ üzerinden gerçekleştiricez.Linux üzerinde hazır bulunan beef aracı ve XSS açıklı testasp sitesi üzerinden işlem gerçekleştireceğim.

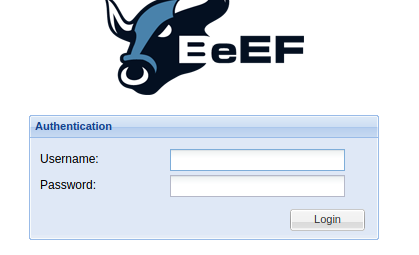
-Linux sanal makinemi başlatıyorum.



- Öncelikle Linux üzerinde “ beefxssframework” aracını çalıştıracağım fakat bende kurulu olmadığı için önce “apt-get “komutu ile kurulum gerçekleştiriyorum.



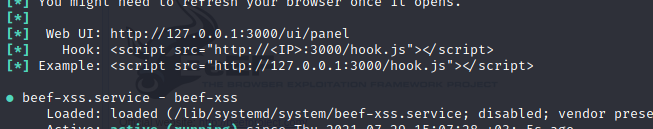
-Kurulum sonrasında arama kısmından beef aracını bulup çalıştırıyorum.



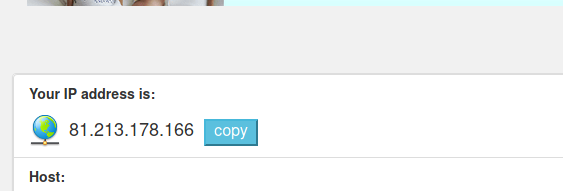
-Araç çalıştığında bizi böyle bir ekran karşılayacaktır.Default olarak Kullanıcı adı ve şifre “beef” ‘dir.

-Bana zafiyet olan URL üzerinde çalıştırabilmem için bir “.js” uzantısı veriyor.Eğer bunu bir XSS açıklı sitede çalıştırırsam ele geçirebilirim.

-İşlem yapacağım sitenin linki “<http://testasp.vulnweb.com/>” dir.



-Example bölümünde ki script kodunu kopyalıyorum.



-Öncelikle dış ağ üzerinde kullanacağım IP adresini öğrenmek için tarayıcı üzerinde “My Ip” yazıp herhangi bir siteye giriyorum ve Ip adresimi öğreniyorum.



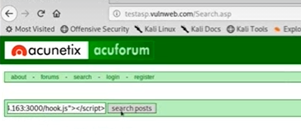
-Ardından “gedit deneme.txt” komutu ile bir txt dosyası açıyorum ve buraya kopyaladığım JS kodunu yapıştırıyorum ve IP adresimi ekliyorum.

-Modem arayüzüne geçiş yapıyorum.

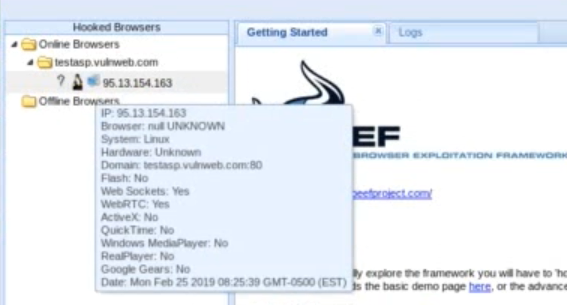


-Şuan yapacağım işlem 3000 portunu açmak,modem arayüzünü açıp Port adreslerine 3000 ve IP adresi kısmına “ifconfig” bilgisi üzerinden öğrendiğim IP adresimi yazıyorum ve kaydediyorum.

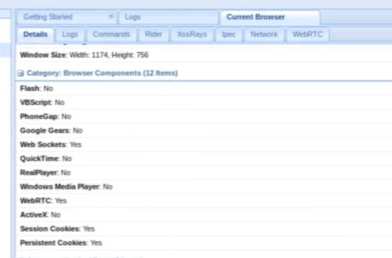
-Kullandığım internet kaynaklı modem arayüzüne giriş yapamadığım için görseller temsilidir.Bir sonraki uygulamada local üzerinden işlem gerçekleştireceğiz.O zaman resimler daha net hale gelecektir.



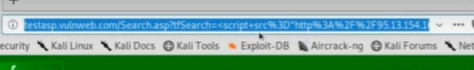
-Farklı bir makine üzerine geçiş yapıyorum ve kopyalamış olduğum “beef” içerisinde ki scripti burada çalıştırıyorum.



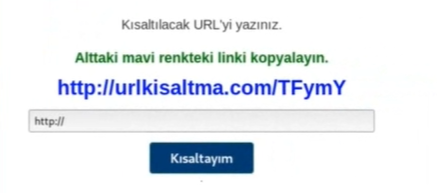
-Script çalıştıktan sonra bu scripti çalıştıran IP adresi Beef uygulaması üzerine düşmüştür.



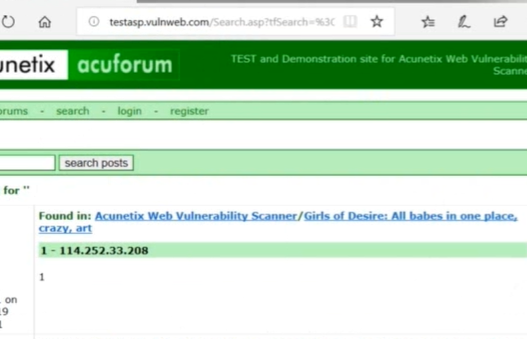
-Detail bölümüne geçiş yaptıktan sonra burada tarayıcıya ait bütün bilgilere erişebiliyorum.



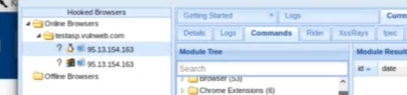
-Bunu başka kişiler üzerinde denemek için ise “testasp” web sitesi üzerinde ki URL'i kopyalıyorum ve bunu başka bir cihaz üzerinde çalıştırma işlemi gerçekleştirildiğinde beef browser üzerinde düşecektir.



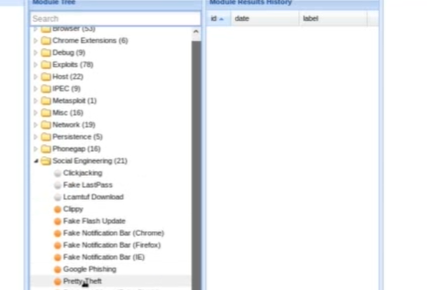
-Bu link dikkat çektiği için link kısaltma web sitesi yardımıyla linki kısaltıyorum.



-Kısalttığım linki browser üzerinde çalıştırıyorum ve aynı sayfa açılıyor.



-Beef üzerine baktığımızda ise bilgilerin düşmüş olduğunu görüntülüyoruz.



-Zafiyet bulunan tarayıcı üzerinden “SocialEngineering” kısmında “Pretty thieft” aracını çalıştırıyorum.



-Kullanıcının eğer bir facebook hesabı var ise bu bilgileri ele geçirmek için kullanılabilir.Bunu execute ediyorum.

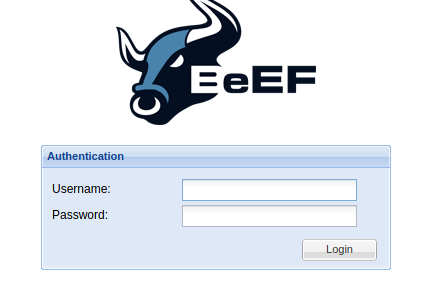


-Bu işlemi execute ettiğimde karşı tarafa böyle bir ekran gelicek ve girdiği kullanıcı adı ve şifreler bana gelicek.

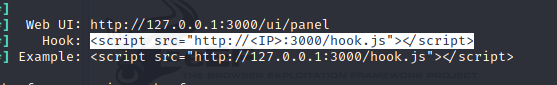
***XXS ile Yerel Ağ Taraması***

-XSS zafiyeti kullanarak ele geçirilen cihazın tarayıcısının üzerinden yerel ağda port taraması yapma işlemini gerçekleştireceğiz.

-Bu uygulama için Beef aracını kullanacağız.



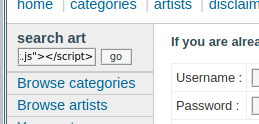
-Beef aracının kurulumuyla ilgili bilgilendirme vermiştim beef aracını çalıştırıyorum ve giriş yapıyorum. Default olarak kullanıcı adı/şifre > beef/beeftir.



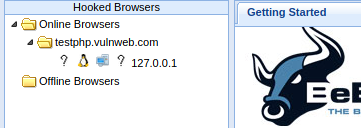
-Daha sonrasında beef aracının bana vermiş olduğu JS kodunu kurbana çalıştırtmam lazım local ağ üzerinden işlemde yapacağım için direk example bölümünü kopyaladım.



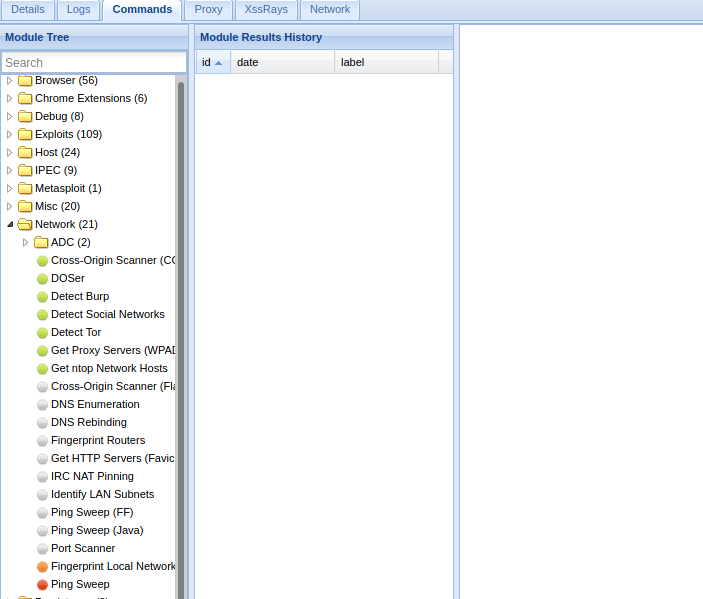
-Zafiyet bulunan Vulnmep sitesine geçiş yapıyorum.



- Ardından arama yerine kopyalamış olduğum Script kodunu yazıyorum ve go ile gönderiyorum.



- Beef üzerine geçiş yapıyorum ve bağlantımın buraya gelmiş olduğunu görüntülüyorum.



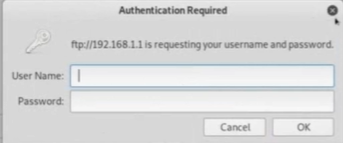
- Ardından commands bölümüne geçiş yapıyorum ve PortScanner aracını çalıştırıyorum.



- 192.168.1.1 Ip adresinin üzerinden tarama başlattım.Bu modemin portu olduğu için modem üzerinde ki tüm portları şuanda tarıyor.



-21.Portun açık olduğunu buldu.



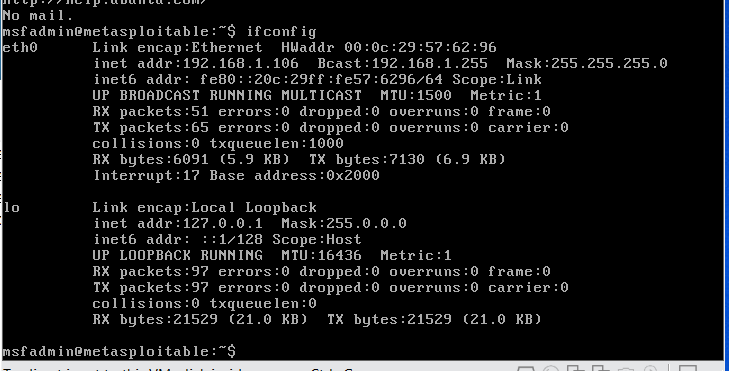
- Ayrıca 21.port üzerine bir kadı ve şifre text'i gönderdi buradan da bilgi almak mümkündür.

***HTTP Metodları ve Güvenlik Zafiyetleri***

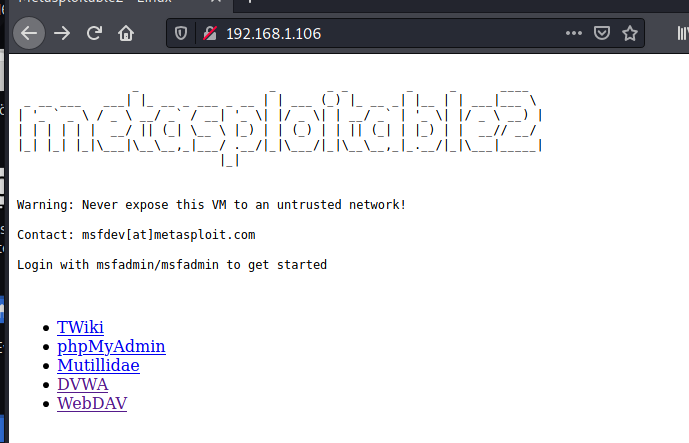
-Bu uygulama için Metaploitable2’ye ihtiyaç vardır.

-Bu aracı“<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/> “ bağlantısı üzerinden indirebiliriz.

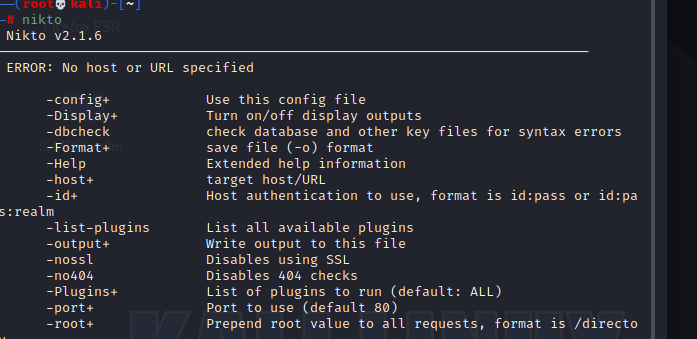
-İndirme işlemi sonrasında Vmware üzerinden OPEN komutu ile açıyorum.



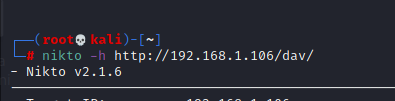
- Ardından ifconfig komutu ile IP adresini öğreniyorum.



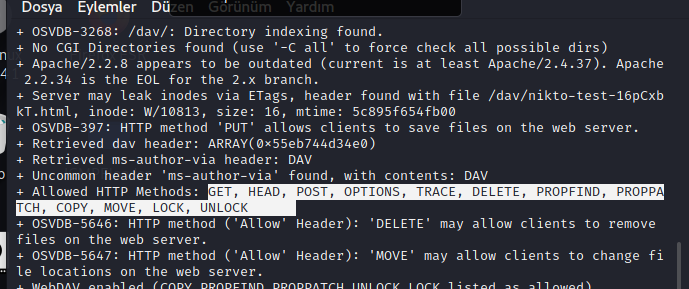
- Kali linux makinem üzerinden tarayıcıyı açıyorum ve IP adresini görüntülüyorum. Açılan sayfa üzerinde WebDAV ile devam ediyorum.



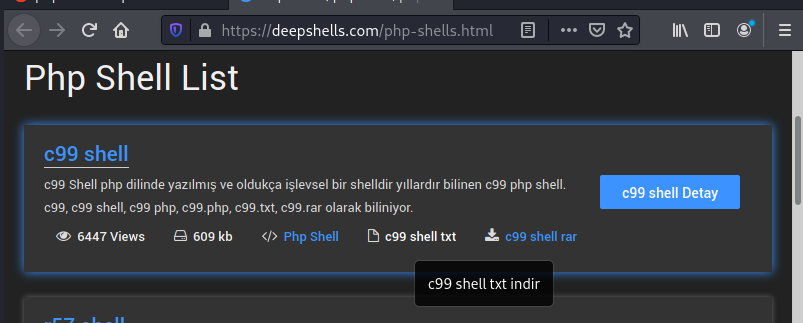
- Nikto programı üzerinden bu IP adresini tarama işlemi gerçekleştireceğim fakat ilk önce kullanımına bakıyorum.



- Linux üzerinde hazır olarak kurulu gelen Nikto aracı ile bu IP adresinin zafiyetlerini denetliyorum.



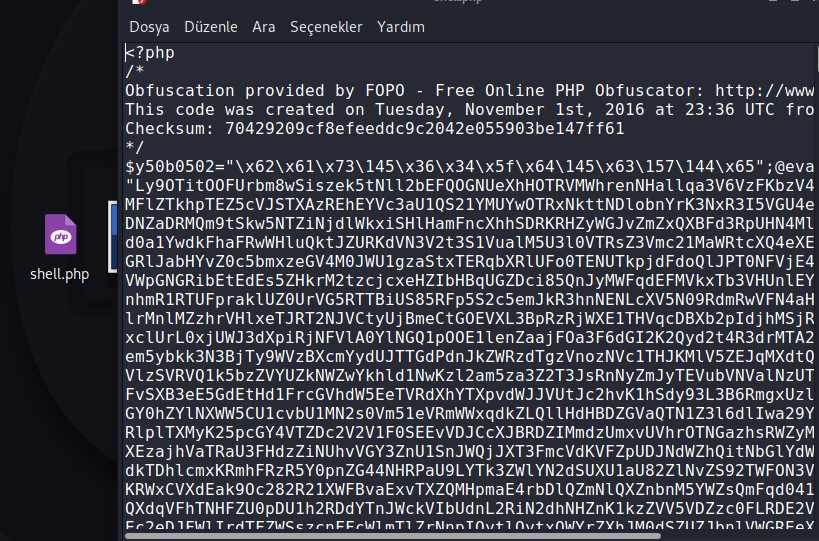
-Zafiyet testi sonucunda HTTP üzerinden çokca zafiyeti bulunduğunu görüntülüyorum.



-Bu zafiyetten .php kullanarak yararlanacağım.Bu sebeple Network üzerinden bir c99 php indiriyorum.

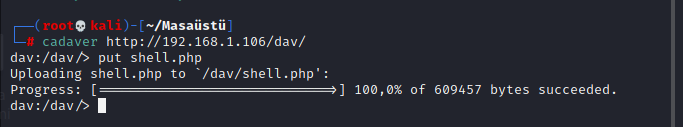


-Görüntülediğim bu txt sayfasını kopyalıyorum ve bir metin belgesi oluşturup içine kopyalıyorum.



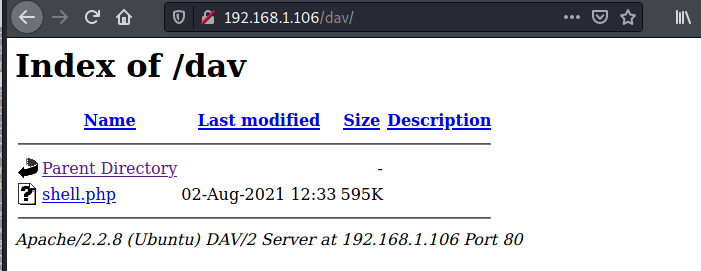
-Metin belgesi oluşturup içine kopyalıyorum.İsmini de shell.php koyuyorum.

-Ardından bu zafiyet için linux üzerinde kurulu olarak gelen cadaver aracını kullanacağım.

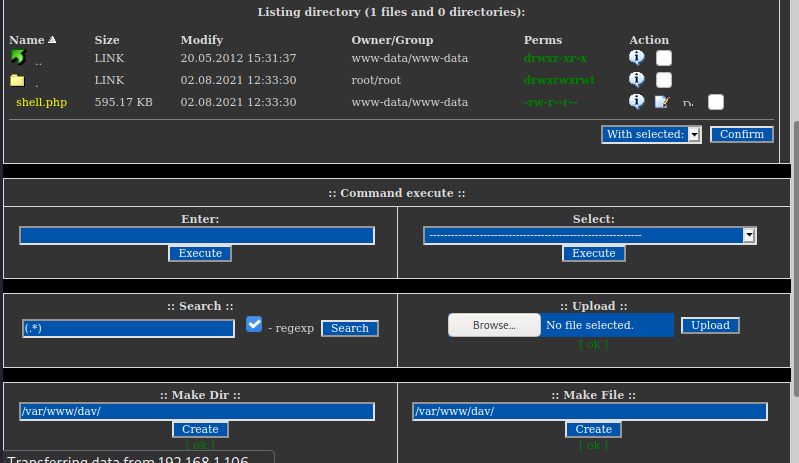


-Uçbirimi açıyorum ve ardından cadaver http://Siteismi.com ile işlemi başlatıyorum.

-Ardından put shell.php komutu ile shell dosyasını site içerisine aktarıyorum.



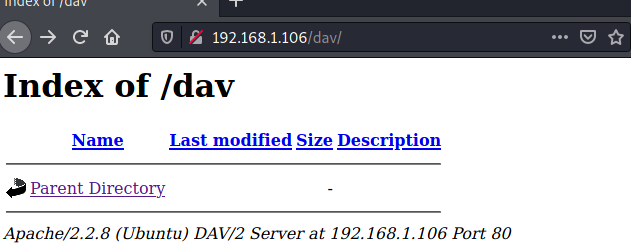
-Metasploit sitesine geçiş yaptığımızda shell dosyasının buraya geldiğini görüntülüyoruz ve shell.php ile başlatıyorum.



-Shell.php üzerinden istediğim işlemi gerçekleştirebiliyorum.



-Eğer bu işlem sonrasında shell.php veya başka bir dosya silinmek istenir ise cadaver üzerinden delete shell.php komutu ile silme işlemi gerçekleştirilir.



-Dosya silme işleminin gerçekleştiğini görüntülüyoruz.