|  |
| --- |
| ***Directory Traversal*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Directory Traversal nedir ve Web for Pentester laboratuvarı üzerinde Directory Traversal zafiyeti nasıl uygulanır bunun hakkında bilgi vereceğim. |

**27.07.2021**

***Directory Traversal***

-Kullanıcı girdisinin web sunucusu veya başka bir sistem üzerindeki dosyaları okuma veya yazma amacıyla güvensiz bir şekilde kullanılmasıyla ortaya çıkan zafiyet türüdür.

-Bu güvenlik açığından en iyi şekilde yararlanmak için Linux/Windows vb. işletim sistemlerinin dosya yapısı iyi bilinmelidir.

-Windows dosya sistemine kullanım esnasında az çok hakimiz fakat Linux için böyle bir şey söz konusu olmadığı için Linux dosya sistem yapısıyla ilgili bir doküman oluşturdum.

-Örnek olarak bir .png uzantılı bir resim dosyası üzerinden sunucu üzerinde bulunan başka dosyalara erişim sağlayıp okuma işlemi gerçekleştirilebilir.

-Bu zafiyetle ilgili Web for Pentester üzerinden 3 Adet uygulama gerçekleştireceğiz.

**Uygulama 1 :** Temel kullanım.

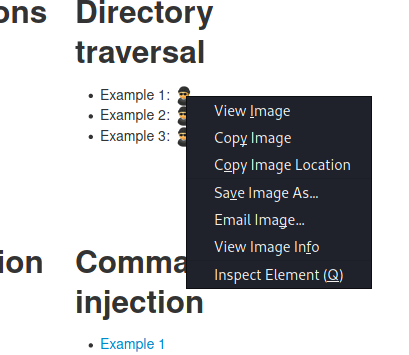
-Diğer zafiyet türlerinde olduğu gibi yine zaproxy ve skipfish araçları ile tarama gerçekleştirdim.



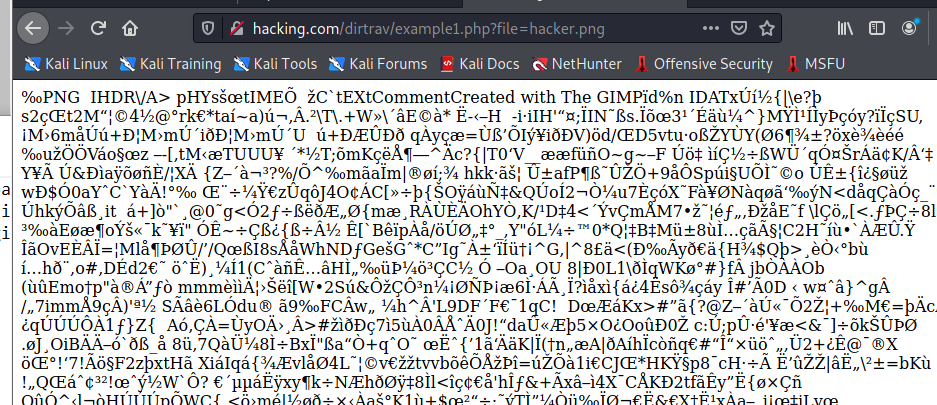
-Zaproxy aracı zafiyeti başarılı bir şekilde tespit etti.



-Skipfish aracıda zafiyeti başarılı bir şekilde tespit etti.



-Önce WFP üzerinden Directory traversal bölümüne geliyorum ve burada sağ tıklayıp “Copy İmage Location” butonu ile URL kopyalama işlemi yapıyorum.

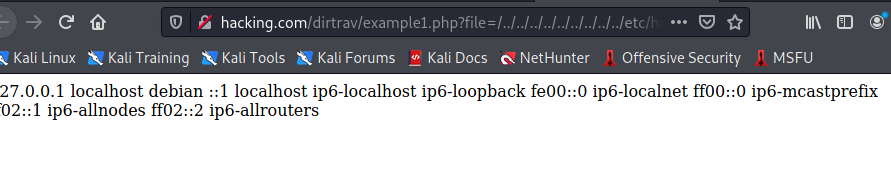


-Linki tarayıcı üzerinde çalıştırdığım zaman URL ve İçeriği bu şekilde görüntüleniyor.

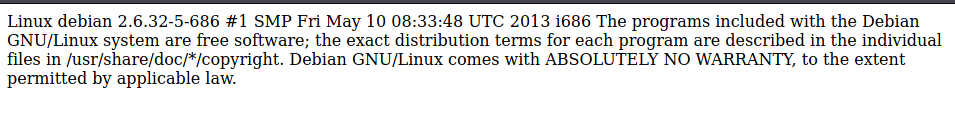
-Bu zafiyet hakkında daha fazla bilgi elde edebilmek için skipfish aracında vermiş olduğu URL üzerinden işlem gerçekleştireceğim.



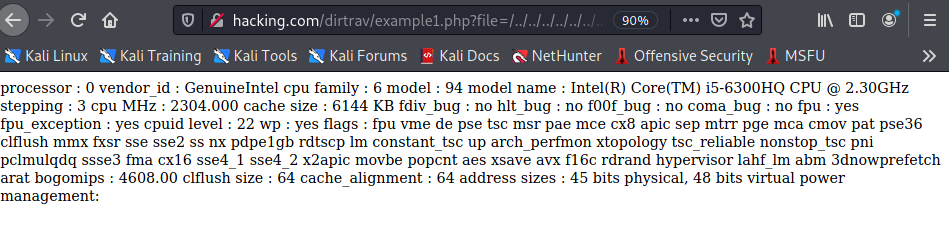
-Skipfish aracının bulmuş olduğu zaafiyetin passwd linkine girdiğimde karşıma böyle bir ekran geliyor.Burada dizinler hakkında fazlasıyla bilgi sahibi oluyorum.



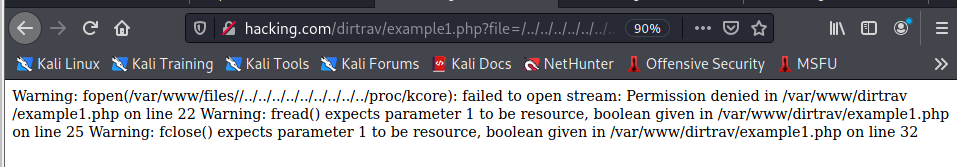
-Skipfish aracının bulmuş olduğu zaafiyetin hosts linkine girdiğimde karşıma böyle bir ekran geliyor.Burada ise hosts dizini içerisinde ki ayarların hepsini görüntülüyorum.



-URL üzerine eklediğim “Motd” komutu ile sistem hakkında bilgi sahibi oluyorum.



-“/../../../../” sonuna eklediğim /proc/cpuinfo komutu ile cpu hakkında bilgi sahibi oluyorum.



- “/../../../../” sonuna eklediğim Kcore komutu ile sistem hafızasının görüntüsüne bakıyorum.

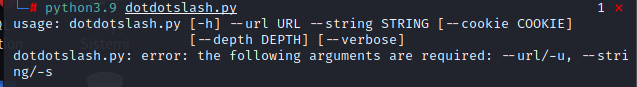
-Sunucuda ki tüm dosyalara erişim mümkün fakat hepsinden başarılı bir dönüt alınmaz. Çalıştırılabilir olanlar herhangi bir geri dönüt vermez.

**Uygulama 2 :** Alternatif araç ile tespit.

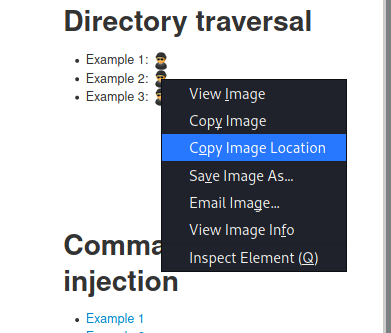
-Zaproxy ve skipfish araçları zaafiyeti tespit edemedi.Bu sebeple “Dotdotslash” aracı üzerinden işlem gerçekleştireceğim.



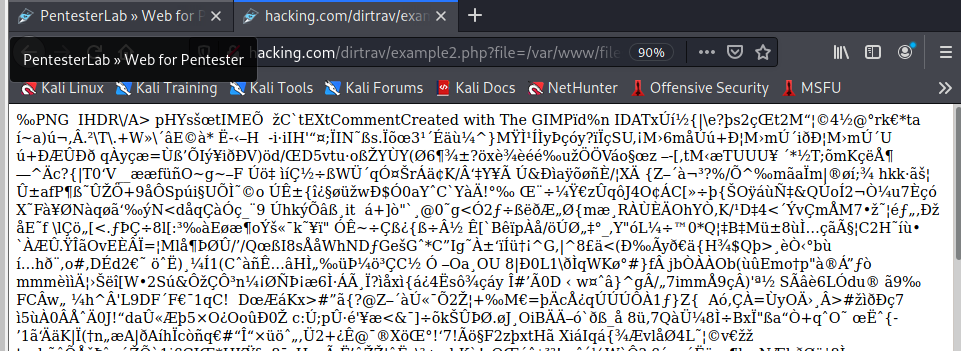
-Öncelikle linux üzerinde kullanılan git clone yardımıyla “Dotdotslash” aracını indiriyorum.



-İndirmiş olduğum dosya üzerinde “python” komutu ile uygulamayı çalıştırıyorum.Bana burada kullanımıyla ilgili yeterli düzeyde bilgi sahibi oldum.

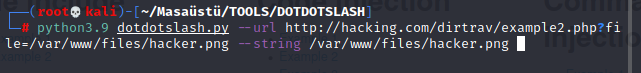


-Ardından WFP’a geçiyorum ve burada Copy İmage Location ile linki kopyalıyorum.



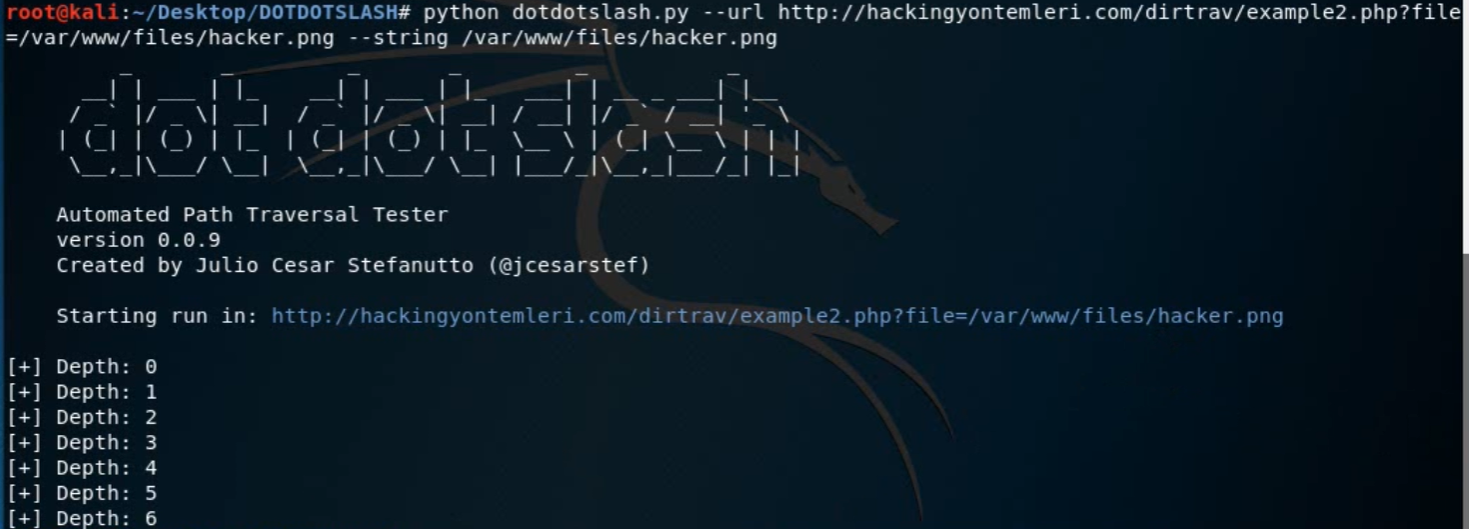
-Kopyaladığım URL’ i bir tarayıcı üzerinde açtığımda; Bizi böyle bir ekran karşılıyor.

-Zafiyet sadece .png uzantılı dosyalarda olduğunu düşünmeyelim.Zafiyet bütün dosya uzantılarında olabilir.Burada dosya yolunu kopyalıyorum.

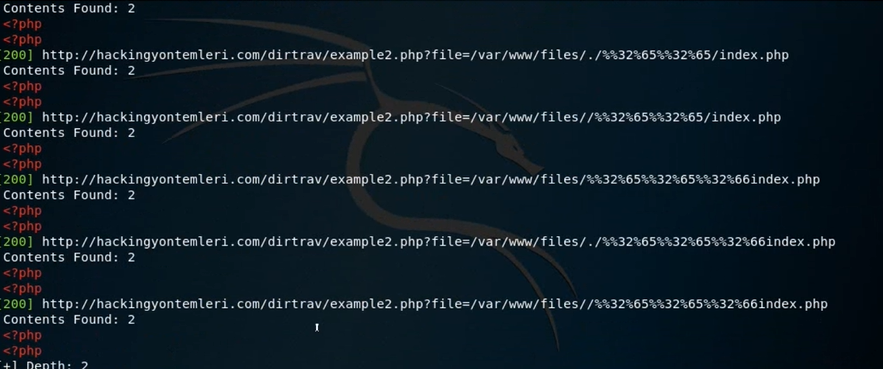


-Python ile dotdotslash toolunu çalıştırıyorum.

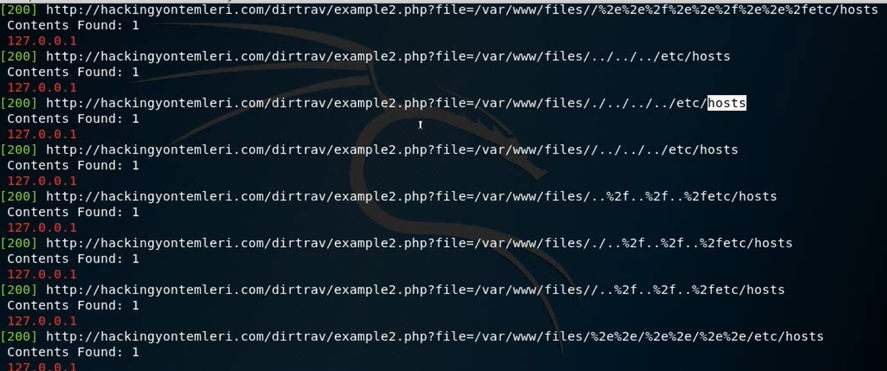
-URL kısmını kopyalıyorum ve zaafiyetin bulunduğu bölümün dizinini ekliyorum.



-İşlemi gerçekleştiriyorum fakat hata alıyorum bu yüzden --string sonrasına sadece .png ekleyip işleme bu şekilde devam ediyorum.



-Bu ve benzeri yaklaşık 30-40 tane zaafiyet buldu.



-Host dosyasına başarılı bir şekilde erişim sağladım ve oradan diğer dosyalara erişimi artık çok basit.



-Host uzantılı bir linki kopyalıyorum ve firefox üzerinde görüntülüyorum.(var/www/ dizini üzerinden erişim sağlanmış) sürekli alt dizinlere geçiş yaparak ana dizine kadar erişim sağlanmaya çalışıyor.

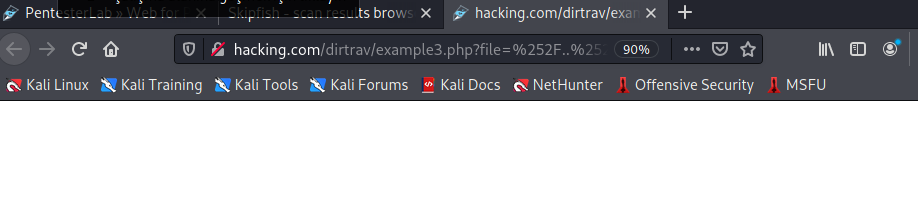
-Şuanda linux üzerinden en alt dizin olan var dizinine erişim sağlanmıştır ve dizinler arası istediğimiz gibi geçiş sağlayabiliriz.

**Uygulama 3 :** Filtreleme atlatma.

-Zaproxy aracı zafiyet tespiti yapamadı.

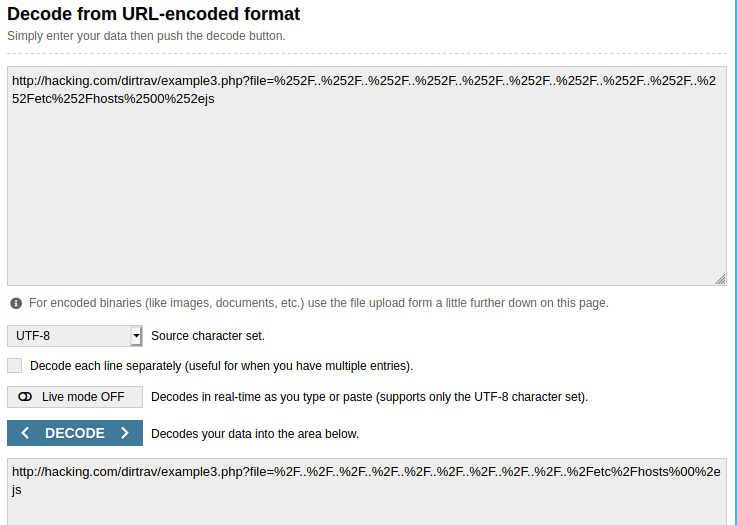


-Skipfish aracı zafiyeti başarılı bir şekilde yakaladı.Yakaladığı zafiyeti Tarayıcı üzerinde görüntülüyorum.



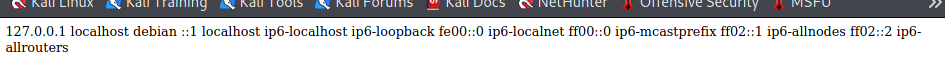
-Zaafiyetin linkini açtığımda herhangi bir geri dönüş alamıyorum.Linkin boş çıkması programın çalışmadığı anlamına kesinlikle gelmez.URL üzerinden bir işlem gerçekleştirebiliriz.

-URL decoder ile link üzerinde deneme yapıp zafiyeti görüntüleyebilirim.

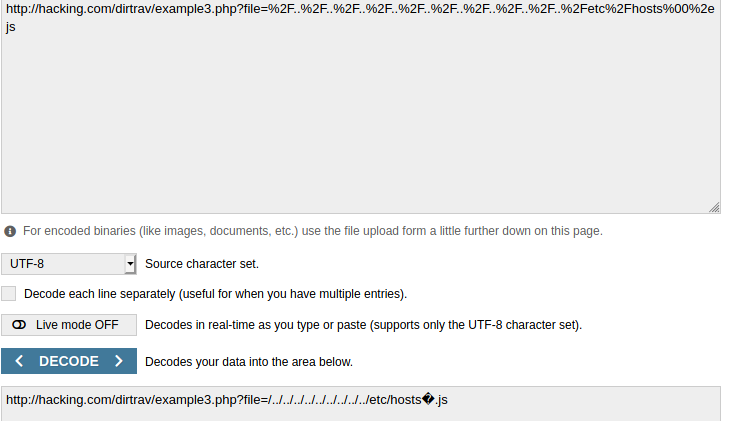


-Tarayıcı üzerinden decoder açıyorum ve dönüştürme işlemini gerçekleştiriyorum.

-Dönüştürme işlemi sonrasında elde ettiğim URL’i tarayıcı üzerinde görüntülüyorum.



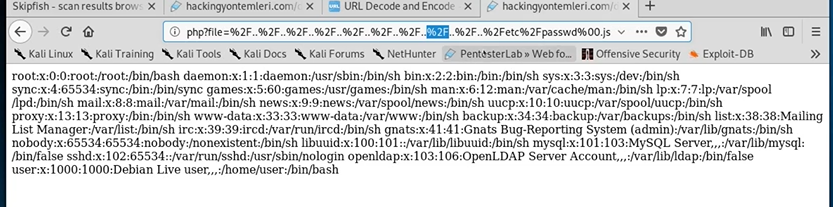
-Dönüştürme işlemi sonucunda istediğime eriştiğimi anladım fakat işlemi Decoder işlemini bir kere daha gerçekleştiriyorum.



-Bir kere daha dönüştürdüm fakat bu sefer farklı bir işaret geldi(? yokluğu ifade ediyor %00 yerine geliyor.

-Deneme sonucunda hata veriyor çünkü URL bunu tanımlayamıyor.

-Yapmış olduğum işlemler sonucunda istediğim dosyaya erişim sağlayabiliyorum.



-Hangi dosyaya erişmek istiyorsak etc en alt dizin oldğu için pwd üzerinde oynama yaparak dosyalara erişim sağlanabilir.