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

**29.07.2021**

Command Injection

-Saldırgan kişinin doğru yapılandırılmamış bir uygulama üzerinden hedef sistemde dilediği komutları çalıştırabilmesidir.

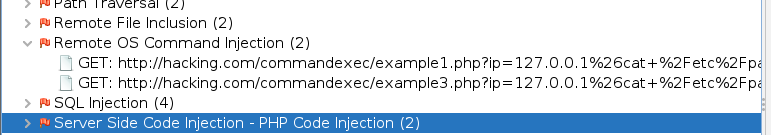
-Command injection üzerinde saldırı yapılan işletim sistemine uygun komutlar kullanılır. Komut ile kastedilen şey Windows da CMD,Linux da Terminal penceresine girilen sistem komutlarıdır.

- Çalışan komutlar uygulamanın yetkileriyle çalışır.

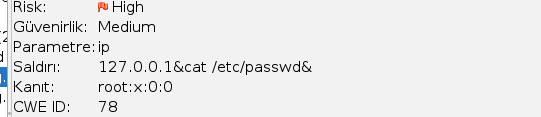
-Kullanıcıdan veri girişi beklenen her noktada bu güvenlik açığı bulunabilir.

-Command Injection zafiyeti için WFP üzerinden 3 uygulama yapılacaktır.

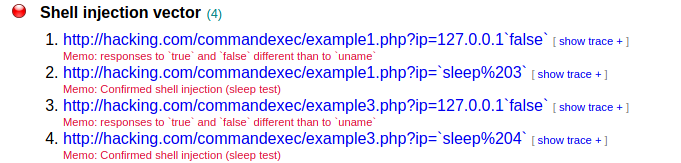
**Uygulama 1 :** Temel Kullanım



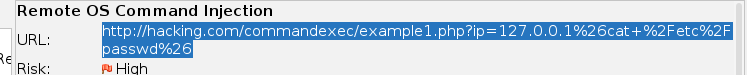
- Zaproxy üzerinden zaafiyeti görüntüleyebiliyoruz.



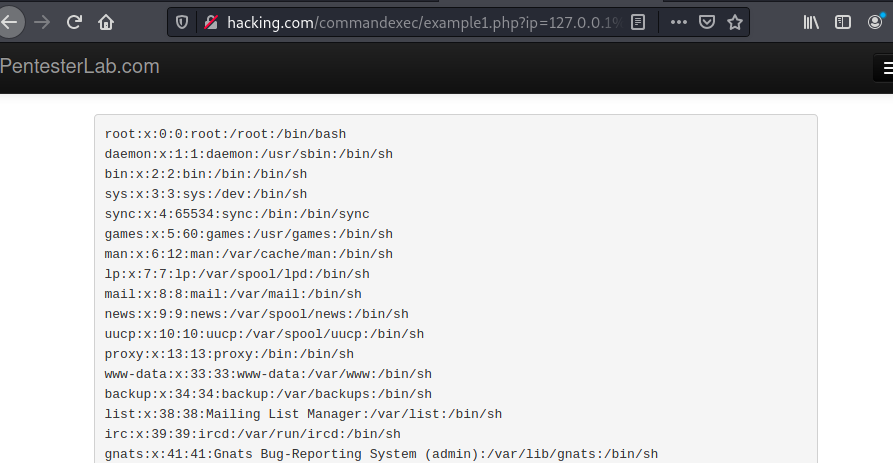
- Ayrıntılarına baktığımızda /etc/passwd dizinini cat aracılığıyla okumuş.



- Skipfish zaafiyeti bulmuş fakat bize bilgi konusunda eksik kalmış.



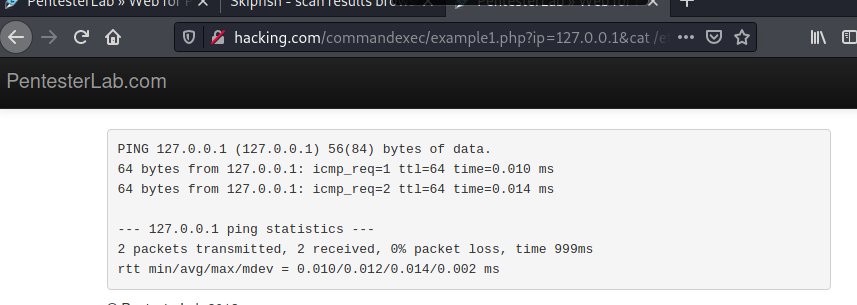
-Owasp zap üzerinden bulmuş olduğum zaafiyetin URL'sini kopyalıyorum ve Firefox üzerinde çalıştırıyorum.



- Firefox üzerinde açtığım zaman karşıma bu ekran geliyor.



- Zaproxy üzerinde saldırı kısmında bulunan ip= kısmından sonraki kısmı kopyalıyorum.



-Önceki ekranda sonuçlarını görürken bu ekran üzerinde sonuçları göremiyoruz.Bunun sebebi; URL formatında olmamasıdır.

-Bu sebeple bu adımda URL formatına encoder ile getireceğim.

>>>>>>



-Encode işlemi gerçekleştiriyoruz ve burada yapılan işlemi daha net görebiliyorum.

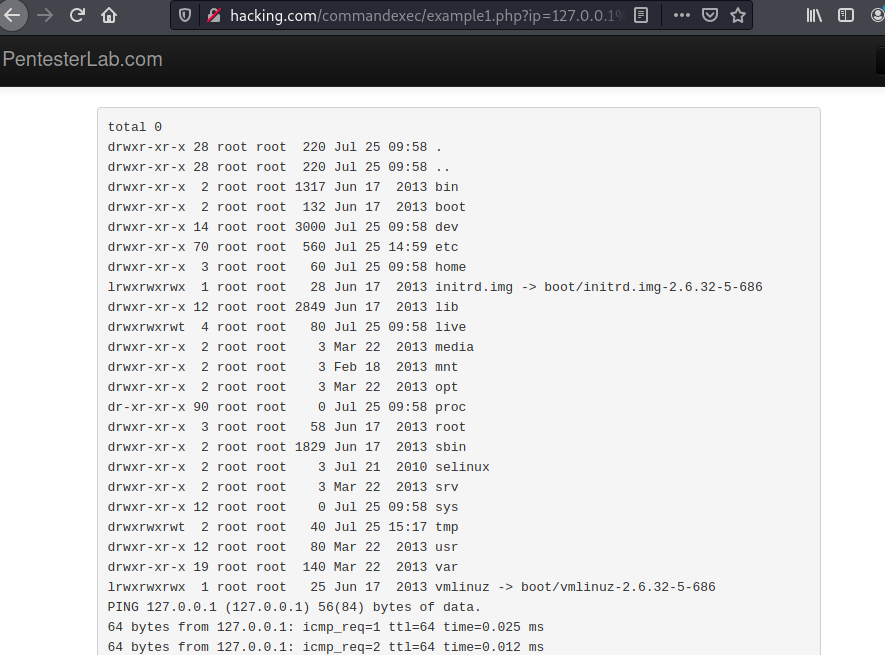
-

>>>>>>>>>>>



-Şimdi ise decode işlemi gerçekleştiriyorum ve istediğim komutları gömüyorum.

-Eklemiş olduğum komutlar ile Decode ediyorum ve URL biçimine getiriyorum.

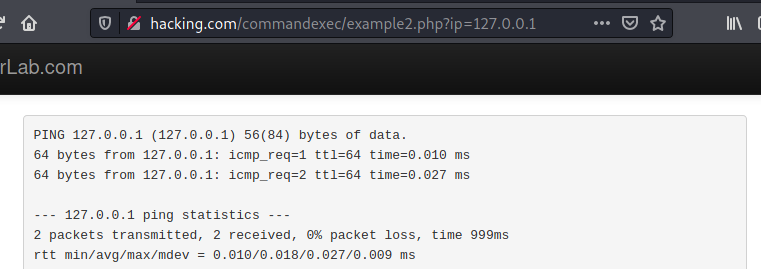


-Decode işleminden sonra çalıştırdığımda zafiyetten başarılı bir şekilde yararlandığımı görüntülüyorum.

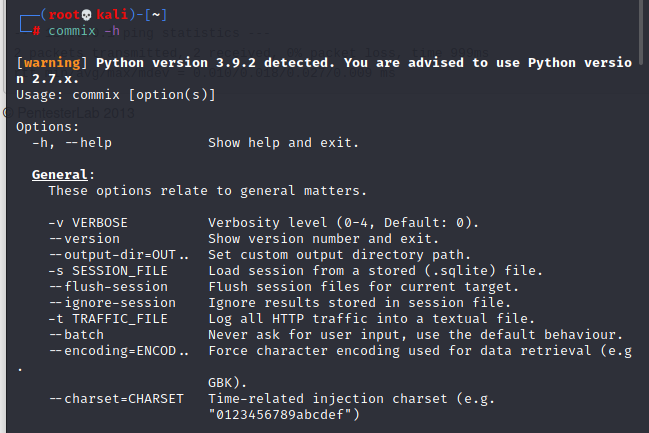
**Uygulama 2 :** Otomatik olarak sunucuya sızma

-Zaproxy ve skipfish araçları zaafiyet testlerini yaptı fakat bir zaafiyet bulamadı.Zaafiyet bulamadı diye bırakmıyoruz.

-Otomatik olarak işlem yapan program olan commix aracından yararlanacağız.

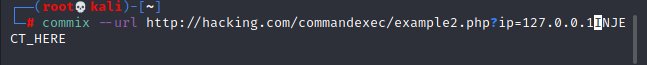


-WFP üzerinden ilk önce zaafiyet olan linkimize bakalım.Ayrıca bu esnada commix aracında kullanabilmek için URL’i kopyalıyorum.

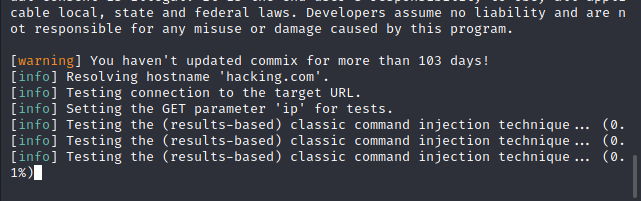


-Commix -h komutu ile commix aracının nasıl kullanıldığına bakabiliyorum.

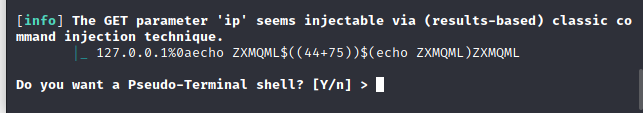
-Kurulu değilse "apt-get install commix" komutu ile kurulum yapabilirsiniz.



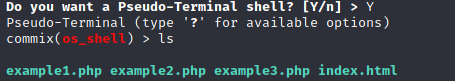
-“commix --url http://Saldırılacaksite.com INJECT\_HERE” formatında çalışmaktadır.Bu işlem biraz uzun sürecektir.



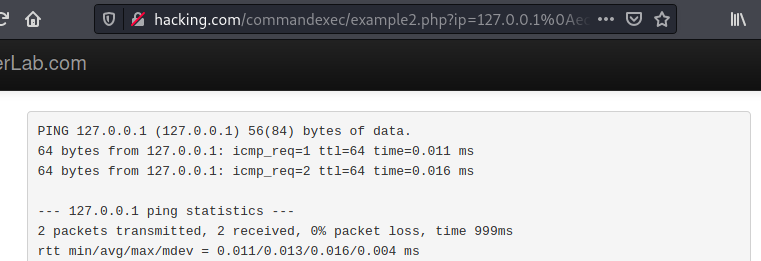
-Arka planda payload denemesi gerçekleştirmektedir.



-Şuanda denediği payloadlar sonucunda zaafiyeti tespit etti ve bana gelen dönüt ile powershell üzerinden sunucuya bağlantı yapmak istiyor musun diyor bunu da Y ile başlatıp bağlantı kuruyorum.



-Şuanda sunucuya direk bağlantı işlemi sağladım.”Ls “komutu ile dizindeki dosyaları görüntüleyebildim ayrıca ” ?” komutu ile de yapılabilecek işlemler hakkında bilgi alabilirdim.

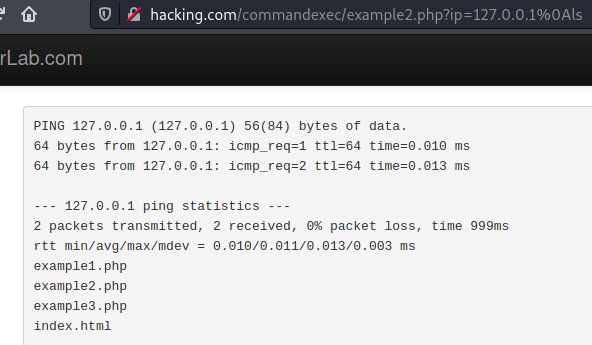


-Programın bana vermiş olduğu 5. adımda gösterdiğim ss deki linki kopyalıyorum ve manuel olarak test ediyorum.

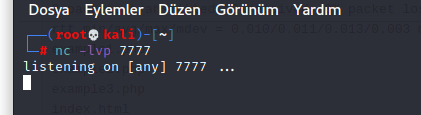


-Link üzerinde baktığımızda %0A komutu ilgimizi çekiyor.Bunun bir alt dizine geçmek olduğunu biliyoruz.Gerekli bilgi verildikten sonra tekrardan işlem yapılamıyor bu yüzden alt dizine geçip işleme devam ediyor.

-Ayrıca echo komutu linux üzerinde yazdırma olduğunu biliyoruz ve burada da echo komutunu değiştirip istediğimiz işlemi yaptırabiliriz.



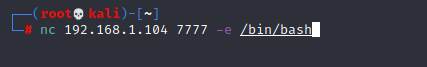
- Burada link üzerinde echo komutunu siliyorum ve yerine “ls” komutunu ekliyorum.



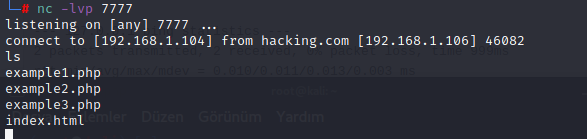
-Kesin yol olarak netcat ile dinlemeye alabilirim ve hedef üzerinden kendime bağlantı kuruyorum.



-“İfconfig” komutu ile İP adresimi sorguluyorum.



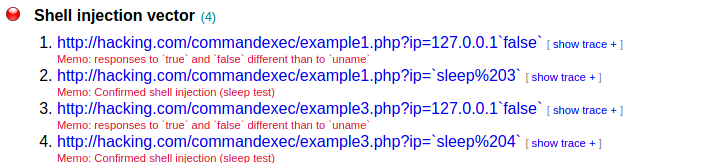
- Bağlantı kurulur kurulmaz hedefin komut satırına düşmek içinde -e parametresiyle /bin/bash parametresini çalıştırıyorum.Eğer bu parametre yazılmazsa bağlantı kurulur fakat herhangi bir işlem yapılamaz.



-Yazmış olduğum ” nc “komutunu kopyalıyorum.Link üzerinde ki ls komutunun yerine yazıp çalıştırıyorum.

-Burada istediğim linux komutunu çalıştırıp işlem yapabilirim.

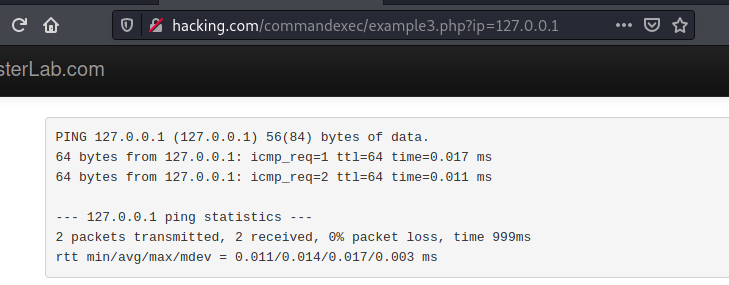
**Uygulama 3 :** Filtreleme atlatma.



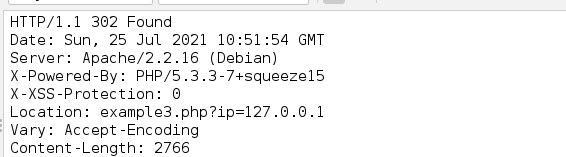
-Skipfish aracı da zafiyeti tespit etti.Fakat daha yüzeysel ele aldığını görebiliyoruz.



-Zaproxy aracı zafiyeti tespit etti.Burada ki linki kopyalıyorum.



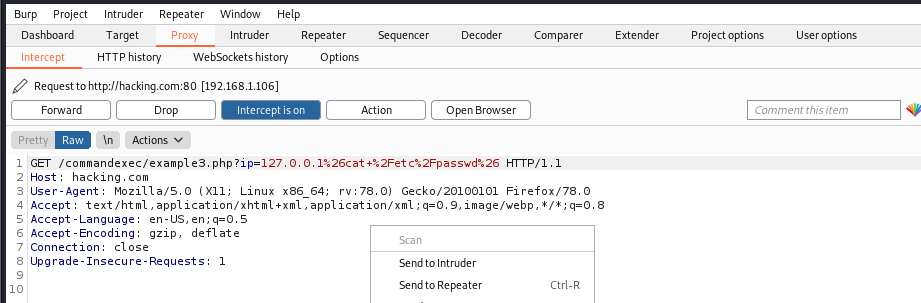
-Tarayıcı üzerinde kopyaladığım bağlantıyı çalıştırıyorum ve karşıma böyle bir ekran geliyor.



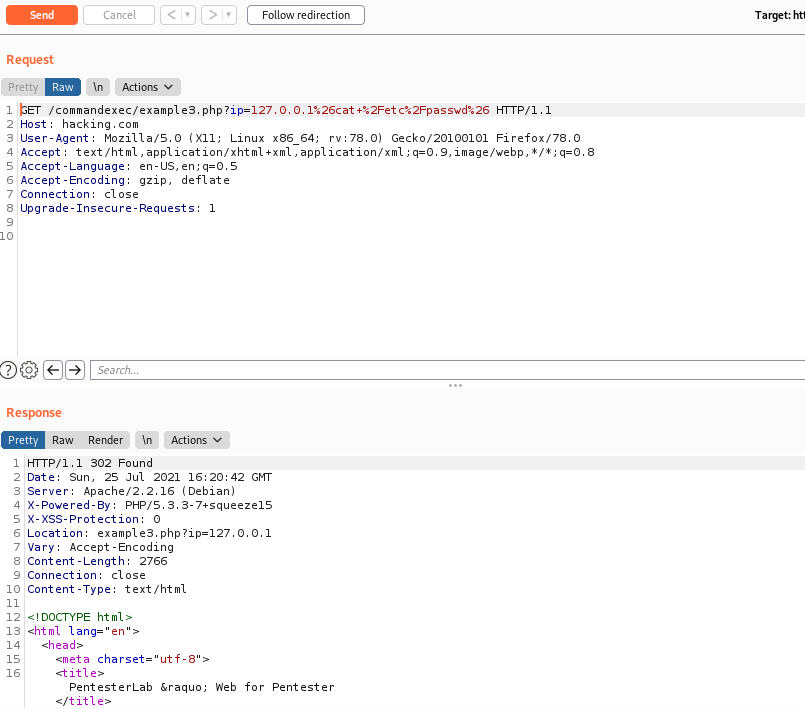
- Bu yüzden zaproxy'e geri dönüyorum ve incelemeye başlıyorum.302 kodunu görüyorum bu yönlendirme komutudur.

-İşlemi gerçekleştikten sonra ana hale tekrardan geri geliyor.

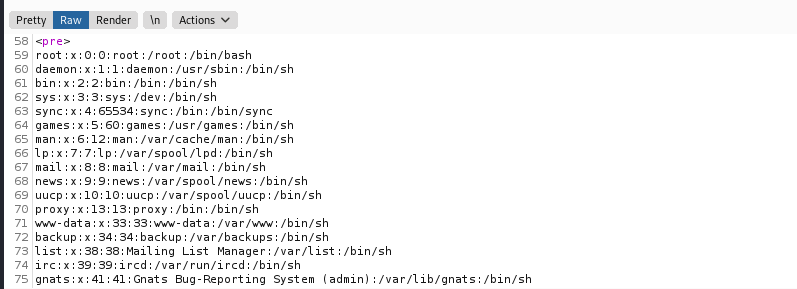
-Passwd dosyasını görüntüleyemedik.Bu zaafiyetide yine burpsuite'in proxy üzerinden elde edicez.



-Proxy intercept ayarını açıyorum ve sayfayı yenileyip bilgileri burpsuite üzerine çekiyorum. İşlemleri daha rahat takip edebilmek için Repeater a gönderiyorum.



-Repeater sekmesine geçiş yapıyorum ve send işlemiyle gönderim yapıyorum.



-Sayfa kaynağına baktığımda aslında istediğimiz işlemler burada gerçekleşmiş durumda eğer repeater üzerinde işlem yapmasaydık bu kaynak kodlarını görüntüleyemeyecektik.

-Zafiyetten arka planda aslında yararlandık fakat görüntüleyemedik bu sebeple bütün kaynakları tekrar ve tekrar incelememiz gerektiğini öğreniyoruz.

***Korunma Yöntemleri***

-Tüm kullanıcı girdileri doğrulanmalıdır.

-Kullanıcı girdilerini kullanan programların yetkileri kontrol edilmelidir.

-Sadece belirli kelimeleri içeren girdilere izin verilebilir.

-Olası saldırı simülasyonları ile testler yapılmalıdır.