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

**29.07.2021**

***Code Injection***

-Uzaktan kod yürütme olarak düşünebiliriz.Saldırganın uygulamaya kötü amaçlı kod enjekte etmesiyle gerçekleşir.

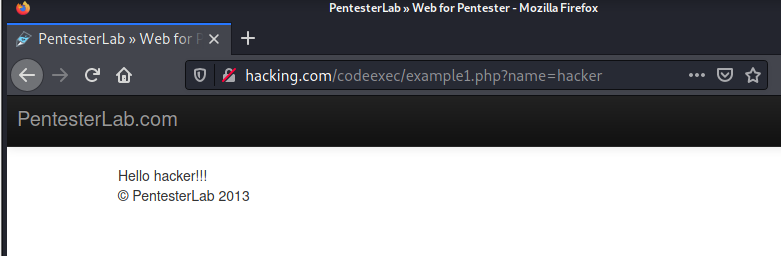
-Doğru yapılandırılmamış bir web uygulaması her zaman bu zafiyet ile karşı karşıyadır.

- SQL güvenlik açığıyla benzerlik gösterir SQLİ da sql kodlarıyla işlem yapılırken.Code Injection ‘da Web uygulaması geliştirilirken kullanılan programlama dili kullanılır.

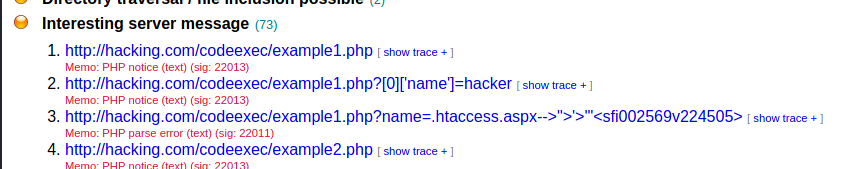
-Kullanıcı girdisinin bulunduğu her noktada bu açık bulunabilir.

-Code Injection için WFP laboratuvarı üzerinden 4 Adet uygulama yapacağız.

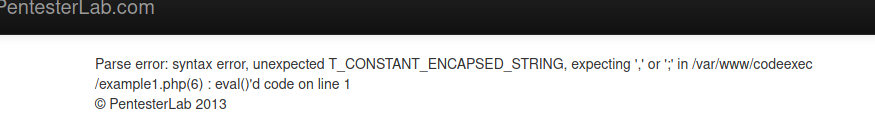
**Uygulama 1 :** Temel Kullanım



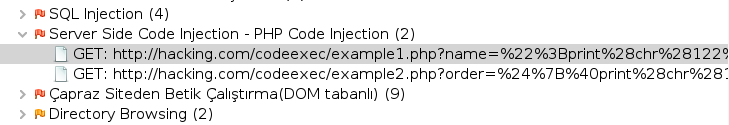
- WFP üzerinden EXAMPLE1’ i açıyorum ve böyle bir ekran bizi karşılıyor.



- Skipfish üzerinden yapmış olduğum teste bakalım.Çok fazla ufuk açıcı bir şeyle karşılaşmıyoruz.



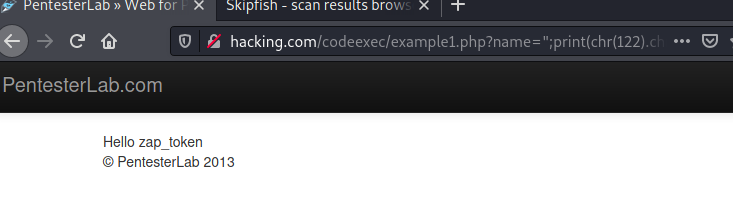
-Skipfish'in bulmuş olduğu zaafiyeti tarayıcı üzerinde açtığımda karşıma böyle bir ekran çıkıyor.



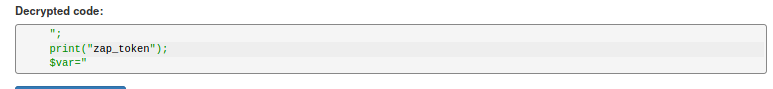
-Zaproxy ile işlem yaptığımızda zaafiyeti bu şekilde buluyor.



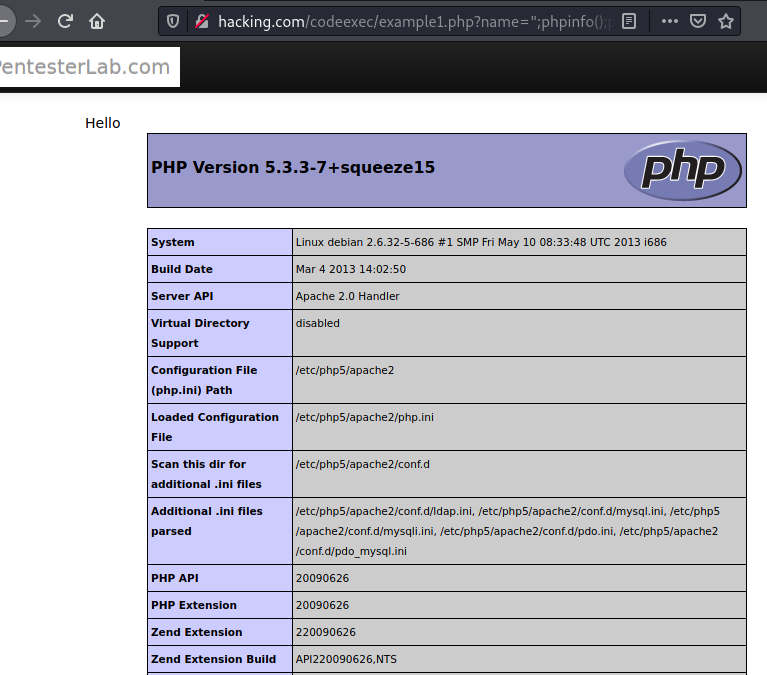
-Saldırı kısmındaki bağlantıyı kopyalıyorum.



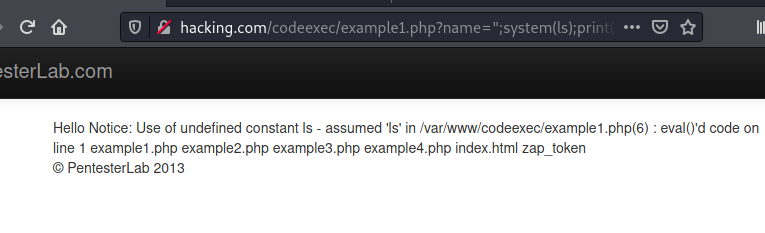
- Kopyaladığım bağlantıyı name= sonrasına yapıştırıyorum ve karşıma böyle bir ekran çıkıyor önceki sayfa bilgisine baktığımda farklı olarak sistemin bu sefer ünlem vermediğini görebiliyorum.



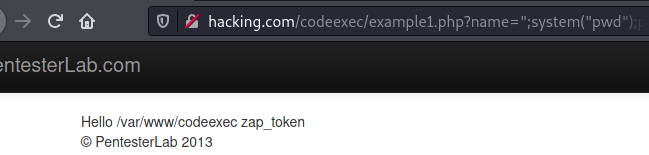
-URL’i PHP decoder ile dönüştürdüğümde print("zap\_token"); işlemini gömülü bir şekilde yaptığını görüntülüyorum.



-Url üzerinden araya kattığım phpinfo() komutu ile php bilgisini getirebildim.

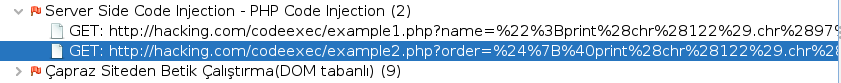


- Sistemin linux olduğunu gördüğüm için system(ls) komutu ile bulunduğum dizinde ki php dosyalarını görüntüleyebiliyorum.

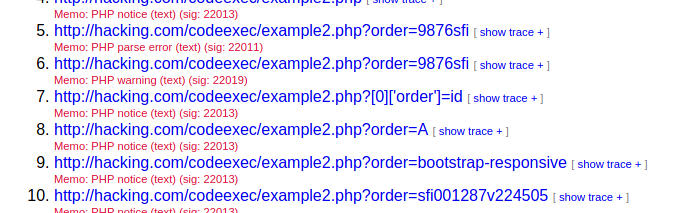


- “system("pwd")” komutu ile hangi dizinin içerisinde olduğumu görüntüleyebiliyorum.

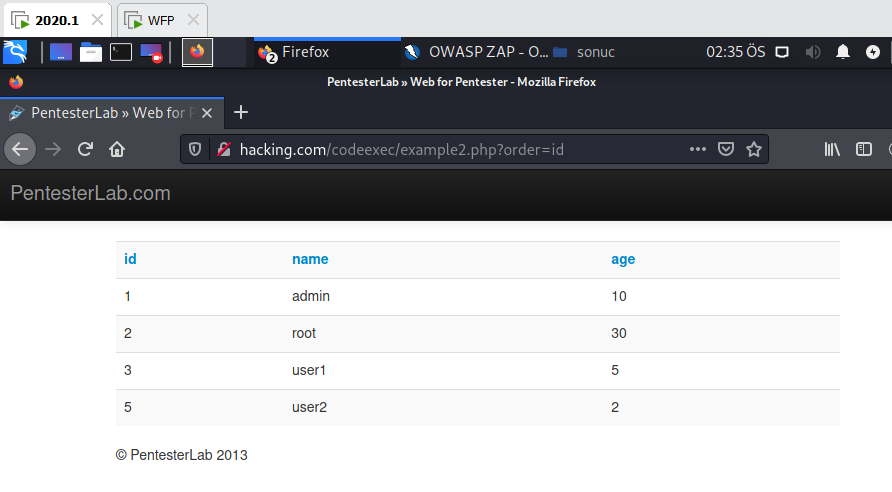
**Uygulama 2 :** Filtreleme atlatma



-Zaproxy üzerinde baktığımızda zaafiyeti bulduğunu görüntüleyebiliyoruz.



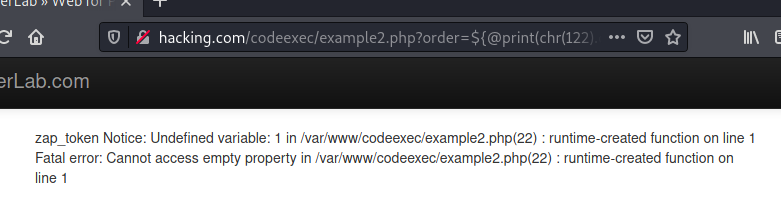
- Skipfish aracıda zaafiyeti algılıyor fakat çok anlaşılır düzeyde bilgiler vermiyor.



-WFP üzerinden de baktığımız zaman zafiyet sayfamız bu şekilde gözüküyor.



-Zaproxy üzerinden saldırı kısmında ki bağlantıyı kopyalıyorum.

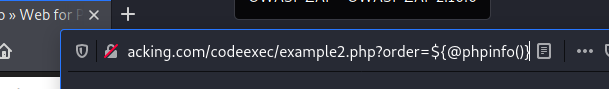


-Ardından WFP üzerindeki order= sonrasına yapıştırıyorum çıkan ekran üzerinde hata alsam da işlemin aslında çalıştığını görebiliyorum.

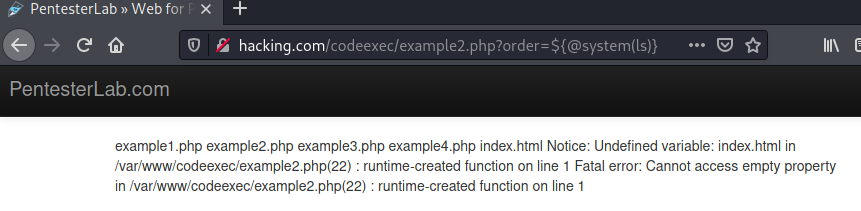
- Bu sebeple link üzerinden birazcık daha oynamaya başlıyorum. Bir önceki örnekte gösterdiğim decoder kısmında ki kod ile yine zap\_token yazdırıyor fakat burayı silip başka bir komut girersem çalışacağını düşünüyorum ve deniyorum.



-Link içerisine Encoder sayesinde phpinfo() komutunu gizliyorum ve çalıştırdığımda başarılı bir şekilde çalışıyor.

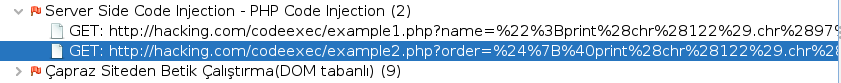


-Çalıştırdığım linki tam olarak göstermek istiyorum.

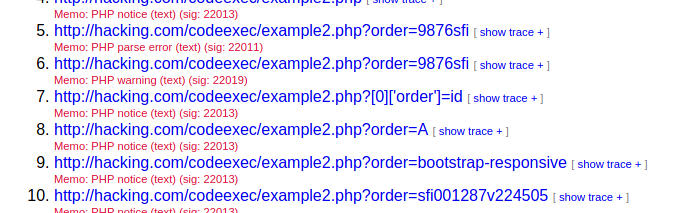


- Bir önceki örnekteki gibi system(ls) komutu ile zafiyetten yararlanıyorum.

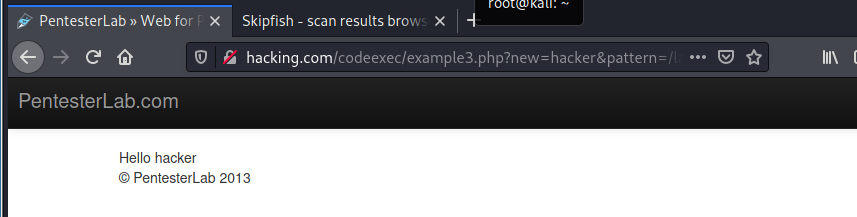
**Uygulama 3 :** Burpsuite ve Payload listeleriyle çalışma.



-Zaproxy aracı zafiyeti buldu fakat yüzeysel bir bilgilendirme yaptı.



-Skipfish aracı da zafiyeti buldu fakat o da yüzeysel bir bilgilendirme yaptı.

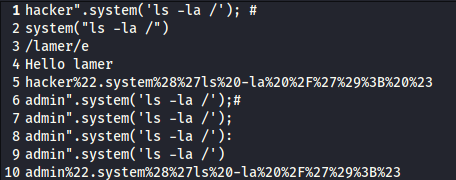


-Önce zafiyetimizin sayfasına bakalım.

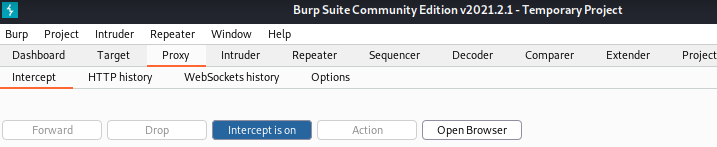
-Zafiyet testlerimden de çok fazla bilgi alamadığım için Burpsuite üzerinden payload denemesi yapmak istiyorum.



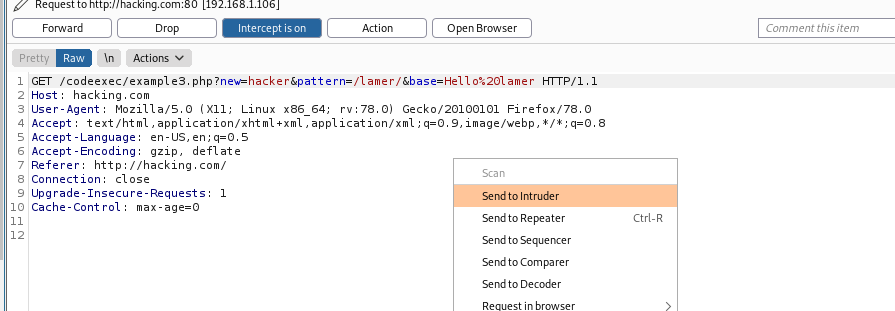
-Git clone komutu ile payload dosyamızı indiriyoruz.Siz isterseniz başka bir payload ile çalışabilirsiniz.



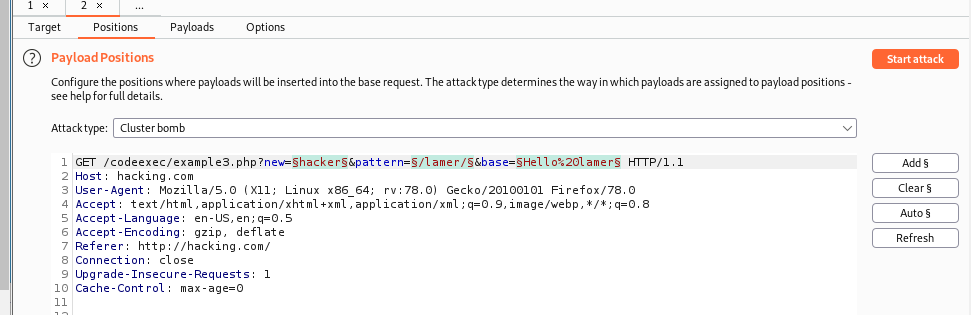
-İndirdiğimiz payload listesinin içeriğini az da olsa göstermek istiyorum.



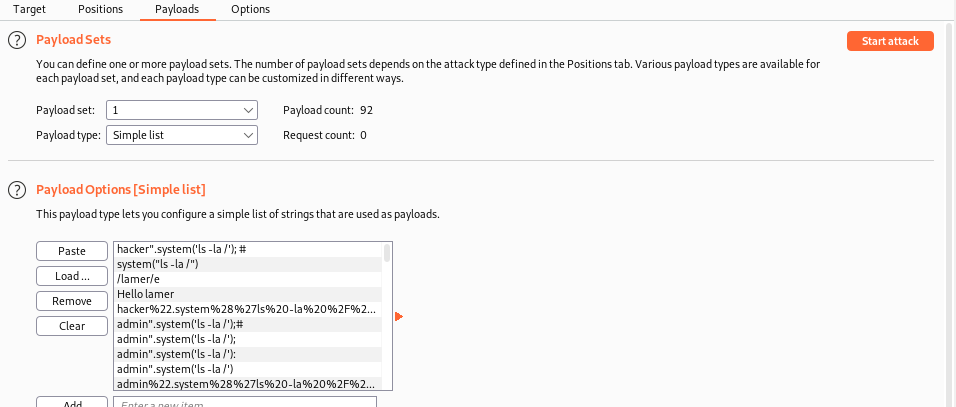
-Payload işlemi için kullanacağım Burpsuite aracını çalıştırıyorum.Öncelikle proxy konumundan İntercept ayarını On konumuna getiriyorum.Bu ayar ile dinleme moduna geçiş yapıyor.



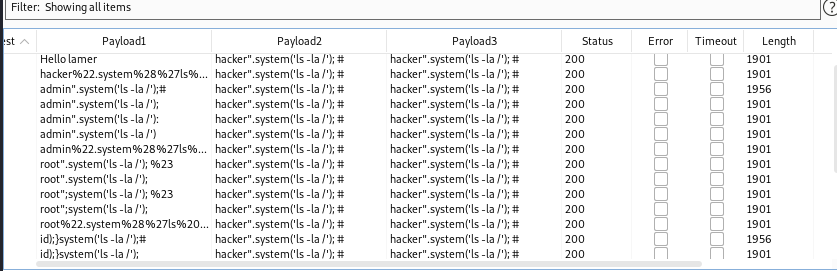
-Ardından WFP üzerinden sayfa yenileme işlemi yapıyorum ve BurpSuite üzerine bilgileri çekiyorum.Ardından bilgileri Intruder kısmına gönderiyorum.



-İntruder sekmesine geçiş yapıyorum.Önceki yaptığımız örneklerde tek alan üzerinde deneme yapıyorduk bu sefer 3 alan üzerinde çalışıcaz.Attack type'ini Cluster Bomb olarak ayarlıyorum.



-Ardından payload kısmına geçiş yapıyorum ve Payload set kısmından 1-2 ve 3 alanları için de Payload options bölümünden paste butonuna basıp payloadımı ekliyorum ve Start attack ile işlemi başlatıyorum.

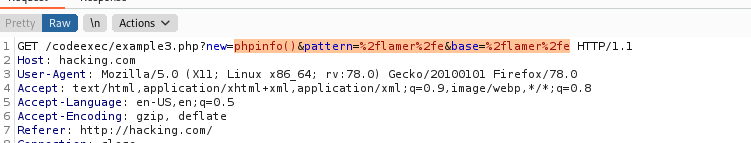


-Burpsuite üzerinden işlemi başlatıyorum ve önceki yapmış olduğumuz Burpsuite işlemlerinde length üzerinden farklı olanları deniyorduk bu sefer ise uzunluğu en yüksek olan değer üzerinden işlem yapacağız.

-Yaklaşık olarak 770.000 deneme yapılacak biraz deneme sayısı arttığında tekrardan sonuçlara bakacağım.



-Yaklaşık 10-15 dakika sonrasında uzunluk değeri diğerlerinden çok çok fazla olan bir değer yakaladım.



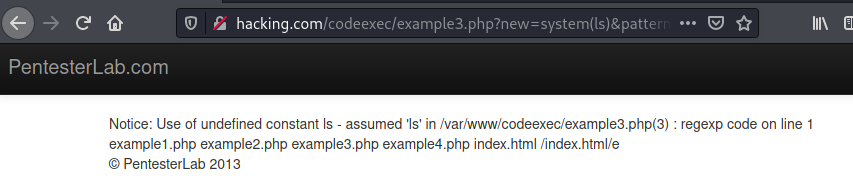
-Yüksek değerli zafiyetin linkini kopyalıyorum.



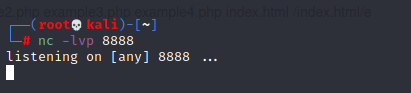
-Kopyaladığım bağlantıyı wfp sitesi üzerinde çalıştırıyorum ve php komutu açıldığını görüyorum.



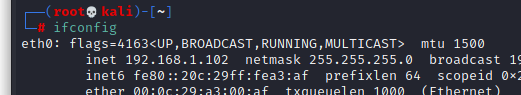
-Linki incelediğimiz zaman phpinfo() kısmını değiştirdiğimizde istediğimiz bilgilere erişim sağlayabiliriz.



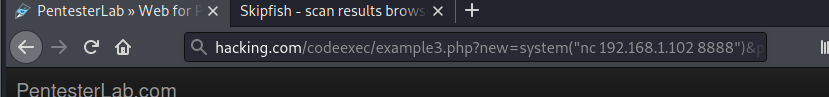
-System(ls) komutunu phpinfo içerisine koyarak başarılı şekilde .php dosyalarını listeleyebildik.Hata gözüküyor ama istediğimiz zaafiyeti elde ettik.



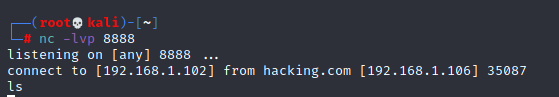
-Şuanda sistem üzerinde netcat kurulu ise bağlantı kurmam mümkün hale gelicektir.Bunun için ilk önce rastgele bir portu dinlemeye alıyorum.



-Ardından kendi IP adresimi öğreniyorum ve bir sonraki işlemde link üzerinden bağlantı göndereceğim.

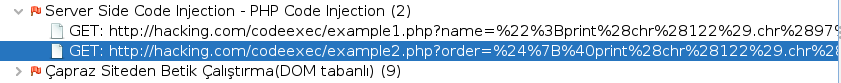


-Link içerisine eklediğim komut ile kendi IP adresime ve dinlediğim porta bir istek gönderdim.

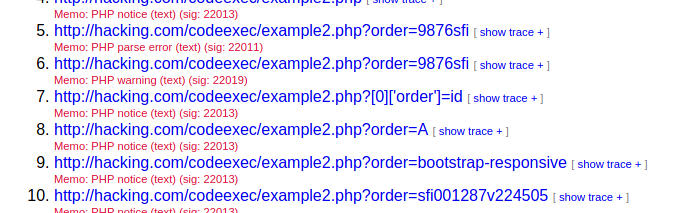


-WFP üzerinde işlem yapıyorum bundan sonrasına sisteme zarar gelmesin diye engellenmiş normalde bir sunucuya bu şeklde erişim sağladığımızda devamını çok rahat bir şekilde getirebiliriz.

**Uygulama 4 :** BurpSuite ile güvenlik açığı tespiti



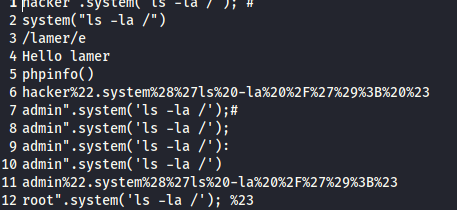
-Zaproxy üzerinden zafiyeti görüntüleyemedim.Bu yüzden skipfish üzerinde bir arama gerçekleştireceğim.



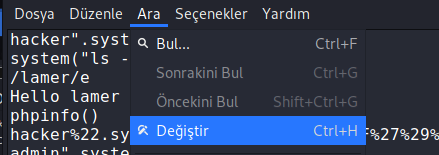
-Skipfish uygulaması yüzeysel olarak bilgilendirme yaptı.

-Bir önceki uygulamamızda length değeri yüksek olan üzerinden işlem yapmıştık fakat bu her zaman çalışacak diye bir kesinlik yoktur.Altta kalan bir değer de zaafiyet kullandırtabilir.

-Şuan yapacağımız işlem ise en doğru sonucu elde edeceğimiz yöntemdir.

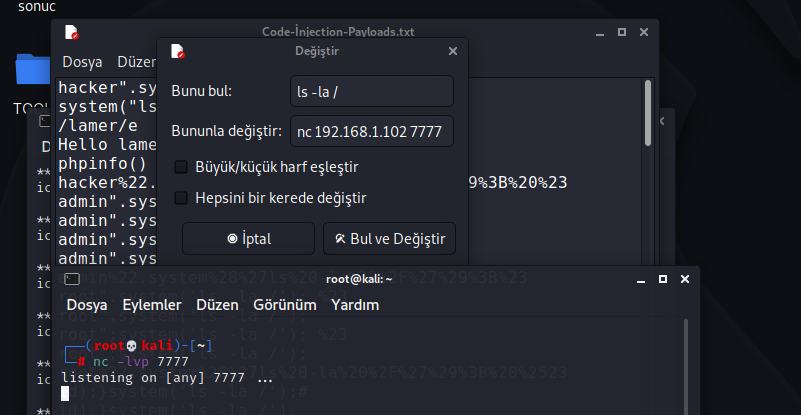


-” ls -la “ komutu üzerinde oynama yaparsam zafiyeti farklı bir yoldan kullanabilirim.

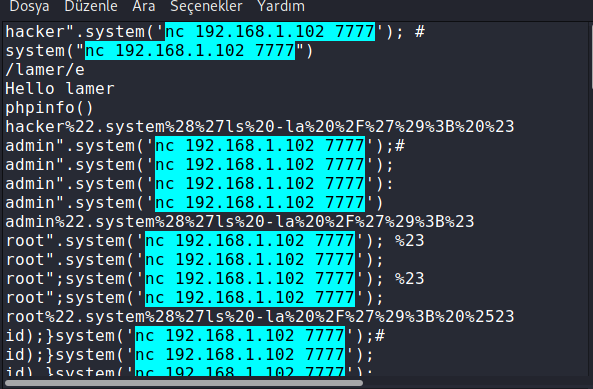


-Buraya nc komutunu ekleyip direk erişimi deneyeceğim.Bunu tek tek yapamayacağım için dizinin içerisinde uç birim açıyorum ve “leafpad” ile düzenleme yapıyorum.

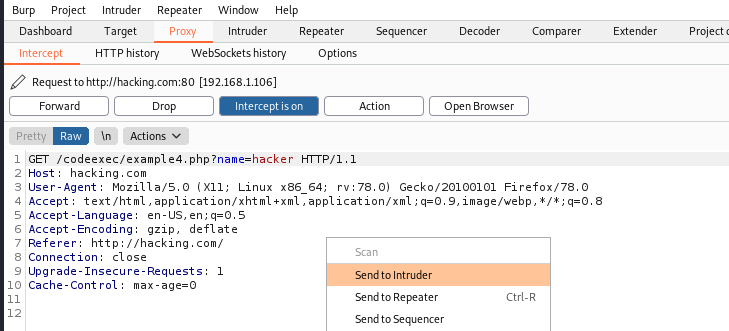
-Leafpad ile açtıktan sonra değiştireceğim kısmı kopyalıyorum ve ara bölümünden değiştir seçeneğine giriş yapıyorum.



-7777 portunu dinlemeye alıyorum ardından kendi IP numaram ve dinlemeye aldığım port ile değiştirme işlemini gerçekleştiriyorum.



-Değişim işlemi tamamlandı şuanda yapmış olduğum işlemde payloadlardan herhangi biri çalışır ise direk sunucuyla bağlantım kurulacak.

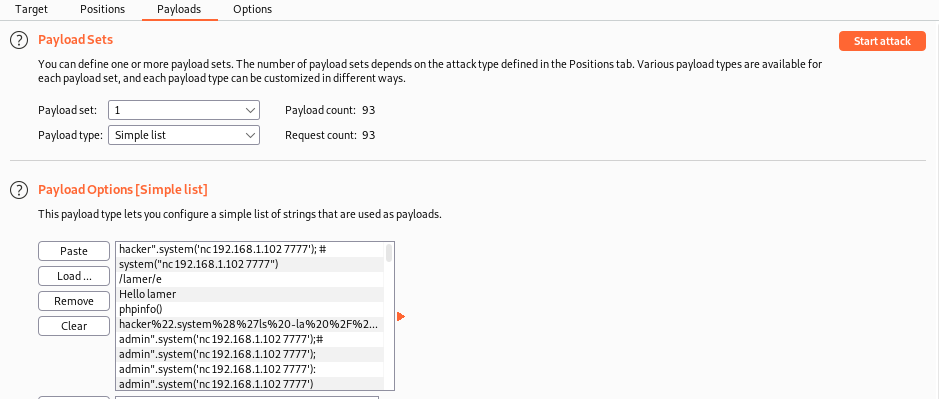


-Burpsuite uygulamasını açıyorum ve proxy İntercept On ayarını açıyorum ve Firefox üzerinden zafiyetimin bulunduğu sayfayı açıp yeniliyorum.

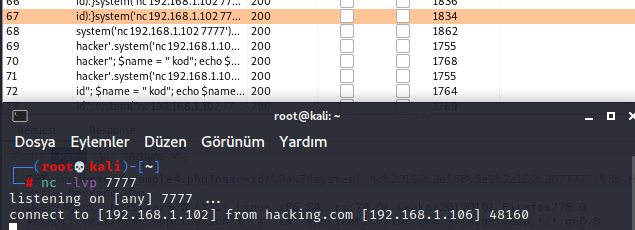
-Sağ tıklayıp Intruder sekmesine gönderim yapıyorum.



-İntruder sekmesi üzerinde positions kısmını kontrol ediyorum.Doğru konum üzerinde işlem yapıyor.Ardından payloads kısmına geçiş yapıyorum.



-Payloadlarımı ekleyip saldırıyı başlatıyorum.Doğru sonuca ulaştığımda nc üzerinden dinlediğim porta bilgi çekilecek.



-Kullanmış olduğum payloadlar başarılı bir şekilde çalıştı ve nc üzerinden dinlediğim porta bağlantı geldi.

-Kısıtlama olduğu için burada işlem tıkanıyor normalde başka bir sunucu üzerinde işlem yapsaydık devamını getirebilirdik.