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

**30.07.2021**

**XML**

-Hem insanlar hem de bilgi işlem sistemleri tarafından kolayca okunabilecek dökümanlar oluşturmaya yarayan bir işaretleme dilidir.Bilginin yer değiştirmesi gerektiği durumlarda birkaç adımda bilgi olduğu şekilde diğer platforma taşınabilir.

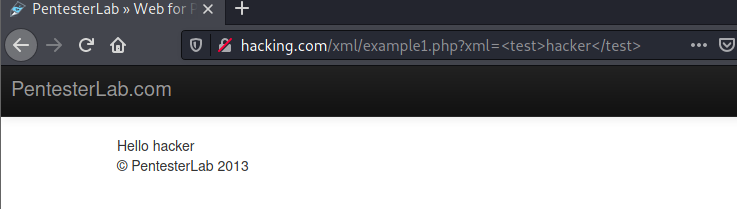
Örneğin;Web site sayfalarının arama motorları tarafından kısa sürede taranması çin XML’le oluşturulacak bir site haritası kullanılabilir.

**XXE**

-XML uygulamalarında oluşan güvenlik açıklarına XXE(XML External Entity) denmektedir.XXE güvenlik açığı kullanılarak hedef sistemdeki hassas dosyalar okunabilir,dos atak saldırısı,port tarama,ssrf ve uzaktan kod çalıştırma gibi ciddi saldırılar yapılabilir.

-Bu zafiyetle ilgili WFP üzerinden 2 adet uygulama gerçekleştireceğim.

**Uygulama 1 :** Burpsuite ile Payload çalışması.

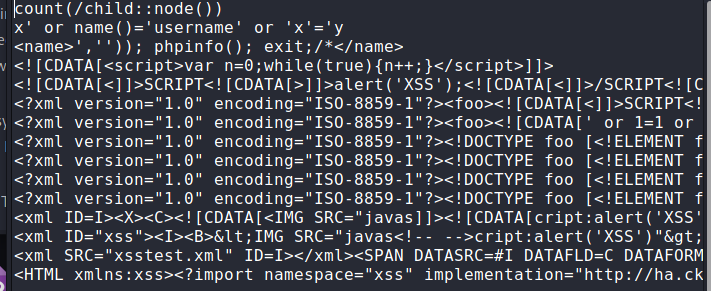


**-** Öncelikle WFP üzerinden zafiyetimi açıyorum ve karşıma böyle bir ekran geliyor.Bu site üzerinden dikkatimi çeken şey HTML diliyle taglenmiş link kısmı çekiyor.Buradan bir zafiyete ulaşabileceğimi düşünüyorum.

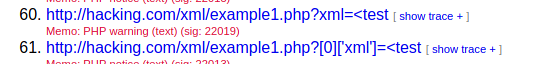
-Aklıma Burpsuite üzerinden payload attack yapmak geliyor.



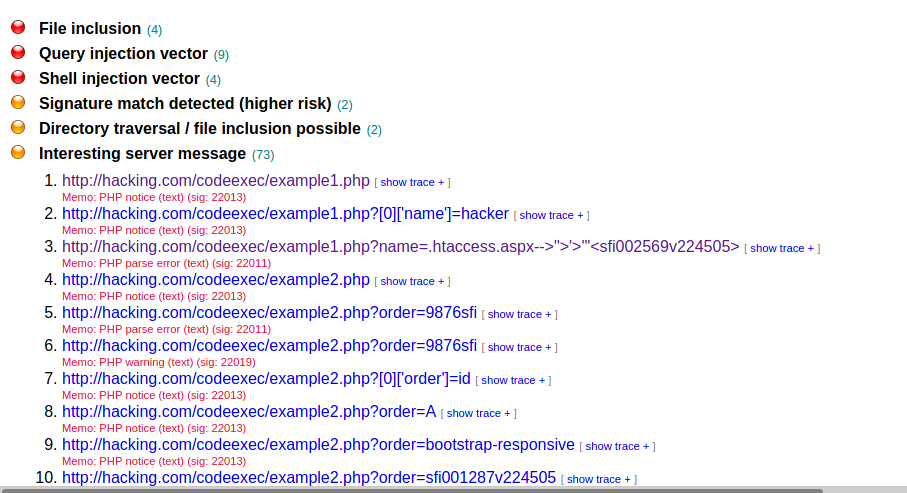
-Verdiğim bağlantı üzerinden payload kodlarına erişim sağlıyorum.



-Verdiğim bağlantı üzerinden indirdiğimiz payloadlara göz atıyoruz. Bu konuda çok fazla kullanılan payload yoktur bu sebeple sayısı biraz az.

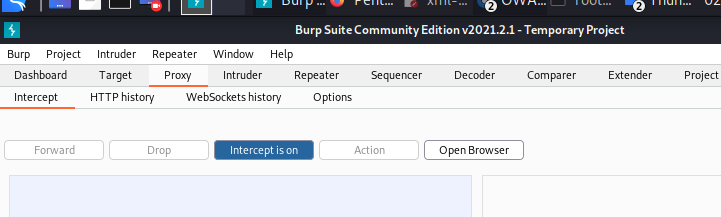


-Skipfish aracına baktığımda HTML denemeleri yapldığını ve sitenin bir hata mesajı döndürdüğünü bildiriyor.

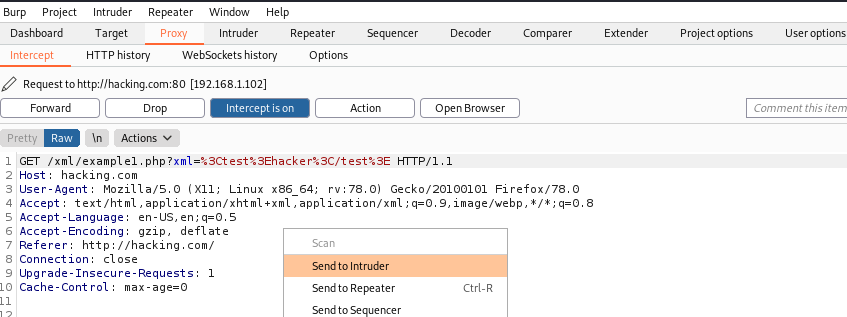


- Ayrıca skipfish üzerinde baktığımda bunun bir açık değil sadece sitenin bu denemeler

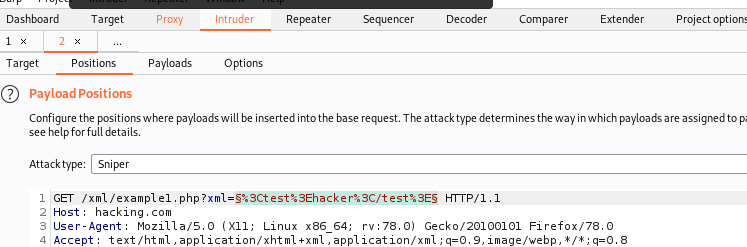
“sonuç –hata” mesajı döndürdüğünü aktarıyor.



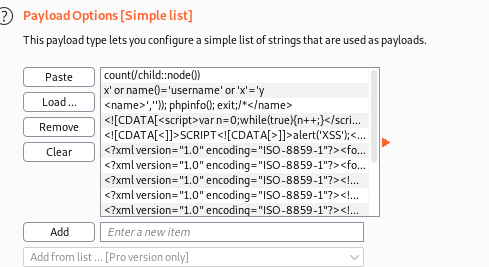
- Öncelikle payload atağı için Burpsuite'i çalıştırıyorum ve gerekli port bağlantılarını yaptıktan sonra Intercept ayarını on konumuna getiriyorum.



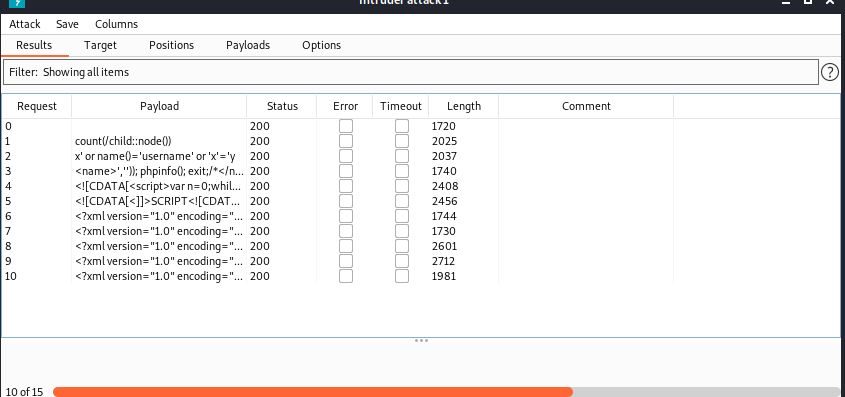
-Ardından WFP'a geçiş yapıp sayfayı yeniliyorum ve bilgileri Burpsuite üzerine çekiyorum.Ardından “Send to intruder “sekmesi ile Intruder bölümüne gönderiyorum.



- Intruder kısmında Attack gerçekleşecek bölüme bakıyorum değişecek bir ayar yok.Ardından Payloads bölümüne geçiyorum.

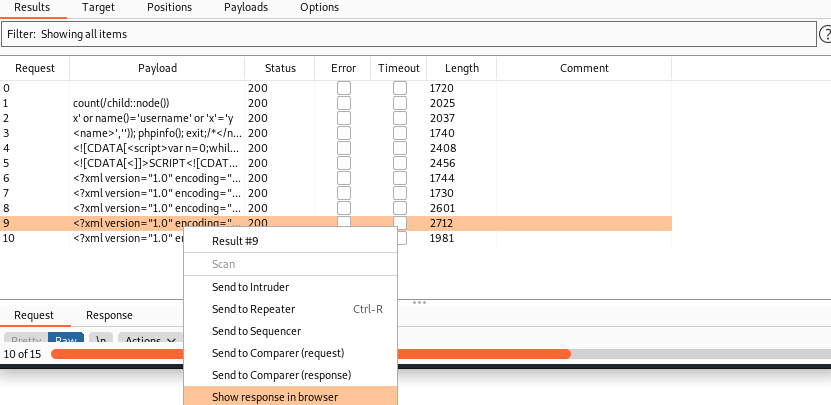


- İndirmiş olduğum Payloadları kopyalıyorum ve Burpsuite üzerine aktarıp işlemi başlatıyorum.

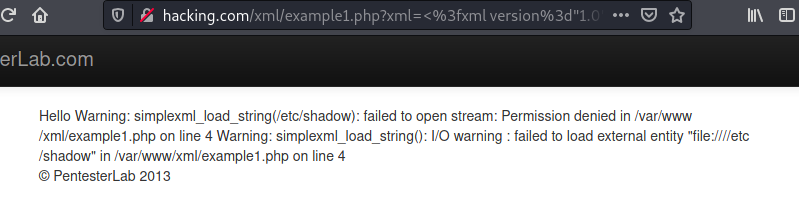


- Önceki yapmış olduğumuz işlemlerde uzunluklar üzerinden işlem yapıyorduk burada baktığımızda hepsinin uzunluğu birbirinden farklı.

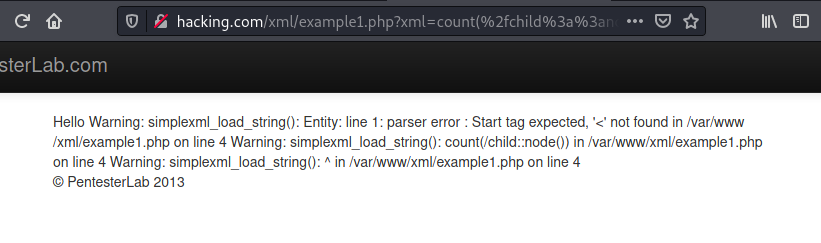
-İşlem 10 denemesinde durdu bunun sebebi çalıştırmış olduğu html komutlarında işlem başarılı oldu ve kendini duraksattı.Eğer sistem durmasaydı çıkan sonuçları tek tek denemek zorundaydık.



- Çıkan sonuçları web üzerinde görüntülemek için Show Response in browser seçeneğini kullanıyorum.



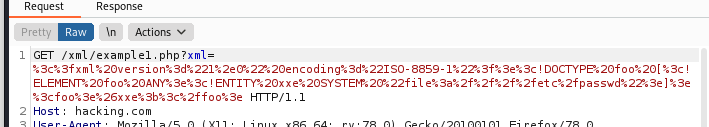
- 10.Satırdaki kodu görüntülediğimde böyle bir hatayla karşılaşıyorum demek ki bu işlem başarısız kalan işlemlere bakıyorum.



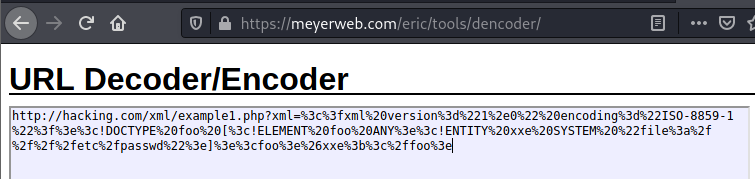
- 1.Satırdaki kodu görüntülediğimde böyle bir hatayla karşılaşıyorum demek ki bu işlem başarısız kalan işlemlere bakıyorum.



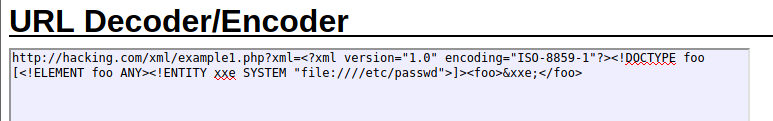
- 9.Satırdaki kodu çalıştırdığımda istediğim sonuca ulaşıyorum.



-Dönütü daha anlamlı hale getirmek için Burpsuite üzerinden kopyalıyorum. ve “URL decoder” üzerinden bir dönüştürme işlemi yapacağım.

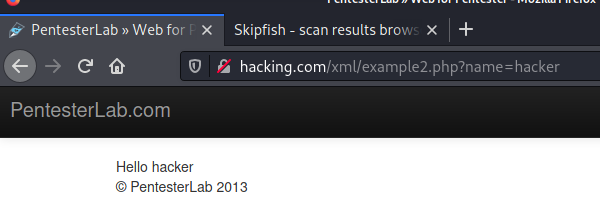


- Kopyaladığım URL'i decodera yapıştırım DECODE ediyorum.

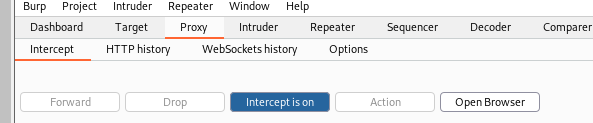


- Decode işlemi gerçekleştirdiğimde xml kodunu çalıştırdığını ve bana passwd dosyasını aktardığını anlayabiliyorum.

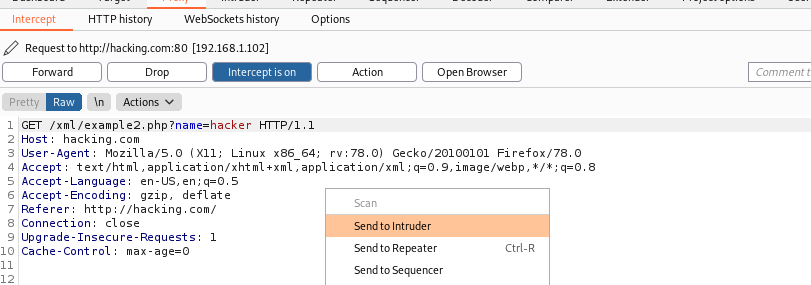
**Uygulama 2 :** SQL Tarzı Sonuç Elde Etme.



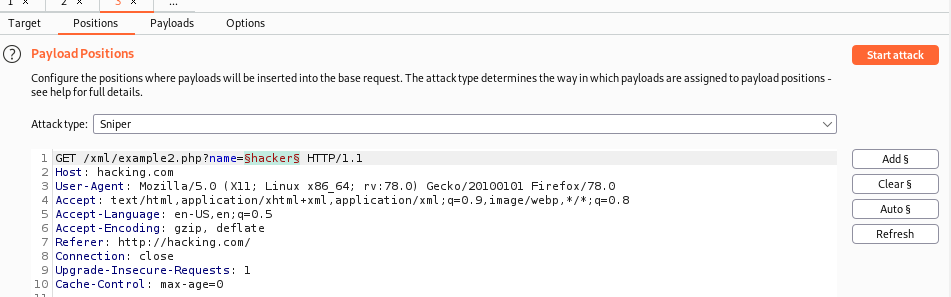
-Öncelikle WFP üzerinden zaafiyetli olan siteye bakıyorum.Yine payload üzerinden işlemimi gerçekleştireceğim.



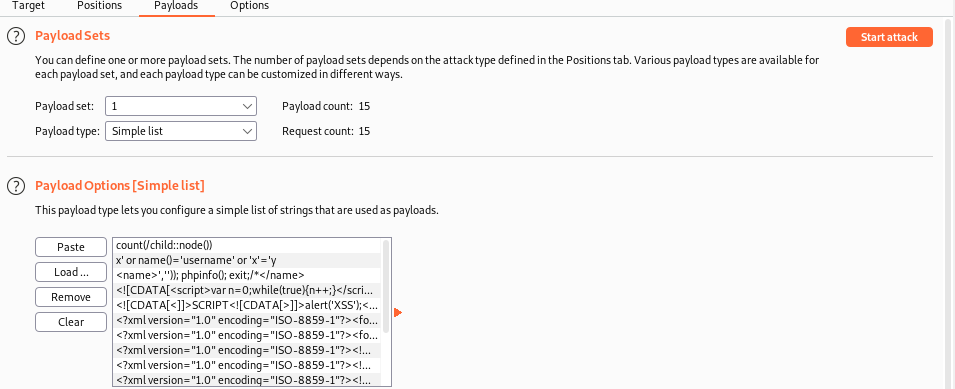
- İşlemlerime Burpsuite üzerinden devam edeceğim için Burpsuite üzerinden Intercept on ayarını açıyorum ve linkimi yeniliyorum.



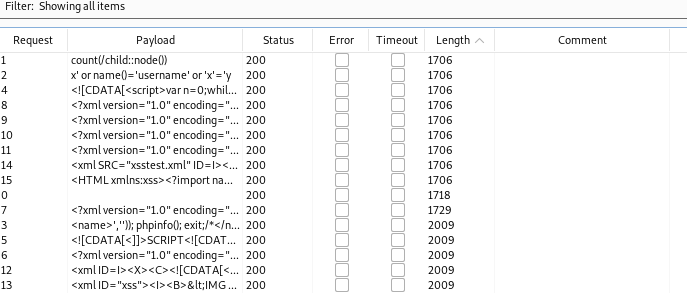
-Önce sağ tıklayıp “Send to Intruder” ile Intruder sekmesine gönderiyorum.



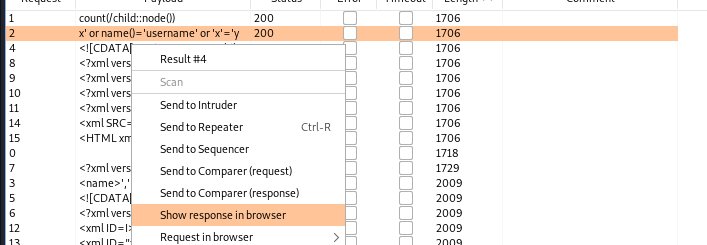
- Attack yapılacak yerin doğru konumda olduğunu görüntülüyorum ve “Sniper attack” yapacağım için burada bir düzenleme yapmıyorum.



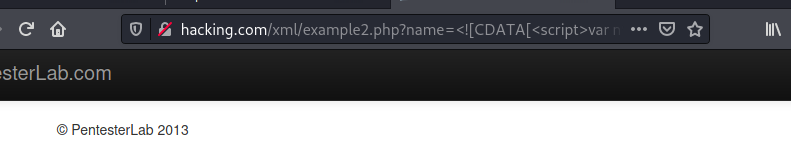
- Ardından “payloads” bölümüne geçip indirmiş olduğum payloadı ekliyorum.Ardından işlemi başlatıyorum.



- Payload denemesi sonrasında çıkan sonuçlar bu şekildedir.

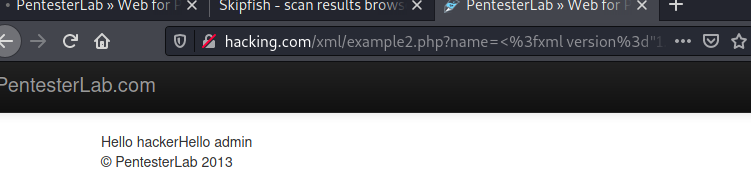


- Uzunlukları farklı olanlara tek tek web üzerinden görüntüleyeceğim.Bunun için sağ tklayıp “Show Response” sekmesine basıyorum.



-Önce 1706 uzunluğuyla başlıyorum buraya baktığımda tarafıma bir şey dönmediğini görüyorum.

- 1718 Değeri boş olduğu için geçiyorum.



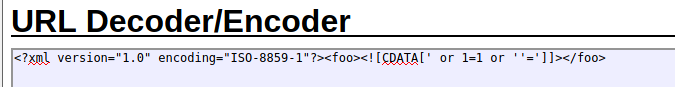
- 1729 değeri ile devam ediyorum.Tarafıma tüm kullanıcıların listelenmesini sağladı.



- Linkin daha anlaşılabilir olması için Burpsuite üzerinden linki kopyalıyorum.



- Herhangi bir Decoder üzerinden URL dönüştürmesi işlemi yapıyorum.



- Kullanılan HTML kodlarıyla tarafıma sistemdeki kullanıcıları getiren kodu görüntüleyebiliyorum.Bu kodlara baktığımda SQL Attack sırasında kullanılan Payloadlara benzerlik sağladığını görüntüleyebiliyorum.