**BASIC XXE WRİTE-UP**

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında XXE zafiyetinin Basic XXE labının çözümünü anlatacağım.

**SENARYO:** Bu laboratuvar, sistem içindeki yerel dosyalara yetkisiz erişime yol açan bir XML External Entity Injection (XXE) zafiyeti içerir.

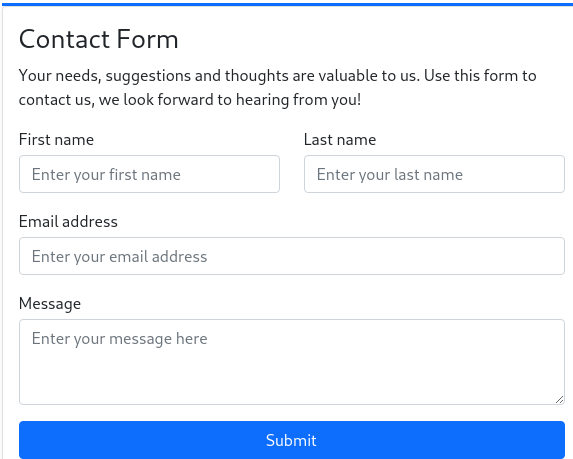
Laboratuvarı tamamlamak için web sayfasındaki iletişim formundaki XXE zafiyetini istismar ederek ve /etc/password dosyasının içeriğine erişin.

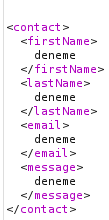
**/etc/passwd dosyasına eklenen son kullanıcının adı nedir?**

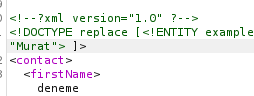
**ÇÖZÜM:**

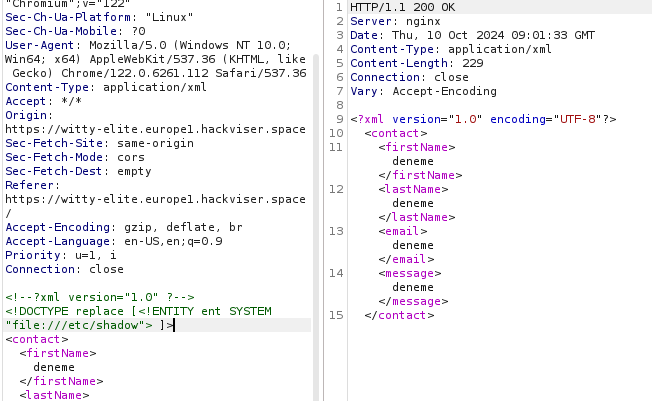
*XXE: Bir saldırganın bir uygulamanın XML verilerini işlemesine müdahele etmesine izin veren bir web güvenlik açığıdır.*

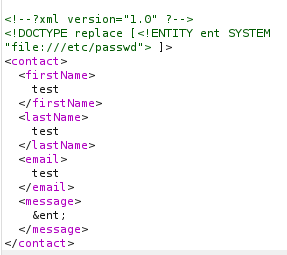
Şimdi lab’ımızı çözmeye başlayalım. Siteye giriş yapıyoruz.

 Bizi böyle bir sayfa karşılıyor. Herhangi bir şey yazdığında başarılı bir şekilde gönderiyor. Şimdi bunu Burp Suite pogramına atalım.

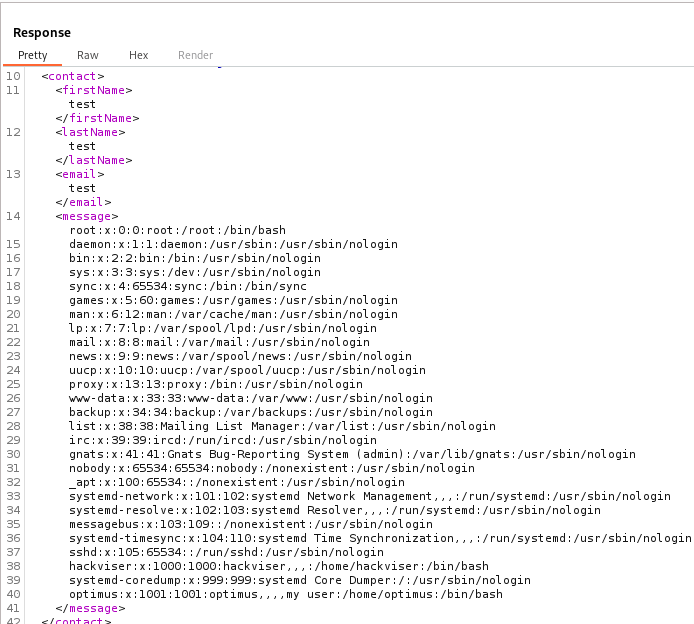
 Bu şekilde istek düşüyor. XXE açığı olduğundan şüphelendim. [Github](https://github.com/payloadbox/xxe-injection-payload-list) sayfasında XXE açığı ile ilgili payload’lar mevcut. En çok kullanılan payload’lardan birisini deniyorum.

 Kodun başına bu payload’ı ekleyip çalıştırınca 200 döndüğünü gördüm. Sayfada XXE açığının olduğunu bulduk. Şimdi sınırları zorlamanın zamanı☺

 /etc/shadow dosyasını okumak için bir payload denediğimde 200 döndüğünü gördüm. Şimdi sorunun cevabı olan /etc/passwd dosyasını okumak için payload’ımızı düzenliyoruz.

 Burada dikkat edilmesi gereken şey:

Message etiketi arasında “&ent;” kodu. Bu kod eğer yukarıdaki payload çalışırsan message kısmının bizlere dönüş yapıldığı yerde cevabı yazdıracaktır. Şimdi isteği gönderelim.

 CEVAP: **optimus**