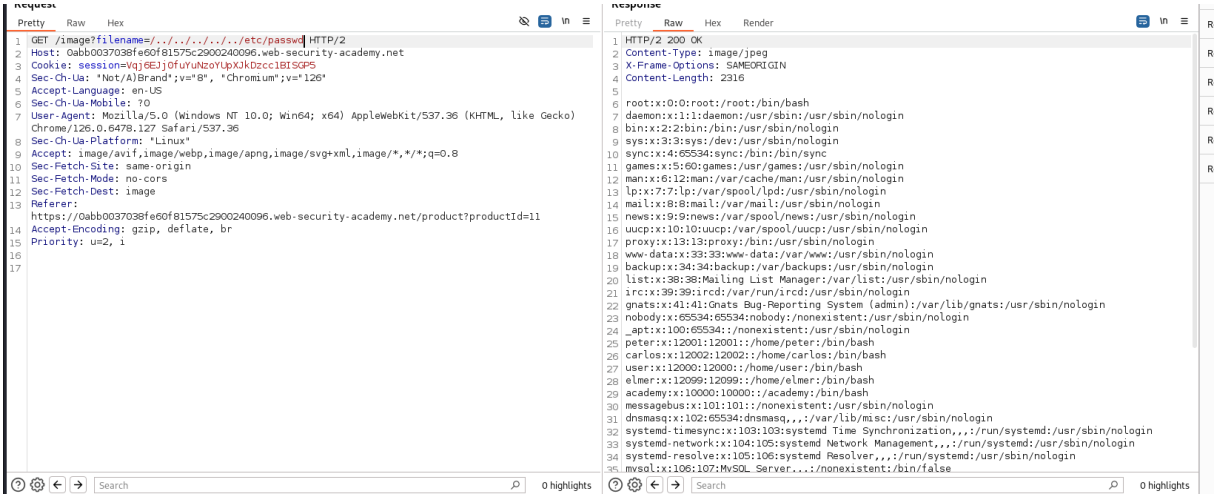
WebSec Academy Path Traversal Labları

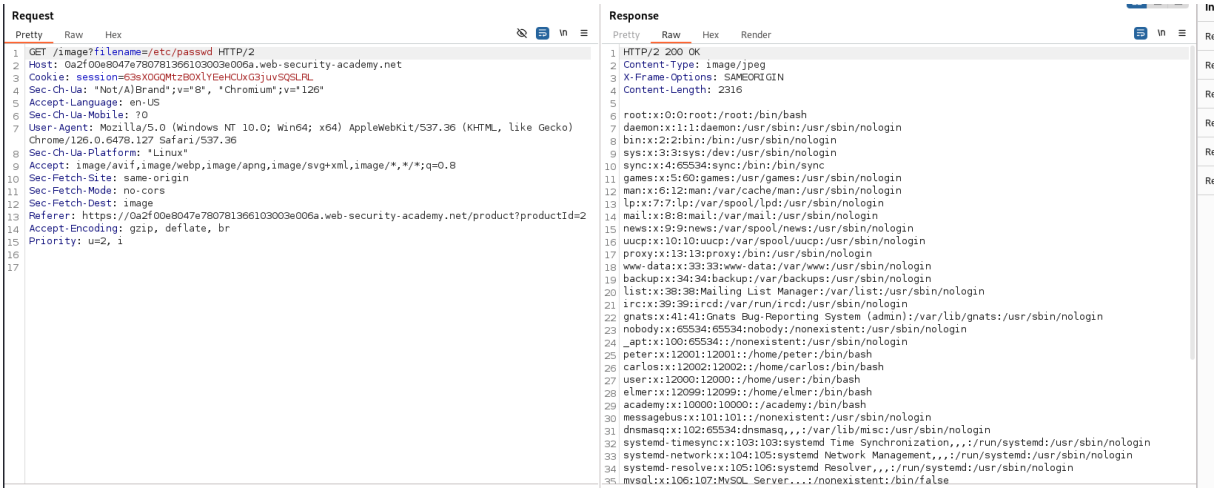
Lab 1: **File path traversal, simple case**

Çözüm için sitede bulunan bir ürünü açıp requesti yakalamak ve filename parametresini değiştirerek dosya dizininde geriye gitmek yeterlidir.



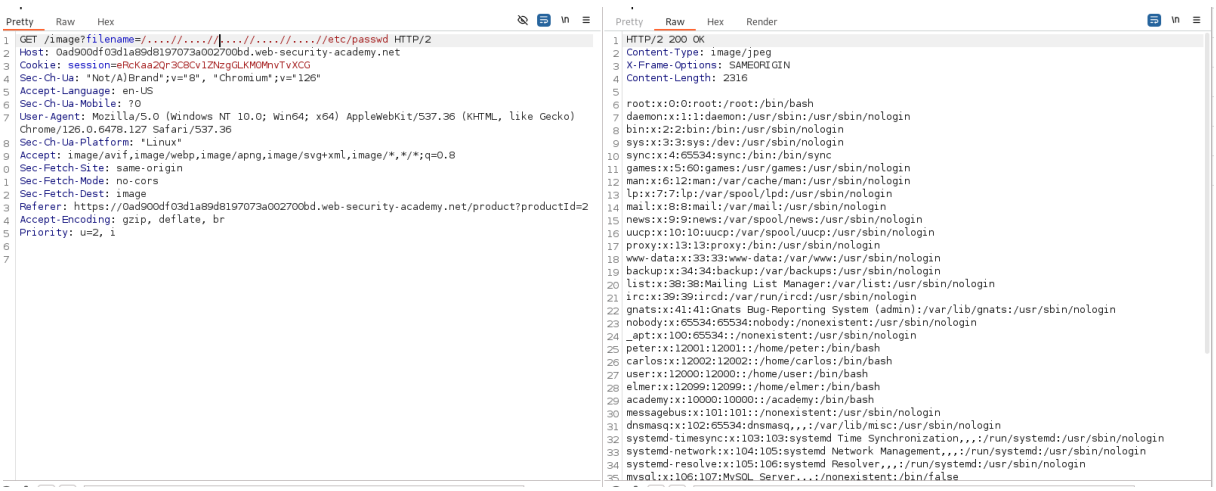
Lab 2: **File path traversal, traversal sequences blocked with absolute path bypass**

Burada herhangi bir kontrol yapılmamaktadır. Direkt olarak istenilen dosyalara erişilebilir.



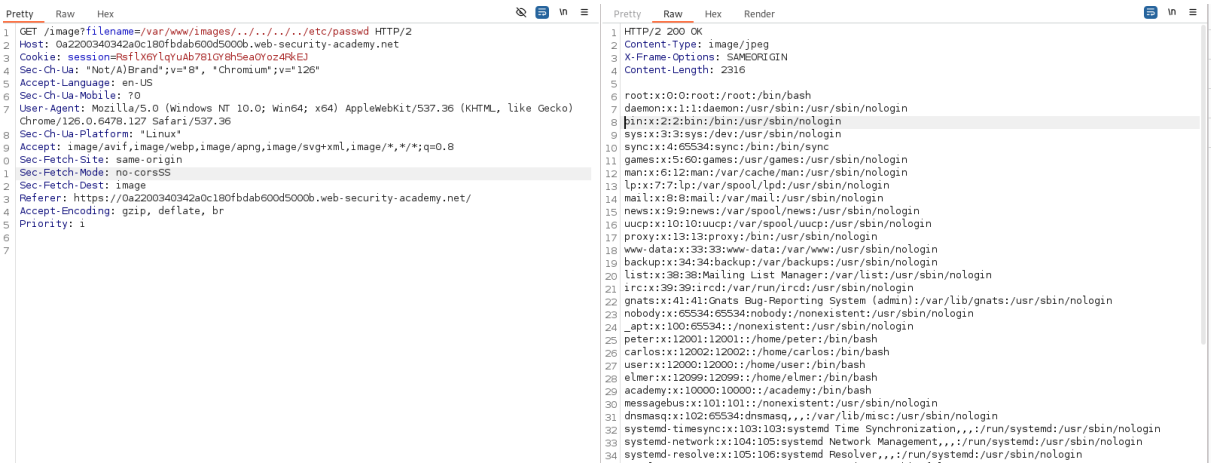
Lab 3: **File path traversal, traversal sequences stripped non-recursively**

Burada uygulama iç içe olan path traversal denemelerini kontrol etmediği için nested (iç içe birkaç adet koyulmuş) path eklenerek istenilen dosyalara erişilebilir. Uygulama ilk gördüğü traversal denemelerini kaldırdığı için iç kısma konulmuş olan dizin atlama sekanslarına dokunmaz. Bu sayede istenilen dizin ziyaret edilebilir.



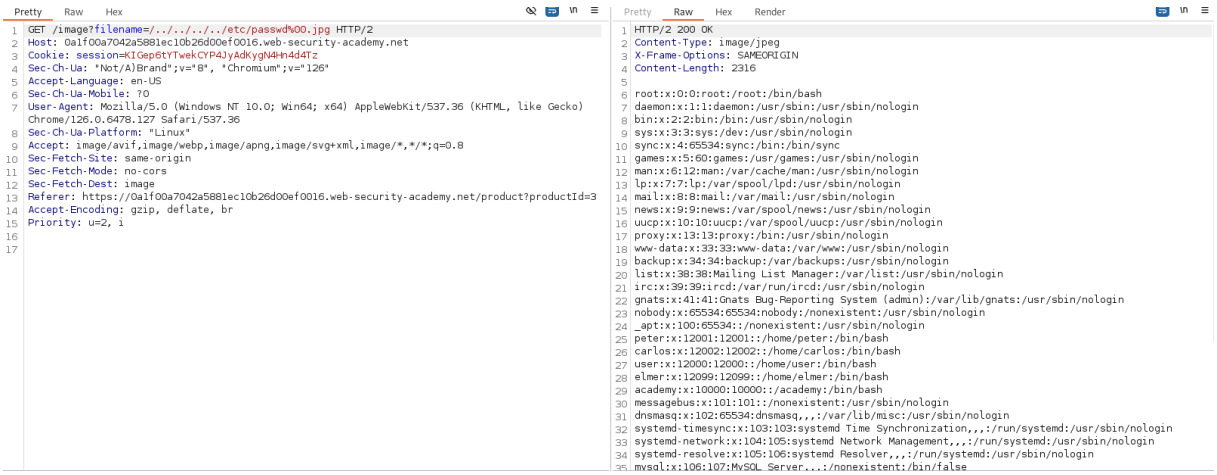
Lab 4: **File path traversal, validation of start of path**

Bu labda uygulama ilk erişim istenen dizini kontrol eder ve aynı olup olmadığını kontrol eder. Eğer istenilen dizinden başlanıp sonrasında geri ve ileri gidilirse istenilen dosyalara erişilebilir.



Lab 5: **File path traversal, validation of file extension with null byte bypass**

Burada uygulama istek atılan dosyanın tipine bakmakta ve belirli formatları kabul etmektedir. Eğer istediğimiz dosyayı yazıp null byte ile sonlandırırsak ve sonuna kabul edilen dosya formatını yazarsak uygulama bunu doğrulamadığından erişilmemesi gereken dosyaları bize gösterecektir. Bu durum modern framework'lerde çalışmayabilir.



Lab 6: **File path traversal, traversal sequences stripped with superfluous URL-decode**

Burada uygulama dosya parametresini kontrol ederken decode ettiği için url encoding işe yaramamaktadır. Buradaki sorun uygulamanın decoding işlemini recursive bir şekilde yapmamasıdır. Eğer kullanıcı iki veya daha fazla sayıda encoding işlemi yaparsa uygulama sadece bir defa decode işlemi yapar. Bu durum kullanılarak path traversal yapılabilir.