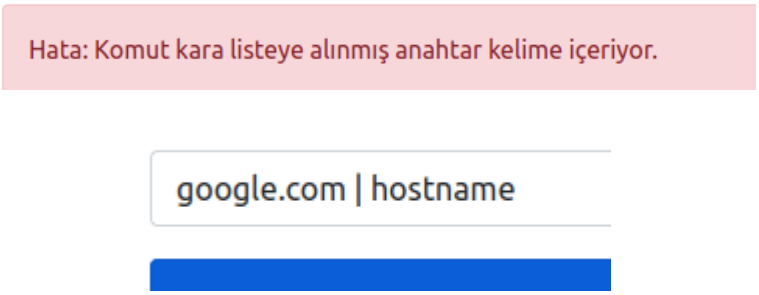
Command Injection

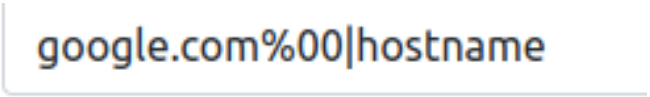
5.2 Command Injection Filter Bypass

Yine aynı şekil bir nslookup çalışan uygulamamız bulunmakta ama bu sefer bazı operatörler black liste alınmış ve kısıtlanmış/filtrelenmiş.
Kullanamıyoruz.

Şu şekilde arama yapınca



Komutun yasaklandığını görüyoruz, benim burada ilk aklıma gelen paylaod;



`google.com%00|hostname` **Payload'unun Açıklaması ;**
`google.com`: Normal bir DNS istek hedefi. Web uygulaması, kullanıcıdan aldığı girdiyi `nslookup` komutuna parametre olarak geçiriyor. Yani bu durumda `nslookup google.com` komutu çalıştırılıyor.

`%00` (Null Byte): Bu özel karakter, dizenin sonunu belirlemeye çalışıyor. Normalde, birçok programlama dili ve uygulama, `nslookup google.com` komutunu işleyip çalıştıracakken, Null Byte enjeksiyonu kullanıldığında dizenin bu noktada sonlandığı kabul edilir. Yani, `google.com%00` kısmı çalıştırıldığında, kalan kısmı (`|hostname`) sistem tarafından görmezden gelinebilir. Ancak, bazı uygulamalar ve güvenlik önlemleri Null Byte karakterini düzgün şekilde yönetemediklerinde, enjeksiyonun geri kalan kısmı yürütülebilir. Ve bizde bu şekilde bypass etmiş olduk.

Cevap : **legend**

```
legend
```