Hackviser Command Injection

Basic Command Injection

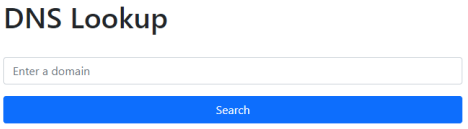
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, uzaktan komut çalıştırmaya yol açan bir Komut Enjeksiyonu güvenlik açığı içerir.

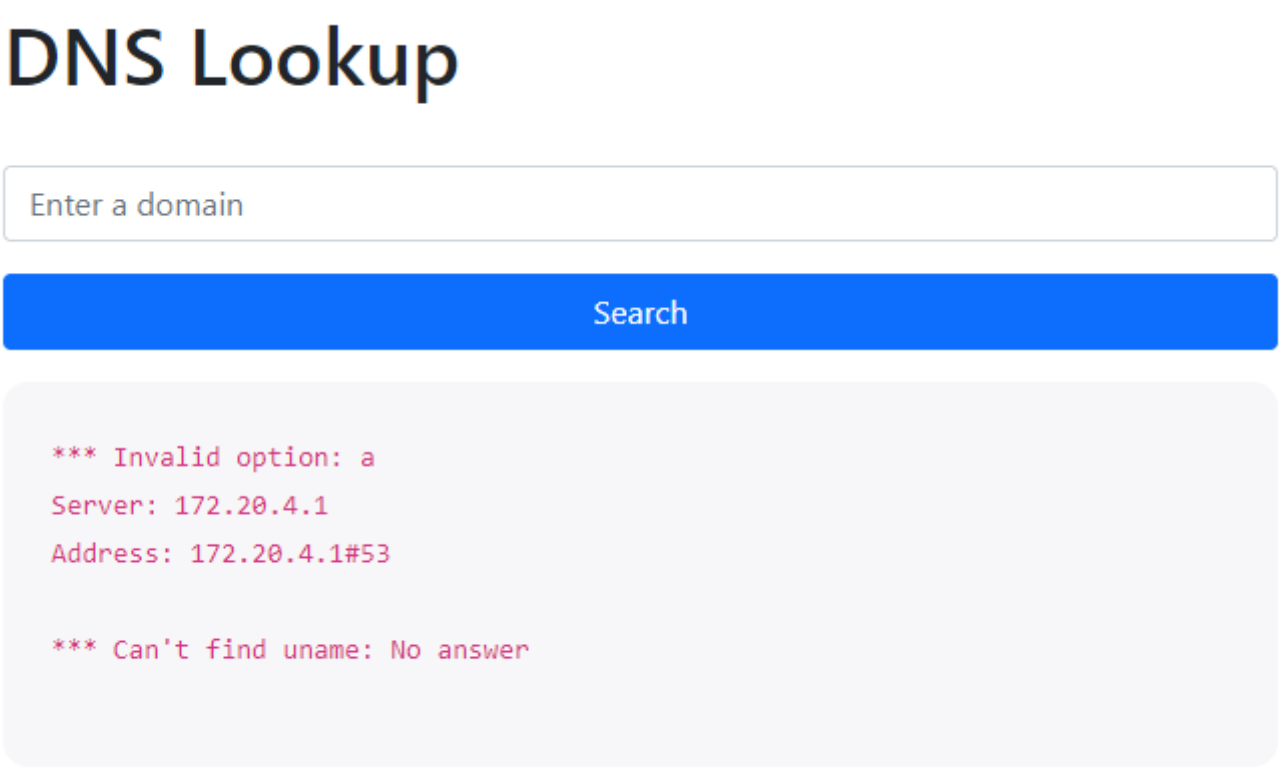
Web uygulaması, kontrol etmek istediğiniz alan adını terminalde çalışan "nslookup" aracına parametre olarak verir. Sistem üzerinde bir komut çalıştırmanın bir yolunu bulun.

Web sitesinin çalıştığı sunucunun ana bilgisayar adı adresi nedir?

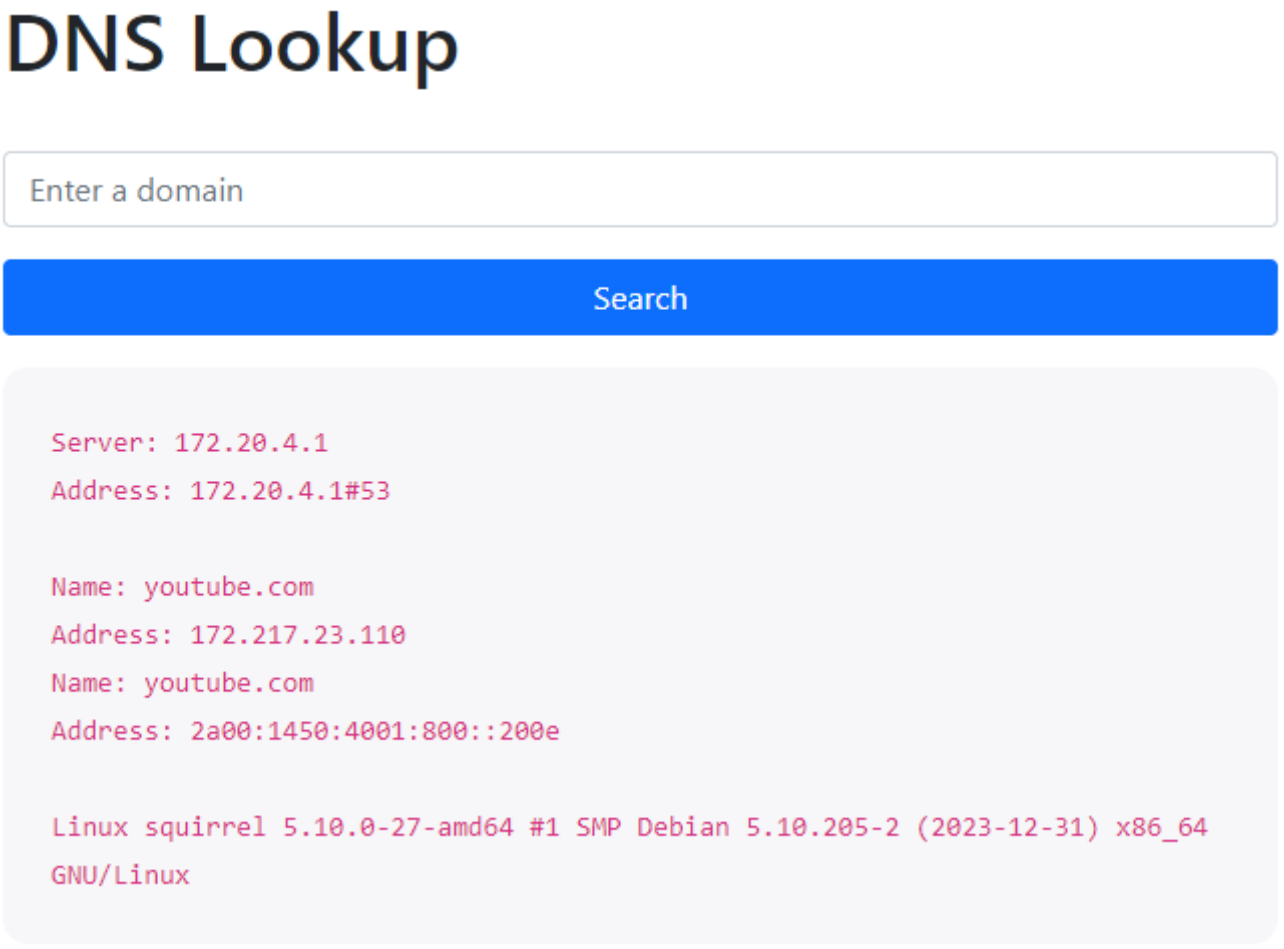
Öncelikle web sitesine gidelim



Öncelikle ana bilgisayar adını bulmak için uname -a komutunu çalıştırmamız gerekiyor bunu doğrudan yapayı denediğimizde



Bu komutu çalıştırmamıza izin vermiyor. Ondan dolayı bir domain adresi vererek hemen sonra çalıştırması için bu komutu yazacağım yani şu şekilde **youtube.com;uname -a** .Hadi deneyelim



Ve evet komutumuzu çalıştırmayı başardık. Ana bilgisayar adının squirrel olduğunu görüyoruz.

Command Injection Filter Bypass

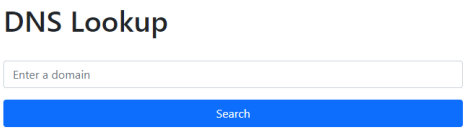
Başlangıçta bize lab hakkında bilgi vermiş

Bu laboratuvar, uzaktan komut çalıştırmaya yol açan bir Command Injection zafiyeti içerir.

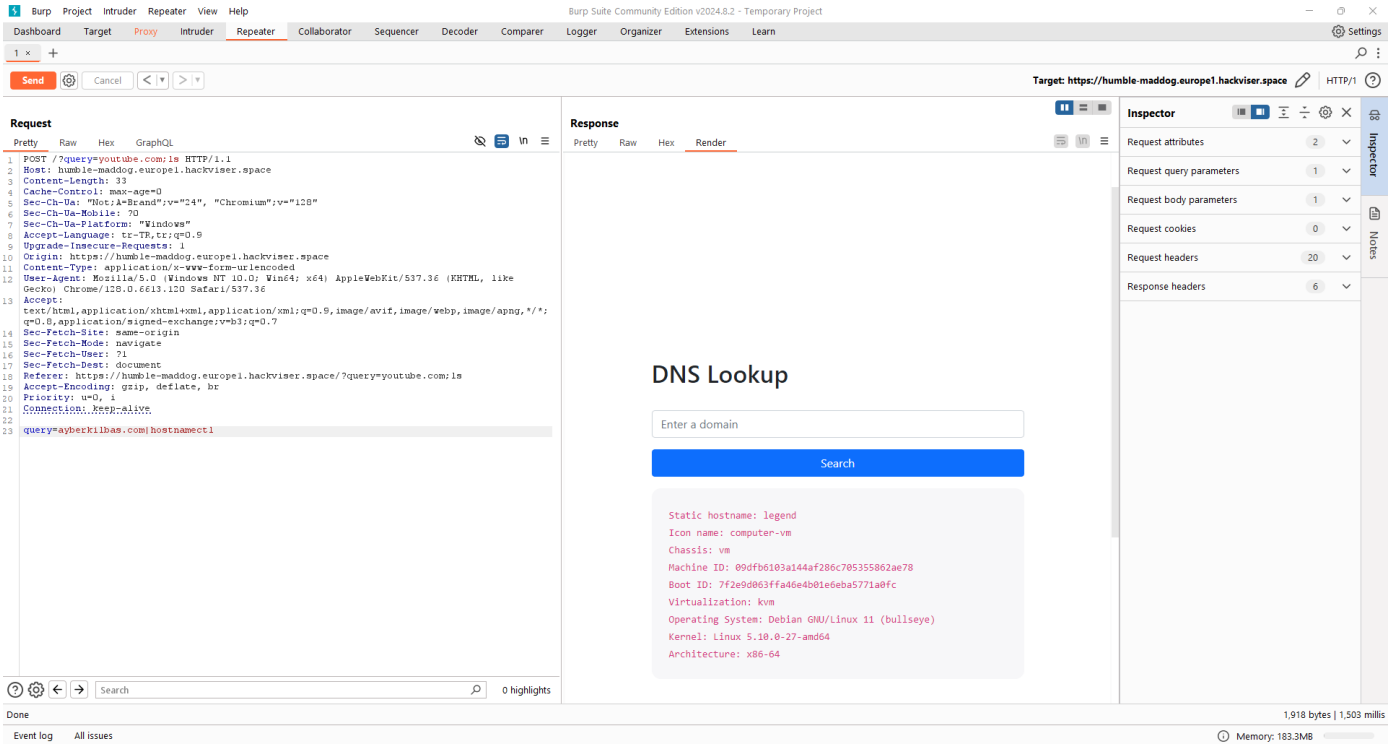
Web uygulaması, kontrol etmek istediğiniz alan adını terminalde çalışan "nslookup" isimli araca parametre olarak verir. Gönderdiğiniz alan adı yaygın komutlar veya operatörler içeriyorsa, sorgunuz engellenecektir. Sistem üzerinde komut çalıştırmanın bir yolunu bulun.

Web sitesinin çalıştığı sunucunun ana bilgisayar adı adresi nedir?

Öncelikle web sitesine gidelim



Burada birsürü komut çalıştırmayı deniyorum fakat hiçbiri olmuyor bunu daha rahat deneyebilmek için burpsuite ile araya girdim ve bunu repeater'a attım



ayberkilbas.com|hostnamectl komutunu denediğimde ise bypass etmeyi başardım. Ana bilgisayar adının legend olduğunu görüyoruz.

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş