COMMAND INJECTION FILTER BYPASS WRİTE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında Command Injection zafiyetinin Command Injection Filter Bypass labının çözümünü anlatacağım.

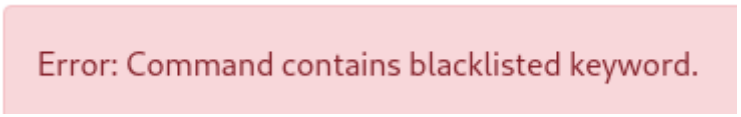
SENARYO: Bu laboratuvar, uzaktan komut çalıştırmaya yol açan bir Command Injection zafiyeti içerir.

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?

ÇÖZÜM: Bir önceki write-up'da 8.8.8.8 ||hostname komutunu denemiştik ve olmuştu.

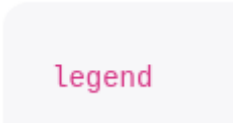
Burada aynı komutu tekrar denediğimizde:



Hatasını aldık.

Uzun araştırmalar sonucunda her türlü payloadı denedim. Lakin sonuç alamadım. Daha sonra boşluk bırakmadan çalıştırmayı denedim. Çünkü bu durum da bir bypass yöntemidir.

"8.8.8.8|hostname" komutunu deneyince cevaba ulaştık.



Cevabımız: **legend.**