Command Injection

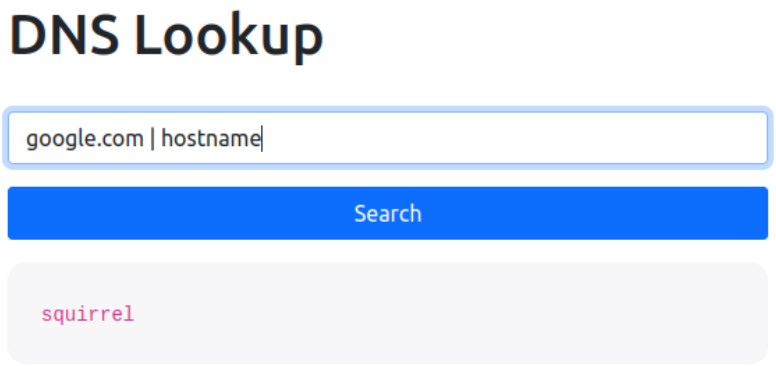
Nedir; Kötü niyetli bir kullanıcının, bir uygulamanın dış komutlarına zararlı komutlar enjekte ederek sistem üzerinde yetkisiz işlemler yapmasına olanak tanıyan bir güvenlik açığıdır.
Önlem; Önlemek için, kullanıcı girdileri daima doğrulanmalı, dış komut çalıştıran işlemler sınırlanmalı ve mümkünse güvenli API'ler kullanılmalıdır.

5.1 Basic Command Injection

ÇÖZÜM

Bu şekilde bir dns arama aracı var buraya kod enjekte etmemiz gerekiyor sorumuz, sunucuda ki bilgisayar ismi nedir.

Buraya 2 komut birden çalıştırmak için || | & && ; gibi operatörleri kullanabiliriz, bilgisayar adı dediği için hostname komutunu çalıştırıcam.



CEVAP : squirrel