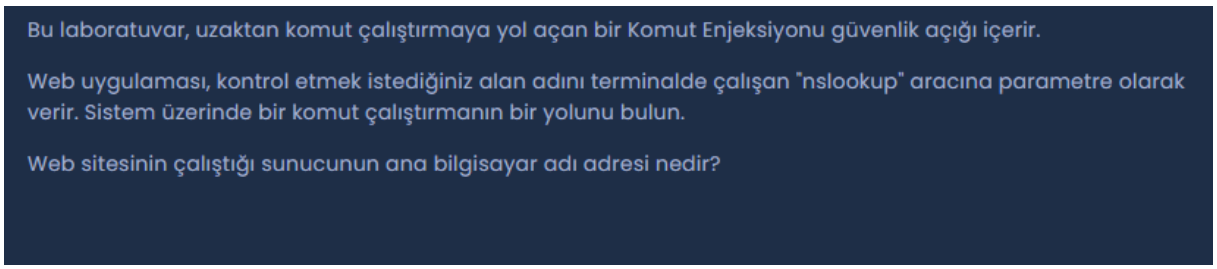
Command Injection

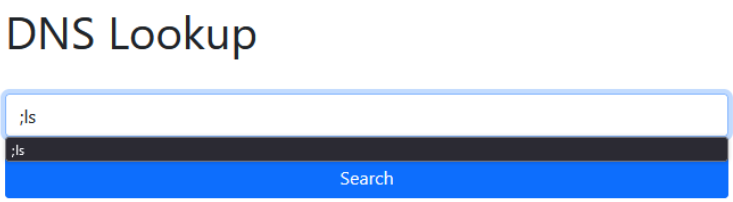
Command Injection, uygulamanın kötü niyetli kullanıcılar tarafından komut çalıştırmasına olanak sağlayan bir zafiyettir. Genelde kullanıcıdan aldığı veriyi sistemde komut ile çalıştırmaktan kaynaklanır. Ve başlıca nedenlerinden biri yetersiz input doğrulaması. Bir php uygulaması düşünelim düşünelim,

```
<?php
 $filename = $_GET['filename'];
 system("cat " . $filename);
 ?>
```

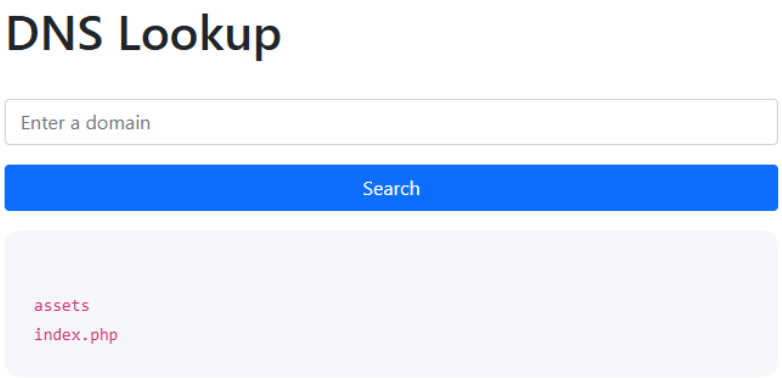
Kullanıcı girdiye ; yerleştirerek komutu kapatıp kendi istediği komutları çalıştırabilir. Buradaki labımızda command injection zafiyeti var.



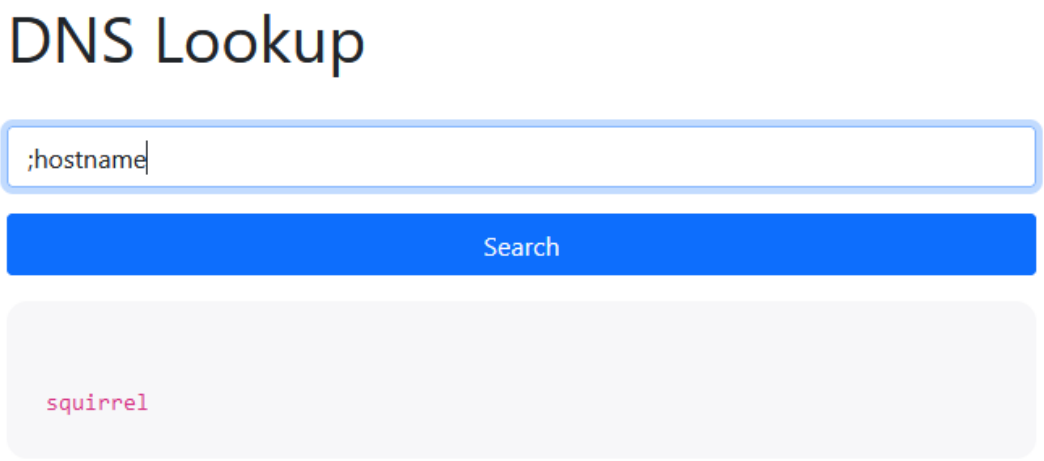
Bizden bu zafiyeti kullanarak sitenin çalıştığı sunucunun ana bilgisayar adını bulmamız isteniyor.



;ls ile zafiyet belirlemeye çalışıyorum. Eğer herhangi bir listeleme gelirse ilk adım için oldukça başarılı sonuçlar elde etmiş olacağız.

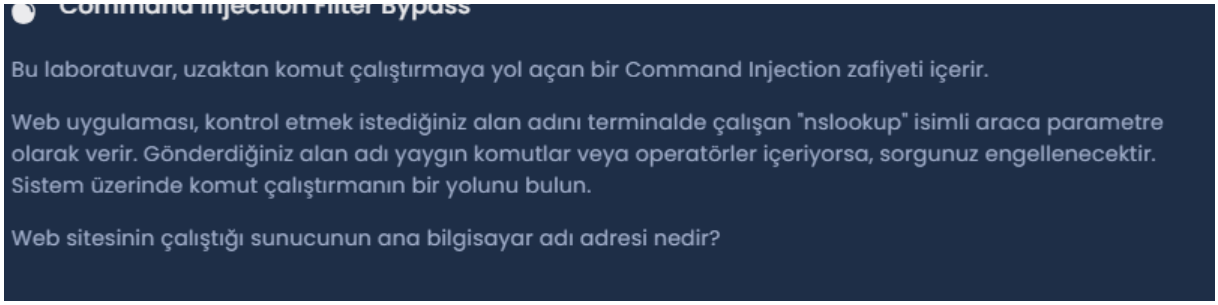


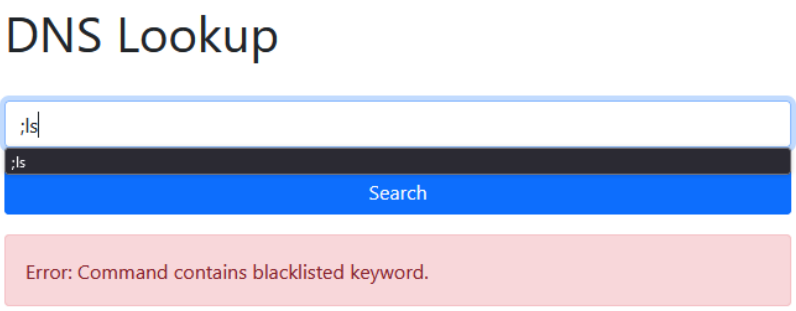
Başarılı bir aşama! Şimdi ise ; ile kapatıp hostname komutunu çalıştırmayı deniyoruz…



Görev başarılı!

Bir diğer örneğimizde ise yaygın komutları ve operatörleri engelleyen bir sistem kurulmuştur.

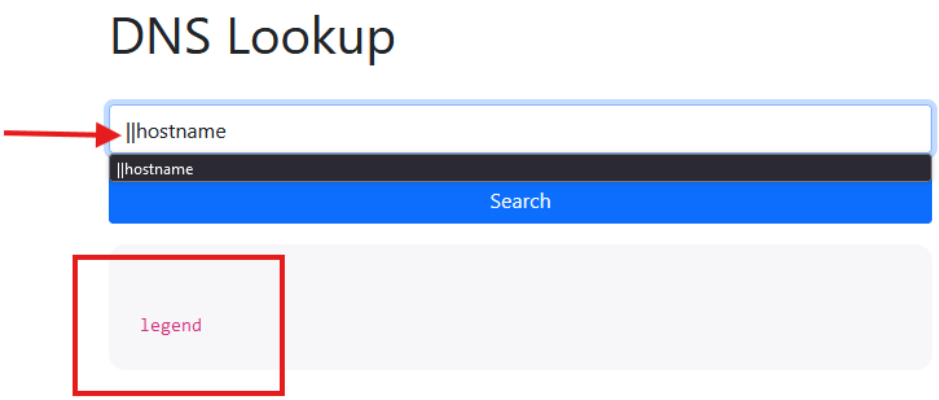




Görüldüğü gibi bu sefer ls komutumuz işe yaramadı.

Peki burada bir örnekle gidelim…

echo Hello Yavuz || ls komutunun ne işe yaradığını açıklayalım || operatörü sayesinde eğer ilk komut bir şekilde başarısız olursa ikinci komutu çalıştır demektir. Kısacası eğer echo herhangi bir nedenden kaynaklı çalışmazsa bize ls komutunu çalıştıracak. Hemen bu operatör yasaklanmış mı diye deniyorum.



Tahmin ettiğimiz gibi. || komutu sayesinde başarılı bir şekilde labımızı tamamlıyoruz.